

# Topics in Ring Theory

Jacob Barshay



# Contents

<b>1</b>	<b>PRELIMINARY TERMINOLOGY AND EXAMPLES</b>	<b>3</b>
<b>2</b>	<b>IDEALS AND RESIDUE RINGS</b>	<b>9</b>
<b>3</b>	<b>RINGS OF QUOTIENTS AND LOCALIZATION</b>	<b>15</b>
<b>4</b>	<b>UNIQUE FACTORIZATION DOMAINS</b>	<b>21</b>
<b>5</b>	<b>MODULES AND EXACT SEQUENCES</b>	<b>29</b>
<b>6</b>	<b>NOETHERIAN RINGS AND MODULES</b>	<b>31</b>
<b>7</b>	<b>DEDEKIND DOMAINS</b>	<b>33</b>
<b>8</b>	<b>ARTIN RINGS AND MODULES</b>	<b>35</b>
<b>9</b>	<b>SEMISIMPLE RINGS</b>	<b>37</b>



# Preface

This book is an outgrowth of a one-quarter, first-year graduate course that I taught at Northeastern University in 1966 and 1967. The lectures were based in turn on an algebra course given by Dock Sang Rim at Brandeis University in 1961–62. The book is a self-contained, general, and modern treatment of some classical theorems of commutative and noncommutative ring theory. Principally these theorems are the primary decomposition of ideals in commutative Noetherian rings and the Artin-Wedderburn structure theory for semisimple rings. By “general” and “modern” I mean that, as much as possible, theorems are proved for modules over the rings being considered and then specialized to obtain classical statements. Furthermore the techniques employed are among those which have proved fruitful in modern ring theory, for example, localization. In some sense, localization is the unifying idea in the commutative ring theory covered here.

The book begins with material usually treated in an undergraduate modern algebra course, namely, various kinds of ideals and operations on ideals, isomorphism theorems and the Chinese Remainder Theorem (Chapter 2), and Euclidean, principal ideal, and unique factorization domains (Chapter 4). However, proofs of standard theorems on unique factorization domains are not those generally given in such courses since they rely heavily on the notion of rings of quotients developed in Chapter 3. Chapter 5, an introduction to homological notions, is devoted to modules and exact sequences including the splitting of exact sequences and characterization of free and projective modules. Noetherian rings and modules are treated in Chapter 6. Since the motivation for this study is the search for a class of rings in which every ideal is a unique product of prime ideals, we are naturally led to Dedekind domain in Chapter 7. Chapter 8 and 9 are devoted to noncommutative Artin rings, including the connection between the two chain condition by way of the ideal of Jordan-Hölder series, and the structure of semisimple rings. Thus Chapters 7 and 9 can be viewed as deeper investigations of special classes of those rings studied in Chapter 6 and 8, respectively. Each chapter concludes with a set of exercises of varying degrees of difficulty.

Since the book has been expanded from the original one-quarter course of lecture, it now appears to be the appropriate amount of material for a one-semester course. Although primarily designed for beginning graduate students, it should be accessible to undergraduates who have taken the modern algebra

and linear algebra courses usually offered to sophomores or juniors. For the graduate student it should provide a convenient place to learn the ring theory often expected on qualifying examinations. For the undergraduate, particularly one who is interested in algebra, the book should offer some insight into one direction his future studies might take him.

I would like to thank Professor Rim and the various authors from whom I have borrowed ideas. Their works are included in the bibliography. I would further like to acknowledge the helpful suggestions of Mark Bridger, Burton Fein, Marvin Freedman, and Kenneth Ireland. Finally, I am grateful to Delphine Radcliffe and Cindy Feldman for typing the manuscript.

JACOB BARSHAY

Cambridge, Massachusetts  
July 1969

# Chapter 1

## PRELIMINARY TERMINOLOGY AND EXAMPLES

We begin with a brief discussion of just two notions from set theory. The first is that of an equivalence relation on a set and its associated decomposition ; the second is Zorn's lemma. The notation used here for set membership, set inclusion, union and intersection of sets, and so forth, is standard.

**Definition 1-1.** A binary relation  $\sim$  on a set  $A$  is called an *equivalence relation* if for any element  $a, b, c \in A$

- (1)  $a \sim a$  ( $\sim$  is reflexive) ;
- (2) if  $a \sim b$ , then  $b \sim a$  ( $\sim$  is symmetric) ;
- (3) if  $a \sim b$  and  $b \sim c$ , then  $a \sim c$  ( $\sim$  is transitive).

