# Mat735
# Commutative Algebra I

## Lecture Notes

Bülent Saraç
Hacettepe University
Department of Mathematics
http://www.mat.hacettepe.edu.tr/personel/akademik/bsarac/

# Contents

# List of Symbols

| | | |
|---|---|---|
| $\mathbb{N}$ | : | the set of nonnegative integers |
| $\mathcal{C}[0,1]$ | : | the ring of continuous real–valued functions on $[0,1]$ |
| $R[X]$ | : | the ring of polynomials over $R$ in the indeterminate $X$ |
| $R[[X]]$ | : | the ring of formal power series over $R$ in the indeterminate $X$ |
| $\sqrt{I}$ | : | the radical of $I$ |
| $I^e$ | : | extension of $I$ with respect to a ring homomorphism |
| $J^c$ | : | contraction of $J$ with respect to a ring homomorphism |
| $\mathrm{Min}(I)$ | : | the set of minimal prime ideals of $I$ |
| $\mathrm{Jac}(R)$ | : | Jacobson radical of $R$ |
| $\mathbb{Z}$ | : | the ring of integers |
| $\mathrm{Spec}(R)$ | : | prime spectrum of $R$ |
| $\mathrm{Var}(I)$ | : | variety of $I$ |
| $\mathbb{Q}$ | : | the field of rationals |
| $\mathbb{C}$ | : | the field of complex numbers |
| $\subseteq$ | : | contained in |
| $\subset$ | : | strictly contained in |
| $\supseteq$ | : | contains |
| $\supset$ | : | strictly contains |
| $\mathbb{Z}[i]$ | : | the ring of Gaussian integers |

CHAPTER 1

# Preliminaries

## Historical Backgroud

Commutative ring theory originated in number theory, algebraic geometry, and invariant theory. The rings of "integers" in algebraic number fields and algebraic function fields, and the ring of polynomials in two or more variables played central roles in development of these subjects.

The ring $\mathbb{Z}[i]$ was used in a paper of Gauss (1828), in which he proved that non-unit elements in $\mathbb{Z}[i]$ can be factored uniquely into product of "prime" elements, which is a central property of ordinary integers. He then used this property to prove results on ordinary integers. For example, it is possible to use unique factorization in $\mathbb{Z}[i]$ to show that every prime number congruent to 1 modulo 4 can be written as a sum of two squares. It has then become more clear that to derive results even on ordinary integers, it was useful to study broader sets of numbers, so number theory had to be expanded to include new classes of commutative rings.

It had also become clear, by the middle of the nineteenth century, that the study of finite field extensions of the rational numbers is indispensable to number theory. However, the "integers" in such extensions may fail to satisfy the unique factorization property. In attempting to solve the Fermat's last theorem, the rings $\mathbb{Z}[\zeta]$ (where $\zeta$ is a root of unity) were studied by Gauss, Dirichlet, Kummer, and others. Kummer (1844) observed that unlike $\mathbb{Z}[i]$, the rings $\mathbb{Z}[\zeta]$ fails to have unique factorization property where $\zeta$ is a primitive twenty–third root of unity. In 1847, he wrote a paper on his theory of ideal divisors ([1]).

FIGURE 1.0.1. Carl Friedrich Gauss

Dedekind came up with a general approach to the theory, which had been based widely on calculations until that time. He introduced the notion of an ideal, and generalized prime numbers to prime ideals (1871). He proved that although elements of a ring might not satisfy unique factorization property, ideals can be expressed uniquely as a product of prime ideals. Dedekind attended Dirichlet's lectures on number theory while he was at Göttingen. Later, he edited his notes, and published them in 1863 as Lectures on Number Theory, under Dirichlet's name. In the third and fourth editions, in 1879 and 1894 respectively, he wrote supplements that gave an exposition of his own work on ideals ([3]).

FIGURE 1.0.2. Richard Dedekind

After the introduction of Cartesian coordinates and complex numbers, it became possible to connect geometry and algebra. To any subset $I$ of the polynomial ring $R = \mathbb{C}[X_1, \dots, X_n]$, we can associate the algebraic subset

$$\mathcal{Z}(I) = \{(a_1, \dots, a_n) \in \mathbb{C}^n : f(a_1, \dots, a_n) = 0 \, \text{for all } f \in I\}.$$

of $\mathbb{C}^n$ called an affine variety. On the other hand, to every set $X \subseteq \mathbb{C}^n$, we can associate the subset

$$\mathcal{I}(X) = \{f \in \mathbb{C}[X_1, \dots, X_n] : f(X_1, \dots, X_n) = 0 \, \text{for all } (a_1, \dots, a_n) \in X\}$$

of $R$, which is indeed an (radical) ideal of $R$. Hilbert's Nulstellensatz (1893) provides a one–to–one correspondence between affine varieties (which are geometric objects) and radical ideals (which are algebraic objects). So, it is reasonable to think that algebraic geometry starts with Hilbert's Nulstellensatz.

FIGURE 1.0.3. David Hilbert

The study of geometric properties of plane curves that remain invariant under certain classes of transformations led to the study of elements of the polynomial ring $F[X_1, \dots, X_n]$ left fixed by the action of a group of automorphisms of $R$, which gave rise to what is known as invariant theory. The fundamental problem was to find a finite system of generators for the subalgebra consisting of fixed elements. In a series of papers at the end of 1800's, Hilbert solved the problem by giving an existence proof. The first step in the solution is now generally known as Hilbert basis theorem [3].

The axiomatic treatment of commutative rings was not developed until the 1920's in the work of Emmy Noether and Krull. In about 1921, Emmy Noether managed to bring the theory of polynomial rings and the theory of rings of numbers under a single theory of abstract commutative rings. [5]. In her 1921 paper, she recognized that a representation could be thought of as a module over the group algebra. She was able to develop the theory in greater generality, by working with rings satisfying the descending chain condition rather than just algebras over a field. Emmy Noether's use of the ascending chain condition for commutative rings led to the study of noncommutative rings satisfying the same condition ([3]). She also influenced many leading 20th century contributors of the theory including Artin, for whom the class of Artinian rings is named, and Krull, who made important contributions to the theory of ideals in commutative rings, introducing concepts that are now central to the subject such as localization and completion of a ring, as well as regular local rings. Wolfgang Krull established the concept of the Krull dimension of a ring first for Noetherian rings. Then he expanded his theory to cover general valuation rings and Krull rings. To this day, Krull's principal ideal theorem is regarded as one of the most important foundational theorems in commutative algebra.

FIGURE 1.0.4. Emmy Noether

The credit for raising Commutative Algebra to a fully-fledged branch of mathematics belongs to many famous mathematicians; including Ernst Kummer (1810-1893), Leopold Kronecker (1823-1891), Richard Dedekind (1831-1916), David Hilbert (1862-1943), Emanuel Lasker (1868-1941), Emmy Noether (1882-1935), Emil Artin (1898-1962), Wolfgang Krull (1899-1971), and Van Der Waerden (1903-1996). Nowadays, Commutative Algebra is rapidly growing and developing in many different directions. It has multiple connections with such diverse fields as complex analysis, topology, homological algebra, algebraic number theory, algebraic geometry, finite fields, and computational algebra.

## 1.1. Rings, Homomorphisms, Subrings

In this section, we give a brief account of some preliminary concepts as well as conventions that we will use throughout this course.

By a *ring* $R$, we mean a (nonempty) set with two binary operations (addition and multiplication) satisfying the following conditions:

**(1)** $(R, +)$ is an abelian group,
**(2)** multiplication is associative, i.e., for all elements $x$, $y$, and $z$ in $R$, $x(yz) = (xy)z$, and distributive over addition, i.e., for all $x$, $y$, and $z$ in $R$, we have $x(y+z) = xy + xz$ and $(y+z)x = yx + zx$.

*We shall consider only commutative rings*, namely rings in which $xy = yx$ for all elements $x$ and $y$, with an identity element (denoted by 1), namely $1x = x1$ for all elements $x$.

When $0 = 1$ in a ring, it is clear that the ring consists only of its zero element, in which case we call the ring "*zero ring*". *Throughout, we assume our rings to be nonzero.*

Examples 1.1. (*i*) One of the most fundamental example of commutative rings is the ring of integers $\mathbb{Z}$.

(*ii*) The subset $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$ of complex numbers forms a commutative ring where the ring operations are ordinary addition and multiplication. This ring is called *the ring of Gaussian integers.*

(*iii*) For an integer $n > 1$, the ring of residue classes of integers modulo $n$, denoted $\mathbb{Z}_n$, is an example of finite commutative rings.

(*iv*) Another example of commutative ring is given by the set $\mathcal{C}[0,1]$ of all continuous real–valued functions defined on the closed interval $[0,1]$ equipped with the operations as follows: for $f, g \in \mathcal{C}[0,1]$

$$(f+g)(x) = f(x) + g(x) \text{ for all } x \in [0,1]$$

and

$$(fg)(x) = f(x)g(x) \text{ for all } x \in [0,1].$$

(*v*)For a commutative ring $R$, the set of all polynomial in the indeterminate $X$ with coefficients in $R$ will be denoted by $R[X]$. Note that $R[X]$ turns out to be a commutative ring with identity with respect to ordinary polynomial addition and multiplication. We can also form the ring of polynomials over $R[X]$ in another indeterminate $Y$. The new ring can be denoted by $R[X][Y]$. A typical element of this polynomial ring is of the form $f_0 + f_1 Y + \cdots + f_n Y^n$ for some integer $n \geq 0$ and elements $f_0, \ldots, f_n \in R[X]$. Such an element can be expressed as

$$\sum_{i=0}^{n} \sum_{j=0}^{m} a_{ij} X^i Y^j,$$

where $a_{ij} \in R$ for all $1 \leq i \leq n$ and $1 \leq j \leq m$, which can be viewed as a polynomial in two indeterminates $X$ and $Y$. It follows that we denote the ring $R[X][Y]$ by $R[X, Y]$.

It should be noted that a polynomial

$$\sum_{i=0}^{n}\sum_{j=0}^{m} a_{ij}X^iY^j$$

is zero if and only if $a_{ij} = 0$ for all $1 \leq i \leq n$ and $1 \leq j \leq m$. This property is summarized by saying that "$X$ and $Y$ are *algebraically independent over* $R$". In general, for a ring $S$, a subring $R$ of $S$, and elements $\alpha_1, \ldots, \alpha_n \in S$, we say that $\alpha_1, \ldots, \alpha_n$ are algebraically independent over $R$ (or, the set $\{\alpha_1, \ldots, \alpha_n\}$ is algebraically independent over $R$ if whenever

$$\sum_{(i_1,\ldots,i_n)\in\Psi} r_{i_1,\ldots,i_n}\alpha_1^{i_1}\ldots\alpha_n^{i_n} = 0$$

for some finite subset $\Psi$ of $\mathbb{N}^n$ and $r_{i_1,\ldots,i_n} \in R$, then $r_{i_1,\ldots,i_n} = 0$ for all $(i_1, \ldots, i_n) \in \Psi$. In a similar fashion, we can form polynomial rings successively by defining $R_0 = R$, $R_i = R_{i-1}[X_i]$ for $1 \leq i \leq n$, where $X_1, \ldots, X_n$ are indeterminates. We denote $R_n$ by $R[X_1, \ldots, X_n]$ and call it the ring of polynomials over $R$ in indeterminates $X_1, \ldots, X_n$. Note that the indeterminates $X_1, \ldots X_n$ are algebraically independent and that a typical element of $R[X_1, \ldots, X_n]$ is of the form

$$\sum r_{i_1,\ldots,i_n}X_1^{i_1}\ldots X_n^{i_n},$$

where the sum is finite, $i_1, \ldots i_n$ are nonnegative integers, and $r_{i_1,\ldots,i_n} \in R$. The total degree of such a polynomial is defined to be the sum $i_1 + \cdots + i_n$ if it is nonzero, and $-\infty$ if it is zero.

(*vi*)Let $R$ be a commutative ring and $X$ an indeterminate. An expression such as $a_0 + a_1X + \cdots + a_nX^n + \cdots$ where the coefficients $a_0, a_1, \ldots, a_n, \ldots \in R$ is called a *formal power series* (in $X$) over $R$. Two formal power series $\sum_{i=0}^{\infty} a_iX^i$ and $\sum_{i=0}^{\infty} b_iX^i$ are thought of as equal when $a_i = b_i$ for all $i \geq 0$. The set of all formal power series over $R$, denoted $R[[X]]$, can be turned into a commutative ring with the following operations: for all $\sum_{i=0}^{\infty} a_iX^i$ and $\sum_{i=0}^{\infty} b_iX^i$ in $R[[X]]$,

$$\sum_{i=0}^{\infty} a_iX^i + \sum_{i=0}^{\infty} b_iX^i = \sum_{i=0}^{\infty} (a_i + b_i)\, X^i,$$

and

$$\left(\sum_{i=0}^{\infty} a_iX^i\right)\left(\sum_{i=0}^{\infty} b_jX^j\right) = \sum_{k=0}^{\infty} c_kX^k,$$

where, for every $k \geq 0$,

$$c_k = \sum_{i=0}^{k} a_ib_{k-i}.$$

The zero element of $R[[X]]$ is the element $\sum_{i=0}^{\infty} 0X^i$, which is denoted by 0 and the identity element is $1 + 0X + 0X^2 + \cdots$, denoted simply 1. Assuming coefficients after the highest degree term all zero, any polynomial can be regarded as a formal power series as well. So we can regard $R[X]$ as a subset of $R[[X]]$.

(*vii*) Let $R$ be a commutative ring and let $X_1, \ldots, X_n$ are indeterminates. As in the case of polynomials, we can form power series rings iteratively as follows: set $R_0 = R$, and $R_i = R_{i-1}[[X_i]]$ for $1 \leq i \leq n$. To understand how elements occur in such a power series ring, we introduce the concept of *homogeneous polynomial* in $R[X_1, \ldots, X_n]$: a polynomial in $R[X_1, \ldots, X_n]$ is called homogeneous if it is of the form

$$\sum_{i_1+\cdots+i_n=d} r_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}$$

for some $d \geq 0$ and $r_{i_1,\ldots,i_n} \in R$. Here $d$ is called the (homogeneous) degree of the polynomial. Note that we consider the zero polynomial as homogeneous. It is easy to prove that the finite sum of homogeneous polynomials with the same degree is again a homogeneous polynomial, and also that any finite set of homogeneous polynomials with different degrees is algebraically independent over $R$. Moreover; any element in the ring $R_n$ can be written as a sum of the form

$$\sum_{i=0}^{\infty} f_i,$$

in a unique way, where $f_i$ is a homogeneous polynomial in $R[X_1, \ldots, X_n]$ which is either zero or of degree $i$. We denote the ring $R_n$ by $R[[X_1, \ldots, X_n]]$ and call it the *formal power series ring* over $R$ in $n$ indeterminates $X_1, \ldots, X_n$. For two 'formal power series' $\sum_{i=0}^{\infty} f_i$ and $\sum_{i=0}^{\infty} g_i$ are equal precisely when $f_i = g_i$ for all $i \geq 0$. Also, the operations of addition and multiplication are as follows:

$$\left(\sum_{i=0}^{\infty} f_i\right) + \left(\sum_{i=0}^{\infty} g_i\right) = \sum_{i=0}^{\infty} (f_i + g_i),$$

$$\left(\sum_{i=0}^{\infty} f_i\right) \left(\sum_{i=0}^{\infty} g_i\right) = \sum_{i=0}^{\infty} \left(\sum_{j+k=i} f_j g_k\right).$$

DEFINITION 1.2. A *ring homomorphism* is a mapping $f$ from a ring $R$ into a ring $S$ such that for all $x$ and $y$ in $R$,

$(i)$ $f(x+y) = f(x) + f(y)$,
$(ii) f(xy) = f(x)f(y)$, and
$(iii)$ $f(1_R) = 1_S$.
The subset $\{f(x) : x \in R\}$, denoted $\operatorname{Im} f$, is called the image of $f$.

Note that composition of two homomorphisms of rings (when possible) is again a homomorphism.

EXAMPLE 1.3. Let $S$ be a commutative ring and $R$ a subring of $S$. Let $\alpha_1 \ldots, \alpha_n \in S$. Then there is a unique ring homomorphism $\epsilon : R[X_1, \ldots, X_n] \to S$ such that $\epsilon(r) = r$ and $\epsilon(X_i) = \alpha_i$ for all $1 \leq i \leq n$. This homomorphism is called the *evaluation homomorphism* (or simply evaluation) at $\alpha_1, \ldots, \alpha_n$.

DEFINITION 1.4. Let $R$ and S be rings. If there is a ring homomorphism $f : R \to S$, then we shall say that $S$ is an *$R$–algebra*(or an algebra over $R$).

If $R$ is a ring, then the mapping $f : \mathbb{Z} \to R$ defined by $f(n) = n(1_R)$ for all $n \in \mathbb{Z}$ is a ring homomorphism. It follows that every ring has a natural $\mathbb{Z}$–algebra structure.

DEFINITION 1.5. A subset $S$ of a ring $R$ is said to be a *subring* of $R$ if $S$ is closed under addition and multiplication and contains the identity element of $R$.

By definition, any nonzero commutative ring is an algebra over its subrings.

Examples 1.6. ($i$) If $R$ is a commutative ring, and $X$ is an indeterminate, then $R$ is a subring of $R[X]$, and $R[X]$ is a subring of $R[[X]]$.

($ii$) Let $R$ be a ring. It is not difficult to see that the intersection of subrings of $R$ is again a subring of $R$. This observation leads to the following special type of subrings of $R$. Let $S$ be a subring of $R$, and let $A$ be a subset of $R$. We define the *subalgebra* of $R$ generated by the subset $A$ over the subring $S$ to be the intersection of all subrings of $R$ containing both $S$ and $A$, and denote it by $S[A]$. Notice that $S[A]$ is the smallest subring of $R$ containing both $S$ and $A$. Since $S$ is a subring of $S[A]$, $S[A]$ is an algebra over $S$, which explains the name "subalgebra". In the case in which $A = \{\alpha_1, \ldots, \alpha_n\}$ is a finite subset of $R$, we write $S[A]$ as $S[\alpha_1, \ldots, \alpha_n]$. In this case it turns out that

$$S[\alpha_1, \ldots, \alpha_n] = \left\{ \sum_{\text{finite}} s_{m_1,\ldots,m_n} \alpha_1^{m_1} \ldots \alpha_n^{m_n} : m_1, \ldots, m_n \geq 0, \text{ and } s_{m_1,\ldots,m_n} \in S \right\}.$$

(Note that we make the convention that the symbol $a^0$ represents 1.) It should be now clear why we use the notation $\mathbb{Z}[i]$ for the ring of Gaussian integers (observe that since $i^2 = -1 \in \mathbb{Z}$, $i^n$ is either $\pm 1$ or $\pm i$, and so $\mathbb{Z}[i]$ is just the subalgebra of $\mathbb{C}$ generated by the subset $\{i\}$ over the subring $\mathbb{Z}$). It can be easily seen that for any subsets $A$ and $B$ of $R$, $S[A \cup B] = S[A][B]$. We can also conclude that $S[A]$ is the union of subalgebras $S[B]$, where $B$ ranges over all finite subsets of $A$.

Exercise 1.7. Let $S$ be a commutative ring and $R$ a subring of $S$. Let $\alpha_1, \ldots, \alpha_n \in S$ be algebraically independent over $R$. Show that the subalgebra $R[\alpha_1, \ldots, \alpha_n]$ is isomorphic to the polynomial ring $R[X_1, \ldots, X_n]$.

## 1.2. Zero–divisors, Nilpotent and Unit Elements

An element $a$ of a ring $R$ is said to be a *zero–divisor* if there exists a non–zero element $b \in R$ such that $ab = 0$. In other words, a zero–divisor is an element which divides zero. If a ring $R$ has no zero–divisors other than zero, then we call $R$ an *integral domain* (or, simply, *domain*).

Exercise 1.8. Let $R$ be commutative ring and let $X, X_1, \ldots, X_n$ be indeterminates.

($i$) Show that if $f \in R[X]$ is a zero–divisor in $R[X]$, then there exists a nonzero element $c \in R$ such that $cf = 0$.

($ii$)Show that if $R$ is an integral domain, then so is $R[X_1, \ldots, X_n]$.

($iii$) Show that $R$ is an integral domain if and only if $R[[X_1, \ldots, X_n]]$.

There is a special type of zero–divisors: nilpotent elements. An element $x$ of a ring is called *nilpotent* if it vanishes when raised to a power, i.e., $x^n = 0$ for some $n > 0$.

Exercise 1.9. Let $R$ be a commutative ring and let $X$ be an indeterminate. Let $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$. Show that $f$ is nilpotent if and only if $a_0, \ldots, a_n$are all nilpotent.

A unit in $R$ is an element $x$ if there exists an element $y \in R$ such that $xy = 1$. Here we call $y$ an inverse of $x$. Note that once we have an inverse of $x$, it is unique. So, we call $y$ "the" inverse of $x$ and and write $y = x^{-1}$. Note that the units of a ring constitute a multiplicative abelian group. One can see that a nonzero commutative ring is a field if and only if it has only two ideals, namely 0 and $R$. A field is a nonzero ring in which every nonzero element is unit. Note that every finite integral domain is a field. Moreover; for an integer $n > 1$, $\mathbb{Z}_n$ is a field if and only if $\mathbb{Z}_n$ is a domain if and only if $n$ is a prime number.

Exercise 1.10. Let $R$ be a commutative ring and let $a$ be a nilpotent element of $R$. Then show that for any unit element $u$ of $R$, $u + a$ is unit in $R$.

Exercise 1.11. Let $R$ be a commutative ring and let $X$ be an indeterminate. Let $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$.

($i$)Show that $f$ is a unit element of $R[X]$ if and only if $a_0$ is unit and $a_1, \ldots, a_n$ are all nilpotent.

($ii$) Show that $R[X]$ is never a field.

Exercise 1.12. Let $R$ be a commutative ring and let $X_1, \ldots, X_n$ be indeterminates. Let

$$f = \sum_{i=0}^{\infty} f_i \in R[[X_1, \ldots, X_n]],$$

where $f_i$ is either zero or a homogeneous polynomial of degree $i$ in $R[X_1, \ldots, X_n]$ for every $i \geq 0$. Prove that $f$ is a unit of $R[[X_1, \ldots, X_n]]$ if and only if $f_0$ is a unit of $R$.

## 1.3. Field of Fractions of an Integral Domain

Let $R$ be an integral domain. Set $S := \{(a, b) : a, b \in R \,\text{and}\, b \neq 0\}$. For $(a, b), (c, d) \in S$ we define a relation as follows:

$$(a, b) \sim (c, d) \iff ad = bc.$$

It is easy to see that $\sim$ is an equivalence relation. For $(a, b) \in S$, we denote the equivalence class containing $(a, b)$ by $a/b$ or

$$\frac{a}{b}.$$

Let $Q$ denote the set of all equivalence classes. Then we can make $Q$ into a field with the following operations: for $a/b$, $c/d \in Q$,

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

and

$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

Note that we have a mapping

$$\begin{aligned} \iota : R &\to Q \\ r &\mapsto r/1 \end{aligned}$$

which is indeed an embedding of $R$ into $Q$ as a subring. Redefining elements $r$ of $R$ as $r/1$ in $Q$, we can also assume that $R$, itself, is a subring of $Q$. Moreover; if $F$ is a field and $f : R \to F$ is a ring homomorphism, then there is a ring homomorphism

$g : Q \to F$ such that $g\iota = f$, i.e., there is a ring homomorphism $g : Q \to F$which makes the following diagram commute:

$$\begin{tikzcd} R \arrow[r, "\iota"] \arrow[d, "f"'] & Q \\ F \arrow[ur, "g"'] & \end{tikzcd}$$

It follows that every integral domain $R$ is contained in a field which is contained in every field containing $R$.

## 1.4. Factorization of Elements in a Commutative Ring

Definition 1.13. Let $R$ be an integral domain. A nonzero element $p \in R$ is called *irreducible if*

($i$) $p$ is not a unit element of $R$, and

($ii$) whenever $p = ab$ for some $a, b \in R$, then either $a$ or $b$ is a unit element of $R$.

Definition 1.14. Let $R$ be an integral domain. We say that $R$ is a *unique factorization domain* (UFD for short) if

($i$) each nonzero element which is not a unit in $R$ is expressible as a product $p_1 p_2 \ldots p_n$ of irreducible elements $p_1, p_2, \ldots, p_n$ of $R$, and

($ii$) whenever $s, t \in \mathbb{N}$ and $p_1, \ldots, p_n, q_1, \ldots, q_m$ are irreducible elements of $R$ such that

$$p_1 p_2 \ldots p_n = q_1 q_2 \ldots q_m$$

then $n = m$ and there exists units $u_1, \ldots, u_n$ in $R$ such that, after a suitable reindexing,

$$p_i = uq_i \quad \text{for all } 1 \leq i \leq n.$$

Definition 1.15. Let $R$ be an integral domain. We say that $R$ is a *Euclidean domain* if there is a function $\partial : R \setminus \{0\} \to \mathbb{N}$, called the *degree function* of $R$, such that

($i$) whenever $a, b \in R \setminus \{0\}$ and $a = bc$ for some $c \in R$, then $\partial(b) \leq \partial(a)$, and

($ii$) whenever $a, b \in R \setminus \{0\}$ with $b \neq 0$, then there exist $q, r \in R$ such that

$$a = qb + r \,\text{with either}\, r = 0 \,\text{or}\, r \neq 0 \,\text{and}\, \partial(r) < \partial(b).$$

Note that the ring of integers $\mathbb{Z}$, the ring of Gaussian integers $\mathbb{Z}[i]$ and the ring of polynomials $F[X]$ over a field $F$ in indeterminate $X$ are examples of Euclidean domains.

Theorem 1.16. *Every Euclidean domain is a UFD.*

Theorem 1.17. *If $R$ is a UFD, then so is $R[X]$.*

*It follows from above results that if $F$ is a field, then the polynomial ring $F[X_1, \ldots, X_n]$ in $n$ indeterminates $X_1, \ldots, X_n$ is a UFD. Also, the same applies when $F = \mathbb{Z}$.*

## 1.5. Ideals, Quotient (Factor) Rings

An *ideal* $I$ of a ring $R$ is a nonempty subset of $R$ which is an additive subgroup for which $x \in R$ and $y \in I$ imply $xy \in I$. Notice that a ring has at least two natural ideals, namely $\{0\}$ and $R$ itself, where the first one is called the *zero ideal* denoted simply 0.

Exercise 1.18. Let $R_1, \ldots, R_n$ be commutative rings. Show that the Cartesian product set $R_1 \times \cdots \times R_n$ can be given a commutative ring structure with respect to componentwise operations of addition and multiplication. In other words we define operations by

$$(r_1, \ldots, r_n) + (s_1, \ldots, s_n) = (r_1 + s_1, \ldots, r_n + s_n)$$

and

$$(r_1, \ldots, r_n)(s_1, \ldots, s_n) = (r_1 s_1, \ldots, r_n s_n)$$

for all $r_i, s_i \in R_i$ $(i = 1, \ldots, n)$. We call this new ring the direct product of $R_1, \ldots, R_n$.

Show that, if $I_i$ is an ideal of $R_i$ for each $i = 1, \ldots, n$, then $I_1 \times \cdots \times I_n$ is an ideal of the direct product ring $\prod_{i=1}^n R_i$. Also prove that each ideal of $\prod_{i=1}^n R_i$ is of this form.

When $I$ is an ideal of a ring $R$, the quotient additive group $R/I$ inherits a multiplication from $R$ which makes it into a ring, called the *quotient ring* (or *factor ring*) of $R$ modulo $I$. The elements of $R/I$ are cosets of $I$ in $R$, and the mapping $\phi : R \longrightarrow R/I$ such that $\phi(a) = a + I$ is a surjective ring homomorphism, which is usually referred to as the *natural* or *canonical ring homomorphism* from $R$ to $R/I$. The following fact about ideals of quotient rings is used very often.

the ideals of a quotient ring. *Let $I$ be an ideal of a commutative ring $R$.*

*(i) If $J$ is an ideal of $R$ containing $I$, then the Abelian group $J/I$ is an ideal of $R/I$. Also, for $r \in R$, $r + I \in J/I$ if and only if $r \in J$.*

*(ii) If $\mathcal{J}$ is an ideal of the quotient ring $R/I$, then there exists a unique ideal $J$ of $R$ containing $I$ such that $\mathcal{J} = J/I$; indeed, this $J$ is given by*

$$J = \{a \in R : a + I \in \mathcal{J}\}.$$

Proposition 1.19. *If $R$ is a ring and $I$ is an ideal of $R$, then there is a one–to–one order–preserving correspondence between the ideals $J$ of $R$ containing $I$ and the ideals $\mathcal{J}$ of $R/I$, given by $J = \phi^{-1}(\mathcal{J})$. We can give this correspondence explicitly by*

$$\begin{aligned} \tau : \{J : J \text{ is an ideal of } R \text{ and } J \supseteq I\} &\rightarrow \{\text{ideals of } R/I\} \\ J &\mapsto J/I \end{aligned}$$

Theorem 1.20. *Let $I$ and $J$be ideals of a commutative ring $R$ such that $I \subseteq J$. Then the mapping*

$$\eta : (R/I)/(J/I) \rightarrow R/J$$

*defined by $\eta((r + I) + J/I) = r + J$ for all $r \in R$ is a ring isomorphism.*

Theorem 1.21. *Let $R$ and $S$ be commutative rings, and let $f : R \rightarrow S$ be a ring homomorphism. Then the mapping $\bar{f} : R/\ker f \rightarrow \operatorname{Im} f$ defined by $\bar{f}(r + \ker f) = f(r)$ for all $r \in R$ is a ring isomorphism.*

For any ring homomorphism $f : R \rightarrow S$, the subset $f^{-1}(0)$ is an ideal of $R$, called the *kernel* of $f$. We denote the kernel of $f$ by $\ker(f)$. It is well–known that $R/\ker(f) \cong f(R)$.

Let $R$ be ring and let $S$ be a subset of $R$. Then the intersection of all ideals of $R$ containing $S$ (which is known to be an ideal of $R$) is called the ideal of $R$ *generated by the subset* $S$, denoted $(S)$ (or, sometimes, $\langle S \rangle$). If $I = (S)$, then we say that $S$ is a *generator set* for $I$ or $I$ is generated by $S$. Then we have

($i$) $(S)$ is an ideal of $R$,
($ii$) $S \subseteq (S)$, and
($ii$) $(S)$ is the smallest ideal of $R$ among the ideals which contain $S$.
It can also be shown that

$$(S) = \left\{ \sum_{i=1}^{n} a_i x_i : n \in \mathbb{N},\, a_i \in R \,\text{and}\, x_i \in S \,\text{for}\, i = 1, \ldots, n \right\}.$$

If $S = \{x_1, \ldots, x_n\}$ is a finite subset of $R$ and $I = (S)$, then we say that $I$ is a *finitely generated* ideal of $R$, in which case we write $I = (x_1, \ldots, x_n)$. If $n = 1$, then $I = (x_1)$ is called a *principal ideal* generated by $x_1$. In this case, for any element $x \in R$, we have $(x) = \{rx : r \in R\}$. We often denote the principal ideal $(x)$ in $R$ by $Rx$. Note that in any ring, 0 and $R$ are principal ideals since $0 = (0) = (\emptyset)$ and $R = (1)$. A ring whose every ideal is principal is called a *principal ideal ring.* If a domain is also a principal ideal ring, then it is a *principal ideal domain* (*PID*, for short). For example, $\mathbb{Z}$ and $\mathbb{Z}[i]$ are examples of principal ideal domains. It is also a well–known fact that if $F$ is a field, then the polynomial ring $F[X]$ in one indeterminate $X$ over $F$ is a PID (but the same is not true in general if $F$ is not a field; for example, if $F = \mathbb{Z}$).

Theorem 1.22. *Every Euclidean domain is a PID. Indeed, we have the following sequence of implications (none of which can be reversed):*

$$\textit{Euclidean domain} \Longrightarrow \textit{PID} \Longrightarrow \textit{UFD}$$

Exercise 1.23. Prove that the polynomial ring $F[X, Y]$ over the field $F$ in indeterminates $X$ and $Y$ is not a principal ideal domain (and so, not a Euclidean domain) by showing that the ideal $(X, Y)$ of $F[X, Y]$ is not principal. (We remark that this exercise provide an example of a UFD which is not a PID).

Exercise 1.24. Find a commutative ring in which there is an ideal that cannot be generated by a finite set.

Exercise 1.25. Let $R$ be a commutative ring and $X_1, \ldots, X_n$ indeterminates. Let $a_1, \ldots, a_n \in R$, and let

$$f : R[X_1, \ldots, X_n] \to R$$

be the evaluation homomorphism at $a_1, \ldots, a_n$. Show that the kernel of $f$ is the ideal of $R[X_1, \ldots, X_n]$ generated by elements $X_1 - a_1, \ldots, X_n - a_n$, i.e.,

$$\ker f = (X_1 - a_1, \ldots, X_n - a_n)\,.$$

## 1.6. Operations on Ideals

In this section, we give some basic arithmetic of ideals which is crucial for studying commutative rings. Ideals provide a strong connection relating geometric ideas to the realm of number theory. Indeed, ideals are considered first, in Dedekind's famous work in 1871, as a continuation of study of numbers which was, then, mostly related to the Fermat's last theorem. Just as with numbers, there are some operations on ideals which are widely used in the theory as effective ways to produce new ideals from old ones. We start with addition and multiplication.

**Addition and Multiplication.** It is easy to see that the intersection of any number of ideals gives again an ideal. However; the union of ideals does not necessarily give rise to an ideal. Indeed, the union $I \cup J$ of ideals $I$ and $J$ is again an ideal if and only if one of $I$ and $J$ contains the other. Although a union of ideals is generally not an ideal, we can still consider an ideal which contains such a union, namely the ideal generated by the union and call it the sum of the ideals which participate in the union. More precisely, if $\Lambda$ is a nonempty index set and $\{I_\lambda : \lambda \in \Lambda\}$ is a family of ideals of a ring $R$, then the *sum of the ideals* $I_\lambda$, denoted $\sum_{\lambda \in \Lambda} I_\lambda$, is defined to be the ideal of $R$ generated by the subset $\bigcup_{\lambda \in \Lambda} I_\lambda$. In case $\Lambda = \emptyset$, we assume $\sum_{\lambda \in \Lambda} I_\lambda = 0$. By definition, one can show, when $\Lambda \neq \emptyset$, that an element $x \in R$ lies in the sum $\sum_{\lambda \in \Lambda} I_\lambda$ if and only if there exist $n \in \mathbb{N}$, $\lambda_1, \dots, \lambda_n \in \Lambda$, and $a_{\lambda_i} \in I_{\lambda_i}$ $(i = 1, \dots, n)$ such that $x = \sum_{i=1}^n a_{\lambda_i}$. In particular, for elements $a_1, \dots, a_n$in a commutative ring $R$, we have $(a_1, \dots, a_n) = (a_1) + \cdots + (a_n)$.

Just as we can add ideals, we can also multiply (finitely many of) them. Let $I_1, \dots, I_n$ be ideals of $R$. Then the ideal of $R$ generated by the subset

$$\{a_1, \dots, a_n : a_i \in I_i \,\text{for each}\, i = 1, \dots, n\}$$

is defined as the *product of the ideals* $I_1, \dots, I_n$, denoted $I_1 \dots I_n$ or $\prod_{i=1}^n I_i$. It follows that an element $x \in R$ lies in the product $\prod_{i=1}^n I_i$ if and only if $x = \sum r_{(i_1, \dots, i_n)} a_{i_1} \dots a_{i_n}$ for some $r_{(i_1, \dots, i_n)} \in R$ and $a_{i_j} \in I_j$ $(i = 1, \dots, n)$, where for all but a finite number of $r_{(i_1, \dots, i_n)}$ are zero. Notice that, in particular, positive powers of ideals are defined. Conventionally, we write $I^0 = R$ for any ideal $I$. Notice that for ideals $I$ and $J$ of $R$, we always have $IJ = JI \subseteq I \cap J$.

The three operations (intersection, addition, and multiplication) are all commutative and associative. Also, multiplication of ideals is distributive over addition, i.e., for ideals $I$, $J$, and $K$, $I(J + K) = IJ + IK$.

In the ring $\mathbb{Z}$, intersection and addition are distributive over one another, which is not the case for a general commutative ring. However, we have the following rule, known as the *modular law*: for ideals $I$, $J$, and $K$, if $I \supseteq J$ or $I \supseteq K$, then

$$I \cap (J + K) = (I \cap J) + (I \cap K)\,.$$

Let $R_1, \dots, R_n$ be commutative rings. Then the Cartesian product set

$$\prod_{i=1}^n R_i = R_1 \times \cdots \times R_n$$

can be turned into a commutative ring under componentwise operations of addition and multiplication. More precisely, we define addition and multiplication on the Cartesian product set by

$$(r_1, \dots, r_n) + (s_1, \dots, s_n) = (r_1 + s_1, \dots, r_n + s_n)$$

and

$$(r_1, \dots, r_n)(s_1, \dots, s_n) = (r_1 s_1, \dots, r_n s_n)$$

for all $r_i, s_i \in R_i$ $(i = 1, \dots, n)$. We call this ring the *direct product* of $R_1, \dots, R_n$. It is not difficult to see that any ideal of $\prod_{i=1}^n R_i$ has the form $I_1 \times \cdots \times I_n$, where $I_i$ is an ideal of $R_i$ for each $i = 1, \dots, n$.

We call two ideals $I$ and $J$ of a ring $R$ *comaximal* if $I + J = R$. It is not difficult to see that for a pair of comaximal ideals $I$ and $J$, $I \cap J = IJ$. In general, for ideals $I_1, \ldots, I_n$ which are pairwise comaximal, we have

$(i)$ $I_1 \ldots I_n = I_1 \cap \ldots \cap I_n$,

$(ii)$ for every $j$, $I_j$ and $\bigcap_{i \neq j} I_i$ are comaximal, and

$(iii)$ the mapping $\phi : R \to \prod_{i=1}^{n} R/I_i$ defined by $\phi : r \mapsto (r + I_1, \ldots, r + I_n)$ is a surjective ring homomorphism whose kernel is equal to $\bigcap_{i=1}^{n} I_i$.

Proposition 1.26. *Let $I$ be an ideal of a commutative ring $R$, and let $J, K$ be ideals of $R$ containing $I$. Then we have*

*$(i)$ $(J/I) \cap (K/I) = (J \cap K)/I$,*

*$(ii)$ $(J/I) + (K/I) = (J + K)/I$,*

*$(iii)$ $(J/I)(K/I) = (JK + I)/I$; in particular, $(J/I)^n = (J^n + I)/I$ for all $n \geq 0$, and*

*$(iv)$ for elements $a_1, \ldots, a_n \in R$, $\sum_{i=1}^{n}(R/I)(a_i + I) = \left[\left(\sum_{i=1}^{n} Ra_i\right) + I\right]/I$.*

**Radicals.** Let $R$ be a commutative ring, and let $I$ be an ideal of $R$. It can be easily proved that the subset

$$\{r \in R : \text{there exists}\, n \in \mathbb{N}\, \text{with}\, r^n \in I\}$$

of $R$ is an ideal of $R$. This ideal, denoted $\sqrt{I}$, is called the *radical* of $I$ (in $R$). In particular, if $I = 0$, then we call the radical $\sqrt{0}$, the *nilradical* of $R$. It is clear, by definition, that $I \subseteq \sqrt{I}$ for all ideals $I$ of $R$. We shall describe later the radical of an ideal as the intersection of all prime ideals containing the ideal.

Exercise 1.27. Let $R$ be a commutative ring, and let $I, J$ be ideals of $R$. Prove that

$(i)$ $\sqrt{I + J} = \sqrt{\left(\sqrt{I} + \sqrt{J}\right)}$;

$(ii)$ $\sqrt{\sqrt{I}} = \sqrt{I}$;

$(iii)$ $\sqrt{I} \neq R$ if and only if $I \neq R$;

$(iv)$ if $\sqrt{I}$ and $\sqrt{J}$ are comaximal ideals, then so are $I$ and $J$;

$(v)$ $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

**Ideal Quotients (Colon Ideals).** If $I$ and $J$ are ideals of a ring $R$, then their *ideal quotient* is

$$(I : J) = \{x \in R : xJ \subseteq I\},$$

which is an ideal. The ideal $(I : J)$ is sometimes referred to as a *colon ideal* because of the notation. In particular, the ideal $(0 : J)$ is called the *annihilator* of $J$, denoted $\operatorname{ann}(J)$ or $\operatorname{ann}_R(J)$.

It should be noted that we could have defined the ideal quotient $(I : J)$ by assuming $J$ to be only a subset (i.e., not an ideal) of $R$ because for any subset $A \subseteq R$, $(I : (A)) = \{r \in R : ra \in I\, \text{for all}\ a \in A\}$. We denote the set on the right by simply $(I : A)$. In particular, for an element $a \in R$, the ideal $(I : \{a\})$ will be abbreviated to $(I : a)$. Note also that all these apply particularly to annihilators.

EXERCISE 1.28. Let $I, J, K$ be ideals of a commutative ring $R$, and let $\{I_\lambda : \lambda \in \Lambda\}$ be a family of ideals of $R$. Show that
*(i)* $((I : J) : K) = (I : JK) = ((I : K) : J)$;
*(ii)* $(\bigcap_{\lambda\in\Lambda} I_\lambda : J) = \bigcap_{\lambda\in\Lambda} (I_\lambda : J)$ ;
*(iii)*$(J : \sum_{\lambda\in\Lambda} I_\lambda) = \bigcap_{\lambda\in\Lambda} (J : I_\lambda)$.

**Extension and Contraction.** Let $R$ and $S$ be commutative rings and let $f : R \to S$ be a ring homomorphism. If $J$ is an ideal of $S$, $f^{-1}(J) = \{r \in R : f(r) \in J\}$ is an ideal of $R$ which is usually denoted by $J^c$. We call $J^c$ the contraction of $J$ to $R$. On the other hand, for an ideal $I$ of $R$, the subset $f(I) = \{f(r) : r \in R\}$ need not be an ideal of $S$. Instead, we will consider the ideal of $S$ generated by the subset $f(I)$, namely, $f(I)S$, which is denoted by $I^e$. We call $I^e$ the extension of $I$ to $S$.

EXERCISE 1.29. Let $R$ and $S$ be commutative rings and let $f : R \to S$ be a ring homomorphism. Let $I, I_1, I_2$ be ideals of $R$ and $J, J_1, J_2$ be ideals of $S$. Shoe that
*(i)* $(I_1 + I_2)^e = I_1^e + I_2^e$;
*(ii)* $(I_1I_2)^e = I_1^eI_2^e$;
*(iii)* $(J_1 \cap J_2)^c = J_1^c \cap J_2^c$;
*(iv)* $\left(\sqrt{J}\right)^c = \sqrt{J^c}$;
*(v)* $I \subseteq I^{ec}$;
*(vi)* $J^{ce} \subseteq J$;
*(vii)* $I^e = I^{ece}$;
*(viii)* $J^c = J^{cec}$.

Let $R$ and $S$ be commutative rings and let $f : R \to S$ be a ring homomorphism. In the following discussion, all extension and contraction notations will be taken under $f$. We fix some notation, at this point, which will be used throughout these notes. We let $\mathcal{I}_R$ denote the set of all ideals of the ring $R$. We also set

$$\mathcal{C}_R = \{J^c : J \in \mathcal{I}_R\},$$

and

$$\mathcal{E}_S = \{I^e : I \in \mathcal{I}_R\}.$$

Observe that, the above exercise leads us to obtain one to one correspondence between $\mathcal{C}_R$ and $\mathcal{E}_S$ defined by

$$\begin{array}{rcl} \mathcal{C}_R & \to & \mathcal{E}_S \\ I & \mapsto & I^e \end{array}$$

whose inverse is given by

$$\begin{array}{rcl} \mathcal{E}_S & \to & \mathcal{C}_R \\ J & \mapsto & J^c. \end{array}$$

In particular, if $f$ is surjective, then $\mathcal{C}_R = \{I \in \mathcal{I}_R : I \supseteq \ker f\}$ and $\mathcal{E}_S = \mathcal{I}_S$. Moreover; we have a bijection mapping

$$\begin{array}{rcl} \{I \in \mathcal{I}_R : I \supseteq \ker f\} & \to & \mathcal{I}_S \\ I & \mapsto & f(I) \end{array}$$

whose inverse is given by contraction.

Exercise 1.30. Let $R$ be a commutative ring and let $X$ be an indeterminate. Let $f : R \to R[X]$ denote the natural ring homomorphism, and use the extension and contraction notations in connection with $f$.

Let $I$ be an ideal of $R$, and for $r \in R$, denote the natural image of $r$ in $R/I$ by $\bar{r}$. Then show that

$(i)$ there is a ring homomorhism

$$\eta : R[X] \to (R/I)[X]$$

such that

$$\eta\left(\sum_{i=0}^{n} r_i X^i\right) = \sum_{i=0}^{n} \bar{r}_i X^i$$

for all $n \in \mathbb{N}$ and $r_0, r_1, \ldots, r_n \in R$;

$(ii)$ $I^e = \ker \eta$, i.e.,

$$I^e = IR[X] = \left\{\sum_{i=0}^{n} r_i X^i \in R[X] : n \in \mathbb{N},\ r_i \in I \,\text{for all}\ 1 \leq i \leq n\right\};$$

$(iii)$ $I^{ec} = I$, and hence $\mathcal{C}_R = \mathcal{I}_R$;

$(iv)R[X]/I^e = R[X]/IR[X] \cong (R/I)[X]$; and

$(v)$ if $I_1, \ldots, I_n$ are ideals of $R$, then

$$(I_1 \cap \ldots \cap I_n)^e = I_1^e \cap \ldots \cap I_n^e.$$

## 1.7. Maximal Ideal, Quasi–local Ring and Jacobson Radical

An ideal $M$ of a commutative ring $R$ is said to be *maximal* if $M$ is a maximal member, with respect to inclusion, of the set of proper ideals $R$. Equivalently, an ideal $M$of $R$ is a maximal ideal if and only if

$(i)$ $M \subset R$, i.e., $M$ is a proper ideal in $R$, and

$(ii)$ there is no proper ideal of $R$ strictly containing $M$, i.e., $M \subseteq I \subseteq R$ for some ideal $I$ of $R$ implies either $M = I$ or $I = R$.

It is clear that an ideal $I$ of a commutative ring $R$ is a maximal ideal in $R$ if and only if $R/I$ is a field. Also, $M$ is a maximal ideal of a commutative ring $R$ containing an ideal $I$ of $R$ if and only if $M/I$ is a maximal ideal of $R/I$.

Exercise 1.31. Let $K$ be a field and let $a_1, \ldots, a_n \in K$. Show that the ideal

$$(X_1 - a_1, \ldots, X_n - a_n)$$

of the ring $K[X_1, \ldots, X_n]$,where $X_1, \ldots, X_n$ are indeterminates, is maximal.

Exercise 1.32. Recall that the set of all continuous real–valued functions on the closed interval $[0, 1]$, denoted $\mathcal{C}[0, 1]$, is a commutative ring. Let $z \in [0, 1]$. Show that

$$M_z := \{f \in \mathcal{C}[0, 1] : f(z) = 0\}$$

is a maximal ideal of $\mathcal{C}[0, 1]$. Show further that every maximal ideal of $\mathcal{C}[0, 1]$ is of this form. (Hint for the second part: Let $M$ be a maximal ideal of $\mathcal{C}[0, 1]$. Argue by contradiction to show that the sets

$$\{a \in [0, 1] : f(a) = 0 \,\text{for all}\ f \in M\}$$

is non–empty: use the fact that that $[0, 1]$ is a compact subset of $\mathbb{R}$.)

We remark that an easy application of Zorn's Lemma says that every non–trivial commutative ring has at least one maximal ideal. This, in particular, yields that every proper ideal of a commutative ring $R$ is contained at least one maximal ideal of $R$. It follows that an element of a commutative ring is a unit if and only if it lies outside all maximal ideals.

Definition 1.33. A commutative ring $R$ which has exactly one maximal ideal, say $M$, is called a *quasi–local ring.* In this case, the field $R/M$ is called the *residue field* of $R$.

Theorem 1.34. *Let $R$ be a commutative ring. Then $R$ is a quasi–local ring if and only if the set of non–units of $R$ form an ideal. It follows that the unique maximal ideal of a quasi–local ring is precisely the set of non–units of $R$.*

Definition 1.35. Let $R$ be a commutative ring. The intersection of all the maximal ideals of $R$ is called the *Jacobson radical of $R$.* The Jacobson radical of $R$ is denoted by $\mathrm{Jac}(R)$.

Theorem 1.36. *Let $R$ be a commutative ring and let $r \in R$. Then $r \in \mathrm{Jac}(R)$ if and only if, for every $a \in R$, the element $1 - ra$ is a unit of $R$.*

Exercise 1.37. Let $R$ be a quasi–local commutative ring with maximal ideal $M$. Show that the ring $R[[X_1, \ldots, X_n]]$ of formal power series over $R$ in indeterminates $X_1, \ldots, X_n$ is again a quasi–local ring, and that its maximal ideal is generated by $M \cup \{X_1, \ldots, X_n\}$.

## 1.8. Prime Ideals

Let $P$ be an ideal of a commutative ring $R$. We say that $P$ is a *prime ideal* of $R$ if
($i$) $P \subset R$, i.e., $P$ is a proper ideal of $R$, and
($ii$) whenever $ab \in P$ for some $a, b \in R$, then either $a \in P$ or $b \in P$.

Observe that the zero ideal in a commutative ring $R$ is a prime ideal if and only if $R$ is an integral domain. More generally, a proper ideal $P$ of a commutative ring $R$ is a prime ideal if and only if $R/P$ is an integral domain. In particular, we conclude that every maximal ideal of a commutative ring is also a prime ideal. Note that, in a PID, nonzero prime ideals are precisely those principal ideals which are generated by irreducible elements. Thus nonzero prime ideals of a PID are also maximal. For instance, in $\mathbb{Z}$, all prime ideals are of the form $p\mathbb{Z}$, where $p$ is a prime number, and also, in the polynomial ring $K[X]$ where $K$ is a field, nonzero prime ideals are those principal ideals generated by irreducible polynomials.

Definition 1.38. Let $R$ be a commutative ring. We call the set of all prime ideals of $R$ the *prime spectrum* or just the *spectrum* of $R$. We denote the spectrum of $R$ by $\mathrm{Spec}(R)$.

We remark that $\mathrm{Spec}(R)$ is always non–empty for a commutative ring $R$ since $R$ has at least one maximal ideal which is also a prime ideal.

Let $R$ and $S$ be commutative rings and let $f : R \to S$ be a ring homomorphism. It is not difficult to see that prime ideals of $S$ remain prime when contracted into $R$, i.e., if $Q \in \mathrm{Spec}(S)$, then $Q^c \in \mathrm{Spec}(R)$. Note that the same does not apply to maximal ideals; to see this, consider the embedding $\mathbb{Z} \to \mathbb{Q}$.

Exercise 1.39. Let $R_1, \dots, R_n$ be commutative rings. Determine all prime and maximal ideals of the direct product ring $\prod_{i=1}^{n} R_i$.

Definition 1.40. Let $R$ be a commutative ring and $I$ a proper ideal of $R$. If $J$ is another ideal of $R$ containing $I$ such that $J/I \in \operatorname{Spec}(R/I)$, then $J \in \operatorname{Spec}(R)$ since prime ideals are preserved under contractions. It should be also noted that prime ideals of a quotient ring $R/I$ are of the form $P/I$ where $P \in \operatorname{Spec}(R)$ such that $P \supseteq I$. The following exercise says the same thing in the language of extension and contraction.

Exercise 1.41. Let $R$ and $S$ be commutative rings, and let $f : R \to S$ be a surjective ring homomorphism. Use the extension and contraction notation in connection with $f$. Let $I \in \mathcal{C}_R$. Show that $I$ is a prime (resp. maximal) ideal of $R$ if and only if $I^e$ is a prime (resp. maximal) ideal of $S$.

Definition 1.42. We say that a subset $S$ of a commutative ring $R$ is *multiplicatively closed* if

($i$) $1 \in S$, and

($ii$) for all $s_1, s_2 \in S$, we have $s_1 s_2 \in S$.

Notice that if $P$ is a prime ideal of a commutative ring $R$, then $R \setminus P$ is a multiplicatively closed subset of $R$. Also, for any nonzero element $r \in R$, $\{r^n : n \geq 0\}$ is an example of a multiplicatively closed subset of $R$. By Zorn's Lemma, we have the following crucial result which connects the idea of multiplicatively closed sets to that of prime ideals.

Theorem 1.43. *Let $I$ be an ideal of a commutative ring $R$, let $S$ be a multiplicatively closed subset of $R$ such that $I \cap S = \emptyset$. Then the set*

$$\Psi = \{J \in \mathcal{I}_R : J \supseteq I \text{ and } J \cap S = \emptyset\}$$

*of ideals of $R$ has a maximal element (with respect to inclusion), and any such maximal element of $\Psi$ is a prime ideal of $R$.*

Definition 1.44. Let $I$ be an ideal of a commutative ring $R$. We define the *variety* of $I$, denoted $\operatorname{Var}(I)$, to be the set

$$\{P \in \operatorname{Spec}(R) : P \supseteq I\}.$$

Corollary 1.45. *Let $I$ be an ideal of a commutative ring $R$. Then*

$$\sqrt{I} = \bigcap_{P \in \operatorname{Var}(I)} P.$$

*In particular, the nilradical $\sqrt{0}$ of $R$ is equal to*

$$\bigcap_{P \in \operatorname{Spec}(R)} P.$$

Following above corollary, we can conclude that the nilradical of the factor ring $R/\sqrt{0}$ is zero. Such a ring (namely, a ring with zero nilradical) is said to be *reduced.*

Exercise 1.46. Let $R$ be a commutative ring and let $X$ be an indeterminate. Use the extension and contraction notation with reference to the natural ring homomorphism $f : R \to R[X]$. Let $I$ be an ideal of $R$. Then show that

($i$) $I \in \operatorname{Spec}(R)$ if and only if $I^e \in \operatorname{Spec}(R[X])$, and

($ii$) $\sqrt{I^e} = \left(\sqrt{I}\right)^e$.

Exercise 1.47. Let $K$ be a field, and let $R = K[X_1, \dots, X_n]$ where $X_1, \dots, X_n$ are indeterminates. Let $a_1, \dots, a_n \in K$. Show that, in $R$,

$$\begin{aligned} 0 \subset (X_1 - a_1) \; &\subset \; (X_1 - a_1, X_2 - a_2) \subset \dots \\ &\subset \; (X_1 - a_1, \dots, X_i - a_i) \subset \dots \\ &\subset \; (X_1 - a_1, \dots, X_n - a_n) \end{aligned}$$

is a strictly ascending chain of prime ideals.

By another application of Zorn's Lemma on the partially ordered set $\operatorname{Var}(I)$ by *reverse* inclusion (for an ideal $I$ of a commutative ring), we obtain the following important result.

Theorem 1.48. *Let $I$ be a proper ideal of a commutative ring $R$. Then the set $\operatorname{Var}(I)$ contains a minimal element with respect to inclusion. We call any such minimal member a minimal prime ideal of $I$ or a minimal prime ideal containing $I$. In the case when $R$ is not trivial, the minimal prime ideals of the zero ideal are referred to as the minimal prime ideals of $R$.*

For an ideal $I$ of a commutative ring $R$, we denote the set of all minimal prime ideals of $R$ by $\operatorname{Min}(I)$. Then $\operatorname{Min}(I) \subseteq \operatorname{Var}(I)$.