**Definition 1-2.** If  $A$  is a set,  $\sim$  is an equivalence relation on  $A$ , and  $a \in A$ , then the *equivalence class of  $a$*  is equal to  $\{x \in A | a \sim x\}$  and is denoted by  $\bar{a}$ .

In particular, observe that the equivalence class of an element of  $A$  is a subset of  $A$ . To say that two equivalence class are distinct is to say that they are not equal as sets.

**Theorem 1-1.** The distinct equivalence classes of an equivalence relation  $\sim$  on a set  $A$  provide a decomposition of  $A$  as a union of mutually disjoint subsets.

*Proof.* Since  $a \sim a$ , we have  $a \in \bar{a}$  for any  $a \in A$ . Thus  $A \subseteq \bigcup_{a \in A} \bar{a}$ . On the other hand, each  $\bar{a}$  is a subset of  $A$  so  $\bigcup_{a \in A} \bar{a} \subseteq A$  whence  $A = \bigcup_{a \in A} \bar{a}$ . To complete the proof it suffices to show that distinct equivalence classes are mutually disjoint, that is, if  $a, b \in A$  then either  $\bar{a} = \bar{b}$  or  $\bar{a} \cap \bar{b} = \emptyset$ . Suppose

then that  $\bar{a} \cap \bar{b} \neq \emptyset$  and let  $x \in \bar{a} \cap \bar{b}$ . Thus  $a \sim x$  and  $b \sim x$ . But by Definition 1-1(2),  $x \sim b$  and by (3)  $a \sim b$ . Now if  $y \in \bar{b}$ , then  $b \sim y$  so again by (3)  $a \sim y$  whence  $y \in \bar{a}$ . We conclude that  $\bar{b} \subseteq \bar{a}$ . By a similar argument, we could show  $\bar{a} \subseteq \bar{b}$ . Therefore  $\bar{a} = \bar{b}$ .  $\square$

**Definition 1-3.** A binary relation  $\leq$  on a set  $A$  is called a *partial ordering* if for any  $a, b, c \in A$

- (1)  $a \leq a$  ;
- (2) if  $a \leq b$  and  $b \leq c$ , then  $a \leq c$  ;
- (3) if  $a \leq b$  and  $b \leq a$ , then  $a = b$ .

$A$  together with the partial ordering  $\leq$  is called a *partially ordered set*.

**Definition 1-4.** A subset  $B$  of a partially ordered set  $A$  is said to be totally ordered if for any  $a, b \in B$  either  $a \leq b$  or  $b \leq a$ . A *totally ordered* subset will also be referred to as a *chain*.

**Definition 1-5.** An element  $a$  in a partially ordered set  $A$  is called an *upper bound* for a subset  $B$  of  $A$  if for any  $b \in B$ ,  $b \leq a$ .

**Definition 1-6.** A partially ordered set  $A$  is called *inductive* if any chain in  $A$  has an upper bound in  $A$ .

**Definition 1-7.** An element  $m$  in a partially ordered set  $A$  is called a *maximal element* if for any  $a \in A$ ,  $m \leq a$  implies  $a = m$ .

**Zorn's Lemma.** Every nonempty, inductive set has a maximal element.

**Definition 1-8.** Let  $f : A \rightarrow B$  be a mapping (map, function) from a set  $A$  to a set  $B$ . Then  $f$  is said to be

- (1) *surjective* (onto) if for any element  $b \in B$  there exists an element  $a \in A$  such that  $f(a) = b$ .
- (2) *injective* (one-to-one) if for any elements  $a_1, a_2 \in A$ ,  $f(a_1) = f(a_2)$  implies  $a_1 = a_2$ . [Equivalently,  $a_1 \neq a_2$  implies  $f(a_1) \neq f(a_2)$ .]
- (3) *bijective* (a one-to-one correspondence) if it is both surjective and injective.

**Definition 1-9.** A *group* is a nonempty set  $G$  on which is defined a binary operation  $*$  satisfying the following conditions :

- (1) If  $a, b \in G$ , then  $a * b \in G$ . (Closure Law) ;
- (2) If  $a, b \in G$ , then  $(a * b) * c = a * (b * c)$ . (Associative Law) ;

- (3) There exists an element  $e \in G$  such that for any  $a \in G$ ,  $e * a = a * e = a$ .  $e$  is called the *identity element* of  $G$ .
- (4) For any  $a \in G$ , there exists an element  $\bar{a} \in G$  such that  $a * \bar{a} = \bar{a} * a = e$ .  $\bar{a}$  is called the *inverse of  $a$* .

The identity element of a group is unique as is the inverse of a given element.