Theorem 1.49. *Let $R$ be a commutative ring, $I$ an ideal of $R$, and $P \in \operatorname{Var}(I)$. Then there exists a minimal prime ideal $P'$ of $I$ such that $P \supseteq P'$.*

Corollary 1.50. *Let $I$ be a proper ideal of a commutative ring $R$. Then*

$$\sqrt{I} = \bigcap_{P \in \operatorname{Min}(I)} P.$$

Lemma 1.51. *Let $P$ be a prime ideal of a commutative ring $R$, and let $I_1, \dots, I_n$ be ideals of $R$. Then the following statements are equivalent:*
*(i) $P \supseteq I_j$ for some $1 \leq j \leq n$;*
*(ii) $P \supseteq \bigcap_{i=1}^{n} I_i$;*
*(iii) $P \supseteq \prod_{i=1}^{n} I_i$.*

Corollary 1.52. *Let $I_1, \dots, I_n$ be ideals of a commutative ring $R$, and let $P$ be a prime ideal of $R$ such that $P = \bigcap_{i=1}^{n} I_i$. Then $P = I_j$ for some $1 \leq j \leq n$.*

Exercise 1.53. Let $P$ be a prime ideal of a commutative ring $R$. Show that $\sqrt{P^n} = P$ for all $n \geq 0$.

the prime avoidance theorem. *Let $P_1, \dots, P_n$, where $n \geq 2$, be ideals of the commutative ring $R$ such that at most two of $P_1, \dots, P_n$ are not prime. Let $S$ be an additive subgroup of $R$ which is closed under multiplication. Suppose that*

$$S \subseteq \bigcup_{i=1}^{n} P_i.$$

*Then $S \subseteq P_j$ for some $1 \leq j \leq n$.*

The reason for the name 'prime avoidance' becomes clear after the following reformulation of the above theorem:

With the notation of above theorem, if $S \nsubseteq P_i$ for every $1 \leq i \leq n$, then there exists

$$s \in S \setminus \bigcup_{i=1}^{n} P_i,$$

so that $s$ 'avoids' all the ideals $P_1, \ldots, P_n$, most of which are prime.

Theorem 1.54. *Let $R$ be a commutative ring and let $P_1, \ldots, P_n \in \operatorname{Spec}(R)$. If $I$ is an ideal of $R$ and $a$ is an element of $R$ such that*

$$aR + I \nsubseteq \bigcup_{i=1}^{n} P_i,$$

*then there exists $b \in I$ such that*

$$a + b \notin \bigcup_{i=1}^{n} P_i.$$

Exercise 1.55. Let $R$ be a commutative ring, and let $f = \sum_{i=0}^{\infty} f_i \in R[[X]]$, where $X$ is an indeterminate, $f_i$ is a homogeneous polynomial in $R[X]$ which is either 0 or of degree $i$, for each $i \geq 0$. Use the contraction notation with reference to the natural inclusion ring homomorphism form $R$ to $R[[X]]$.

($i$) Show that $f \in \operatorname{Jac}(R[[X]])$ if and only if $f_0 \in \operatorname{Jac}(R)$.

($ii$) Let $M$ be a maximal ideal of $R[[X]]$. Show that $M$ is generated by $M^c \cup \{X\}$, and that $M^c$ is a maximal ideal of $R$.

($iii$) Show that each prime ideal of $R$ is the contraction of a prime ideal of $R[[X]]$.

## 1.9. Modules

Although there is an extensive theory of modules over arbitrary rings, we shall confine ourselves to deal with modules over commutative rings.

Let $R$ be commutative ring. An *$R$–module* (or, a *module over $R$*) is an additive Abelian group $M$ equipped with a 'scalar multiplication' of its elements by elements of $R$, that is, a mapping

$$\cdot : R \times M \to M,$$

such that

($i$) $r \cdot (m + m') = r \cdot m + r \cdot m'$ for all $r \in R$, $m, m' \in M$,

($ii$) $(r + r') \cdot m = r \cdot m + r' \cdot m$ for all $r, r' \in R$, $m \in M$,

($iii$) $(rr') \cdot m = r \cdot (r' \cdot m)$ for all $r, r' \in R$, $m \in M$, and

($iv$) $1_R \cdot m = m$ for all $m \in M$.

Remark. Note that we usually omit the notation '$\cdot$' to denote scalar multiplication and just use juxtaposition for it. Note also that these axioms have many easy consequences regarding addition, subtraction and scalar multiplication, just as with vector spaces, which we shall not mention here at all.

Examples 1.56. ($i$) Any commutative ring $R$ is a module over itself with respect to the scalar multiplication taken as the multiplication of $R$. More generally, any ideal of $R$ is an $R$–module under the addition and multiplication of $R$.

(*ii*) For an ideal $I$ of a commutative ring $R$, the quotient ring can be given an $R$–module structure. We know that $R/I$ is an additive Abelian group. Now we define, in a canonical way, a scalar multiplication on $R/I$ by elements of $R$ as follows:

$$\begin{aligned} \cdot : R \times (R/I) &\rightarrow R/I \\ (r, a+I) &\mapsto ra + I. \end{aligned}$$

This scalar multiplication together with the standard addition on $R/I$ turns $R/I$ into an $R$–module.

(*iii*) Let $R$ be a commutative ring, and let $S$ be an $R$–algebra with ring homomorphism $f : R \rightarrow S$. Then $S$ is an $R$–module with respect to its own addition and scalar multiplication defined by

$$\begin{aligned} R \times S &\rightarrow S \\ (r, s) &\mapsto f(r)s. \end{aligned}$$

(*iv*) Let $G$ be an additive Abelian group. Then with the scalar multiplication given by

$$ng = \begin{cases} g + \cdots + g & (n\,\text{terms}) \quad \text{for } n > 0 \\ 0 & \qquad\qquad\quad\ \text{for } n = 0 \\ (-g) + \cdots + (-g) & (n\,\text{terms}) \quad \text{for } n < 0 \end{cases}$$

for all $g \in G$ and $n \in \mathbb{Z}$, $G$ becomes a $\mathbb{Z}$–module. Indeed, this is the only scalar multiplication which turns $G$ into a $\mathbb{Z}$–module. It follows that the concept of Abelian group is the same as the concept of $\mathbb{Z}$–module.

Let $R$ and $S$ be commutative rings, and let $f : R \rightarrow S$ be a ring homomorphism. Let $N$ be an $S$–module. Then $N$ has also an $R$–module structure with respect to the same addition and scalar multiplication given by

$$\begin{aligned} R \times N &\rightarrow N \\ (r, n) &\mapsto f(r)n. \end{aligned}$$

In this case, we say that $N$ is regarded as an $R$–module *by means of* $f$, or *by restriction of scalars* when there is no danger of confusion about which ring homomorphism is being used. In particular, if we take $S$, itself, as an $S$–module, then $S$ turns into an $R$–module by restricting scalars using $f$.

Let $M$ be a module over a commutative ring $R$, and let $N$ be a nonempty subset of $M$. If $N$ is itself an $R$–module with respect to the operations for $M$, then we say that $N$ is a *submodule* of $M$. To indicate that $N$ is a submodule of $M$, we write $N \leq M$. Note that we distinguish between the notations $\leq$ and $<$, where the latter means proper containment. For a module $M$ over a commutative ring $R$, and a nonempty subset $N$ of $M$, it is easy to see that $N \leq M$ if and only if $rn + r'n' \in N$ for all $r, r' \in R$ and $n, n' \in N$. Let $J \subseteq M$. We define the *submodule* of $M$ *generated by* $J$ to be the intersection of the family of all submodules of $M$which contain $J$. Note that this is the smallest submodule of $M$containing $J$ with respect to the inclusion relation. Clearly, if $J = \emptyset$, then $N = 0$,and if $J \neq \emptyset$, then

$$N = \left\{ \sum_{i=1}^{n} r_i j_i : n \in \mathbb{N}^+,\, r_1, \ldots, r_n \in R,\, j_1, \ldots, j_n \in J \right\}.$$

If $J = \{j_1, \dots, j_m\}$ is a finite set, then

$$N = \left\{ \sum_{i=1}^{m} r_i j_i : r_1 \dots, r_m \in R \right\},$$

in which case we say that $N$ is a finitely generated $R$–module. In particular, if $J = \{j\}$, then we have $N = \{rj : r \in R\}$. Such an $R$–module is called *cyclic*.

Let $M$ be a module over a commutative ring $R$. Let $\{G_\lambda\}_{\lambda \in \Lambda}$ be a family of submodules of $M$. We define the *sum* $\sum_{\lambda \in \Lambda} G_\lambda$ to be the submodule of $M$ generated by $\bigcup_{\lambda \in \Lambda} G_\lambda$. In particular, this sum is zero when $\Lambda = \emptyset$. It is not difficult to see that this operation is both commutative and associative. Moreover; we may write

$$\sum_{\lambda \in \Lambda} G_\lambda = \left\{ \sum_{i=1}^{n} g_{\lambda_i} : n \in \mathbb{N}^+,\ \lambda_1, \dots, \lambda_n \in \Lambda, \text{ and } g_{\lambda_i} \in G_{\lambda_i} \text{ for all } i = 1, \dots, n \right\}.$$

If $\Lambda = \{1, \dots, n\}$, then we have

$$\sum_{i=1}^{n} G_i = \left\{ \sum_{i=1}^{n} g_i : g_i \in G_i \text{ for all } i = 1, \dots, n \right\}.$$

We often denote $\sum_{i=1}^{n} G_i$ by $G_1 + \cdots + G_n$. We can write a submodule generated by a subset of $M$ in terms of the sum of cyclic modules; namely if $m_1, \dots, m_n \in M$, then the submodule of $M$ generated by $m_1, \dots, m_n$ is $Rm_1 + \cdots + Rm_n$.

Let $M$ be a module over a commutative ring $R$. Let $I$ and $J$ be ideals of $R$. We denote by $IM$ the submodule of $M$generated by the subset $\{rm : r \in R,\ m \in M\}\}$. Then

$$IM = \left\{ \sum_{i=1}^{n} r_i m_i : n \in \mathbb{N}^+,\ r_1, \dots, r_n \in R,\ m_1, \dots, m_n \in M \right\}.$$

Note that $I(I'M) = (II')M$. Note also that for $a \in R$, we write $aM$ instead of $(Ra)M$. In fact, $(Ra)M = \{am : m \in M\}$.

Definition 1.57. Let $M$ be a module over a commutative ring $R$. Let $N \leq M$, and let $U \subseteq M$ with $U \neq \emptyset$. It is clear that the subset

$$\{r \in R : ru \in N \text{ for all } u \in U\} of$$

is an ideal of $R$ denoted $(N : U)$ (or $(N :_R U)$). Observe that if $L$ is a submodule of $M$ generated by $U$, then $(N : U) = (N : L)$.

In the special case when $N = 0$, the ideal

$$(0 : U) = \{r \in R : ru = 0 \text{ for all } u \in U\}$$

is called the *annihilator of* $U$, and denoted by $\operatorname{ann}(U)$ or $\operatorname{ann}_R(U)$. Also for $m \in M$, we call $(0 : m)$ the annihilator of $m$.

Exercise 1.58. Let $I$ be an ideal of a commutative ring $R$. Show that $I = \operatorname{ann}_R(R/I) = (0 :_R 1 + I)$.

Exercise 1.59. Let $M$ be a module over a commutative ring $R$, let $N$, $L$ be submodules of $M$, and let $\{N_\lambda\}_{\lambda \in \Lambda}$ and $\{L_\gamma\}_{\gamma \in \Gamma}$ be two families of submodules of $M$.

*(i)* $(\bigcap_{\lambda \in \Lambda} N_\lambda : L) = \bigcap_{\lambda \in \Lambda} (N_\lambda : L)$;

*(ii)* $\left(N : \sum_{\gamma \in \Gamma} L_\gamma\right) = \bigcap_{\gamma \in \Gamma} (N : L_\gamma)$.

Change of Rings. *Let $M$ be a module over a commutative ring $R$. Let $I$ be an ideal of $R$ such that $I \subseteq \operatorname{ann}(M)$. Then it is easy to see that $M$ has also an $(R/I)$–module structure with respect to its own addition and scalar multiplication given by*

$$\begin{array}{rcl}(R/I)\times M & \to & M\\ (r+I,m) & \mapsto & rm.\end{array}$$

*Note that the condition that $I \subseteq \operatorname{ann}(M)$ is used to make the mapping above unambiguous. It should be also noted that a subset of $M$ is an $R$–module if and only if it is an $(R/I)$–submodule.*

Definition 1.60. Let $M$ be a module over a commutative ring $R$, let $G$ be a submodule of $M$, let $I$ be an ideal of $R$. Then we write $(G :_M I)$ to denote the submodule $\{m \in M : rm \in G \, \text{for all} \; r \in I\}$ of $M$. Observe that $G \subseteq (G :_M I)$. In the particular case when $G = 0$, the submodule $(0 :_M I) = \{m \in M : rm = 0 \, \text{for all} \; r \in I\}$ can be regarded as the annihilator of $I$ in $M$.

Exercise 1.61. Let $M$ be a module over a commutative ring $R$, let $N$ be a submodule of $M$, and let $\{N_\lambda\}_{\lambda\in\Lambda}$ be a family of submodule of $M$. Also let $I$, $J$, $K$ be ideals of $R$, and let $\{I_\alpha\}_{\alpha\in A}$ be a family of ideals of $R$. Show that
(*i*) $((N :_M J) :_M K) = (N :_M JK) = ((N :_M K) :_M J)$;
(*ii*) $(\bigcap_{\lambda\in\Lambda} N_\lambda :_M I) = \bigcap_{\lambda\in\Lambda}(N_\lambda : I)$;
(*iii*)$(N :_M \sum_{\alpha\in A} I_\alpha) = \bigcap_{\alpha\in A}(N :_M I_\alpha)$;

Construction of Quotient (Factor) modules. *Let $M$ be a module over a commutative ring $R$, let $N$ be a submodule of $M$. Since $N$ is a submodule of the Abelian group $M$, $M/N$ is defined as an Abelian group written additively. In addition to the operation of addition on $M/N$ we define the scalar multiplication as*

$$\begin{array}{rcl}R\times(M/N) & \to & M/N\\ (r,m+N) & \mapsto & rm+N\end{array}$$

*to make $M/N$ into an $R$–module.*

*Note that if $M$ is a module over a commutative ring $R$ and $I$ is an ideal of $R$, then $I \subseteq \operatorname{ann}_R(M/IM)$ and hence $M/IM$ is also an $(R/I)$–module under that scalar multiplication defined by $(r+I)(m+IM) = rm+IM$ for all $r \in R$ and $m \in M$ (check this!).*

*If $N$ is a submodule of $M$, then for any submodule $N'$ of $M$ containing $N$, $N'/N$ is a submodule of the factor module $M/N$. As a matter of fact, all submodules of $M/N$ are of this form. Let $N_1$ and $N_2$ be submodules of $M$ which contain $N$. Then $N_1/N \subseteq N_2/N$ if and only if $N_1 \subseteq N_2$. It therefore follows that there is a one–to–one order preserving correspondence between the submodules of $M/N$ and submodule of $M$ containing $N$. Moreover; we have*
*(i) $(N_1/N) + (N_2/N) = (N_1 + N_2)/N$,*
*(ii) $I(N_1/N) = (IN_1 + N)/N$ for any ideal $I$ of $R$,*
*(iii) $(N_1/N) \cap (N_2/N) = (N_1 \cap N_2)/N$, and*
*(iv) $\operatorname{ann}((N_1 + N_2)/N_1) = (N_1 : N_2)$.*

*We also remark that when a module $M$ is finitely generated then so is any factor module $M/N$ of $M$ for if $M$ is generated by a set $\{m_1, \ldots, m_n\}$, then $M/N$ is generated by the set $\{m_1 + N, \ldots, m_n + N\}$.*

Definition 1.62. Let $M$ and $N$ be two modules over a commutative ring $R$, and let $f : M \to N$ be a mapping. We say that $f$ is a *homomorphism of $R$–modules* or $R$–module homomorphism, or only $R$–homomorphism if

$$f(rm + r'm') = rf(m) + r'f(m')$$

for all $r, r' \in R$ and $m, m' \in M$. Such an $R$–homomorphism is called a monomorphism if it is injective, an epimorphism if it is surjective, and an isomorphism if it is both injective and surjective. Also, $f$ is said to be a $R$–module *endomorphism* (or, *$R$–endomorphism*) of $M$ if $f : M \to M$ is an $R$–homomorphism. An endomorphism of a module $M$ which is both injective and surjective is called an *automorphism* of $M$. The unit automorphism of a module $M$ will be denoted by $\mathrm{Id}_M$.

The mapping $M \to N$ which sends every element of $M$ to the zero element of $N$ is called the *zero homomorphism,* denoted 0.

If $f_i : M \to N$ (for $i = 1, 2$) are $R$–homomorphisms, then the mapping $f_1 + f_2 : M \to N$ defined by $(f_1 + f_2)(m) = f_1(m) + f_2(m)$ for all $m \in M$ is also an $R$–homomorphism, called the sum of $f_1$ and $f_2$. Note that if $f : M \to N$ is an $R$–isomorphism, then the mapping $f^{-1} : N \to M$ is also an $R$–isomorphism, in which case we say that $M$ and $N$ are isomorphic $R$–modules and write $M \cong N$. It is clear that isomorphic $R$–modules have equal annihilators. It should be also noted that the composition of two $R$–homomorphisms (resp., $R$–isomorphisms)– when possible – is again an $R$–homomorphism (resp., $R$–isomorphism). It follows that the set of all endomorphisms of a module $M$ (denoted $\mathrm{End}_R(M)$) becomes a ring (not necessarily commutative) with identity with respect to the operations of addition and composition.

Observe that there is a ring homomorphism $\varphi : R \to \mathrm{End}_R(M)$ defined by

$$\begin{aligned} \varphi(r) : M &\longrightarrow M \\ m &\longmapsto rm \end{aligned}$$

for all $r \in R$ and all $m \in M$. It follows that $\varphi$ allows us to view $\mathrm{End}_R(M)$ as an $R$–algebra although it is usually noncommutative. Thus we can think of elements of $R$ as acting on $\mathrm{End}_R(M)$ via $\varphi$. That is, we can define the multiplication $rf \in \mathrm{End}_R(M)$ for $r \in R$ and $f \in \mathrm{End}(M)$ by

$$\begin{aligned} rf : M &\to M \\ m &\mapsto rf(m). \end{aligned}$$

Proposition 1.63. *Let $M$ be a module over a commutative ring $R$, let $I$ be an ideal of $R$, and let $f$ be an $R$–endomorphism of $M$ such that $f(M) \subseteq IM$. Then $f$ satisfies an equation of the form*

$$f^n + a_1 f^{n-1} + \cdots + a_{n-1} f + a_n = 0,$$

*where the $a_i$ are in $I^i$.*

Proof. Let $\{m_1, \ldots, m_n\}$ be a set of generators of $M$. Since $f(M) \subseteq IM$, for every $1 \leq i \leq n$, there exist $a_{ij} \in I$ $(j = 1, \ldots, n)$ such that $f(m_i) = \sum_{j=1}^n a_{ij} m_j$. This gives that $\sum_{j=1}^n (\delta_{ij} f - a_{ij}) m_j = 0$ for every $1 \leq i \leq n$, where $\delta_{ij}$ denotes the Kronecker delta. It follows that we have the equation of matrices $\Phi X = 0$, where

$$\Phi = \begin{bmatrix} f - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & f - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & f - a_{nn} \end{bmatrix}$$

and

$$X = \begin{bmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{bmatrix}.$$

Multiplying both sides by the adjoint matrix of $\Phi$, just as in the usual theory of matrices over fields, we obtain $[\det(\Phi)I_n]\, X = 0$, where $I_n$denotes the identity matrix of order $n$. It follows that $\det(\Phi)$ annihilates all the generators $m_i$ of $M$which yields $\det(\Phi)M = 0$. However; $\det(\Phi)$ is an $R$–endomorphism of $M$ of the form

$$f^n + a_{n-1}f^{n-1} + \cdots + a_n.$$

This completes the proof. □

We remark that $\det(\Phi)$, in the proof of the above proposition, is obtained by substituting $f$ for $X$ into the characteristic polynomial of the matrix $A = [a_{ij}]$, namely, $P(X) = \det[XI_n - A]$. If $M$ is the free $R$–module with basis $m_1, \ldots, m_n$ and $I = R$, then this proposition is just what is known as Cayley–Hamilton theorem: let $P(X)$ be the characteristic polynomial of a square matrix $A$, then $P(A) = 0$.

Theorem 1.64 (Nakayama's Lemma). *Let $M$ be a finitely generated module over a commutative ring $R$, and let $I$ be an ideal of $R$. If $M = IM$, then there exists $a \in R$ such that $aM = 0$ and $1 - a \in I$. If, in addition, $I \subseteq \operatorname{Jac}(R)$, then $M = 0$.*

Proof. Setting $f = \mathrm{Id}_M$ in the preceding theorem, we get the relation $a = 1 + a_1 + \cdots + a_n = 0$ as an endomorphism of $M$ which yields that $aM = 0$, and $1 - a \in I$. Now, if $I \subseteq \operatorname{Jac}(R)$, then $a$ is a unit of $R$, and hence $0 = a^{-1}aM = M$. □

Corollary 1.65. *Let $M$ be a module over a commutative ring $R$, $N$ a submodule of $M$, and $I$ an ideal of $R$ contained in $\operatorname{Jac}(R)$. If $M/N$ is a finitely generated $R$–module and $M = N + IM$, then $M = N$.*

Let $\Gamma$ be a set of generators of a module $M$ over a commutative ring $R$. We say that $\Gamma$ is a *minimal generating set* of $M$ if any proper subset of $\Gamma$ does not generate $M$. Two minimal generating set do not necessarily have the same cardinality; for example, when $M = R$, if $x$ and $y$ are non–units of $R$such that $x + y = 1$, then both $\{1\}$ and $\{x, y\}$ are minimal generating sets of $R$. Notice that such an example does not arise for quasi–local rings. The following theorem says that the cardinality of a minimal generating set of a finitely generated module over a quasi–local ring is an invariant property for the module.

Theorem 1.66. *Let $(R, \mathfrak{M})$ be a quasi–local ring and let $M$ be a finitely generated $R$–module. Set $k = R/\mathfrak{M}$ and $\overline{M} = M/\mathfrak{M}M$. Now $\overline{M}$ is a finite dimensional vector space over $k$, and we write $n$ for its dimension. Then*

*$(i)$ If we take a basis $\{\gamma_1, \dots, \gamma_n\}$ for $\overline{M}$ over $k$, and choose an inverse image $u_i \in M$ of each $\gamma_i$ (i.e., $\gamma_i = u_i + \mathfrak{M}M$), then $\{u_1, \dots, u_n\}$ is a minimal generating set of $M$. Conversely, every minimal generating set of $M$ is obtained in this way.*

*$(ii)$ Any minimal generating set of $M$ has $n$ elements.*

*$(iii)$ If $\{u_1, \dots, u_n\}$ and $\{v_1, \dots, v_n\}$ are both minimal generating sets of $M$, and $v_i = \sum a_{ij} u_j$ with $a_{ij} \in R$, then $\det[a_{ij}]$ is a unit in $R$, so that $[a_{ij}]$ is an invertible matrix.*

Proof. $(i)$ Since $\overline{M} = \sum_{i=1}^{n} R\gamma_i = \sum_{i=1}^{n} R(m_i + \mathfrak{M}M) = (\sum_{i=1}^{n} Rm_i + \mathfrak{M}M)/\mathfrak{M}M$, we have $M = \sum_{i=1}^{n} Rm_i + \mathfrak{M}M$. Since $M/(\sum_{i=1}^{n} Rm_i)$ is also finitely generated, by Corollary 1.65, $M = \sum_{i=1}^{n} Rm_i$. If $\{m_1, \dots, m_n\}$ is not minimal, that is, if a proper subset, for example $\{m_{i_1}, \dots, m_{i_k}\}$ $(k < n)$, generates $M$, then $\{\bar{m}_{i_1}, \dots, \bar{m}_{i_k}\}$ generates $\overline{M}$, which is a contradiction. Hence $\{m_1, \dots, m_n\}$ is a minimal generating set of $M$.

Now, if $\{m_1, \dots, m_t\}$ is a minimal generating set of $M$ and $\bar{u}_i$ is the image of $u_i$ in $\overline{M}$ for every $1 \leq i \leq t$, then $\bar{u}_1, \dots, \bar{u}_t$ generate $\overline{M}$ over $k$. Hence $\{\bar{m}_1 \dots, \bar{m}_t\}$ is a basis for $\overline{M}$ since otherwise some proper subset of $\{\bar{m}_1, \dots, \bar{m}_t\}$ would be a basis for $\overline{M}$, and then by above a proper subset of $\{u_1, \dots, u_t\}$ would generate $M$, a contradiction.

$(ii)$ Let $\{m_1, \dots, m_t\}$ be a minimal generating set of $M$. Then by $(i)$, $\{\bar{m}_1, \dots, \bar{m}_t\}$ is a basis for $\overline{M}$. Since $\dim_k \overline{M} = n$ by assumption, we must have $t = n$.

$(iii)$ Left to the student. □

Exercise 1.67. Prove part $(iii)$ of Theorem 1.66.

Definition 1.68. Let $R'$ and $R''$ be two algebras over a commutative ring $R$, and let $\varphi : R' \to R''$ be a ring homomorphism. We say that $\varphi$ is an *$R$–algebra homomorphism* if it is a homomorphism of $R$–modules when $R'$ and $R''$ are regarded as $R$–modules by means of their structural ring homomorphisms.

Exercise 1.69. Let $R$ be a commutative ring, and let $R'$, $R''$ be commutative $R$–algebras having structural ring homomorphisms $f' : R \to R'$ and $f'' : R \to R''$. Let $\varphi : R' \to R''$ be a ring homomorphism. Then show that $\varphi$ is an $R$–algebra homomorphism if and only if $\varphi \circ f' = f''$.

Let $M$ be a module over a commutative ring $R$, and $N$ a submodule of $M$. Then the mapping $\pi : M \to M/N$ defined by $\pi(m) = m + N$ for all $m \in M$ is surjective, and hence, an epimorphism, called the *canonical projection* of $M$ onto $M/N$. Suppose that $M'$ is a second $R$–module, and that $f : M \to M'$ is a homomorphism of $R$–modules. The *kernel* of $f$, denoted by $\ker f$, is the set $\{m \in M : f(m) = 0_{M'}\}$. It is clear that $\ker f = 0$ if and only if $f$ is a monomorphism. The image of $f$, denoted by $\operatorname{Im} f$, is the subset $f(M) = \{f(m) : m \in M\}$ of $M'$. Evidently, $\operatorname{Im} f$ is a submodule of $M'$. Notice that the kernel of the canonical projection of $M$ onto $M/N$ is equal to the submodule $N$. Thus the projection from $M$ onto $M/0$ is an isomorphism. One can easily deduce that a subset $N$ of a module $M$ is a submodule of $M$ if and only if $N$ is a kernel of a homomorphism from $M$ to some $R$–module.

Let $R$ be commutative ring, $M$ an $R$–module, and $f : M \to M$ an $R$–endomorphism. For $P(X) = a_0 + a_1X + \cdots + a_nX^n \in R[X]$, we put $P(f) = a_0 + a_1f + \cdots + a_nf^n \in$

$\mathrm{End}_R(M)$. Define a scalar multiplication on the additive abelian group $M$ by

$$\begin{array}{rcl} \cdot : R[X] \times M & \longrightarrow & M \\ (P(X), m) & \longmapsto & P(f)(m). \end{array}$$

With this multiplication, $M$ becomes a module over $R[X]$.

Theorem 1.70. *Let $M$ be a finitely generated module over a commutative ring $R$. If $f : M \to M$ is an $R$–endomorphism and $f$ is surjective, then $f$ is also injective, so $f$ is an automorphism of $M$.*

Proof. (Vasconcelos) Since $M$ can be viewed as an $R[X]$–module by setting $X \cdot m = f(m)$ for $m \in M$, we have $XM = M$. By Nakayama's Lemma, there exists $P(X) \in R[X]$ such that $(1 + XP)M = 0$. Now, if $u \in \ker f$ , then $0 = (1 + XP)(u) = u + P(f)u = u$. It follows that $f$ is injective, and so an automorphism. □

the first isomorphism theorem for modules. *Let $M$ and $M'$ be modules over a commutative ring $R$, and let $f : M \to M'$ be an $R$–homomorphism. Then $f$ induces an isomorphism $\bar{f} : M/\ker f \to \mathrm{Im}\, f$ for which $\bar{f}(m + \ker f) = f(m)$ for all $m \in M$.*

Corollary 1.71. *Let $R$ be a commutative ring. For an $R$–module $M$, let $\mathcal{S}_M$ denote the set of all submodules of $M$. Let $f : M \to M'$ be an epimorphism of $R$–modules. Then the mapping*

$$\begin{array}{rcl} \tau : \{N \in \mathcal{S}_M : N \supseteq \ker f\} & \to & \mathcal{S}_{M'} \\ N & \mapsto & f(N) \end{array}$$

*is an inclusion preserving bijection.*

Proposition 1.72. *Let $M$ and $M'$ be modules over a commutative ring $R$, and let $f : M \to M'$ be an $R$–homomorphism. Let $N$ be a submodule of $M$ such that $N \subseteq \ker f$ . Then $f$ induces an $R$–homomorphism $g : M/N \to M'$ for which $g(m + N) = f(m)$ for all $m \in M$. Moreover; if $G$ is a submodule of $M$ and $G'$ is a submodule of $M'$ such that $f(G) \subseteq G'$, then $f$ induces an $R$–homomorphism $\tilde{f} : M/G \to M'/G'$ for which $\tilde{f}(m + G) = f(m) + G'$ for all $m \in M$.*

second isomorphism theorem for modules. *Let $M$ be a module over a commutative ring $R$. Let $N$, $N'$ be submodules of $M$such that $N' \supseteq N$. Then there is an isomorphism*

$$\alpha : (M/N) \,/\, (N'/N) \to M/N'$$

*by $\alpha((m + N) + N'/N) = m + N'$ for all $m \in M$.*

the third isomorphism theorem for modules. *Let $M$ be a module over a commutative ring $R$, and let $K$, $L$ be submodules of $M$. Then there is an isomorphism*

$$\sigma : K/(K \cap L) \to (K + L)/L$$

*such that $\sigma(k + K \cap L) = k + L$ for all $k \in K$.*

Definition 1.73. Let $R$ be a commutative ring, let $M$, $M'$, and $M''$ be $R$–modules, and let $f : M' \to M$ and $g : M \to M''$ be $R$–homomorphisms. We say that the sequence

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

is exact if $\operatorname{Im} f = \ker g$.

More generally, we say that a sequence

$$\cdots \longrightarrow M_{n-1} \xrightarrow{d_{n-1}} M_n \xrightarrow{d_n} M_{n+1} \xrightarrow{d_{n+1}} M_{n+2} \longrightarrow \cdots$$

of $R$–modules and $R$–homomorphisms is exact at a term $M^r$ in the sequence for which both $d_{r-1}$ and $d_r$ are defined if

$$M_{r-1} \xrightarrow{d_{r-1}} M_r \xrightarrow{d_r} M_{r+1}$$

is an exact sequence; and we say that the whole sequence is exact if and only if it is exact at every term $M_r$ for which both $d_{r-1}$ and $d_r$ are defined.

Let $M$, $N$ be modules over a commutative ring $R$, and let $h : M \to N$ be an $R$–homomorphism.

($i$) The sequence

$$0 \longrightarrow M \xrightarrow{h} N$$

is exact if and only if $h$ is a monomorphism.

($ii$) The sequence

$$M \xrightarrow{h} N \longrightarrow 0$$

is exact if and only if $h$ is an epimorphism.

($iii$) For any submodule $G$ of $M$, there is an exact sequence

$$0 \longrightarrow G \xrightarrow{i} M \xrightarrow{\pi} M/G \longrightarrow 0$$

in which $i$ is the inclusion homomorphism and $\pi$ is the canonical epimorphism.

Definition 1.74. Let $R$ be a commutative ring. An exact sequence of $R$–modules and $R$–homomorphisms of the form

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

is called a *short exact sequence.*

In order that a sequence

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

of $R$–modules and $R$–homomorphisms be a short exact sequence, we must have

($i$) $f$ is a monomorphism,

($ii$) $g$ is an epimorphism, and

($iii$) $\operatorname{Im} f = \ker g$.

**Direct Products and Direct Sums of Modules.** Let $R$ be a commutative ring and let $\{M_\lambda : \lambda \in \Lambda\}$ be a non–empty family of $R$–modules. Then the Cartesian product set $\prod_{\lambda\in\Lambda} M_\lambda$ is an $R$–module under componentwise operations of addition and scalar multiplication. In other words we define the operations by

$$(m_\lambda) + (m'_\lambda) = (m_\lambda + m'_\lambda)$$

and

$$r(m_\lambda) = (rm_\lambda)$$

for all $(m_\lambda), (m'_\lambda) \in \prod_{\lambda\in\Lambda} M_\lambda$ and $r \in R$. We call this new $R$–module the direct product of the family $\{M_\lambda : \lambda \in \Lambda\}$.

The subset of $\prod_{\lambda\in\Lambda} M_\lambda$ consisting of all $(m_\lambda)_{\lambda\in\Lambda}\in \prod_{\lambda\in\Lambda} M_\lambda$ with the property that all but finite number of $m_\lambda$ are zero, is an $R$–submodule of $\prod_{\lambda\in\Lambda} M_\lambda$. We denote this submodule by $\bigoplus_{\lambda\in\Lambda} M_\lambda$, and call it the *direct sum*, or sometimes the *external direct sum*, of the family $\{M_\lambda : \lambda \in \Lambda\}$.

Note that in the case when $\Lambda$ is finite, we have $\bigoplus_{\lambda\in\Lambda} M_\lambda = \prod_{\lambda\in\Lambda} M_\lambda$.

Now let $M'_\mu$ denote the subset

$$\left\{ (m_\lambda) \in \bigoplus_{\lambda\in\Lambda} M_\lambda : m_\lambda = 0 \,\text{for all}\; \lambda \in \Lambda \,\text{with}\; \lambda \neq \mu \right\}$$

of $\bigoplus_{\lambda\in\Lambda} M_\lambda$. It can be easily shown that

(*i*) $M'_\mu$ is an $R$–submodule of $\bigoplus_{\lambda\in\Lambda} M_\lambda$ and $M'_\mu \cong M_\mu$ for all $\mu \in \Lambda$,

(*ii*) $\sum_{\lambda\in\Lambda} M'_\lambda = \bigoplus_{\lambda\in\Lambda} M_\lambda$, and

(*iii*) for each $\mu \in \Lambda$, we have

$$M'_\mu \bigcap \sum_{\substack{\lambda\in\Lambda \\ \lambda\neq\mu}} M'_\lambda = 0.$$

Definition 1.75. Let $M$ be a module over a commutative ring $R$, and let $\{M_\lambda : \lambda \in \Lambda\}$ be a family of submodules of $M$. If

[(1)]$M = \sum_{\lambda\in\Lambda} M_\lambda$

[(2)] for each $\mu \in \Lambda$,

$$M_\mu \bigcap \sum_{\substack{\lambda\in\Lambda \\ \lambda\neq\mu}} M_\lambda = 0,$$

then we say that $M$ is the *direct sum*, or sometimes the *internal direct sum, of its family of submodules* $\{M_\lambda : \lambda \in \Lambda\}$ *and write*

$$\bigoplus_{\lambda\in\Lambda} M_\lambda.$$

Note that if $M = \bigoplus_{\lambda\in\Lambda} M_\lambda$ for a family of submodules $\{M_\lambda : \lambda \in \Lambda\}$ of $M$, then by condition (1) in the above definition, for any element $m \in M$, there exist $n \in \mathbb{N}_0$, $\lambda_1, \ldots, \lambda_n \in \Lambda$ and $m_i \in M_{\lambda_i}$ $(i = 1, \ldots, n)$ such that

$$m = \sum_{i=1}^{n} m_i.$$

Now, the condition (2) implies that the number $n$, the $\lambda_i$'s, and the elements $m_i \in M_{\lambda_i}$ are uniquely determined by $m$. This property distinguishes the internal direct sums from ordinary sums.

Note also that, by the arguments given before the above definition, for a family $\{M_\lambda : \lambda \in \Lambda\}$ of modules over a commutative ring $R$, and derived submodules

$$M'_\mu = \left\{ (m_\lambda) \in \bigoplus_{\lambda\in\Lambda} M_\lambda : m_\lambda = 0 \, \text{for all } \lambda \in \Lambda \, \text{with } \lambda \neq \mu \right\},$$

the external direct sum $\bigoplus_{\lambda\in\Lambda} M_\lambda$ of $M_\lambda$'s is equal to the internal direct sum $\bigoplus_{\lambda\in\Lambda} M'_\lambda$ of its family of submodules $\{M'_\lambda : \lambda \in \Lambda\}$.

Suppose that $R$ is a commutative ring and $\{M_\lambda : \lambda \in \Lambda\}$ is a non–empty family of $R$–modules. The *canonical projection of* $M = \bigoplus_{\lambda\in\Lambda} M_\lambda$ *onto* $M_\mu$ is the mapping $p_\mu : M \to M_\mu$ defined by $p_\mu((m_\lambda)) = m_\mu$ for all $(m_\lambda) \in M$ (where all but a finite number of $m_\lambda$ are nonzero). The *canonical injection of* $M_\mu$ *into* $M = \bigoplus_{\lambda\in\Lambda} M_\lambda$ is the mapping $q_\mu : M_\mu \to M$ defined by $q_\mu(x) = (m_\lambda)$, for all $x \in M_\mu$, where $m_\lambda = 0$ for all $\lambda \in \Lambda$ with $\lambda \neq \mu$ and $m_\mu = x$. It is easy to see that canonical projections $p_\lambda$ are surjective while canonical injections $q_\lambda$ are injective. Moreover; we have

(*i*) $p_\mu \circ q_\mu = \mathrm{I}_{M_\mu}$,
(*ii*) $p_\lambda \circ q_\mu = 0$ for all $\mu \in \Lambda$ with $\mu \neq \lambda$, and
(*iii*) when $\Lambda$ is finite, $\sum_{\lambda\in\Lambda} q_\lambda \circ p_\lambda = \mathrm{I}_M$.

Exercise 1.76. Let $M, M_1, \ldots M_n$ be modules over a commutative ring $R$.

(*i*) Show that there is an exact sequence

$$0 \longrightarrow M_j \xrightarrow{q_j} \bigoplus_{i=1}^{n} M_i \xrightarrow{p'_j} \bigoplus_{\substack{i=1 \\ i\neq j}}^{n} M_i \longrightarrow 0$$

of $R$–modules and $R$–homomorphisms in which $q_j$ is the canonical injection and

$$p'_j((m_1, \ldots, m_n)) = (m_1, \ldots, \hat{m}_j, \ldots, m_n)$$

(where $\hat{m}_j$ denotes the absence of the $j$–th coordinate in $(m_1, \ldots, m_n)$) for all $(m_1, \ldots, m_n) \in \bigoplus_{i=1}^n M_i$.

(*ii*) Suppose that there exist, for each $1 \leq i \leq n$, homomorphisms $\tilde{p}_i : M \to M_i$ and $\tilde{q}_i : M_i \to M$ such that, for $1 \leq i, j \leq n$,

$$\tilde{p}_i \circ \tilde{q}_i = \mathrm{I}_{M_i} \qquad \text{and} \qquad \tilde{p}_i \circ \tilde{q}_j = 0 \, \text{for } i \neq j,$$

and $\sum_{i=1}^n \tilde{q}_i \circ \tilde{p}_i = \mathrm{I}_M$. Show that the mapping $f : M \to \bigoplus_{i=1}^n M_i$ defined by

$$f(m) = (\tilde{p}_1(m), \ldots, \tilde{p}_n(m)) \quad \text{for all } m \in M$$

is an isomorphism.

Definition 1.77. Let $R$ be a commutative ring. A short exact sequence

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

is said to split if $\operatorname{Im} f = \ker g$ is a direct summand of $M$, i.e., if there is a submodule $N$ of $M$ such that $M = \ker g \oplus N$.

An example of a split short exact sequence is

$$0 \longrightarrow M' \xrightarrow{q_1} M' \oplus M'' \xrightarrow{p_2} M'' \longrightarrow 0,$$

where $M'$ and $M''$ are $R$–modules, $q_1$ is the canonical injection, and $p_2$ is the canonical projection.

Exercise 1.78. Let $R$ be a commutative ring, and let

$$(*) \qquad 0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

be a short exact sequence of $R$–modules and $R$–homomorphisms. Show that the following conditions are equivalent:

($i$) The short exact sequence $(*)$ splits;

($ii$) There exists an $R$–homomorphism $h : M'' \to M$ such that $gh = \mathrm{I}_{M''}$;

($iii$) There exists an $R$–homomorphism $e : M \to M'$ such that $ef = \mathrm{I}_{M'}$.

Definition 1.79. Let $M$ be a module over a commutative ring $R$. Suppose that $M$ contains a subset $\{e_\lambda : \lambda \in \Lambda\}$ with the following properties:

($i$) $\{e_\lambda : \lambda \in \Lambda\}$ generates $M$, and

($ii$) each $m \in M$ can be uniquely written in the form $m = \sum_{\lambda\in\Lambda} r_\lambda e_\lambda$, where $r_\lambda \in R$ for all $\lambda \in \Lambda$ and only finitely many of the $r_\lambda$ are nonzero.

Then we say that $M$ is a *free $R$–module* with a base $\{e_\lambda : \lambda \in \Lambda\}$.

Note that $R$ is a free $R$–module with base $\{1_R\}$. The zero module 0 is a free $R$–module with an empty base.

Remark 1.80. Let $M$ be a module over a commutative ring $R$, and let $\{e_\lambda : \lambda \in \Lambda\}$ be a subset of $M$ such that $M = \sum_{\lambda\in\Lambda} Rm_\lambda$. Then $M$ is a free $R$–module with base $\{e_\lambda : \lambda \in \Lambda\}$ if and only if whenever

$$\sum_{\lambda\in\Lambda} r_\lambda e_\lambda = 0$$

for some $r_\lambda \in R$ $(\lambda \in \Lambda)$ in which only a finite number of the $r_\lambda$'s are nonzero, then $r_\lambda = 0$ for all $\lambda \in \Lambda$.

Proposition 1.81. *Let $R$ be a commutative ring.*

($i$) *Let $\{R_\lambda : \lambda \in \Lambda\}$ be a nonempty family of $R$–modules with $R_\lambda = R$ for all $\lambda \in \Lambda$. Then $\bigoplus_{\lambda\in\Lambda} R_\lambda$ is a free $R$–module, with base $\{e_\lambda : \lambda \in \Lambda\}$, where for each $\mu \in \Lambda$, the element $e_\mu \in \bigoplus_{\lambda\in\Lambda} R_\lambda$ has its components in $R_\mu$equal to 1 and all its other components zero.*

($ii$) *Let $M$ be an $R$–module. Then $M$ is free if and only if $M$ is isomorphic to an $R$–module of the type described in part (i) above. In fact, if $M$ has a base $\{e_\lambda : \lambda \in \Lambda\}$,then $M \cong \bigoplus_{\lambda\in\Lambda} R_\lambda$, where $R_\lambda = R$ for all $\lambda \in \Lambda$.*

Exercise 1.82. Let $R$ be a commutative ring, and let $\{e_\lambda : \lambda \in \Lambda\}$ be a set of *symbols*, indexed by a non–empty set $\Lambda$. Construct a free $R$–module having $\{e_\lambda : \lambda \in \Lambda\}$ as a base.

Proposition 1.83. *Let $M$ be a module over a commutative ring $R$. Then there exist a free $R$–module $F$ and an $R$–module epimorphism $f : F \to M$.*

*Also, if $M$ is finitely generated by $n$ elements, then $F$ can be taken to be a free $R$–module with a finite base of $n$ elements.*

Proposition 1.84. *Let $R$ be a nontrivial commutative ring, and let $F$ be a free $R$–module with a finite base. Then every base for $F$ is finite, and any two bases for $F$ have the same number of members. The number of members in a base for $F$ is called the* rank of $F$.

Proof. (Sketch) Let $F$ be a free $R$–module with a base $\{e_1, \dots, e_n\}$. Take a maximal ideal $\mathfrak{M}$ of $R$ and consider the $R$–module $F/\mathfrak{M}F$ . Since $F/\mathfrak{M}F$ is annihilated by $\mathfrak{M}$, it is also a vector space over $R/\mathfrak{M}$. Now, the proposition follows if one shows that the set $\{e_1 + \mathfrak{M}F, \dots, e_n + \mathfrak{M}F\}$ forms a basis for $F/\mathfrak{M}F$ over $R/\mathfrak{M}$. □

Exercise 1.85. Suppose that $F$ is a free module over a nontrivial commutative ring $R$, and that $F$ is finitely generated. Show that every base for $F$ is finite.

CHAPTER 2

# Chain Conditions

Let $(S, \leq)$ be a partially ordered set. One can easily see that the following two conditions are equivalent:

(***i***) Every ascending chain $x_1 \leq x_2 \leq \ldots \leq x_i \leq x_{i+1} \leq \ldots$ of elements in $S$ is stationary, i.e., there exists a positive integer $n$ such that $x_n = x_{n+i}$ for all $i \in \mathbb{N}$.

(***ii***) Every non–empty subset of $S$ has a maximal element.

We say that $(S, \leq)$ satisfies *the ascending chain condition* (abbreviated *a.c.c.*) if it satisfies one of the above conditions. Note that if we define a new relation on $S$ by reversing $\leq$, then we again have a partially ordered set, and hence we can adapt the above conclusion for also descending chains in $(S, \leq)$, namely, for every descending chain $x_1 \geq x_2 \geq \ldots \geq x_i \geq x_{i+1} \geq \ldots$ of elements in $S$, there exists a positive integer $n$ such that $x_n = x_{n+i}$ for all $i \in \mathbb{N}$ if and only if every non–empty subset of $S$ has a minimal element, in which case we say that $(S, \leq)$ satisfies the *descending chain condition* (abbreviated *d.c.c.*).

Let $M$ be a module over a commutative ring $R$. We denote the set of all submodules of $M$ by $\mathcal{S}_M$. If $\mathcal{S}_M$ satisfies a.c.c., then we say that $M$ is a *Noetherian* $R$–module (after Emmy Noether), and if $\mathcal{S}_M$ satisfies d.c.c., then we say that $M$ is an *Artinian* $R$–module (after Emil Artin). It follows that an $R$–module $M$ is Noetherian if and only if, for every descending chain

$$L_1 \subseteq L_2 \subseteq \ldots \subseteq L_i \subseteq L_{i+1} \subseteq \ldots$$

of submodules of $M$, there exists a positive integer $n$ such that $L_n = L_{n+i}$ for all $i \in \mathbb{N}$ if and only if every non–empty subset of $\mathcal{S}_M$ has a maximal element with respect to inclusion. Moreover; $M$ is an Artinian $R$–module if and only if, for every descending chain

$$L_1 \supseteq L_2 \supseteq \ldots \supseteq L_i \supseteq L_{i+1} \supseteq \ldots$$

of submodules of $M$, there exists a positive integer $n$ such that $L_n = L_{n+i}$ for all $i \in \mathbb{N}$.

A commutative ring $R$ is said to be a Noetherian ring (resp., Artinian ring) if $R$ is a Noetherian (resp., Artinian) module when considered as a module over itself in the natural way. For example, the ring of integers $\mathbb{Z}$ is a Noetherian ring. However; $\mathbb{Z}$ is not an Artinian ring since for any prime number $p$, we have the infinite strictly descending chain

$$(p) \supset (p^2) \supset \cdots \supset (p^i) \supset (p^{i+1}) \supset \cdots$$

of ideals of $\mathbb{Z}$. Indeed, every principal ideal domain is Noetherian (see Exercise 2.1 $(i)$), and no integral domain which is not a field is Artinian (see Exercise 2.1 $(ii)$). Note also that a field is both Noetherian and Artinian.

Exercise 2.1. ($i$) Prove that every P.I.D. is a Noetherian ring.
($ii$) Show that an Artinian integral domain is a field.

Exercise 2.2. Let $M$ be an Artinian module over a commutative ring $R$. Let $f : M \to M$ be an $R$–endomorphism of $M$ which is injective. Prove that $f$ is also surjective, so $f$ is an automorphism of $M$.

Example 2.3. Let $p$ be a fixed prime number. Then

$$\mathbb{Z}_{p^\infty} := \{\alpha \in \mathbb{Q}/\mathbb{Z} : \alpha = \frac{r}{p^n} + \mathbb{Z} \text{ for some } r \in \mathbb{Z} \text{ and } n \in \mathbb{N}_0\}$$

is a submodule of the $\mathbb{Z}$–module $\mathbb{Q}/\mathbb{Z}$. For each $t \in \mathbb{N}_0$ we set

$$G_t := \{\alpha \in \mathbb{Q}/\mathbb{Z} : \alpha = \frac{r}{p^t} + \mathbb{Z} \text{ for some } r \in \mathbb{Z}\}.$$

Then
($i$) $G_t$ is the submodule of $\mathbb{Z}_{p^\infty}$ generated by $(1/p^t) + \mathbb{Z}$, for each $t \in \mathbb{N}_0$. (Here we assume that $G_0 = 0$),
($ii$) each proper submodule of $\mathbb{Z}_{p^\infty}$ is equal to $G_i$ for some $i \in \mathbb{N}_0$, and
($iii$) the set of all proper submodules of $\mathbb{Z}_{p^\infty}$ forms the strictly ascending (non–terminating) chain

$$G_0 \subset G_1 \subset \ldots \subset G_n \subset G_{n+1} \subset \ldots,$$

and so $\mathbb{Z}_{p^\infty}$ is an Artinian, non–Noetherian $\mathbb{Z}$–module.

Proof. It is easy to check that $\mathbb{Z}_{p^\infty}$ is a $\mathbb{Z}$–submodule of $\mathbb{Q}/\mathbb{Z}$. Also, since $(r/p^t) + \mathbb{Z} = r[(1/p^t) + \mathbb{Z}]$, part ($i$) is clear.

($ii$) Let $H$ be a proper submodule of $\mathbb{Z}_{p^\infty}$. We may assume that $H \neq 0$ since otherwise we have $H = G_0$. By definition, we have $\mathbb{Z}_{p^\infty} = \bigcup_{i\in\mathbb{N}_0} G_i$. Also, since $(1/p^n) + \mathbb{Z} = p((1/p^{n+1}) + \mathbb{Z})$ for each $n \in \mathbb{N}_0$, we have the chain

$$G_0 \subseteq G_1 \subseteq \ldots \subseteq G_n \subseteq G_{n+1} \subseteq \ldots$$

of submodules of $\mathbb{Z}_{p^\infty}$. Since $H$ is a proper submodule of $\mathbb{Z}_{p^\infty}$, there is a greatest integer $i \in \mathbb{N}$ such that $G_j \subseteq H$. If this were not the case, then, for each $j \in \mathbb{N}$, there would exist $n_j \in \mathbb{N}$ with $n_j \geq j$ and $G_{n_j} \subseteq H$, so that $G_j \subseteq H$, and this would lead to he contradiction that $H = \mathbb{Z}_{p^\infty}$. Let $m$ be this greatest integer. Then $G_m \subseteq H$.

We shall show that $H = G_m$. Suppose, on the contrary, that $G_m \neq H$. Then there exists $\alpha \in H \setminus G_m$. Now, there exist $r \in \mathbb{Z}$ and $t \in \mathbb{N}_0$ such that $\alpha = (r/p^t) + \mathbb{Z}$. Since $\alpha \neq 0$, if $r$ has a factor which is a power of $p$, then this power should be smaller than $p^t$. It follows that, without loss of generality, we may take $r \notin p\mathbb{Z}$, that is, $(r, p^t) = 1$. Then there exist $a, b \in \mathbb{Z}$ such that $ar + bp^t = 1$, and so

$$\frac{1}{p^t} + \mathbb{Z} = \frac{ar}{p^t} + \mathbb{Z} = a\alpha \in H.$$

This gives that

$$G_t = \left(\frac{1}{p^t} + \mathbb{Z}\right)\mathbb{Z} \subseteq H,$$

which contradicts with the choice of $m$. Hence $H = G_m$, as claimed.

$(iii)$ We shall show that, for all $i \in \mathbb{N}_0$, $(1/p^{i+1}) + \mathbb{Z} \notin G_i$. Indeed, if we had $(1/p^{i+1}) + \mathbb{Z} \in G_i$, then there would exist $r \in \mathbb{Z}$ such that

$$\frac{1}{p^{i+1}} - \frac{r}{p^i} \in \mathbb{Z},$$

so that $1 - rp \in p^{i+1}\mathbb{Z}$, a contradiction. Hence

$$G_0 \subset G_1 \subset \ldots \subset G_n \subset G_{n+1} \subset \ldots . \tag{2.1}$$

This, in particular, shows that $\mathbb{Z}_{p^\infty}$ is not a Noetherian $\mathbb{Z}$–module. On the other hand, since the chain in 2.1 forms up the total list of proper submodules of $\mathbb{Z}_{p^\infty}$, any descending chain of submodules of $\mathbb{Z}_{p^\infty}$ contains only finitely many submodules which are essentially equal to some $G_i$ (except possibly the first term). This shows that $\mathbb{Z}_{p^\infty}$ is an Artinian $\mathbb{Z}$–module. □

Proposition 2.4. *Let $K$ be a field, and $V$ be a vector space over $K$. Then the following statements are equivalent:*
*$(i)$ $V$ is a finite–dimensional $K$–space;*
*$(ii)$ $V$ is a Noetherian $K$–module;*
*$(iii)$ $V$ is an Artinian $K$–module.*

Proof. By comparing dimensions of subspaces, we see that any chain of subspaces in a finite–dimensional vector space has finitely many terms. This establishes both $(i) \Rightarrow (ii)$ and $(i) \Rightarrow (iii)$. For implications $(ii) \Rightarrow (i)$ and $(iii) \Rightarrow (i)$, we assume that $V$ is not finite–dimensional and show that $V$ is neither Noetherian nor Artinian as a $K$–space. Let $\{v_i\}_{i\in\mathbb{N}}$ be a linearly independent subset of $V$. We set

$$L_n := \bigoplus_{i=1}^{n} Kv_i \text{ and } M_n := \bigoplus_{i=n+1}^{\infty} Kv_i.$$

Now, we have the strictly ascending chain

$$L_1 \subset L_2 \subset \ldots \subset L_n \subset L_{n+1} \subset \ldots$$

and the strictly descending chain

$$M_1 \supset M_2 \supset \ldots \supset M_n \supset M_{n+1} \supset \ldots$$

of subspaces of $V$. This proves that $V$ is neither a Noetherian nor an Artinian $K$–module. □

Proposition 2.5. *Let $M$ be a module over a commutative ring $R$. Then $M$ is Noetherian if and only if every submodule of $M$ is finitely generated.*

Proof. $(\Rightarrow)$ Let $N$ be a submodule of $M$. Suppose that $N$ is not finitely generated. Let $\Gamma$ be the set of all submodule of $N$ which are finitely generated. Then $\Gamma \neq \emptyset$ since $0 \in \Gamma$. Since every submodule of $N$ is also a submodule of $M$, by maximal condition on $M$ (i.e., $M$ is Noetherian), $\Gamma$ has a maximal member with respect to inclusion. Let this maximal member be $L$. We have $L \subset N$ since $N$ is not finitely generated. Let $n \in N \setminus L$. Then $L + Rn$ is a finitely generated submodule of $N$and $L \subset L + Rn$ since $n \in (L + Rn) \setminus N$. This is a contradiction. Thus $N$ must be finitely generated.