**Definition 1-10.** A group is said to be *Abelian* if it satisfies the additional condition:

- (5) For any  $a, b \in G$ ,  $a * b = b * a$ .

**Definition 1-11.** If  $(G, *)$  and  $(H, \circ)$  are groups and  $f : G \rightarrow H$ , then  $f$  is called a *group homomorphism* if for any  $a, b \in G$ ,  $f(a * b) = f(a) \circ f(b)$ .

**Definition 1-12.** A *ring* is a set  $\Lambda$  on which are defined two binary operations  $+$  and  $\cdot$  satisfying the following conditions :

- (1)  $\Lambda$  is an Abelian group under  $+$  ;
- (2) if  $a, b \in \Lambda$ , then  $a \cdot b \in \Lambda$  (Closure Law) ;
- (3) if  $a, b, c \in \Lambda$ , then  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$  (Associative Law) ;
- (4) if  $a, b, c \in \Lambda$ , then  $a \cdot (b + c) = a \cdot b + a \cdot c$  and  $(a + b) \cdot c = a \cdot c + b \cdot c$ . (Distribution Laws).

There are other properties that a ring may or may not possess, among which are the following :

- (5) there exists an element  $1 \in \Lambda$  such that for any element  $a \in \Lambda$ ,  $1 \cdot a = a \cdot 1 = a$ .  $1$  is called the *unit element* of  $\Lambda$  ;
- (6) for any element  $0 \neq a \in \Lambda$ , there exists an element  $a^{-1} \in \Lambda$  such that  $a \cdot a^{-1} = a^{-1} \cdot a = 1$ .
- (7) for any  $a, b \in \Lambda$ ,  $a \cdot b = b \cdot a$ .

In a ring, the identity element for the operation  $+$  is denoted by  $0$  and the inverse of  $a$  is denoted by  $-a$ . The multiplication symbol  $\cdot$  is generally omitted.

**Definition 1-13.**

- (a) (7) is called a *commutative ring* ;
- (b) (5) is called a *ring with unit* ;
- (c) (5) and (6) is called a *division ring* ;
- (d) (5) and (7) is called a *commutative ring with unit* ;

(e) (5), (6) and (7) is called a *field*.

**Definition 1-14.** If  $(\Lambda, +, \cdot)$  and  $(\Lambda', *, \circ)$  are rings and  $f : \Lambda \rightarrow \Lambda'$ , then  $f$  is called a *ring homomorphism* if for any  $a, b \in \Lambda$ ,  $f(a + b) = f(a) * f(b)$  and  $f(a \cdot b) = f(a) \circ f(b)$ .

**Definition 1-15.** If  $\Lambda$  and  $\Lambda'$  have units 1 and  $1'$  and  $f : \Lambda \rightarrow \Lambda'$ , then  $f$  is said to be *unitary* if  $f(1) = 1'$ .

**Definition 1-16.** A group or ring homomorphism is called an

- (1) *epimorphism* if it is surjective ;
- (2) *monomorphism* if it is injective ;
- (3) *isomorphism* if it is bijective.

**Examples.**

1.  $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ , the set of integers with  $+$  and  $\cdot$  having the usual meaning is a commutative ring with unit element.
2.  $\mathbb{Q}$ , the set of rational numbers,  $\mathbb{R}$ , the set of real numbers, and  $\mathbb{C}$ , the set of complex numbers, under the usual rules of addition and multiplication are all examples of fields.
3. Let  $k$  be any field. Then  $k[X]$ , the set of polynomials in one variable with coefficient in  $k$ , under the usual rules for addition and multiplication of polynomials forms a commutative ring with unit. Similarly for  $k[X_1, \dots, X_n]$ , the set of polynomials in  $n$  variables with coefficients in  $k$ .
4.  $\mathbb{Z}_m$ , the set of integers modulo  $m$  where  $+$  and  $\cdot$  mean addition and multiplication modulo  $m$ , forms a commutative ring with unit element. Furthermore  $\mathbb{Z}_m$  is a field if and only if  $m$  is a prime number.
5.  $M_n(k)$ , the set of all  $n \times n$  matrices with entries in a field  $k$ , under the usual rules for addition and multiplication of matrices, forms a ring with unit element, which is not commutative if  $n \geq 2$ .
6.  $2\mathbb{Z} = \{0, \pm 2, \pm 4, \dots\}$ , the set of even integers, forms a commutative ring but has no unit element.
7.  $\Delta$ , the real quaternions.

$$\Delta = \{x = x_0 + x_1i + x_2j + x_3k \mid x_0, x_1, x_2, x_3 \in \mathbb{R}\}$$