$(\Leftarrow)$ Let

$$L_1 \subseteq L_2 \subseteq \ldots \subseteq L_n \subseteq L_{n+1} \subseteq \ldots$$

be an ascending chain of submodules of $M$. Then $G = \bigcup_{i\in\mathbb{N}} L_i$ is a submodule of $M$. By hypothesis $G$ is finitely generated, say by $g_1, \ldots, g_t$ . Then there is a sufficiently large $n \in \mathbb{N}$ such that $g_1, \ldots, g_t \in L_n$. It follows that

$$G = \sum_{i=1}^{t} Rg_i \subseteq L_n \subseteq L_{n+1} \subseteq \ldots \subseteq G.$$

Hence $L_n = L_{n+i}$ for all $i \in \mathbb{N}$. It follows that $M$ is Noetherian. □

Proposition 2.6. *Let $M$ be a module over a commutative ring $R$, let $N$ be a submodule of $M$. Then the $R$–module $M$ is Noetherian (resp. Artinian) if and only if both $M$ and $M/N$ are Noetherian (resp. Artinian).*

Proof. Let $M$ be Noetherian as $R$–module. Since every submodule of $N$ is also a submodule of $M$, it is clear that $N$ is also a Noetherian $R$–module. Also, any ascending chain of submodules of $M/N$ must be of the form

$$N_1/N \subseteq N_2/N \subseteq \ldots \subseteq N_i/N \subseteq N_{i+1}/N \subseteq \ldots,$$

where

$$N_1 \subseteq N_2 \subseteq \ldots \subseteq N_i \subseteq N_{i+1} \subseteq \ldots$$

is an ascending chain of submodules of $M$ containing $N$. Since the latter chain must stop, so must the former. The case in which $M$ is Artinian can be handled similarly.

Now suppose both $M$ and $M/N$ are Noetherian. Let

$$L_1 \subseteq L_2 \subseteq \ldots \subseteq L_i \subseteq L_{i+1} \subseteq \ldots$$

be an ascending chain of submodules of $M$. Consider the ascending chain

$$N \cap L_1 \subseteq N \cap L_2 \subseteq \ldots \subseteq N \cap L_i \subseteq N \cap L_{i+1} \subseteq \ldots$$

of submodules of $N$ and the ascending chain

$$(N + L_1)/N \subseteq (N + L_2)/N \subseteq \ldots \subseteq (N + L_i)/N \subseteq (N + L_{i+1})/N \subseteq \ldots$$

of submodules of $M/N$. Since both $N$ and $M/N$ are Noetherian, there exist $n, m \in \mathbb{N}$ such that

$$N \cap L_n = N \cap L_{n+i} \text{ for all } i \in \mathbb{N}_0$$

and

$$N + L_m = N + L_{m+j} \text{ for all } j \in \mathbb{N}_0.$$

Let $k = \max\{n, m\}$. We claim that $L_k = L_{k+i}$ for all $i \in \mathbb{N}_0$. We already know that $L_k \subseteq L_{k+i}$. Let $l \in L_{k+i}$. Since

$$l \in L_{k+i} \subseteq N + L_{k+i} = N + L_k,$$

there exists $a \in N$ and $b \in L_k$ such that $l = a + b$. Hence

$$a = l - b \in N \cap L_{k+i} = N \cap L_k,$$

so that both $a$ and $b$ lie in $L_k$ and $l = a + b \in L_k$. Therefore $L_{k+i} \subseteq L_k$, and so $L_k = L_{k+i}$ for all $i \in \mathbb{N}_0$. The proof of the case when both $N$ and $M/N$ are Artinian can be given in a similar way. □

Corollary 2.7. *Let $R$ be a commutative ring, and let*

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

*be a short exact sequence of $R$–modules and $R$–homomorphisms. Then the $R$–module $M$ is Noetherian (resp. Artinian) if and only if $L$ and $N$ are Noetherian (resp. Artinian).*

Corollary 2.8. *Let $M_1, \dots, M_n$ be modules over a commutative ring $R$. Then the direct sum $\bigoplus_{i=1}^n M_i$ is Noetherian (resp. Artinian) if and only if $M_1, \dots, M_n$ are all Noetherian (resp. Artinian).*

Proof. The proof follows easily by induction on $n$ (together with the above corollary). □

Corollary 2.9. *Let $R$ be a commutative ring. If $R$ is Noetherian (resp. Artinian), then every finitely generated $R$–module is Noetherian (resp. Artinian).*

Proof. If $M$ is a finitely generated $R$–module, where $R$ is a Noetherian (resp. Artinian) ring, then it can viewed as a factor module of a finitely generated free $R$–module. By Corollary 2.8, such a free module (and hence any of its factors) must be Noetherian (resp. Artinian). This completes the proof. □

Lemma 2.10. *Let $M$ be module over a commutative ring $R$, and let $m \in M$. Then there is an isomorphism of $R$–modules*

$$f : R/(0 : m) \longrightarrow Rm$$

*such that $f(r + (0 : m)) = rm$ for all $r \in R$. Furthermore, $M$ is cyclic if and only if $M$ is isomorphic to an $R$–module of the form $R/I$ for some ideal $I$ of $R$.*

Remark 2.11. Let $M$ be a module over a commutative ring $R$, and let $I$ be an ideal of $R$ such that $I \subseteq \operatorname{ann}(M)$. Then $M$ is also an $(R/I)$–module and a subset of $M$ is an $R$–submodule of $M$ if and only if it is an $(R/I)$–submodule of $M$. It follows that $M$ is Noetherian (reps. Artinian) as an $R$–module if and only if it is Noetherian (resp. Artinian) as an $(R/I)$–module.

In particular, if $I$ is an ideal of $R$, then $R/I$ is Noetherian (resp. Artinian) as $R$–module if and only if it is a Noetherian (resp. Artinian) ring.

Exercise 2.12. Let $M$ be a module over a commutative ring $R$. Show that

($i$) if $M$ is a Noetherian $R$–module, then $R/\operatorname{ann}(M)$ is a Noetherian ring, and

($ii$) if $M$ is a finitelty generated Artinian $R$–module, then $R/\operatorname{ann}(M)$ is an Artinian ring.

Note that part ($i$) of the above exercise shows, in particular, that if one is going to study Noetherian modules over commutative rings, then one might just study finitely generated modules over commutative Noetherian rings because $M$ is a finitely generated module over $R/\operatorname{ann}(M)$, as well, and a subset of $M$ is an $R$–submodule of $M$ if and only if it is an $(R/\operatorname{ann}(M))$–submodule of $M$.

Exercise 2.13. ($i$) What can we say about $\mathbb{Q}$? Is it Noetherian or Artinian as a $\mathbb{Z}$–module?

($ii$) Answer the same question in ($i$) for $\mathbb{Q}/\mathbb{Z}$.

Theorem 2.14. *Let $G$ be a module over a commutative ring $R$, and assume that $G$ is annihilated by the product of finitely many (not necessarily distinct) maximal ideals of $R$, that is, there exist $n \in \mathbb{N}$ and maximal ideals $\mathfrak{M}_1, \dots, \mathfrak{M}_n$ of $R$ such that*

$$\mathfrak{M}_1 \dots \mathfrak{M}_n G = 0.$$

*Then $G$ is a Noetherian $R$–module if and only if $G$ is an Artinian $R$–module.*

Proof. We use induction on $n$. Let $n = 1$. Then there exists a maximal ideal $\mathfrak{M}$ of $R$ such that $\mathfrak{M}G = 0$. It follows that $G$ is an $R/\mathfrak{M}$–space. By Proposition 2.4, $G$ is a Noetherian $R/\mathfrak{M}$–module if and only if it is an Artinian $R/\mathfrak{M}$–module. However; the set of $R$–submodules of $G$ is the same as the set of $R/\mathfrak{M}$–subspaces of $G$. This gives that $G$ is Noetherian (resp. Artinian) as $R$–module if and only if it is Noetherian (resp. Artinian) as $R/\mathfrak{M}$–module. This completes the proof the proposition for $n = 1$.

Now, suppose that $n > 1$ and that the result has been proved for smaller values of $n$. Since we can write $(\mathfrak{M}_1 \dots \mathfrak{M}_{n-1})\mathfrak{M}_n G = 0$, by induction hypothesis, we obtain that the $R$–module $\mathfrak{M}_n G$ is Noetherian if and only if it is Artinian. Also, since $G/\mathfrak{M}_n G$ is annihilated by the maximal ideal $\mathfrak{M}_n$ of $R$, one can conclude, by the above paragraph, that $G/\mathfrak{M}_n$ is a Noetherian $R$–module if and only if $G/\mathfrak{M}_n G$ is an Artinian $R$–module. On the other hand, if we consider the natural short exact sequence

$$0 \longrightarrow \mathfrak{M}_n G \longrightarrow G \longrightarrow G/\mathfrak{M}_n G \longrightarrow 0,$$

then we get that $G$ is Noetherian if and only if $\mathfrak{M}_n G$ and $G/\mathfrak{M}_n G$ are Noetherian if and only if $\mathfrak{M}_n G$ and $G/\mathfrak{M}_n G$ are Artinian (by above facts) if and only if $G$ is Artinian (by Corollary 2.7). This completes the proof. □

Remark 2.15. With the help of above theorem, we can find many examples of modules which are both Noetherian and Artinian. Indeed, if $G$ is a finitely generated module over a commutative Noetherian ring $R$ and $\mathfrak{M}_1, \dots, \mathfrak{M}_n$ are maximal ideals of $R$, then $G$ and $G/\mathfrak{M}_1 \dots \mathfrak{M}_n G$ are both Noetherian. Since $G/\mathfrak{M}_1 \dots \mathfrak{M}_n G$ is annihilated by the product $\mathfrak{M}_1 \dots \mathfrak{M}_n$ of maximal ideals, it is both Noetherian and Artinian.

Definition 2.16. Let $G$ be a module over a commutative ring $R$. We say that $G$ is a *simple* $R$–module if $G \neq 0$ and the only submodules of $G$ are 0 and $G$ itself.

Lemma 2.17. *Let $G$ be a module over a commutative ring $R$. Then $G$ is a simple $R$–module if and only if $G$ is isomorphic to an $R$–module of the form $R/\mathfrak{M}$ for some maximal ideal $\mathfrak{M}$ of $R$.*

Proof. Suppose first that $G$ is simple. Then $G$ is a cyclic $R$–module. Thus $G \cong R/I$ for some ideal $I$ of $R$ . Since $R/I$ is simple as an $R$–module, $I$ must be a maximal $R$–submodule (or, equivalently a maximal ideal) of $R$. Now, let $I$ be maximal ideal of $R$. Since $R/I$ has exactly two ideals, namely 0 and $R/I$ itself, the $R$–module $R/M$ has exactly two submodules, namely 0 and $R/I$. This completes the proof. □

Definition 2.18. Let $G$ be a module over a commutative ring $R$. The *length* of a strictly increasing chain

$$G_0 \subset G_1 \subset \dots \subset G_{n-1} \subset G_n$$

of submodules of $G$ is the number of links, that is, one less than the number of terms. We consider

$$G_0$$

to be a chain of length 0.

A strictly increasing chain

$$G_0 \subset G_1 \subset \ldots \subset G_{n-1} \subset G_n$$

of submodules of $G$ such that $G_0 = 0$ and $G_n = G$ is called a composition series for $G$ if $G_i/G_{i-1}$is a simple $R$–module for each $i = 1, \ldots, n$.

By definition, a composition series of a module $G$ is a strictly ascending chain of submodules starting from 0 and ending in $G$ which cannot be extended to a longer strictly ascending chain by inserting an extra term.

Theorem 2.19. *Let $G$ be a module over a commutative ring $R$, and assume that $G$ has a composition series of length $n$. Then*

($i$) *no strictly ascending chain of submodules of $G$ of finite length with the first term* 0 *and last term $G$ can have length greater than $n$,*

($ii$) *every composition series for $G$ has length exactly $n$, and*

($iii$) *each strictly ascending chain of submodules of $G$ of length $n' \leq n$ with the first term* 0 *and last term $G$ can be extended to a composition series for $G$ by insertion of $n - n'$ additional terms; in particular,*

($iv$) *each strictly ascending chain of submodules of $G$ of length $n$ with the first term* 0 *and last term $G$ is a composition series for $G$.*

Proof. Clearly we can assume that $n > 0$. For each $R$–module $M$ with a composition series, we denote the smallest length of a composition series for $M$ by $\ell(M)$. We set $\ell(M) = \infty$ if $M$ does not have a composition series. We shall first show that if $H$ is a proper submodule of $G$, than $\ell(H) < \ell(G)$.

Let $\ell(G) = t$ and let

$$0 = G_0 \subset G_1 \subset \ldots \subset G_{t-1} \subset G_t = G$$

gives us a composition series for $G$ of length $t$. We set $H_i := H \cap G_i$ for each $i = 1, \ldots, t$. Then by the First Isomorphism Theorem, for each $i = 1, \ldots, t$, the composite $R$–homomorphism

$$H_i = H \cap G_i \xrightarrow{i} G_i \xrightarrow{\pi} G_i/G_{i-1},$$

where $i$ is the inclusion map and $\pi$ is the canonical epimorphism, has kernel equal to $H \cap G_i \cap G_{i-1} = H_{i-1}$ and so induces an $R$–monomorphism

$$\begin{array}{rcl} \psi_i : H_i/H_{i-1} & \longrightarrow & G_i/G_{i-1} \\ h + H_{i-1} & \longmapsto & h + G_{i-1}. \end{array}$$

Thus $H_i/H_{i-1}$ is isomorphic to a submodule of $G_i/G_{i-1}$. Since $G_i/G_{i-1}$ is a simple $R$–module, $H_i/H_{i-1}$ is either 0 or simple. Also, $H_i/H_{i-1}$ is a simple module if and only if $\psi_i$ is an isomorphism. Thus, if we remove any repetitions of terms in

$$0 = H_0 \subseteq H_1 \subseteq \ldots \subseteq H_t = H \cap G_t = H,$$

we obtain a composition series for $H$. Thus $\ell(H) \leq \ell(G)$. Furthermore, we must have $\ell(H) < \ell(G)$, for otherwise the above process must lead to

$$H_0 \subset H_1 \subset \ldots \subset H_{t-1} \subset H_t$$

as a composition series for $H$, so that $H_i/H_i \cap G_{i-1} = H_i/H_{i-1} \neq 0$ for all $i = 1, \ldots, t$. Since $H_0 = 0 = G_0$, it would then follow successively that

$$H_1 = G_1,\ H_2 = G_2,\ \ldots,\ H_t = G_t,$$

contradicting the fact that $H \subset G$. Thus we have shown that $\ell(H) < \ell(G)$, as claimed. Note also that we have shown that every submodule of $G$ has a composition series.

$(i)$ Now let

$$G'_0 \subset G'_1 \subset \ldots \subset G'_{r-1} \subset G'_r$$

be a strictly ascending chain of submodules of $G$ such that $G'_0 = 0$ and $G'_r = G$. Now $\ell(0) = 0$, and so it follows from the receding paragraph that

$$0 = \ell(G'_0) < \ell(G'_1) < \ldots < \ell(G'_{r-1}) < \ell(G'_r) = \ell(G).$$

Hence $r \leq \ell(G) \leq n$. Therefore, since $G$ has a composition series of length $n$ and a composition series for $G$ is, in particular, a strictly ascending chain of submodules of $G$ with the first term 0 and last term $G$, we must have, by above, $n \leq \ell(G)$, so that $n = \ell(G)$.

$(ii)$ Now suppose that $G$ has a composition series of length $n_1$. Then $n_1 \leq \ell(G) = n$ by part $(i)$ because a composition series is a strictly ascending chain from 0 to $G$. Also, we have $\ell(G) \leq n_1$ by definition of $\ell(G)$.

$(iii)$ and $(iv)$ A strictly ascending chain from 0 to $G$ of length $n' < n = \ell(G)$ cannot be a composition series for $G$ because, by part $(ii)$, all composition series for $G$ have length $n$, and so it can be extended to a strictly ascending chain of length $n'+1$ by the insertion of an extra term; on the other hand, a strictly ascending chain of submodules of $G$ from 0 to $G$ of length $n$ must already be a composition series for $G$ because otherwise it could be extended to a strictly ascending chain of submodules of length $n+1$, contrary to part $(i)$. □

Definition 2.20. Let $G$ be a module over a commutative ring $R$. We say that $G$ *has finite length* if $G$ has a composition series. When this is the case, the *length* of $G$, denoted by $\ell(G)$, is defined to be the length of any composition series for $G$.

When $G$ does not have finite length, that is, when $G$ has no composition series, we write $\ell(G) = \infty$.

Proposition 2.21. *Let $G$ be a module over a commutative ring $R$. Then $G$ has finite length if and only if $G$ is both Noetherian and Artinian.*

Proof. $(\Rightarrow)$: Assume that $G$ has finite length $n$. Then by Theorem 2.19, any strictly ascending chain must have length at most $n$. Thus any strictly ascending chain must be stationary, so that $G$ is Noetherian. Similarly, any strictly descending chain of submodules of $G$ is stationary, and so $G$ is also Artinian.

$(\Leftarrow)$: Assume that $G$ is both Noetherian and Artinian. Set

$$\Phi := \{H \leq G : \ell(H) < \infty\}.$$

Since $0 \in \Phi$, $\Phi \neq \emptyset$. It follows that $\Phi$ has a maximal elements, say $H$ because $G$ is Noetherian (or, in other words, any non–empty set of submodules of $G$ has a maximal member with respect to inclusion). We shall show that $H = G$. Suppose, on the contrary, that $H$ is a proper submodule of $G$. Since $H \in \Phi$, $H$ has a composition series. Let $\ell(H) = n$ and suppose that

$$0 = H_0 \subset H_1 \subset \ldots \subset H_n = H$$

is a composition series for $H$. The fact that $G$ is Artinian implies that $G/H$ is an Artinian (non–zero) $R$–module by Proposition 2.6. It follows that $G/H$ has a simple submodule, say $H'/H$. Then

$$0 = H_0 \subset H_1 \subset \ldots \subset H_n \subset H'$$

is a composition series for $H'$, which contradicts the maximality of $H$. Therefore $H = G$, and hence $\ell(G) < \infty$. □

Definition 2.22. Let $G$ be a module over a commutative ring $R$, and suppose that $G$ has finite length. Let

$$0 = G_0 \subset G_1 \subset \ldots \subset G_{n-1} \subset G_n = G$$

be a composition series for $G$ (so that $\ell(G) = n$). Then the set $\{G_i/G_{i-1} : i = 1, \ldots, n\}$ of simple $R$–modules is called the set of *composition factors* of the above composition series. Note that this set is empty if $G = 0$.

Now assume that $G \neq 0$ and that

$$0 = G'_0 \subset G'_1 \subset \ldots \subset G'_{n-1} \subset G'_n = G$$

is another composition series for $G$. We say that two composition series for $G$ are isomorphic if there exists a permutation $\sigma$ of the set $\{1, \ldots, n\}$ of the first $n$ positive integers such that, for all $i = 1, \ldots, n$,

$$G_i/G_{i-1} \cong G'_{\sigma(i)}/G'_{\sigma(i)-1}.$$

One useful way of interpreting simplicity of a factor module is by the concept of maximal submodules. For a module $G$ and a submodule $H$ of $G$, we say that $H$ is a maximal submodule of $G$ if $H \neq G$ and there is no submodule of $G$ that lies properly between $H$ and $G$. Notice that the quotient module $G/H$ is simple if and only if $H$ is a maximal submodule of $G$.

Lemma 2.23. *Let $G$ be a module over a commutative ring $R$, and let $H, H'$ be submodules of $G$ such that $H \neq H'$ and both $G/H$ and $G'/H'$ are simple. Then*

$$G/H \cong H'/(H \cap H') \qquad \textit{and} \qquad G/H \cong H/(H \cap H').$$

Proof. Suppose that $H = H + H'$. Then we have $H' \subseteq H$. Since $G/H'$ is simple, $H'$ is a maximal submodule of $G$. Also since $G/H$ is simple, $H \neq G$, and hence, by maximality of $H'$, $H = H'$, a contradiction. Now, by the Third Isomorphism Theorem for modules, it suffices to show that $H + H' = G$. However, this follows easily because $H \subset H + H'$ and $H$ is a maximal submodule of $G$. □

Theorem 2.24 (The Jordan–Hölder Theorem). *Let $G$ be a nonzero module of finite length over a commutative ring $R$. Then every pair of composition series for $G$ are isomorphic.*

Proof. Since $G \neq 0$, we have $n := \ell(G) \geq 1$. We use induction on $n$. The claim is clear when $n = 1$, and so we assume that $n > 1$ and that the result has been proved for smaller values of $n$. Let

$$0 = G_0 \subset G_1 \subset \ldots \subset G_{n-1} \subset G_n = G$$

and

$$0 = G'_0 \subset G'_1 \subset \ldots \subset G'_{n-1} \subset G'_n = G$$

be two composition series for $G$. We first assume that $G_{n-1} = G'_{n-1}$. Then we have

$$G_n/G_{n-1} = G'_n/G'_{n-1}$$

and both

$$G_0 \subset G_1 \subset \ldots \subset G_{n-1}$$

and

$$G'_0 \subset G'_1 \subset \ldots \subset G'_{n-1}$$

are composition series for $G_{n-1} = G'_{n-1}$. Since $\ell(G_{n-1}) = n - 1$, we can apply the inductive hypothesis to these two composition series for $G_{n-1}$ and the desired result in this case follows easily.

Now, assume that $G_{n-1} \neq G'_{n-1}$. We set $H := G_{n-1} \cap G'_{n-1}$. Then, by above lemma, we have the isomorphisms

$$G_n/G_{n-1} \cong G'_{n-1}/H \qquad \text{and} \qquad G'_n/G'_{n-1} \cong G_{n-1}/H,$$

so that four of these modules are simple. Thus, if $H = 0$ (so that both $G_{n-1}$ and $G'_{n-1}$ are simple and $n = 2$), the desired conclusion has been obtained. Thus we assume that $H \neq 0$.

In this case,

$$0 \subset H \subset G_{n-1} \subset G_n$$

is a strictly ascending chain of submodules of $G$, and both $G_n/G_{n-1}$ and $G_{n-1}/H$ are simple. Now, by Theorem 2.19 (*iii*), the above chain can be extended to a composition series for $G$. Also we have $\ell(H) = n - 2$. In particular, we obtain a composition series

$$0 = H_0 \subset H_1 \subset \ldots \subset H_{n-3} \subset H_{n-2} = H$$

for $H$. Now the two composition series

$$H_0 \subset H_1 \subset \ldots \subset H_{n-3} \subset H_{n-2} \subset G_{n-1} \subset G_n$$

and

$$H_0 \subset H_1 \subset \ldots \subset H_{n-3} \subset H_{n-2} \subset G'_{n-1} \subset G'_n$$

for $G$ are isomorphic. But we can use the inductive hypothesis (on two composition series for $G_{n-1}$) to see that the two composition series

$$G_0 \subset G_1 \subset \ldots \subset G_{n-1} \subset G_n$$

and

$$H_0 \subset H_1 \subset \ldots \subset H_{n-3} \subset H_{n-2} \subset G_{n-1} \subset G_n$$

for $G$ are isomorphic. Similarly, the composition series

$$H_0 \subset H_1 \subset \ldots \subset H_{n-3} \subset H_{n-2} \subset G'_{n-1} \subset G'_n$$

and

$$G'_0 \subset G'_1 \subset \ldots \subset G'_{n-1} \subset G'_n$$

are isomorphic, and so we can complete the inductive step.

The theorem is therefore proved by induction. □

Remark 2.25. Let $M$ and $M'$ be two isomorphic modules over a commutative ring $R$. Since submodules of $M$ and $M'$ lie in one-to-one correspondence which preserves inclusion, it is clear that $M$ is Noetherian (resp., Artinian) if and only if $M'$ is Noetherian (resp. Artinian). It follows that $M$ has finite length if and only if $M'$ has finite length, in which case $\ell(M) = \ell(M')$.

Proposition 2.26. *Let $R$ be a commutative ring, and let*

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

*be a short exact sequence of $R$–modules and $R$–homomorphisms. Then $M$ has finite length if and only if $L$ and $N$ both have finite length. Moreover; if $L$, $M$, $N$ all have finite length, then*

$$\ell(M) = \ell(L) + \ell(N).$$

Proof. Notice that the $R$–module $M$ has finite length if and only if it is both Noetherian and Artinian; this is the case if and only if $L$ and $N$ are both Noetherian and Artinian; and this is the case if and only if both $L$ and $N$ have finite length.

For the rest of the proposition, we note that $L \cong \operatorname{Im} f = \ker g$, and that by the First Isomorphism Theorem for modules, we also have $M/\ker g \cong N$. Thus, by above remark, $\ker g$ and $M/\ker g$ have finite length, and $\ell(L) = \ell(\ker g)$ and $\ell(N) = \ell(M/\ker g)$. It is thus sufficient to show that if $G$ is a submodule of the $R$–module $M$, where $M$ has finite length, then $\ell(M) = \ell(G) + \ell(M/G)$. This equation is valid for $G = 0$ or $G = M$. So assume that $G \neq 0$ and $G \neq M$. Then the strictly ascending chain

$$0 \subset G \subset M$$

of submodules of $M$ can be extended to a composition series for $M$, say

$$0 = M_0 \subset M_1 \subset \ldots \subset M_{n-1} \subset M_n = M,$$

(where we assume that $\ell(M) = n$). Suppose that $M_t = G$. Then

$$M_0 \subset M_1 \subset \ldots \subset M_t$$

is a composition series for $G$, and it follows that

$$M_t/G \subset M_{t+1}/G \subset \ldots \subset M_n/G$$

is a composition series for $M/G$. Hence $\ell(G) + \ell(M/G) = t + (n - t) = n = \ell(M)$, as required. □

Proposition 2.27. *Let $V$ be a vector space over a field $K$. Then $V$ is a finite-dimensional $K$–space if and only if it is a $K$–module of finite length, and when this is the case,* $\dim_K V = \ell(V)$.

Proof. We know, from Proposition 2.4, that $V$ is finite-dimensional if and only $V$ satisfies either ascending or descending (and hence, both) chain conditions as a $K$–module. This established the first part of the proposition. For the second part we assume that $\dim_K(V) = n$, argue by induction on $n$. When $n = 0$, we have $V = 0$, and there is nothing to prove. When $n = 1$, the only subspaces of $V$ are 0 and $V$ itself, and so $0 \subset V$ is a composition series for the $K$–module $V$, so that $\ell(V) = 1$. We therefore suppose that $n > 1$ and that the result has been proved for smaller values of $n$.

Let $v \in V$ with $v \neq 0$. Set $U = Kv$. Now since $\dim_K(U) = 1$ and $\dim_K(V) = \dim_K(U) + \dim_K(V/U)$, we must have $\dim_K(V/U) = n - 1$, and so by the inductive hypothesis, $\ell(U) = 1$ and $\ell(V/U) = n - 1$. This gives, by Proposition 2.26, that

$$\ell(V) = \ell(U) + \ell(V/U) = 1 + n - 1 = n,$$

and so the inductive step is complete.

This completes the proof. □

Exercise 2.28. Let

$$0 \longrightarrow G_n \xrightarrow{d_n} G_{n-1} \longrightarrow \cdots \longrightarrow G_i \xrightarrow{d_i} G_{i-1} \longrightarrow \cdots \longrightarrow G_1 \xrightarrow{d_1} G_0 \longrightarrow 0$$

be an exact sequence of modules and homomorphisms over a commutative ring $R$ (where $n \in \mathbb{N}$ and $n > 1$), and suppose that $G_i$ has finite length for all $i = 1, \ldots, n-1$. Show that $G_0$ and $G_n$ have finite length, and that

$$\sum_{i=0}^{n} (-1)^i \ell(G_i) = 0.$$

Exercise 2.29. Let $G$ be a module over a non-trivial commutative ring Noetherian ring $R$. Show that $G$ has a finite length if and only if $G$ is finitely generated and there exist $n \in \mathbb{N}$ and maximal ideals $\mathfrak{M}_1, \ldots, \mathfrak{M}_n$ of $R$ (not necessarily distinct) such that

$$\mathfrak{M}_1 \ldots \mathfrak{M}_n G = 0.$$

Exercise 2.30. Let $R$ be a PID which is not a field. Let $G$ be an $R$–module. Show that $G$ has finite length if and only if $G$ is finitely generated and there exists $r \in R$ with $r \neq 0$ such that $rG = 0$.