If  $x = x_0 + x_1i + x_2j + x_3k$  and  $y = y_0 + y_1i + y_2j + y_3k$  are in  $\Delta$ , then  $x + y = (x_0 + y_0) + (x_1 + y_1)i + (x_2 + y_2)j + (x_3 + y_3)k$ . The product  $xy$  is found by using the distributive laws and the rules  $ii = jj = kk = -1$ ,

$ij = -ji = k$ ,  $jk = -kj = i$ , and  $ki = -ik = j$ . Then  $\Delta$  forms a division ring under these operations. In particular, the multiplicative inverse of  $x = x_0 + x_1i + x_2j + x_3k$  is

$$x^{-1} = \frac{x_0}{|x|} - \frac{x_1}{|x|}i - \frac{x_2}{|x|}j - \frac{x_3}{|x|}k$$

where  $|x| = x_0^2 + x_1^2 + x_2^2 + x_3^2$ .

### Exercise.

**1-1.** Show that each of the following is an equivalence relation.

- (a) In the set of integers,  $m \sim n$  if and only if  $m - n$  is even.
- (b) In the set of polynomials with real coefficients,  $f(X) \sim g(X)$  if and only if  $\alpha$ , a fixed real number, is a root of  $f(X) - g(X)$ .

**1-2.** Prove that for any two sets  $A$  and  $B$ , either there exists an injection from  $A$  to  $B$  or an injection from  $B$  to  $A$ . (Hint : Consider the set  $\mathfrak{R}$  of triples  $(X, Y, f)$  where  $X \subseteq A$ ,  $Y \subseteq B$ ,  $f : X \rightarrow Y$  is a bijection. Partially order  $\mathfrak{R}$  by  $(X_1, Y_1, f_1) \leq (X_2, Y_2, f_2)$  if and only if  $X_1 \subseteq X_2$ ,  $Y_1 \subseteq Y_2$ ,  $f_2$  restricted to  $X_1$  equals  $f_1$ . Apply Zorn's lemma and show that a maximal element of  $\mathfrak{R}$  must either have  $A$  as its first entry or  $B$  as its second entry.)

**1-3.** Let  $V$  be a vector space over a field  $k$ . Recall that a subset  $X$  of  $V$  is called linearly independent if for any finite sum  $\sum a_i x_i = 0$  with  $a_i \in k$  and  $x_i \in X$ , all  $a_i$  must be zero. Use Zorn's lemma to prove that there exists a maximal linearly independent subset of  $V$ . Then prove that if  $X$  is such a subset and  $v \in V$ , then  $v = \sum a_i x_i$  (finite sum) for some unique  $a_i \in k - \{0\}$ ,  $x_i \in X$ .

**1-4.**  $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ . Define binary operations in the set  $\mathbb{Z}[i]$  by  $(a + bi) + (c + di) = (a + c) + (b + d)i$  and  $(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i$ . Thus  $i^2 = -1$ . Prove that  $\mathbb{Z}[i]$  is a commutative ring with unit.  $\mathbb{Z}[i]$  is called the ring of *Gaussian integers*.

**1-5.** Let  $\Lambda$  be a ring. Prove that for each element  $\lambda \in \Lambda$ , the set  $C(\lambda) = \{\mu \in \Lambda \mid \lambda\mu = \mu\lambda \text{ for all } \mu \in \Lambda\}$  is a commutative subring of  $\Lambda$ .  $C$  is called the *center* of  $\Lambda$ .

**1-6.** Let  $\Lambda$  be a ring and let  $\Gamma$  denote the set  $\mathbb{Z} \times \Lambda$ . Define operations in  $\Gamma$  by  $(m, x) + (n, y) = (m + n, x + y)$  and  $(m, x) \cdot (n, y) = (mn, my + nx + xy)$ . Note that  $my$  should be interpreted as  $y + y + \cdots + y$  ( $m$  times) in  $\Lambda$ . Similarly for  $nx$ . Show that  $\Gamma$  is a ring with unit element  $(1, 0)$ . Furthermore,  $\Gamma$  is commutative if and only if  $\Lambda$  is commutative. Finally, consider the map  $\varphi : \Lambda \rightarrow \Gamma$  given by

$\varphi(x) = (0, x)$ . Prove that  $\varphi$  is a monomorphism and that if  $\Lambda$  possesses a unit element,  $\varphi$  is not uniairy.

**1-7.** Let  $f : \Lambda \rightarrow \Lambda'$  be a homomorphism of rings with unit. Suppose that  $1' = f(\lambda)$  for some  $\lambda \in \Lambda$ . Prove that  $f$  is unitary.