CHAPTER 3

# Primary Decomposition Theory

We start this section with a quotation from [5]. "The decomposition of an integer into the product of powers of primes has an analogue in rings where prime integers are replaced by prime ideals but, rather surprisingly, powers of prime integers are not replaced by powers of prime ideals but rather by *primary ideals*. Primary ideals were introduced in 1905 by Lasker in the context of polynomial rings. (Lasker was World Chess Champion from 1894 to 1921.) Lasker proved the existence of a decomposition of an ideal into primary ideals but the uniqueness properties of the decomposition were not proved until 1915 by Macaulay."

Let's begin our discussion with a principal ideal domain $R$ which is not a field. Let $I$ be a nonzero proper ideal of $R$. Then there is a nonzero, non-unit element $a \in R$ such that $I = (a)$. Since $R$ is, at the same time, a unique factorization domain, there exist irreducible elements $p_1, \dots, p_m$ of $R$, a unit $u$ in $R$, and positive integers $k_1, \dots, k_m$ such that $a = up_1^{k_1} \dots p_m^{k_m}$ . It follows that we may write

$$I = Ra = \prod_{i=1}^{m} Rp_i^{k_i}.$$

Since $\sqrt{Rp_i^{k_i}} = Rp_i$ for each $1 \leq i \leq m$, by Exercise 1.53; and since $Rp_1, \dots, Rp_m$ are pairwise comaximal, $Rp_1^{k_1}, \dots, Rp_m^{k_m}$ are pairwise comaximal, by Exercise 1.27 $(iv)$. This shows that

$$I = Ra = Rp_1^{k_1} \cap \dots \cap Rp_m^{k_m}.$$

It follows that $I$ can be written as an intersection of ideals which are powers of maximal ideals; and, as we shall see, any positive power of a maximal ideal is what we call a primary ideal. Such an expression of $I$ as an intersection of primary ideals is called a primary decomposition of $I$.

## 3.1. Primary Submodules and Primary Ideals

Definition 3.1. Let $M$ be a nonzero module over a commutative ring $R$, and let $\mathcal{Q}$ be a submodule of $M$. We say that $\mathcal{Q}$ is a *primary submodule* of $M$ if it is a proper submodule of $M$ (i.e., $\mathcal{Q} \neq M$) and whenever $rm \in \mathcal{Q}$ for some $r \in R$ and $m \in M$, then either $m \in \mathcal{Q}$ or $r^n M \subseteq \mathcal{Q}$ for some $n \in \mathbb{N}$ (i.e., $r \in \sqrt{(\mathcal{Q} : M)}$).

An ideal $Q$ of $R$ is called a *primary ideal* of $R$ if it is a primary submodule of $R$ when regarded as a submodule of $R$ in the natural way.

Proposition 3.2. *Let $R$ be a commutative ring. Then the following statements hold:*

$(i)$ *The following conditions are equivalent for a proper ideal $Q$ of $R$:*

$(a)$ *$Q$ is a primary ideal of $R$;*

*(b) $ab \in Q$ for some $a, b \in R$ and $a \notin Q$ implies $b^n \in Q$ for some $n \in \mathbb{N}$ (i.e., $b \in \sqrt{Q}$).*

*(c) every zero-divisor in $R/Q$ is nilpotent.*

*(ii) Every prime ideal of $R$ is also a primary ideal of $R$.*

Proof. Note that $(Q : R) = Q$. Now the assertion follows easily from the definitions above. □

Lemma 3.3. *Let $M$ be a nonzero module over a commutative ring $R$, and let $\mathcal{Q}$ be a submodule of $M$. If $\mathcal{Q}$ is a primary submodule of $M$, then $(\mathcal{Q} : M)$ is a primary ideal of $R$.*

Proof. Let $ab \in (\mathcal{Q} : M)$ with $a, b \in R$ and $a \notin (\mathcal{Q} : M)$. Then there exists $m \in M$ such that $am \notin \mathcal{Q}$. Also, we have $b(am) = (ab)m \in \mathcal{Q}$, which implies, by definition, that there exists $n \in \mathbb{N}$ such that $b^n M \subseteq \mathcal{Q}$, that is, $b^n \in (\mathcal{Q} : M)$. This completes the proof. □

Lemma 3.4. *If $Q$ is a primary ideal of a commutative ring $R$, then $P := \sqrt{Q}$, the radical of $Q$, is a prime ideal of $R$. Moreover, $P$ is the only minimal prime ideal of $Q$, that is, every prime ideal of $R$ containing $Q$ must contain $P$.*

Proof. Let $Q$ be a primary ideal of $R$ and let $ab \in \sqrt{Q}$ with $a, b \in R$ and $a \notin \sqrt{Q}$. Then there exists a positive integer $n$ such that $a^n b^n = (ab)^n \in Q$. Since $a \notin \sqrt{Q}$, we have $a^n \notin Q$. It follow that $b^n \in \sqrt{Q}$, and so $b \in \sqrt{Q}$. By Proposition 3.2, this establishes the first part of the lemma.

Now if $P'$ is a prime ideal of $R$ containing $Q$, then $P = \sqrt{P} \supseteq \sqrt{Q} = P$. This completes the proof. □

Remark 3.5. $(i)$ Let $M$ be a nonzero module over a commutative ring $R$ and let $\mathcal{Q}$ be a primary submodule. If we use Lemmas 3.3 and 3.4 together, we conclude that $P := \sqrt{(\mathcal{Q} : M)}$ is a prime ideal of $R$. In this case, we say that $\mathcal{Q}$ is a $P$–primary submodule of $M$. We shall find this way of labeling a primary ideal very useful later.

$(ii)$ As with primary submodules, we can also label primary ideals with their radicals. By Lemma 3.4, the radical $P := \sqrt{Q}$ of a primary ideal $Q$ of $R$ is a prime ideal of $R$, in which case we say that $Q$ is a $P$–primary ideal of $R$. The reader should not be misled into thinking that every ideal with prime radical is primary (see the example below).

Example 3.6. Let $K$ be a field, and let

$$R = K[X_1, X_2, X_3]/(X_1X_3 - X_2^2),$$

where $X_1$, $X_2$, and $X_3$ are indeterminates. For each $i = 1, 2, 3$, let $x_i$ denote the natural image of $X_i$ in $R$. We know from Exercise 1.31 that the ideal $(X_1, X_2)$ of $R[X_1, X_2]$ generated by $X_1$ and $X_2$ is a maximal ideal. Then, by Exercise 1.46, its extension to $K[X_1, X_2][X_3] = K[X_1, X_2, X_3]$ is a prime ideal, and this extension is also generated by $X_1$ and $X_2$ by Exercise 1.30. Now, in $K[X_1, X_2, X_3]$, we have

$$(X_1, X_2) \supseteq (X_1X_3 - X_2^2).$$

This gives that

$$P := (x_1, x_2) = (X_1, X_2)/(X_1X_3 - X_2^2) \in \operatorname{Spec}(R).$$

We show now that $P^2$ is not primary. Note that, by Exercise 1.53, $\sqrt{P^2} = P$. Now $x_1x_3 = x_2^2 \in P^2$. However, we have $x_1 \notin P^2$ and $x_3 \notin P = \sqrt{P^2}$, and so $P^2$ is not primary. The claim that $x_1 \notin P^2$ is proved as follows. If this were not the case, then we should have

$$X_1 = X_1^2 f_1 + X_1X_2f_2 + X_2^2 f_3 + (X_1X_3 - X_2^2)f_4$$

for some $f_i \in K[X_1, X_2, X_3]$ $(i = 1, 2, 3, 4)$. But this is not possible since every term which appears in the right-hand side of the above equation has degree at least 2. Simiarly, if we had $x_3 \in P$, then we should have

$$X_3 = X_1g_1 + X_2g_2 + (X_1X_3 - X_2^2)g_3$$

for some $g_i \in K[X_1, X_2, X_3]$ $(i = 1, 2, 3)$, and we can obtain a contradiction by evaluating $X_1, X_2, X_3$ at $0, 0, X_3$.

This example also shows that every positive power of a prime ideal need not be primary.

Proposition 3.7. *Let $M$ be a nonzero module over a commutative ring $R$, let $\mathcal{Q}$ be a proper submodule of $M$, and let $P$ be a prime ideal of $R$. Then show that $\mathcal{Q}$ is a $P$–primary submodule of $M$ if and only if*

*(i) $P \subseteq \sqrt{(\mathcal{Q} : M)}$, and*

*(ii) whenever $rm \in \mathcal{Q}$ with $r \in R$ and $m \in M \setminus \mathcal{Q}$, then $r \in P$.*

Proof. Straightforward. □

Exercise 3.8. Let $f : M \to M'$ be a homomorphism of nonzero $R$–modules over a commutative ring $R$, and let $P \in \operatorname{Spec}(R)$.

($i$) Prove that if $\mathcal{Q}'$ is a $P$–primary submodule of $M'$ such that $f^{-1}(\mathcal{Q}') \neq M$, then $f^{-1}(\mathcal{Q}')$ is a $P$–primary submodule of $M$.

($ii$) Suppose that $f$ is surjective and that $\mathcal{Q}$ is a submodule of $M$ containing $\ker f$. Then show that $\mathcal{Q}$ is a $P$–primary submodule of $M$ if and only if $f(\mathcal{Q})$ is a $P$–primary submodule of $M'$.

($iii$) Let $N$ be a submodule of $M$, and let $\mathcal{Q}$ be a submodule of $M$ containing $N$. Then show that $\mathcal{Q}$ is a $P$–primary submodule of $M$ if and ony if $\mathcal{Q}/N$ is a $P$–primary submodule of $M/N$.

As an immediate consequence of the above exercise, we may conclude that if $f : R \to R'$ is a ring homomorphism, then for any prime ideal $P'$ of $R'$ and $P'$–primary ideal $Q'$ of $R'$, $Q'^c$ is a $P'^c$–primary ideal of $R$ (where the contraction notation is used in conjunction with $f$); and also that, for ideals $I, Q$ of a commutative ring $R$ such that $I \subseteq Q$, $Q$ is a primary ideal of $R$ if and only if $Q/I$ is a primary ideal of $R/I$.

Exercise 3.9. ($i$)Let $\varphi : R \to R'$ be an epimorphism of commutative rings, let $M$ be a nonzero $R'$–module, and let $\mathcal{Q}$ be an $R'$–submodule of $M$. Then show that $\mathcal{Q}$ is a primary submodule of the $R'$–module $M$ if and only if it is a primary submodule of $M$ as an $R$–module (induced by restriction of scalars). Show also that if $\mathcal{Q}$, considered as $R'$–submodule, is $P'$-primary, then it is $\varphi^{-1}(P')$–primary when considered as an $R$–submodule of $M$.

($ii$) Let $M$ be a module over a commutative ring $R$, and let $I$ be an ideal of $R$ contained in $\operatorname{ann}_R(M)$. Prove that $\mathcal{Q}$ is a $P$–primary submodule of $M$ considered as

$R$–module if and only if $P \supseteq \operatorname{ann}(M)$ and $\mathcal{Q}$ is a $(P/I)$–primary submodule of $M$ considered as $(R/I)$–module.

Proposition 3.10. *Let $\mathcal{Q}$ be a submodule of a nonzero module $M$ over a commutative ring $R$ and let $\sqrt{(\mathcal{Q} : M)} = \mathfrak{M}$ be a maximal ideal of $R$. Then $\mathcal{Q}$ is an $\mathfrak{M}$–primary submodule of $M$.*

*Consequently, $\mathfrak{M}^n M$ is $\mathfrak{M}$–primary for every $n \geq 1$ for which $\mathfrak{M}^n M \neq M$.*

Proof. Since $(\mathcal{Q} : M) \subseteq \sqrt{(\mathcal{Q} : M)} = \mathfrak{M} \subset R$, it is clear that $\mathcal{Q}$ is proper. Let $r \in R$ and $m \in M$be such that $rm \in Q$ but $r \notin \sqrt{(\mathcal{Q} : M)}$. Since $\sqrt{(\mathcal{Q} : M)} = \mathfrak{M}$ is maximal and $r \notin \mathfrak{M}$, we must have $\sqrt{(\mathcal{Q} : M)} + \sqrt{Rr} = R$, so that $(\mathcal{Q} : M) + Rr = R$, by Exercise 1.27 $(iv)$. It follows that

$$Rm = (\mathcal{Q} : M)m + Rrm \subseteq \mathcal{Q}$$

since $rm \in \mathcal{Q}$. This gives that $m \in \mathcal{Q}$, and hence $\mathcal{Q}$ is $\mathfrak{M}$–primary.

The last claim is now immediate because

$$\mathfrak{M} = \sqrt{\mathfrak{M}^n} \subseteq \sqrt{(\mathfrak{M}^n M : M)}$$

for all $n \in \mathbb{N}$ and $\sqrt{(\mathfrak{M}^n M : M)} \neq R$ if $\mathfrak{M}^n M \neq M$. □

Corollary 3.11. *Let $Q$ be an ideal of a commutative ring $R$, and let $\sqrt{Q} = \mathfrak{M}$ be a maximal ideal of $R$. Then $Q$ is an $\mathfrak{M}$–primary ideal of $R$.*

Example 3.12. Let $R$ be a PID which is not a field. Since $0 \in \operatorname{Spec}(R)$, $0$ is a primary ideal of $R$. Also, since for any irreducible element $p$ of $R$, $Rp$ is a maximal ideal and $\sqrt{Rp^n} = \sqrt{(Rp)^n} = Rp$, by Proposition 3.10, $Rp^n$ is a primary ideal of $R$ for all $n \in \mathbb{N}$. On the other hand, a nonzero primary ideal of $R$ must be of the form $Ra$ for some nonzero $a \in R$, and $a$ cannot be a unit since a primary ideal is proper. Since $R$ is a UFD, we may express $a$ as a product of irreducible elements of $R$. If $a$ were divisible by two irreducible elements $p, q \in R$ which are not associates (i.e. $Rp \neq Rq$), then they would be both minimal prime ideals of $Ra$, which contradicts with Lemma 3.4. It follows that $Ra$ is generated by a positive power of some irreducible element of $R$. Therefore, the set of all primary ideals of $R$ is

$$\{0\} \cup \{Rp^n : p \text{ is an irreducible element of } R,\ n \in \mathbb{N}\}.$$

As the following example shows, not every $\mathfrak{M}$–primary ideal, where $\mathfrak{M}$ is a maximal ideal of a commutative ring $R$, has to be a power of $\mathfrak{M}$.

Example 3.13. Let $K$ be a field and let $R$ denote the ring $K[X, Y]$ of polynomials over $K$ in the indeterminates $X, Y$. Let $\mathfrak{M} = RX + RY$, a maximal ideal of $R$. Then, by Proposition 3.10, $(X, Y^2)$ is an $\mathfrak{M}$–primary ideal of $R$ since

$$\mathfrak{M}^2 = (X^2, XY, Y^2) \subseteq (X, Y^2) \subseteq (X, Y) = \mathfrak{M},$$

which implies that

$$\mathfrak{M} = \sqrt{\mathfrak{M}^2} \subseteq \sqrt{(X, Y^2)} \subseteq \sqrt{\mathfrak{M}} = \mathfrak{M},$$

or equivalently

$$\sqrt{(X, Y^2)} = \mathfrak{M}.$$

Furthermore, $(X, Y^2)$ is not a positive power of a prime ideal $P$ of $R$, because, if it were, we should have to have $P = \mathfrak{M}$, and since the powers of $\mathfrak{M}$ form a descending chain

$$\mathfrak{M} \supseteq \mathfrak{M}^2 \supseteq \ldots \supseteq \mathfrak{M}^i \supseteq \mathfrak{M}^{i+1} \supseteq \ldots,$$

we should have to have $(X, Y^2) = \mathfrak{M}$ or $\mathfrak{M}^2$; neither of these is correct because $X \notin \mathfrak{M}^2$,while $Y \notin (X, Y^2)$.

Exercise 3.14. Generalize Proposition 3.10 by showing that for a nonzero module $M$ over a commutative ring $R$ and a submodule $N$ of $M$, if $\sqrt{(N : M)}$ is a maximal ideal of $R$, then $N$ is a primary submodule of $M$.

Although its proof is routine, the following lemma is surprisingly useful when we consider intersections of finite number of primary submodules (that we shall call primary decompositions). So, we omit the proof of the following lemma.

Lemma 3.15. *Let $M$ be a nonzero module over a commutative ring $R$, $P$ a prime ideal of $R$, and $\{\mathcal{Q}_1, \ldots, \mathcal{Q}_n\}$ a set of $P$–primary submodules of $M$. Then the intersection $\mathcal{Q}_1 \cap \ldots \cap \mathcal{Q}_n$ is also a $P$–primary submodule of $M$.*

## 3.2. Primary Decompositions

Now, we can go into details of what we mention at the begining of this chapter, primary decompositions. We shall see that if a submodule (or, in particular, an ideal) is expressed as an intersection of primary submodules (or, primary ideals), then there is a minimal one, in some sense, among all such intersections in which certain terms and prime ideals associated to those terms are uniquely determined. We start with definitions of some required concepts.

Definition 3.16. Let $M$ be a nonzero module over a commutative ring $R$, and let $N$ be a submodule of $M$. A *primary decomposition* of $N$ in $M$ is an expression for $N$ as an intersection of primary submodules of $M$, in which case we say that $N$ *possesses a primary decomposition*, or simply, $N$ is a *decomposable submodule* of $M$. On taking $M = R$, we are led to the notions of *primary decomposition of ideals* and *decomposable ideals.*

A primary decomposition

$$N = \mathcal{Q}_1 \cap \ldots \cap \mathcal{Q}_n \quad \text{with } \sqrt{(\mathcal{Q}_i : M)} = P_i \text{ for all } i = 1, \ldots, n$$

of $N$ (and it is to be understood that $\mathcal{Q}_i$ is $P_i$–primary for all $i = 1, \ldots, n$ whenever we use this type of terminology) is said to be a *minimal primary decomposition* of $N$ if

$(i)$ $P_1, \ldots, P_n$ are distinct prime ideals of $R$, and

$(ii)$ for all $j = 1, \ldots, n$, we have

$$\mathcal{Q}_j \not\supseteq \bigcap_{\substack{i=1\\ i\neq j}}^{n} \mathcal{Q}_i,$$

or equivalently, for all $j = 1, \ldots, n$, we have

$$I \neq \bigcap_{\substack{i=1\\ i\neq j}}^{n} \mathcal{Q}_i$$

(i.e., $\mathcal{Q}_i$ is not redundant for each $i = 1, \ldots, n$ and is needed in the decomposition). If we take $M = R$, then we obtain the definition of minimal primary decomposition of an ideal.

Remark 3.17. Let $N$ be a decomposable submodule of a nonzero module $M$ over a commutative ring $R$, and let

$$N = \mathcal{Q}_1 \cap \ldots \cap \mathcal{Q}_n \quad \text{with } \sqrt{(\mathcal{Q}_i : M)} = P_i \text{ for all } i = 1, \ldots, n$$

be a primary decompostion of $N$.

If for $1 \leq i \neq j \leq n$, $P_i = P_j = P$, then by Lemma 3.15, $\mathcal{Q}_i \cap \mathcal{Q}_j$ is a $P$–primary submodule of $M$. If we delete both $\mathcal{Q}_i$ and $\mathcal{Q}_j$ in the decomposition and write $\mathcal{Q}_i \cap \mathcal{Q}_j$ instead, we obtain a primary decomposition of $N$ of $n-1$ terms. Lemma 3.15 can be applied repeatedly in this way to obtain a primary decomposition of $N$ in which $\sqrt{(\mathcal{Q} : M)}$ for primary terms $\mathcal{Q}$ in the decomposition are all distinct.

We can also refine our primary decomposition by eliminating redundant primary terms inductively. For example if $\mathcal{Q}_1$ is irredundant, that is, if

$$\mathcal{Q}_1 \supseteq \bigcap_{i=2}^{n} \mathcal{Q}_i,$$

then deleting $\mathcal{Q}_1$ does not alter the intersection. Continuing in this way we can eliminate all reduntant terms and obtain a primary decomposition of $N$ in which no primary term is redundant.

It follows that if we start with a primary decomposition of $N$, we can use processes described above and come up with a minimal primary decomposition of $N$. This shows that every decomposable submodule possesses a minimal primary decomposition.

Note also that all above discussions can be adapted for decomposable ideals so that we can conclude that every decomposable ideal has a minimal primary decomposition. More precisely, every primary decomposition of a decomposable ideal can be restricted to a minimal one.

Lemma 3.18. *Let $M$ be a nonzero module over a commutative ring $R$, let $P$ be a prime ideal of $R$, and let $\mathcal{Q}$ be a $P$–primary submodule of $M$. Then the following statements hold for an element $m \in M$.*

*$(i)$ If $m \in \mathcal{Q}$, then $(\mathcal{Q} :_R m) = R$.*

*$(ii)$ If $m \notin \mathcal{Q}$, then $(\mathcal{Q} :_R m)$ is a $P$–primary ideal of $R$.*

Proof. $(i)$ : Obvious.

$(ii)$ : Let $m \notin \mathcal{Q}$. Then, clearly, $(\mathcal{Q} :_R m) \neq R$. We shall first show that $\sqrt{(\mathcal{Q} :_R m)} = P$. To see this let $r \in (\mathcal{Q} :_R m)$. Then $rm \in \mathcal{Q}$. Since $\mathcal{Q}$ is $P$–primary and $m \notin \mathcal{Q}$, we have $r \in P$. Thus $(\mathcal{Q} :_R m) \subseteq P$. Now let $p \in P$. Since $P = \sqrt{(\mathcal{Q} : M)}$, there exists a positive integer $n$ such that $p^n M \subseteq \mathcal{Q}$. It follows that $p^n m \in \mathcal{Q}$, or equivalently, $p \in \sqrt{(\mathcal{Q} :_R m)}$. This establishes the equality $\sqrt{(\mathcal{Q} :_R m)} = P$.

Now let $rs \in (\mathcal{Q} :_R m)$ for some $r, s \in R$ with $s \notin (\mathcal{Q} :_R m)$. Then $r(sm) = (rs)m \in \mathcal{Q}$ where $sm \notin \mathcal{Q}$, and since $\mathcal{Q}$ is a $P$–primary submodule of $M$, we must have $r \in P$. It follows that $(Q :_R m)$ is a $P$–primary ideal of $R$. □

Lemma 3.19. *Let $M$ be a nonzero module over a commutative ring $R$, let $P$ be a prime ideal of $R$, and let $N$ be a decomposable submodule of $M$. Suppose that*

$$N = \mathcal{Q}_1 \cap \ldots \cap \mathcal{Q}_n \quad \textit{with } \sqrt{(\mathcal{Q}_i : M)} = P_i \textit{ for all } i = 1, \ldots, n$$

*is a minimal primary decomposition of $N$ in $M$. Then the following statements are equivalent:*
*(i) $P = P_j$ for some $j = 1, \ldots, n$;*
*(ii) $(N :_R m)$ is a $P$–primary submodule of $M$ for some $m \in M$;*
*(iii) $\sqrt{(N :_R m)} = P$ for some $m \in M$.*

Proof. $(i) \Rightarrow (ii)$ : Let $P = P_i$ for some $i = 1, \ldots, n$. Since the given primary decomposition $N = \bigcap_{i=1}^n \mathcal{Q}_i$ is minimal, we may find an element

$$m_j \in \left( \bigcap_{\substack{i=1 \\ i \neq j}}^{n} \mathcal{Q}_i \right) \setminus \mathcal{Q}_j.$$

Then using Exercise 1.59 $(i)$ together with Lemma 3.18 gives that

$$(N :_R m) = \Big( \bigcap_{i=1}^{n} \mathcal{Q}_i :_R m_j \Big) = \bigcap_{i=1}^{n} (\mathcal{Q}_i :_R m_j) = (\mathcal{Q}_j :_R m_j)$$

is a $P_j$–primary ideal of $R$.

$(ii) \Rightarrow (iii)$ : Straightforward.

$(iii) \Rightarrow (i)$ : Suppose that $\sqrt{(N :_R m)} = P$ for some $m \in M$. By Exercise 1.59, we may write

$$(N :_R m) = \Big( \bigcap_{i=1}^{n} \mathcal{Q}_i :_R m \Big) = \bigcap_{i=1}^{n} (\mathcal{Q}_i :_R m).$$

If $m \in \mathcal{Q}_i$ for all $i = 1, \ldots, n$, then $m \in N$, and so $(N :_R m) = R$, which contradicts with $\sqrt{(N :_R m)} = P$. Then the subset $\{i : m \notin \mathcal{Q}_i\}$ of the set $\{1, \ldots, n\}$ is nonempty. On the other hand, we may write, with the help of Exercise 1.27 and Lemma 3.18,

$$P = \sqrt{(N :_R m)} = \bigcap_{i=1}^{n} \sqrt{(\mathcal{Q}_i :_R m)} = \bigcap_{\substack{i=1 \\ m \notin \mathcal{Q}_i}}^{n} (\mathcal{Q}_i :_R m) = \bigcap_{\substack{i=1 \\ m \notin \mathcal{Q}_i}}^{n} P_i,$$

which implies, by Corollary 1.52, that $P = P_j$ for some $j = 1, \ldots, n$ for which $m \notin \mathcal{Q}_j$. □

Corollary 3.20 (The First Uniqueness Thoerem For Primary Decompositions). *Let $M$ be a nonzero module over a commutative ring $R$, and let $N$ be a decomposable submodule of $M$. Suppose that*

$$N = \mathcal{Q}_1 \cap \ldots \cap \mathcal{Q}_n \quad \textit{with } \sqrt{(\mathcal{Q}_i : M)} = P_i \textit{ for all } i = 1, \ldots, n$$

*and*

$$N = \mathcal{Q}'_1 \cap \ldots \cap \mathcal{Q}'_m \quad \textit{with } \sqrt{(\mathcal{Q}'_i : M)} = P'_i \textit{ for all } i = 1, \ldots, m$$

*are two minimal primary decompositions of $N$ in $M$. Then $n = m$ and $\{P_1, \ldots, P_n\} = \{P'_1, \ldots, P'_n\}$.*

Proof. By Lemma 3.19, if $P \in \{P_1, \ldots, P_n\}$, then $\sqrt{(N :_R m)} = P$ for some $m \in M$. By the same lemma, using the second minimal primary decomposition of $N$, we obtain $P \in \{P'_1, \ldots, P'_m\}$. This gives that $\{P_1, \ldots, P_n\} \subseteq \{P'_1, \ldots, P'_m\}$. Similary, one can see the reverse inclusion, which completes the proof. □

Remark 3.21. Let $R$ be a commutative ring, and let $I$ be a decomposable ideal of $R$ with two minimal pirimary decomposition

$$I = Q_1 \cap \ldots \cap Q_n \quad \text{with } \sqrt{Q_i} = P_i \text{ for all } i = 1, \ldots, n$$

and

$$I = Q'_1 \cap \ldots \cap Q'_m \quad \text{with } \sqrt{Q'_i} = P'_i \text{ for all } i = 1, \ldots, m.$$

Since these are also minimal primary decompositions of $I$ when considered as a submodule of $R$, by The First Uniqueness Theorem, given above, $n = m$ and $\{P_1, \ldots, P_n\} = \{P'_1, \ldots, P'_m\}$. It follows that the number of primary terms as well as prime ideals associated to these primary terms are independent of the choice of the primary decomposition of $I$. This observation leads us to the following definition.