**1-8.** Prove that the map  $\sigma : \mathbb{Z} \rightarrow \mathbb{Z}_m$  which sends each integer to its remainder upon division by  $m$  is a ring epimorphism.

**1-9.** Suppose that  $m$  and  $n$  are relatively prime integers. Prove that only ring homomorphism from  $\mathbb{Z}_m$  to  $\mathbb{Z}_n$  is the zero map.

**1-10.** Suppose that  $f : \mathbb{Q} \rightarrow \mathbb{Q}$  is a ring homomorphism, not identically zero. Prove that  $f$  is the identity map.

## Chapter 2

# IDEALS AND RESIDUE RINGS

For the remainder of the book, "ring" will be understood to mean "ring with unit element." All ring homomorphisms will be assumed to be unitary.

**Definition 2-1.** A *left ideal*  $A$  in a ring  $\Lambda$  is a nonempty subset of  $\Lambda$  such that

- (1)  $a, b \in A$ , then  $a-b \in A$ ;
- (2) if  $a \in A$  and  $\lambda \in \Lambda$ , then  $\lambda a \in A$ .  
A *right ideal*  $A$  in  $\Lambda$  is defined by replacing condition (2) with
- (3) if  $a \in A$  and  $\lambda \in \Lambda$ , then  $a\lambda \in A$ . If  $A$  satisfies (1), (2), and (3), it is called a *two-sided ideal* or simply an *ideal*. Note that in a commutative ring (2) is equivalent to (3) and so all ideals are two-sided.

**Examples.** 1. In a ring  $\mathbb{R}$ ,  $0$  and  $\mathbb{R}$  are ideals. An ideal  $A \neq \mathbb{R}$  is called *proper*.  
2. In the ring of integers  $\mathbb{Z}$ , all multiples of a given integer  $n$  form an ideal.  
3. In the ring of polynomials in one variable with real coefficients  $\mathbb{R}[X]$ , all polynomials in one variable with real coefficients  $\mathbb{R}[X]$ , all polynomials that have a given real number  $\alpha$  as a root form an ideal.  
4. In a field  $k$ , the only ideals are  $0$  and  $k$ . For if  $A \neq 0$  is an ideal of  $k$  and  $a \in A$ ,  $a \neq 0$ , then  $a^{-1} \cdot a = 1 \in A$  whence if  $c \in k$ ,  $c \cdot 1 = c \in A$ . That is,  $A = k$ .

- (1) *Addition of ideals.* If  $A$  and  $B$  are left ideals in  $\Lambda$  then  $A+B = \{a+b \mid a \in A, b \in B\}$  is again a left ideal of  $\Lambda$  called the sum of  $A$  and  $B$ .
- (2) *Multiplication of ideals.* If  $A$  and  $B$  are left ideals in  $\Lambda$ , then  $AB = \{\sum_{finite} a_i b_i \mid a_i \in A, b_i \in B\}$  is again a left ideal in  $\Lambda$  called the intersection of the  $A_i$ .

- (3) *Intersection of ideals.*  $A_i$  ( $i \in I$ , finite or infinite) is a collection of left ideals in  $\Lambda$ , then  $\bigcap_{i \in I} A_i$  is again a left ideal in  $\Lambda$  called the intersection of the  $A_i$ .
- (4) *Quotient of ideals.* If  $A$  and  $B$  are left ideals in  $\Lambda$ , then  $(A:B) = \{\lambda \in \Lambda \mid \lambda b \in A \text{ for all } b \in B\}$  is again a left ideal in  $\Lambda$  called the quotient of  $A$  by  $B$ .

At the end of the chapter, there are exercises exhibiting certain relationships among these operations.

**Definition 2-2.** A left ideal  $A$  in a ring  $\Lambda$  is said to be *finitely generated* if there exist elements  $a_1, a_2, \dots, a_n \in A$  such that every element of  $A$  can be written as  $\sum_{i=1}^n \lambda_i a_i$  for some  $\lambda_i \in \Lambda$ . We then write  $A = (a_1, a_2, \dots, a_n)$  and call  $a_1, a_2, \dots, a_n$  a *set of generators* (basis, base) for  $A$ . On the other hand, given any subset  $B$  of  $\Lambda$ , the set of elements that can be written as  $\sum_{finite} \lambda_i b_i$  where  $\lambda_i \in \Lambda, b_i \in B$  forms an ideal in  $\Lambda$ , denoted by  $(B)$ . It is in fact the smallest ideal of  $\Lambda$  that contains the set  $B$ .