Definition 3.22. Let $R$ be a commutative ring, and let $I$ be a decomposable ideal of $R$ with a minimal primary decomposition

$$I = Q_1 \cap \ldots \cap Q_n \quad \text{with } \sqrt{Q_i} = P_i \text{ for all } i = 1, \ldots, n.$$

Then the set $\{P_1, \ldots, P_n\}$ of prime ideals of $R$ is called the *associated prime ideal*s of $I$ and denoted by $\mathrm{ass}_R(I)$.

Exercise 3.23. Let $f : R \to S$ be a homomorphism of commutative rings, and use the contraction notation in conjunction with $f$. Let $\mathring{I}$ be a decomposable ideal of $S$.

$(i)$ Let

$$\mathring{I} = \mathring{Q}_1 \cap \ldots \cap \mathring{Q}_n \quad \text{with } \sqrt{\mathring{Q}_i} = \mathring{P}_i \text{ for all } i = 1, \ldots, n$$

be a primary decomposition of $\mathring{I}$. Show that

$$\mathring{I}^c = \mathring{Q}_1^c \cap \ldots \cap \mathring{Q}_n^c \quad \text{with } \sqrt{\mathring{Q}_i^c} = \mathring{P}_i^c \text{ for all } i = 1, \ldots, n$$

is a primary decomposition of $\mathring{I}$. Deduce that $\mathring{I}^c$ is a decomposable ideal of $R$ and that

$$\mathrm{ass}_R(\mathring{I}^c) \subseteq \{\mathring{P} : \mathring{P} \in \mathrm{ass}_S(\mathring{I})\}.$$

$(ii)$ Now suppose that $f$ is surjective. Show that if the first primary decomposition in $(i)$ is minimal, then so is the second.

Exercise 3.24. Let $f : R \to S$ be a homomorphism of commutative rings, and use the extension notation in conjunction with $f$. Let $I, Q_1, \ldots, Q_n, P_1, \ldots, P_n$ be ideals of $R$ all of which contain $\ker f$. Show that

$$I = Q_1 \cap \ldots \cap Q_n \quad \text{with } \sqrt{Q_i} = P_i \text{ for all } i = 1, \ldots, n$$

is a primary decomposition of $I$ if and ony if

$$I^e = Q_1^e \cap \ldots \cap Q_n^e \quad \text{with } \sqrt{Q_i^e} = P_i^e \text{ for all } i = 1, \ldots, n$$

is a primary decomposition of $I^e$, and that the first of these primary decompositions is minimal if and only if the second is. Deduce that $I$ is a decomposable ideal of $R$ if and only if $I^e$ is a decomposable ideal of $S$, and when this is the case,

$$\operatorname{ass}_R(I^e) = \{P^e : P \in \operatorname{ass}_R(I)\}.$$

Corollary 3.25. *Let $M$ be a nonzero module over a commutative ring $R$, and let $N$, $L$ be proper submodules of $M$ such that $N \supseteq L$. For a submodule $U$ of $M$ containing $L$, denote the submodule $U/L$ of $M/L$ by $\overline{U}$. Show that*

$$N = \mathcal{Q}_1 \cap \ldots \cap \mathcal{Q}_n \quad \textit{with } \sqrt{(\mathcal{Q}_i : M)} = P_i \textit{ for all } i = 1, \ldots, n$$

*is a primary decomposittion of $N$ in $M$ if and only if Let $M$ be a nonzero module over a commutative ring $R$, and let $N$ be a decomposable submodule of $M$. Suppose that*

$$\overline{N} = \overline{\mathcal{Q}}_1 \cap \ldots \cap \overline{\mathcal{Q}}_n \quad \textit{with } \sqrt{(\overline{\mathcal{Q}}_i : \overline{M})} = P_i \textit{ for all } i = 1, \ldots, n$$

*is a primary decomposition of $N/L$ in $M/L$, and that one of these primary decompositions is minimal if and only if the other is.*

Proposition 3.26. *Let $I$ be an ideal of a commutative ring $R$, and let $P$ be a prime ideal of $R$. Then $P$ is a minimal prime ideal of $I$ (by means of 1.48) if and only if $P \in \operatorname{ass}_R(I)$ and $P$ is minimal in $\operatorname{ass}_R(I)$ with respect to the inclusion relation.*

*In particular, any decompoable ideal has a finite number of minimal prime ideals. Also, if $P_1 \in \operatorname{Spec}(R)$ is such that $P_1 \supseteq I$, then $P_1 \supseteq P_2$ for some $P_2 \in \operatorname{ass}_R(I)$.*

Proof. Let

$$I = Q_1 \cap \ldots \cap Q_n \quad \text{with } \sqrt{Q_i} = P_i \text{ for all } i = 1, \ldots, n$$

be a minimal primary decomposition of $I$. If $P$ is a prime ideal of $R$ such that $P \supseteq I$, then we have

$$P \supseteq \sqrt{I} = \bigcap_{i=1}^{n} \sqrt{Q_i} = \bigcap_{i=1}^{n} P_i,$$

by Lemma 1.27 and Corollary 1.45. This gives, by Lemma 1.51, that $P \supseteq P_j$ for some $j = 1, \ldots, n$. This establishes the last statement of the proposition.

Now, we shall prove the equivalence asserted in the first part of the proposition.

($\Rightarrow$): Let $P$ be a minimal prime ideal of $I$. Then, by above paragraph, there exists $P' \in \operatorname{ass}_R(I)$ such that $P \supseteq P'$. However, since $\operatorname{ass}_R(I) \subseteq \operatorname{Var}(I)$, we must have $P = P'$, which is also the minimal member of $\operatorname{ass}_R(I)$ with respect to the inclusion relation.

($\Leftarrow$): Let $P$ be a minimal element of $\operatorname{ass}_R(I)$ w.r.t. inclusion. Then $P \supseteq I$, and so, by Theorem 1.49, $P \supseteq P'$ for some $P' \in \operatorname{Min}(I)$. On the other hand, by the first paragraph of the proof, there exists $P'' \in \operatorname{ass}_R(I)$ such that $P' \supseteq P''$. But in this case, we have

$$P \supseteq P' \supseteq P'',$$

which implies that $P = P' = P''$ since $P$ is a minimal member of $\operatorname{ass}_R(I)$. It follows that $P = P' \in \operatorname{Min}(I)$.

The proof is complete since $\operatorname{Min}(I) \subseteq \operatorname{ass}_R(I)$ and $\operatorname{ass}_R(I)$ is finite when $I$ is decomposable. □

Definition 3.27. Let $M$ be a nonzero module over a commutative ring $R$, and let $N$ be a decomposable submodule of $M$. Also let

$$N = \mathcal{Q}_1 \cap \ldots \cap \mathcal{Q}_n \quad \text{with } \sqrt{(\mathcal{Q}_i : M)} = P_i \text{ for all } i = 1, \ldots, n$$

be a minimal primary decomposition of $N$ in $M$. Then the minimal members of the subset $\{P_1, \ldots, P_n\}$ of prime ideals of $R$ is said to be the *minimal prime ideals* of $N$ (in $R$). We call non-minimal members of $\{P_1, \ldots, P_n\}$ *embedded prime ideals* of $N$.

Embedded prime ideals of a decomposable ideal can be also defined in a similar fashion by considering the ideal as a submodule of $R$. In the following exercise, we see that the set of embedded prime ideals of a decomposable ideal may empty.

Exercise 3.28. Let $I$ be a decomposable ideal of a commutative ring $R$ with $\sqrt{I} = I$. Show that $I$ has no embedded prime.

Notice that if $I$ is a decomposable ideal of a commutative ring $R$, then the minimal prime ideals of $I$ by means of 1.48 and those defined as in the above definition coincide by Proposition 3.26. This can be generalized as in the following proposition the proof of which is left as an exercise.

Proposition 3.29. *Let $M$ be a nonzero module over a commutative ring $R$, and let $N$ be a decomposable submodule of $M$. Then the set of minimal prime ideals of $(N : M)$ coincides with the set of minimal prime ideals of $N$ (defined as in Definition 3.27).*

Proof. Left to the reader. □

Exercise 3.30. Give a proof to Proposition 3.29.

After The First Uniqueness Theorem for primary decompositions with the motivation from the theory of unique factorization in a PID given at the beginnig of this chapter, it is natural to ask whether primary terms in a minimal primary decomposition of a submodule are determined uniquely or not. The following example show this is not always the case.

Example 3.31. Let $K$ be a field and let $R$ denote the ring $K[X, Y]$ of polynomials over $K$ in two indeterminates $X$ and $Y$. Let's consider the ideals

$$\mathfrak{M} = (X, Y), \quad P = (Y), \quad Q = (X, Y^2), \quad I = (XY, Y^2)$$

of $R$. Then by 1.31, $M$ is a maximal ideal of $R$. Also, if we consider the natural ring homomorphism

$$f : K[X] \longrightarrow K[Y][X]$$

and use the extension notation with reference to this $f$, then by 1.31 and 1.46, we obtain that $P$ is a prime ideal of $R$. On the other hand, we know from Example 3.13, that $(X, Y^2)$ is an $\mathfrak{M}$–primary ideal of $R$ which is not equal to $\mathfrak{M}^2$. We shall show that

$$I = Q \cap P \qquad \text{and} \qquad I = \mathfrak{M}^2 \cap P$$

are two minimal primary decompositions of $I$ which has different $\mathfrak{M}$–primary terms.

It is clear that $I \subseteq P$ and $I \subseteq \mathfrak{M}^2 \subseteq Q$. Then we have

$$I \subseteq \mathfrak{M}^2 \cap P \subseteq Q \cap P.$$

Let $f \in Q \cap P$. Since $f \in P$, we have $f(X,0) = 0$, where $f(X,0)$ denotes the polynomial in $X$ obtained from $f$ by evaluating $X, Y$ at $X, 0$. Since $f \in Q$, we may also write $f = Xg + Y^2h$ for some $g, h \in R$. By evaluating $X, Y$ at $X, 0$, we obtain $0 = Xg(X,0)$, or equivalently $g(X,0) = 0$. This gives that $g = Yg_1$ for some $g_1 \in R$, and so

$$f = Xg + Y^2h = XYg_1 + Y^2h \in I.$$

It follows that

$$I = \mathfrak{M}^2 \cap P = Q \cap P.$$

Finally, since

$$X^2 \in \mathfrak{M}^2 \setminus P, \qquad X^2 \in Q \setminus P, \qquad Y \in P \setminus Q, \qquad Y \in P \setminus \mathfrak{M}^2,$$

we can say that both primary decompositions of $I$ are minimal.

Above example shows that it is not always possible to say that minimal primary decompositions are uniquely determined. Anyways, we can still give a positive result in this direction by restricting our attention to only those primary terms which are associated to minimal prime ideals: these primary terms are independent of the choice of minimal primary decomposition of a fixed decomposable submodule!

Theorem 3.32 (The Second Uniqueness Theorem For Primary Decompositions). *Let $M$ be a nonzero module over a commutative ring $R$, and let $N$ be a decomposable submodule of $M$. Suppose that*

$$N = \mathcal{Q}_1 \cap \ldots \cap \mathcal{Q}_n \quad \textit{with } \sqrt{(\mathcal{Q}_i : M)} = P_i \textit{ for all } i = 1, \ldots, n$$

*and*

$$N = \mathcal{Q}'_1 \cap \ldots \cap \mathcal{Q}'_m \quad \textit{with } \sqrt{(\mathcal{Q}'_i : M)} = P_i \textit{ for all } i = 1, \ldots, n$$

*are two minimal primary decompositions of $N$ in $M$. Then for each $i$ with $1 \le i \le n$ for which $P_i$ is a minimal prime ideal of $N$, we have $Q_i = Q'_i$.*

Proof. The case when $n = 1$ is clear. Thus we assume that $n > 1$. Suppose that $P_j$ is a minimal prime ideal of $N$. If we had

$$\bigcap_{\substack{i=1 \\ i \neq j}}^{n} P_i \subseteq P_j,$$

then there would exist $1 \le i \le n$ with $i \neq j$ such that $P_j \supseteq P_i$, which would contradict with the fact that $P_j$ is a minimal member of the set $\{P_1, \ldots, P_n\}$. Thus there exists

$$a \in \left( \bigcap_{\substack{i=1 \\ i \neq j}}^{n} P_i \right) \setminus P_j.$$

It follows that for each $i$ ($1 \le i \le n$, and $i \neq j$) there exists a positive integer $t_i$ such that $a^{t_i}M \subseteq \mathcal{Q}_i$. Set $t = \max\{t_i : 1 \le i \le n,\, i \neq j\}$. Then for each $i$ with $1 \le i \le n$ and $i \neq j$, $a^tM \subseteq \mathcal{Q}_i$. This gives that $M = (\mathcal{Q}_i :_M a^t)$ for each $i$ with $1 \le i \le n$ and $i \neq j$. On the other hand, if $m \in (\mathcal{Q}_j :_M a^t)$, then $a^tm \in \mathcal{Q}_j$. But since $a \notin P_j$ and $P_j$

is a prime ideal of $R$, we have $a^t \notin P_j$. Since $\mathcal{Q}_j$ is a $P_j$–primary submodule of $M$, we must have $m \in \mathcal{Q}_j$. Thus we have $(\mathcal{Q}_j :_M a^t) = \mathcal{Q}_j$. Finally, using 1.61, we get

$$(N :_M a^t) = \Big( \bigcap_{i=1}^{n} \mathcal{Q}_i :_M a^t \Big) = \bigcap_{i=1}^{n} (\mathcal{Q}_i :_M a^t) = (\mathcal{Q}_j :_M a^t) = \mathcal{Q}_j.$$

In exactly the same way, we can also see that $(N :_M a^t) = \mathcal{Q}'_j$. Therefore, we have $\mathcal{Q}_j = \mathcal{Q}'_j$. □

If we apply the above theorem for a decomposable ideal $I$ of a commutative ring $R$, then we see that the primary terms in any minimal primary decomposition of $I$ that correspond to minimal prime ideals of $I$ remain fixed; they always appear in all minimal primary decompositions.

After uniqueness theorems given above, we shall now focus on the existence of primary decompositions. Unfortunately, not every ideal does necessarily have a primary decomposition, as the following example shows.

Example 3.33. The zero ideal of the commutative ring $\mathcal{C}[0,1]$ of all continuous real valued fucntions on the closed interval $[0,1]$ is not decomposable, i.e. it has no primary decomposition in $\mathcal{C}[0,1]$ at all. Assume that contrary. That is, assume that $0$ has a primary decomposition in $\mathcal{C}[0,1]$. Let $P \in \mathrm{ass}_{\mathcal{C}[0,1]} 0$. By Lemma 3.19, there exists $f \in \mathcal{C}[0,1]$ such that $\sqrt{(0:f)} = P$. Indeed, we have $(0 : f) = P$. We already know that

$$(0 : f) \subseteq \sqrt{(0:f)} = P.$$

Now let $p \in P$. Then $p^n f = 0$ for some $n \in \mathbb{N}$. Assume that $pf \neq 0$. Then we must have $n > 1$. Also we have $pf(a) = p(a)f(a) \neq 0$ for some $a \in [0,1]$. It follows that $p(a) \neq 0$, which implies that $p^{n-1}(a) \neq 0$. However, this is impossible since we also have

$$[p^{n-1}(pf)](a) = 0 \quad \text{and} \quad pf(a) \neq 0.$$

This contradiction yields $pf = 0$, and so $(0 : f) = P$. Since $P \neq R$, $f \neq 0$. It therefore follows that there exists $b \in [0,1]$ such that $f(b) \neq 0$. Choose a real number $\varepsilon$ such that $0 < \varepsilon < |f(b)|$. Since $f$ is continuous, there exists $\delta > 0$ such that $f(x) \in (f(b) - \varepsilon, f(b) + \varepsilon)$ for all $x \in (b - \delta, b + \delta)$, which, in particular, gives that $f(x) \neq 0$ for all $x \in (b - \delta, b + \delta)$. Now define

$$g(x) = \begin{cases} 0 & \text{if } x \leq b \\ x - b & \text{if } x > b \end{cases}$$

and

$$h(x) = \begin{cases} 0 & \text{if } x > b \\ -x + b & \text{if } x \leq b \end{cases}.$$

It is easy to check that $g, h \in \mathcal{C}[0,1]$ with $gh = 0$. Thus $gh \in P$. However, $gf \neq 0$ since $g(x) \neq 0$ for all $x \in (b, b + \delta)$, and $hf \neq 0$ since $h(x) \neq 0$ for all $x \in (b - \delta, b)$. In other words, we have $g \notin (0 : f) = P$ and $h \notin (0 : f) = P$, a contradiction. Therefore $0$ is not decomposable in $\mathcal{C}[0,1]$.

Although we see that there are commutative rings (or modules) containing ideals (or submodules) which are not decomposable, we still have a large supply of commutative rings (or modules) all of whose proper ideals (or proper submodules) are decomposable. To prove this, we first need to introduce the notion of irreducible submodules.

Definition 3.34. Let $M$ be a module over a commutative ring $R$, and let $G$ be a submodule of $M$. We say that $G$ is an *irreducible submodule* of $M$ if

$(i)$ $G \subset M$, and

$(ii)$ whenever $G = G_1 \cap G_2$ for some submodules $G_1$ and $G_2$ of $M$, then $G = G_1$ or $G = G_2$.

Proposition 3.35. *Let $M$ be a Noetherian module over a commutative ring $R$. Then every proper submodule of $M$ can be written as an intersection of finitely many irreducible submodules of $M$.*

Proof. Let $\Omega$ denote the set of all proper submodules of $M$ which cannot be written as intersections of finitely many irreducible submodules of $M$. We shall show that $\Omega = \emptyset$. Assume the contrary. Since $M$ is Noetherian, $\Omega$ contains a maximal member, say $G$. Since we can write $G = G \cap G$, $G$ cannot be irreducible and so there exist submodules $G_1$ and $G_2$ of $M$ such that $G = G_1 \cap G_2$, $G \subset G_1$ and $G \subset G_2$. In this case, both $G_1$ and $G_2$ are proper submodules of $M$ strictly containing $G$. It follows that $G_1, G_2 \notin \Omega$. It follows that $G_1$ and $G_2$ are intersections of finitely many irreducible submodules of $M$. But then $G = G_1 \cap G_2$ inherits the same property, a contradiction. Therefore $\Omega = \emptyset$. □

Proposition 3.36. *Let $M$ be a Noetherian module over a commutative ring $R$, and let $\mathcal{Q}$ be an irreducible submodule of $M$. Then $\mathcal{Q}$ is a primary submodule of $M$.*

Proof. By definition we have $\mathcal{Q} \subset M$. Let $r \in R$ and $m \in M$ be such that $rm \in \mathcal{Q}$. Consider the ascending chain

$$(\mathcal{Q} :_M r) \subseteq (\mathcal{Q} :_M r^2) \subseteq \ldots \subseteq (\mathcal{Q} :_M r^i) \subseteq \ldots$$

of submodules of $M$. Since $M$ is Noetherian, there exists $n \in \mathbb{N}$ such that $(Q :_M r^n) = (\mathcal{Q} :_M r^{n+i})$ for all $i \geq 0$. We shall show that

$$(*) \qquad \mathcal{Q} = (\mathcal{Q} + r^n M) \cap (\mathcal{Q} + Rm).$$

It is enough to show that $(\mathcal{Q}+r^n M) \cap (\mathcal{Q}+Rm) \subseteq G$. Let $q \in (\mathcal{Q}+r^n M) \cap (\mathcal{Q}+Rm)$. Then there exist $r' \in R$, $m' \in M$, and $q', q'' \in \mathcal{Q}$ such that

$$q = q' + r^n m' = q'' + r'm.$$

Since $rq = rq' + r^{n+1}m' = rq'' + rr'm$ and $rm \in \mathcal{Q}$ we have

$$r^{n+1}m' = rq'' + r'(rm) - rq' \in \mathcal{Q}.$$

This gives that $m' \in (\mathcal{Q} :_M r^{n+1}) = (\mathcal{Q} :_M r^n)$. Thus $r^n m' \in \mathcal{Q}$, and hence $q \in \mathcal{Q}$. It follows that the equation $(*)$ holds. Since $\mathcal{Q}$ is irreducible, we have either $\mathcal{Q} = \mathcal{Q}+r^n M$ (or, equivalently $r \in \sqrt{(\mathcal{Q} : M)}$) or $\mathcal{Q} = \mathcal{Q} + Rm$ (or, equivalently $m \in \mathcal{Q}$). This completes the proof. □

Corollary 3.37. *Let $M$ be a Noetherian module over a commutative ring $R$. Then every proper submodule of $M$ is decomposable.*

Proof. Follows directly from Propositions 3.35 and 3.36. □

## 3.3. Associated Prime Ideals of Modules over Noetherian Rings

Lemma 3.38. *Let $I$ be an ideal of a commutative ring $R$. If $\sqrt{I}$ is a finitely generated ideal of $R$, then there exists $n \in \mathbb{N}$ such that $\left(\sqrt{I}\right)^n \subseteq I$.*

Proof. Let $\sqrt{I}$ be generated by $a_1, \ldots, a_k$. Then for each $i = 1, \ldots, k$, there exists $n_i \in \mathbb{N}$ such that $a_i^{n_i} \in I$. Set $n = 1 + \sum_{i=1}^{k}(n_i - 1)$. Now, $\left(\sqrt{I}\right)^n$ is the ideal of $R$ generated by

$$A := \{a_1^{t_1} \ldots a_k^{t_k} : t_1, \ldots, t_k \in \mathbb{N}_0, \sum_{i=1}^{k} t_i = n\}.$$

Notice that if $t_1, \ldots, t_k$ are non-negative integers which sum to $n$, then we must have $t_j \geq n_j$ for some $1 \leq j \leq k$. So,

$$a_1^{t_1} \ldots a_k^{t_k} \in I$$

since $a_j^{t_j} \in I$. This shows that $A \subseteq I$, and hence $\left(\sqrt{I}\right)^n = RA \subseteq I$. □

Proposition 3.39. *Let $I$ be a proper ideal of a commutative Noetherian ring $R$, and let $P \in \operatorname{Spec}(R)$. Then $P \in \operatorname{ass}(I)$ if and only if there exists $\lambda \in R/I$ such that $(0 :_R \lambda) = \operatorname{ann}_R(\lambda) = P$.*

Proof. ($\Leftarrow$) This part easily follows from Lemma 3.19.
($\Rightarrow$) Let

$$I = Q_1 \cap \ldots \cap Q_n \quad \text{with} \quad \sqrt{Q_i} = P_i \text{ for } 1 \leq i \leq n$$

be a minimal primary decomposition of $I$. Let $j$ be a positive integer with $1 \leq j \leq n$, and set

$$I_j = \bigcap_{\substack{i=1 \\ i \neq j}}^{n} Q_i.$$

So, $I \subset I_j \nsubseteq Q_j$ by the minimality of the above primary decomposition. By Lemma 3.38, there exists $t \in \mathbb{N}$ such that $P_j^t \subseteq Q_j$. This gives that

$$P_j^t I_j \subseteq Q_j I_j \subseteq Q_j \cap I_j = I.$$

Let $s$ be the least positive integer $t$ such that $P_j^t I_j \subseteq I$. Thus $P_j^s I_j \subseteq I$ and $P_j^{s-1} I_j \nsubseteq I$ (even if $u = 1$ since $I_j \nsubseteq I$). Then we may choose an element $a \in P_j^{s-1} I_j \setminus I$. Since, at the same time, $a \in I_j \setminus I$, we have $a \notin I_j \setminus Q_j$, and so

$$(I : a) = \left(\bigcap_{i=1}^{n} Q_i : a\right) = \bigcap_{i=1}^{n}(Q_i : a) = (Q_j : a),$$

which is a $P_j$–primary ideal of $R$ by Lemma 3.18 $(ii)$. But, since $aP_j \subseteq P_j^s I_j \subseteq I$, we have

$$P_j \subseteq (I : a) \subseteq P_j,$$

and so $P_j = (I : a)$. If we set $\lambda := a + I \in R/I$, then we obtain that $(0 :_R \lambda) = \operatorname{ann}_R(\lambda) = (I : a) = P_j$. This completes the proof. □

Exercise 3.40. Let $M$ be a Noetherian module over a commutative ring $R$, and let $N$ be a proper submodule of $M$. Suppose that

$$N = \mathcal{Q}_1 \cap \ldots \cap \mathcal{Q}_n \quad \text{with} \quad \sqrt{(\mathcal{Q}_i : M)} = P_i \text{ for } 1 \leq i \leq n$$

is a minimal primary decomposition of $N$ in $M$. Then prove that $P$ is one of $P_1, \ldots, P_n$ if and only if there exists $\lambda \in M/N$ such that $(0 :_R \lambda) = \mathrm{ann}_R(\lambda) = P$.

It should be noted that the conclusion of above exercise apply to a proper submodule $N$ of a finitely generated module $M$ over a commutative Noetherian ring $R$ by Corollary 2.9. Now, 3.39 and 3.40 lead us to define the concept of associated prime ideal of a module over a commutative Noetherian ring.

Definition 3.41. Let $M$ be a module over a commutative Noetherian ring $R$, and let $P \in \mathrm{Spec}(R)$. We call $P$ an associated prime ideal of $M$ if there exists $m \in M$ with $(0 : m) = \mathrm{ann}(m) = P$. The set of associated prime ideals of $M$ is denoted by $\mathrm{Ass}(M)$ (or $\mathrm{Ass}_R(M)$ if we are in need of emphasizing the underliying ring).

Remarks 3.42. $(i)$ Isomorphic modules have the same set of associated prime ideals, i.e., if $M$ and $M'$ are isomorphic modules over a Noetherian ring $R$, then $\mathrm{Ass}_R(M) = \mathrm{Ass}_R(M')$.

$(ii)$ Suppose that $I$ is a proper ideal of a commutative Noetherian ring $R$. Then $I$ is decomposable by Corollary 3.37, and so we can form the finite set $\mathrm{ass}(I)$ of associated prime ideals of $I$. Observe that if $P \in \mathrm{Spec}(R)$, then we have

$$P \in \mathrm{ass}(I) \qquad \Longleftrightarrow \qquad P \in \mathrm{Ass}(R/I).$$

This means that the associated prime ideals of $I$ are precisely the associated prime ideals of the $R$–module $R/I$. Note that when there is a danger of confusing an associated prime ideal $P$ of the $R$–module $I$ (i.e., an element $P \in \mathrm{Ass}_R(I)$) with an element of $\mathrm{ass}(I)$, we shall say that "$P$ is an associated prime ideal of $I$ *as an $R$–module*".

$(iii)$ Let $M$ be a finitely generated module over a commutative Noetherian ring $R$, and let $N$ be a proper submodule of $M$. Again by Corollary 3.37, $N$ is a decomposable submodule of $M$, and so, it has a minimal primary decomposition

$$N = \mathcal{Q}_1 \cap \ldots \cap \mathcal{Q}_n \qquad \text{with } \sqrt{(\mathcal{Q}_i : M)} = P_i \text{ for } 1 \leq i \leq n.$$

Also, by 3.40, we have

$$P \in \{P_1, \ldots, P_n\} \qquad \Longleftrightarrow \qquad P \in \mathrm{Ass}_R(M/N).$$

In particular, we have that $P \in \mathrm{Ass}(M)$ if and only if $P$ is one of the prime ideals which occur in each minimal primary decomposition of the zero submoudule in $M$.

$(iv)$ Notice that we have not assumed that $M$ is a finitely generated module in Definition 3.41, contrary to 3.40. Indeed, as we shall see below, there is an extensive theory of associated prime ideals of *arbitrary modules* over a commutative Noetherian ring.

Exercise 3.43. Let $M$ be a module over a commutative Noetherian ring $R$, and let $P \in \mathrm{Spec}(R)$. Prove that $P \in \mathrm{Ass}(M)$ if and only if $M$ has a submodule isomorphic to $R/P$.

Lemma 3.44. *Let $M$ be a non-zero module over a commutative Noetherian ring $R$. Then each maximal member of the non-empty set*

$$\Omega := \{\operatorname{ann}(m) : m \in M \textit{ and } m \neq 0\}$$

*of ideals of $R$ is prime, and so belongs to* $\operatorname{Ass}(M)$.