**Definition 2-3.** In a commutative ring  $R$  and ideal  $A = (a) = Ra$  generated by a single element is called a *principal ideal*. A commutative ring  $R$  in which every ideal is principal is called a *principal ideal ring*.

**Examples.**  $\mathbb{Z}$  and  $k[X]$  where  $k$  is a field are each principal ideal rings.

**Theorem 2-1.** Let  $P$  be a proper ideal of a commutative ring  $R$ . the following conditions are equivalent :

1. If  $a, b \in R$  and  $ab \in P$ , then  $a \in P$  or  $b \in P$ .
2. If  $A$  and  $B$  are ideals of  $R$  and  $AB \subseteq P$ , then  $A \subseteq P$  or  $B \subseteq P$ .

*Proof.* (1) implies (2). Suppose  $AB \subseteq P$  but  $A \not\subseteq P$  and  $B \not\subseteq P$ . Then there are elements  $a \in A, a \notin P$  and  $b \in B, B \notin P$ . By(1),  $ab \notin P$ . However,  $ab \in AB \subseteq P$ . Contradiction. (2) implies (1). If  $ab \in P$ , then  $(a)(b) \subseteq P$ . Thus by (2), either  $(a) \subseteq P$  or  $(b) \subseteq P$ . In particular either  $a \in P$  or  $b \in P$ .  $\square$

**Definition 2-4.** An ideal  $P$  satisfying either (hence both) of the above conditions is called a *prime ideal*.

**Corollary 2-1.** Let  $P$  be a prime ideal of  $R$ . If  $a_1 a_2 \cdots a_n \in P$  then some  $a_i \in P$ . If  $A_1 A_2 \cdots A_n \subseteq P$ , then some  $A_i \subseteq P$ .

*Proof.* Induction on  $n$ .  $\square$

**Theorem 2-2.** Let  $m$  be a proper left ideal of a ring  $\Lambda$ . The following conditions are equivalent :

1. If  $A$  is a left ideal such that  $m \subseteq A \subseteq \Lambda$ , then  $A = m$  or  $A = \Lambda$ .
2. If  $a \in m, a \notin m$ , then  $(m, a) = \Lambda$ .

*Proof.* (1) implies (2). Since  $a \notin m, A = (m, a) \supset m$ . Thus  $A = \Lambda$ . (2) implies (1). Suppose  $m \subseteq A \subseteq \Lambda$ . If  $A \neq m$  then there exists  $a \in A, a \notin m$ . Thus  $(m, a) = \Lambda$ . But  $(m, a) \subseteq A$  so  $A = \Lambda$ .  $\square$

**Definition 2-5.** A left ideal  $m$  satisfying either (hence both) of the above conditions is called a *maximal left ideal*.

**Theorem 2-3.** In a commutative ring  $R$ , every maximal ideal is prime.

*Proof.* Suppose  $m$  is a maximal ideal and  $ab \in m$ . If  $a \notin m$ , then  $(m, a) = R$ . In particular  $1 = ra + m$  for some  $r \in R, m \in m$ . Then  $b = rab + mb \in m$ .  $\square$

**Definition 2-6.** If  $f : \Lambda \rightarrow \Gamma$  is a ring homomorphism, then the *image of  $f$* , denoted  $im f$ , is equal to  $\{\gamma \in \Gamma \mid \gamma = f(\lambda) \text{ for some } \lambda \in \Lambda\}$ ; the *kernel of  $f$* , denoted  $ker f$ , is equal to  $\{\lambda \in \Lambda \mid f(\lambda) = 0\}$ .

**Theorem 2-4.** Let  $f : \Lambda \rightarrow \Lambda$  with kernel  $K$ . Then  $K$  is an ideal of  $\Lambda$ .

*Proof.* Suppose  $a, b \in K$ . Then  $f(a-b) = f(a) - f(b) = 0$  so  $a-b \in K$ . Also  $f(\lambda a) = f(\lambda)f(a) = f(\lambda) \cdot 0 = 0$  so  $\lambda a \in K$  for any  $\lambda \in \Lambda$ . Similarly  $f(a\lambda) = 0$  so  $a \cdot \lambda \in K$ . Thus  $K$  is a two-sided ideal of  $\Lambda$ .

Conversely, a (two-sided) ideal  $A$  of  $\Lambda$  is the kernel of a homomorphism with domain  $\Lambda$ . To see this we define a relation on  $\Lambda$  by  $a \equiv b \pmod{A}$ , read "a congruent to b modulo A" if and only if  $a - b \in A$ .  $\square$

**Theorem 2-5.**  $\equiv \pmod{A}$  is an equivalence relation on  $\Lambda$ .

*Proof.* The proof is immediate from the definitions of an equivalence relation and an ideal. It is thus left as an exercise.

Let  $\Lambda/A$  be the set of distinct equivalence classes. If  $X, Y \in \Lambda/A$ , say  $X = \bar{a}, Y = \bar{b}$ , then we define  $X + Y = \bar{Z}$  where  $Z = \overline{a+b}$  and  $XY = \bar{W}$  where  $W = \overline{ab}$ .  $\square$

**Theorem 2-6.** Under the operations defined above,  $\Lambda/A$  is a ring.

*Proof.* It must be checked that the operations in  $\Lambda/A$  are well defined. In particular, if  $\bar{a} = \overline{a'}$  and  $\bar{b} = \overline{b'}$ , we must show that  $\overline{a+b} = \overline{a'+b'}$  and  $\overline{ab} = \overline{a'b'}$ . But  $a - a' = x$  and  $b - b' = y$  for some  $x, y \in A$ . Thus  $(a+b) - (a'+b') = x+y \in A$  so  $\overline{a+b} = \overline{a'+b'}$ . Also  $ab - a'b + a'b - a'b' = ab - a'b' = xb + a'y \in A$  so  $\overline{ab} = \overline{a'b'}$ . Hence the operations are well-defined.

Checking that the ring axioms are satisfied is left as an exercise.

There is a natural epimorphism  $\sigma : \Lambda \rightarrow \Lambda/A$  given by  $\sigma(\lambda) = \bar{\lambda}$ .  $\Lambda$  is called the *residue ring* of  $\Lambda$  with respect to  $A$ .  $\square$

**Theorem 2-7.** (First Isomorphism Theorem) Suppose  $f : \Lambda \rightarrow \Gamma$  is a ring homomorphism. Then  $\text{im } f = \Lambda/\ker f$ .

*Proof.* Consider the following diagram : We define a map  $\tau : \Lambda/\ker f \rightarrow \text{im } f$  and show that it is an isomorphism. If  $X = \bar{a} \in \Lambda/\ker f$ , define  $\tau(X) = f(a)$ . To see that this is well-defined, suppose  $\bar{a} = \overline{a'}$ . Then  $a - a' \in \ker f$  so  $f(a - a') = f(a) - f(a') = 0$  or  $f(a) = f(a')$ . Hence  $\tau(\bar{a}) = \tau(\overline{a'})$ . Furthermore, if  $Y = \bar{b}$ ,  $\tau(X+Y) = \tau(\overline{a+b}) = \tau(\overline{a+b}) = f(a+b) = f(a) + f(b) = \tau(\bar{a}) + \tau(\bar{b}) = \tau(X) + \tau(Y)$  and  $\tau(XY) = \tau(\overline{a \cdot b}) = \tau(\overline{ab}) = f(ab) = f(a) \cdot f(b) = \tau(\bar{a}) \tau(\bar{b}) = \tau(X) \tau(Y)$  so  $\tau$  is a homomorphism. If  $\gamma \in \text{im } f$ , then  $\gamma = f(a) = \tau(\bar{a})$  for some  $a \in \Lambda$  so  $\tau$  is surjective.

Finally, if  $\tau(\bar{a}) = f(a) = 0$ , then  $a \in \ker f$  so  $\bar{a} = 0$ . Hence  $\tau$  is injective and so an isomorphism.  $\square$

**Theorem 2-8.** (Second Isomorphism Theorem) If  $f : \Lambda \rightarrow \Lambda'$  is an epimorphism with kernel  $K$ , then there is a bijection between the set of ideals  $A \supseteq K$  of  $\Lambda$  and the set of ideals of  $\Lambda'$ . Furthermore, if  $A$  and  $A'$  are corresponding ideals under this bijection, then  $\Lambda/A \approx \Lambda'/A' \approx (\Lambda/K) / (A/K)$ .

*Proof.* Let  $\zeta$  equal the set of ideals of  $\Lambda$  which contain  $K$  and  $\eta$  equal the set of ideals of  $\Lambda'$ . Define  $g : \zeta \rightarrow \eta$  by  $g(A) = \{f(a) \mid a \in A\}$ , which is clearly an ideal of  $\Lambda'$ , hence in  $\eta$ . Define  $h : \eta \rightarrow \zeta$  by  $h(A') = \{a \in \Lambda \mid f(a) \in A'\}$  which is an ideal of  $\Lambda$  containing  $K$ , hence in  $\zeta$ . It is easy to check that  $g \circ h = I_\eta$  and  $h \circ g = I_\zeta$ , the respective identity maps on the sets  $\eta$  and  $\zeta$ . Hence each is a bijection.