Proof. Since $R$ is Noetherian, we have $\Omega \neq \emptyset$. Suppose $P = (0 : m)$, where $m \in M$ and $m \neq 0$, is a maximal member of $\Omega$. Since $m \neq 0$, we have $P \subset R$. Let $a, b \in P$ be such that $ab \in P$ and $b \notin P$. Then $b(am) = (ab)m = 0$. Since $\operatorname{ann}(m) \subseteq \operatorname{ann}(am)$ and $b \in \operatorname{ann}(am) \setminus \operatorname{ann}(m)$, we must have $am = 0$ by maximality of $\operatorname{ann}(m)$. This shows that $P \in \operatorname{Spec}(R)$. □

Corollary 3.45. *Let $M$ be a module over a commutative Noetherian ring $R$. Then* $\operatorname{Ass}(M) \neq \emptyset$ *if and only if $M \neq 0$.*

Proof. This is immediate from definition and the preceding lemma. □

For a module $M$ over a commutative ring $R$, we define the set of elements of $r$ which are annihilated by a non-zero element of $M$ to be the set of zero-divisors of $M$, denoted $\operatorname{Zdv}(M)$ (or, $\operatorname{Zdv}_R(M)$ if it is necessary to indicate the underlying ring concerned). That is,

$$\operatorname{Zdv}(M) = \{r \in R : rm = \text{ for some non-zero } m \in M\}.$$

The following corollory provides a nice description of the set of zero-divisors of a module over a commutative Noetherian ring in terms of its associated prime ideals.

Corollary 3.46. *Let $M$ be a module over a commutative Noetherian ring $R$. Then*

$$\operatorname{Zdv}(M) = \bigcup_{P \in \operatorname{Ass}(M)} P.$$

Proof. Let $P \in \operatorname{Ass}(M)$. Then there exists $m \in M$ with $(0 : m) = P$. Since $m \neq 0$, it is clear that $P$ consists of zero-divisors of $M$.

On the other hand, consider $r \in \operatorname{Zdv}(M)$, so that there exists a non-zero $m' \in M$ such that $rm' = 0$. Hence

$$\Omega' := \{\operatorname{ann}(m) : m \in M,\ m \neq 0 \text{ and } r \in \operatorname{ann}(m)\}$$

is a non-empty subset of the set $\Omega$ of 3.44. Since $R$ is Noetherian, $\Omega'$ will have at least one maximal member, say $P'$, which will also be a maximal member of the set $\Omega$. Then $P' \in \operatorname{Ass}(M)$, and since $r \in P'$, we have proved that $\operatorname{Zdv}(M) \subseteq \bigcup_{P \in \operatorname{Ass}(M)} P$. □

Exercise 3.47. Let $M$ be a module over a commutative Noetherian ring $R$, and let $\mathcal{Q}$ be submodule of $M$.

(*i*) Prove that if $\mathcal{Q}$ is an irreducible submodule of $M$, then

$$|\operatorname{Ass}_R(M/\mathcal{Q})| = 1.$$

(*ii*) Prove that if $\mathcal{Q}$ is a $P$–primary submodule of $M$, then

$$\operatorname{Ass}_R(M/\mathcal{Q}) = \{P\}.$$

CHAPTER 4

# Modules and Rings of Fractions

## 4.1. Modules of Fractions

Let $M$ be a module over a commutative ring $R$, and let $S$ be a multiplicatively closed subset of $R$. Then the relation on $M \times S$ defined by

$$(m_1, s_1) \sim (m_2, s) \iff s(s_2m_1 - s_1m_2) = 0 \text{ for some } s \in S$$

for all $(m_1, s_1), (m_2, s_2) \in M \times S$ can be easily seen to be an equivalence relation. The equivalence class of any $(m, s) \in M \times S$ with respect to the relation $\sim$ is denoted by $m/s$ (or sometimes by $\frac{m}{s}$). Then for $m_1, m_2 \in M$ and $s_1, s_2 \in S$, we have

$$\frac{m_1}{s_1} = \frac{m_2}{s_2} \iff s(s_2m_1 - s_1m_2) = 0 \text{ for some } s \in S.$$

Note that if $0 \in S$ then all the equivalence classes are equal, which yields trivial cases in our purposes; hence we always assume $0 \notin S$.

Note that if $m \in M$ and $s \in S$, then for all $s' \in S$, we have $0 = s'(sm - sm) = s'sm - ss'm$, and so we may write

$$\frac{m}{s} = \frac{s'm}{s's}.$$

Now let $m_1, m_2, m_1', m_2' \in M$ and $s_1, s_2, s_1', s_2' \in S$, and let $m_1/s_1 = m_1'/s_1'$ and $m_2/s_1 = m_2'/s_2'$. Then there exist $s, t \in S$ such that $s(s_1'm_1 - s_1m_1') = 0$ and $t(s_2'm_2 - s_2m_2') = 0$. This gives that

$$\begin{aligned} sts_1's_2'(s_2m_1 + s_1m_2) &= ts_2s_2'(ss_1'm_1) + ss_1s_1'(ts_2'm_2) \\ &= ts_2s_2'(ss_1m_1') + ss_1'(ts_2m_2') \\ &= sts_1s_2(s_2'm_1' + s_1'm_2'). \end{aligned}$$

It follows that

$$\frac{s_2m_1 + s_1m_2}{s_1s_2} = \frac{s_2'm_1' + s_1'm_2'}{s_1's_2'}.$$

This shows that we may define a well–defined addition operation between the equiavalence classes $m_1/s_1$ and $m_2/s_2$ by

$$\frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{s_2m_1 + s_1m_2}{s_1s_2}.$$

Observe that the addition defined as above is commutative and associative. Moreover, the identity of addition is $0/1$; in fact, if $m \in M$ and $s \in S$ are such that $m/s = 0/1$, then there exists $t \in S$ such that $tm = 0$, and vice versa. Also for every $m \in M$, $s \in S$, we may write $-(m/s) = (-m)/s$. If we denote the set of all equivalence classes $m/s$, where $m \in M$ and $s \in S$, by $S^{-1}M$, then $S^{-1}M$ becomes an additive abelian group. On the other hand, if $r \in R$ and $m/s, m'/s' \in S^{-1}M$ are such that $m/s = m'/s'$, then clearly $rm/s = rm'/s'$. It follows that we can define a scaler multiplication of elements of $R$ by

$$r\frac{m}{s} = \frac{rm}{s},$$

which turns the additive abelian group $S^{-1}M$ into an $R$–module. This module structure of $S^{-1}M$ will be called the natural $R$–module structure of $S^{-1}M$.

Let $m, m' \in M$ and $r \in R$. Since

$$\frac{m}{1} + \frac{m'}{1} = \frac{m+m'}{1}$$

and

$$r\frac{m}{1} = \frac{rm}{1},$$

the map

$$\begin{aligned} \chi_M : M &\longrightarrow S^{-1}M \\ m &\longmapsto \frac{m}{1}, \end{aligned}$$

which is called the canonical map from $M$ to $S^{-1}M$, is an $R$–homomorphism. It is easy to see that the kernel of $\chi_M$ is equal to the set

$$\{m \in M : sm = 0 \text{ for some } s \in S\}.$$

## 4.2. Rings of Fractions

Let $R$ be a commutative ring and let $S$ be a multiplicatively closed subset of $R$. By considering $R$ as a module over itself, we can form the $R$–module of fractions of the form $r/s$, where $r \in R$ and $s \in S$, namely $S^{-1}R$. With the following proposition, we make $S^{-1}R$ into a ring as well.

Proposition 4.1. *Let $R$ be a commutative ring, and let $S$ be a multiplicatively closed subset of $R$. Then the additive abelian group $S^{-1}R$ (defined as in the preceding section) is a commutative ring with the multiplication defined by*

$$\frac{a}{s}\frac{b}{t} = \frac{sb}{st}$$

*for all $a, b \in R$ and $s, t \in S$.*

Proof. Let $a_1/s_1 = a_1'/s_1'$ and $a_2/s_2 = a_2/s_2'$ for some $a_1, a_2, a_1', a_2' \in R$ and $s_1, s_1', s_2, s_2' \in S$. Then there exist $s, t \in S$ such that $ss_1'a_1 = ss_1a_1'$ and $ts_2'a_2 = ts_2a_2'$. This gives that $sts_1's_2'a_1a_2 = sts_1s_2a_1'a_2'$, and so

$$\frac{a_1a_2}{s_1s_2} = \frac{a_1'a_2'}{s_1's_2'}.$$

It follows that the multiplication defined in the proposition is well-defined. Since the multiplication of $R$ is commutative and associative, the multiplication of $S^{-1}R$ defined above is also commutative and associative. On the other hand, since

$$\frac{r}{s}\frac{1}{1} = \frac{r}{s}$$

for all $r/s \in S^{-1}R$, $1/1$ is the identity element of $S^{-1}R$. The distribution law is easily seen to hold. This completes the proof. □

Definition 4.2. Let $R$ be a commutative ring, and let $S$ be a multiplicatively closed subset of $R$. Then the ring $S^{-1}R$ in the preceding proposition is said to be the *ring of fractions* of $R$ with respect to (the multiplicatively closed subset) $S$.

Remark 4.3. Let $R$ be a commutative ring, and let $S$ be a multiplicatively closed subset of $R$. Then the following hold:

$(i)$ $0_{S^{-1}R} = 0/1 = 0/s$ for all $s \in S$.

$(ii)$ For $a \in R$ and $s \in S$, $a/s = 0_{S^{-1}R}$ if and only if $t(1a - s0) = 0$ for some $t \in S$ if and only if $ta = 0$ for some $t \in S$.

$(iii)$ $S^{-1}R$ is trivial if and only if $0 \in S$.

$(iv)$ We can alter the denominator of a given element $r/s$ of $S^{-1}R$ by multipliying both numerator and denominator by an element $t$ of $S$, i.e.,

$$\frac{r}{s} = \frac{rt}{st}.$$

This enables us to put any finite number of fractions in $S^{-1}R$ on a common denominator.

$(v)$ If we think of $R$ as a module over itself, then the ring $S^{-1}R$ is an $R$–module, and hence the map

$$\chi : R \longrightarrow S^{-1}R,$$

which was defined in the previous section, is a homomorphism of $R$–modules. Also, since we have

$$\chi(rr') = \frac{rr'}{1} = \frac{r}{1}\frac{r'}{1} = \chi(r)\chi(r')$$

for all $r, r' \in R$, $\chi$ is also a homomorphism of rings. We call this homomorphism the natural homomorphism (from $R$ to $S^{-1}R$). Throughout this chapter, unless stated otherwise, we shall use the notations of extension and contraction with reference to the natural homomorphism $R \to S^{-1}R$.

$(vi)$ The student should not misled by thinking that the natural homomorphism $\chi : R \to S^{-1}R$ is always injective. Indeed,

$$\ker \chi = \{a \in R : ta = 0 \text{ for some } t \in S\},$$

which may not be zero.

$(vii)$ For each element $s \in S$, the element $\chi(s) = s/1$ is a unit of $S^{-1}R$, having inverse $1/s$.

$(vii)$ If $R$ is an integral domain and $S = R \setminus \{0\}$, then the ring $S^{-1}R$ of fractions of $R$ is nothing but the field of fractions of $R$. In this case, the natural homomorphism $\chi : R \to S^{-1}R$ is injective. It follows that we can embed $R$ into its field of fractions as a subring.

$(viii)$ Each element $a/s$ of $S^{-1}R$ (where $a \in R$ and $s \in S$) can be written as $a/s = \chi(a)\chi(s)^{-1}$, since

$$\frac{a}{s} = \frac{a}{1}\frac{1}{s} = \frac{a}{1}\left(\frac{s}{1}\right)^{-1} = \chi(a)\chi(s)^{-1}.$$

Proposition 4.4. *Let $S$ be a multiplicatively closed subset of a commutative ring $R$, and let $\chi : R \to S^{-1}R$ denote the natural ring homomorphism. Let $R'$ be a second commutative ring, and let $f : R \to R'$ be a ring homomorphism with the property* *that $f(s)$ is a unit in $R'$ for all $s \in S$. Then there is a unique ring homomorphism $g : S^{-1}R \to R'$ such that $g \circ \chi = f$, that is, the diagram*

$$\begin{tikzcd}
R \arrow[r, "f"] \arrow[d, "\chi"'] & R' \\
S^{-1}R \arrow[ru, dashed, "g"'] &
\end{tikzcd}$$

*is commutative.*

*In fact, $g$ is such that*

$$g(a/s) = f(a)f(s)^{-1} \quad \textit{for all } a \in R,\ s \in S.$$

Proof. We first show that the function $g : S^{-1}R \to R'$ defined by $g(a/s) = f(a)f(s)^{-1}$ for all $a/s \in S^{-1}R$ is well-defined. Suppose that $a, a' \in R$ and $s, s' \in S$ are such that $a/s = a'/s'$ in $S^{-1}R$. Thus there exists $t \in S$ such that $t(s'a - sa') = 0$. Apply th ring homomorphism $f$ to this equation to get

$$f(t)(f(s')f(a) - f(s)f(a')) = 0.$$

But, by hypothesis, each of $f(t), f(s), f(s')$ is unit in $R'$. The we obtain that

$$g\left(\frac{a}{s}\right) = f(a)f(s)^{-1} = f(a')f(s')^{-1} = g\left(\frac{a'}{s'}\right).$$

It follows that the formula that we use to define $g$ is unambiguous. It is now an easy exercise to check that $g$ is a ring homomorphism. Observe also that $g \circ \chi = f$ since for all $a \in R$, we have $(g \circ \chi)(a) = g(a/1) = f(a)f(1)^{-1} = f(a)$.

It remains to show that $g$ is the only ring homomorphism with the stated propoerties. So suppose that $g' : S^{-1}R \to R'$ is a ring homomorphism such that $g' \circ \chi = f$. Then for all $a \in R$, we have $g'(a/1) = f(a)$. In particular, for $s \in S$, we have $g'(s/1) = f(s)$. Since $f(s)$ is unit in $R'$, we may write $g'(1/s) = f(s)^{-1}$. It follows that for all $a \in R$, $s \in S$, we must have

$$g'\left(\frac{a}{s}\right) = g'\left(\frac{a}{1}\frac{1}{s}\right) = g'\left(\frac{a}{1}\right)g'\left(\frac{1}{s}\right) = f(a)f(s)^{-1} = g\left(\frac{a}{s}\right),$$

so that there is exactly one ring homomorphism $g$ with the desired properties. □

Exercise 4.5. Let $S$ and $T$ be multiplicatively closed subsets of a commutative ring $R$ such that $S \subseteq T$. Show that there is a ring homomorphism $h : S^{-1}R \to T^{-1}R$ for which $h(a/s) = a/s \in T^{-1}R$ for all $a \in R$ and $s \in S$. Show further that $h$ is an isomorphism if and only if one of the following equivalent conditions hold:

($i$) For each $t \in T$, the element $t/1 \in S^{-1}R$ is a unit of $S^{-1}R$.

($ii$) For each $t \in T$, there exists $a \in R$ such that $st \in S$.

($iii$) Whenever $P \in \mathrm{Spec}(R)$ is such that $P \cap S = \emptyset$, then $P \cap T = \emptyset$ too.

Let $R$ be an integral domain, and let $S$ be a multiplicatively closed subset of $R$ such that $0 \notin S$. Let $K$ denote the field of fractions of $R$ . Then, as we remarked, $K = T^{-1}R$ where $T = R \setminus \{0\}$. Since $S \subseteq T$, by above exercise, we can define a ring homomorphism $h : S^{-1}R \to K$ for which $h(a/s) = a/s$ for all $a \in R$, $s \in S$. It is easy to see that $h$ is injective. So, every ring of fractions $S^{-1}R$ of $R$, where $S$ is a multiplicatively closed subset of $R$, can be embedded into the field of fractions of $R$. Note that there are two uses of the formal symbol $a/s$ here, one to denote an element of

$S^{-1}R$ and the other to denote an element of $K$: the objects concerned are formed using different equivalence relations and should not be confused. However, we can identify elements of $S^{-1}R$ as their images in $K$ and write $S^{-1}R \subseteq K$.

Let $S$ be a multiplicatively closed subset of a commutative ring $R$. From Remark 4.3, we see that the natural ring homomorphism $\chi : R \to S^{-1}R$ has the following properties:

$(i)$ $\chi(s)$ is a unit in $S^{-1}R$ for all $s \in S$,

$(ii)$ if $a \in \ker\chi$, then there exists $s \in S$ such that $sa = 0$, and

$(iii)$ each element of $S^{-1}R$ can be written in the form $\chi(a)\chi(s)^{-1}$ for some $a \in R$ and $s \in S$.

With the following proposition, we deduce that these properties uniquely determine $S^{-1}R$, up to isomorphism, as an $R$–algebra (with the structural ring homomorphism $\chi$).

Proposition 4.6. *Let $S$ be a multiplicatively closed subset of a commutative ring $R$. Suppose that $R'$ is a commutative $R$–algebra with structural ring homomorphism $f : R \to R'$, and assume that*

*$(i)$ $f(s)$ is a unit of $R'$ for all $s \in S$;*

*$(ii)$ if $a \in \ker f$, then there exists $s \in S$ such that $sa = 0$;*

*$(iii)$ each element of $R'$ can be written in the form $f(a)f(s)^{-1}$ for some $a \in R$ and $s \in S$.*

*Then there exists a unique isomorphism of $R$–algebras $g : S^{-1}R \to R'$; in other words, there is a unique ring isomorphism $g : S^{-1}R \to R'$ such that $g \circ \chi = f$.*

Proof. By Proposition 4.4, there is a unique ring homomorphism $g : S^{-1}R \to R'$ such that $g \circ \chi = f$, and, moreover, $g$ is given by

$$g\left(\frac{a}{s}\right) = f(a)f(s)^{-1} \qquad \text{for all } a \in R,\ s \in S.$$

Therefore, it remains only to show that $g$ is bijective.

It is clear from condition $(iii)$ of the hypotheses that $g$ is surjective. Suppose that $a \in R$, $s \in S$ are such that $a/s \in \ker g$. Then $f(a)f(s)^{-1} = 0$, so that $f(a) = 0$ and $a \in \ker f$. Hence by condition $(ii)$ of the hypotheses, there exists $t \in S$ such that $ta = 0$,so that $a/s = 0$ in $s^{-1}R$. Hence $g$ is injective too. □

Examples 4.7. Let $R$ be a commutative ring.

$(i)$ For a fixed $t \in R$, the set $S := \{t^n : n \in \mathbb{N}_0\}$ is a multiplicatively closed subset of $R$. In this case the ring of fractions $S^{-1}R$ is often denoted by $R_t$. Note that $R_t$ is trivial if and only if $0 \in S$, that is, if and only if $t$ is nilpotent.

$(ii)$ Let $J$ be an ideal of $R$. Then the set $1+J = \{1+c : c \in J\}$ is a multiplicattively closed subset of $R$. Now, $(1+J)^{-1}R$ is trivial if and only if $0 \in 1+J$, and it is easy to see that this occurs if and only if $J = R$.

$(iii)$ One of the most important examples of a ring of fractions of a commutative ring $R$ is given when the multiplicatively closed subset is taken to be $R \setminus P$ for some prime ideal $P$ of $R$. We denote the ring $S^{-1}R$, where $S = R \setminus P$, by $R_P$, and call it the *localization* of $R$ at $P$. The reason why we call this ring the localization is best understood by the following lemma: $R_P$ is a quasi-local ring.

Lemma 4.8. *Let $R$ be a commutative ring and let $P \in \operatorname{Spec}(R)$. Then the ring $R_P$ (the localization of $R$ at $P$) is a quasi-local ring with the unique maximal ideal*

$$\{\alpha \in R_P : \alpha = \frac{r}{s} \textit{ for some } r \in P,\ s \in R \setminus P\}.$$

Proof. Let

$$I = \{\alpha \in R_P : \alpha = \frac{r}{s} \text{ for some } r \in P,\ s \in R \setminus P\}.$$

By Theorem 1.34, it is enough to show that $I$ is an ideal of $R$ and it is the set of all non-units of $R$. It is easy to see that $I$ is an ideal of $R_P$ since it is, in fact, the extension of $P$ to $R_P$ (under the natural homomorphism, as we shall always assume for extension and contraction notation in this chapter). Let $\alpha \in R_P \setminus I$. Then $\alpha = a/s$ for some $a \in R$ and $s \in S$. We must have $a \notin P$, so that $\alpha$ is a unit of $R_P$. On the other hand, if $\beta$ is a unit of $R_P$, and $\beta = b/t$ for some $b \in R$, $t \in S$, then there exist $c \in R$, $v \in S$ such that

$$\frac{b}{t}\frac{c}{v} = \frac{1}{1}$$

in $R_P$. Therefore, there exits $w \in S$ such that $w(bc - tv) = 0$,so that $wbc = wtv \in R \setminus P$. Hence $b \notin P$, and since this applies to every representation $\beta = b/t$, with $b \in R$, $t \in S$, of $\alpha$ as a formal fraction, it follows that $\alpha \notin I$.

We have now proved that the ideal $I$ of $R_P$ is equal to the set of non-units of $R_P$, and so the proof is complete. □

Example 4.9. Let $p$ be a prime number. Then $p\mathbb{Z} \in \operatorname{Spec}(\mathbb{Z})$, and the localization $\mathbb{Z}_{p\mathbb{Z}}$ can be identified with

$$\{\lambda \in \mathbb{Q} : \lambda = \frac{m}{n} \text{ for some } m, n \in \mathbb{Z} \text{ with } n \neq 0 \text{ and } p \nmid n\}.$$

Exercise 4.10. Let $K$ be a field and let $a_1, \dots, a_n \in K$. Let $F$ denote the field of fractions of the domain $K[X_1, \dots, X_n]$, where $X_1, \dots, X_n$ are indeterminates. Show that

$$R = \{\gamma \in F : \gamma = \frac{f}{g} \text{ with } f, g \in K[X_1, \dots, X_n] \text{ and } g(a_1, \dots, a_n) \neq 0\}$$

is a subring of $F$ which is isomorphic to a ring of fractions of $K[X_1, \dots, X_n]$. Is $R$ quasi-local? If so, what can you say about its residue field? Justify your responses.

## 4.3. Modules of Fractions (continued)

Now let $M$ be module over a commutative ring $R$, and let $S$ be a multiplicatively closed subset of $R$. In Section 4.1, we defined $S^{-1}M$ to be the set of formal fractions of the form $m/s$ with $m \in M$ and $s \in S$, and made it an $R$–module. In fact, $S^{-1}M$ can be made into an $S^{-1}R$–module by extending scalars from $R$ to $S^{-1}R$ as follows: Let $r/s \in S^{-1}R$ ($r \in R$, $s \in S$) and $m/t \in S^{-1}M$ ($m \in M$, $t \in S$). Define the scalar multiplication by

$$\frac{r}{s} \cdot \frac{m}{t} = \frac{rm}{st}.$$

It is an easy matter to check that this is an unambiguous operation satisfying all necessary conditions to make $S^{-1}M$ an $S^{-1}R$–module. Notice that the $R$–module structure of $S^{-1}M$ defined earlier can now be obtained by restriction of scalar from $S^{-1}R$ to $R$ via the natural ring homomorphism $R \to S^{-1}R$.

Let $f : M' \to M$ be a homomorphism of modules over a commutative ring $R$, and let $S$ be a multiplicatively closed subset of $R$. Then $f$ induces a map

$$\begin{aligned} S^{-1}f : S^{-1}M' &\longrightarrow S^{-1}M \\ \frac{m'}{s} &\longmapsto \frac{f(m')}{s}. \end{aligned}$$

Also, the diagram

$$\begin{tikzcd} M' \arrow[r, "f"] \arrow[d, "\chi_M"'] & M \arrow[d, "\chi_{M'}"] \\ S^{-1}M' \arrow[r, "S^{-1}f"'] & S^{-1}M \end{tikzcd}$$

is commutative.

Theorem 4.11. *Let $S$ be a multiplicatively closed subset of a commutative ring $R$, and let $f, g : M' \longrightarrow M$, $h : M \longrightarrow M''$ be homomorphisms of $R$–modules. Then*

*(i) if $i : M \to M$ is the identity map on $M$, then $S^{-1}i : S^{-1}M \to S^{-1}M$ is the identity map on $S^{-1}M$,*

*(ii) if $z : M' \to M$ denotes the zero homomorphism, then $S^{-1}z$ is the zero homomorphism from $S^{-1}M'$ into $S^{-1}M$,*

*(iii) $S^{-1}(hf) = (S^{-1}h)(S^{-1}f)$,*

*(iv) $S^{-1}(f + g) = S^{-1}f + S^{-1}g$, and*

*(v) if $f$ is an isomorphism of $R$–modules, then $S^{-1}f$ is an isomorphism of $S^{-1}R$–modules.*

Proof. Immediate. □

For the reader who are familiar with "Homological Algebra", we remark that the preceding theorem just means that passing to fractions module with respect to a fixed multiplicatively closed subset $S$ defines an additive (covariant) functor from the category of $R$–modules to the category of $S^{-1}R$–modules.

Theorem 4.12. *Let $R$ be a commutative ring, and let $S$ be a multiplicatively closed subset of $R$. Suppose that we have a short exact sequence*

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r, "f"] & M \arrow[r, "g"] & M'' \arrow[r] & 0 \end{tikzcd}$$

*of $R$–modules and $R$–homomorphisms. Then*

$$\begin{tikzcd} 0 \arrow[r] & S^{-1}M' \arrow[r, "S^{-1}f"] & S^{-1}M \arrow[r, "S^{-1}g"] & S^{-1}M'' \arrow[r] & 0 \end{tikzcd}$$

*is a short exact sequence of $S^{-1}R$–modules and $S^{-1}R$–homomorphisms.*

Proof. It follows, from definition, that $S^{-1}g$ is surjective.

Suppose that $S^{-1}f(m'/s) = 0$ for some $m' \in M'$ and $s \in S$. Then $f(m')/s = 0$ in $S^{-1}M$, and so $tf(m') = 0$ for some $t \in S$. Since $f$ is injective, we have $tm' = 0$. This gives that $m'/s = 0_{S^{-1}M'}$, so that $S^{-1}f$ is injective.

Now we shall show that $\operatorname{Im} S^{-1}f = \ker S^{-1}g$. Since $(S^{-1}g)(S^{-1}f) = S^{-1}(gf) = S^{-1}0 = 0$, we have $\operatorname{Im} S^{-1}g \subseteq \ker S^{-1}f$. On the other hand, if $m/s \in \ker S^{-1}g$, then $g(m)/s = 0$, and so $s'g(m) = 0$ for some $s' \in S$. Then $s'm \in \ker g = \operatorname{Im} f$. It follows that $s'm = f(m')$ for some $m' \in M'$. Thus

$$= \frac{m}{s} = \frac{s'm}{s's} = \frac{f(m')}{s's} = S^{-1}f\left(\frac{m'}{ss'}\right) \in \operatorname{Im} S^{-1}f,$$

which completes the proof since then we get $\ker S^{-1}g \subseteq \operatorname{Im} S^{-1}f$. □

# Bibliography

[1] J. Avigad, Dedekind's 1871 version of the theory of ideals 1

[2] M. F. Atiyah and I. G. Macdonald, Introduction to commutative algebra. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969.

[3] J. A. Beachy, Introductory Lectures on Rings and Modules – Class Notesi, http://www.math.niu.edu/~beachy/rings_modules/notes.html. 1, 2, 3

[4] I. Kaplansky, Commutative rings. Allyn and Bacon, Inc., Boston, Mass. 1970.

[5] J. J. O'Connor and E. F Robertson, The development of Ring Theory, http://www-history.mcs.st-and.ac.uk/HistTopics/Ring_theory.html 2, 45

[6] R. Y. Sharp, Steps in commutative algebra. Second edition. London Mathematical Society Student Texts, 51. Cambridge University Press, Cambridge, 2000.

# Index