To verify the second assertion of the theorem, let  $\sigma : \Lambda' \rightarrow \Lambda'/A'$  be the natural epimorphism. Then  $\tau = \sigma \circ f : \Lambda \rightarrow \Lambda'/A'$  is an epimorphism and

$\lambda \in \ker \tau$  if and only if  $\tau(\lambda) = 0$  if and only if  $\sigma(f(\lambda)) = 0$  if and only if  $f(\lambda) \in A'$  if and only if  $\lambda \in A$ . Hence  $\ker \tau = A$  and by the previous theorem  $\Lambda/A \approx \Lambda'/A'$ .  $\square$

**Definition 2-7.** An element  $a$  in a commutative ring  $R$  is called a *zero divisor* if there exists  $b \neq 0$  in  $R$  such that  $ab=0$ . If  $a \neq 0$ , it is called a *nontrivial zero divisor*.

**Definition 2-8.** A commutative ring is called an *integral domain* (or simply a domain) if it has no nontrivial zero divisors.

**Examples.**  $\mathbb{Z}$ ,  $k$ , and  $k[X_1, \dots, X_n]$  where  $k$  is any field are all integral domains. On the other hand  $M_n(k)$ ,  $n \geq 2$ ,  $\mathbb{Z}_m$  where  $m$  is a nonprime are not integral domains.



## Chapter 3

# RINGS OF QUOTIENTS AND LOCALIZATION

In this chapter we discuss another construction yielding a new ring from a given ring. The reader should keep in mind the method by which the rationals  $\mathbb{Q}$  are constructed from the integers  $\mathbb{Z}$  for it is just this process which is being generalized. In this chapter and the next, all rings are assumed commutative.

**Definition 3-1.** A subset  $S$  of a ring  $R$  is called a *multiplicative set* if

- (1)  $1 \in S$ ;
- (2) if  $a, b \in S$ , then  $ab \in S$ .

Let  $S$  be a multiplicative set in  $R$ . Consider the set  $\{r/s \mid r \in R, s \in S\}$  thought of simply as formal symbols.

We say two such symbols  $r_1/s_1$  and  $r_2/s_2$  are equivalent, denoted  $r_1/s_1 \sim r_2/s_2$ , if there exists  $s \in S$  such that  $s(r_1s_2 - r_2s_1) = 0$ . The reader should check that  $\sim$  is in fact an equivalence relation. Denote by  $[r/s]$  the class of  $r/s$  and by  $R_S$  the set of distinct equivalence classes. We define addition and multiplication in  $R_S$  by

$$[r_1/s_1] + [r_2/s_2] = [r_1s_2 + r_2s_1/s_1s_2]$$

and

$$[r_1/s_1] \cdot [r_2/s_2] = [r_1r_2/s_1s_2].$$

Under these operations  $R_S$  is a ring called the *ring of quotients of  $R$  with respect to  $S$* . Furthermore there is a natural homomorphism  $\varphi : R \rightarrow R_S$

given by  $\varphi(r)=[r/1]$ .

**Theorem 3-1.**

- (1) If  $0 \in S$ , then  $R_S=0$ .
- (2)  $\varphi$  is injective if and only if  $S$  contains no zero divisors.

*Proof.* (1) Note that  $[0/1]$  is the zero element of  $R_S$  since  $[r/s] = [0/1] = [r1 + 0s/s1] = [r/s]$ . If  $0 \in S$  and  $[r/s] \in R_S$ , then  $[r/s] = [0/1]$  since  $0(r1 + 0s) = 0$ . Thus  $R_S$  reduces to just the zero element.

(2)  $r \in \ker\varphi$  if and only if  $\varphi(r) = [r/1] = 0$  in  $R_S$  if and only if there exists  $s \in S$  such that  $sr = 0$ . Thus  $\ker\varphi = 0$  if and only if  $S$  contains no zero divisors.  $\square$

**Examples.**

1. Let  $S$  be the set of all non-zero divisors of  $R$ . Suppose  $a, b \in S$  and  $c \in R$  satisfy  $(ab)c = 0$ . Then  $a(bc) = 0$  which implies  $bc = 0$  since  $a \in S$ . But this implies  $c = 0$  since  $b \in S$ . Thus  $ab \in S$ . Clearly  $1 \in S$  so  $S$  is a multiplicative set.  $R_S$  is called the *total ring of quotients of  $R$* .
2. Let  $P$  be a prime ideal of  $R$  and  $S = R - P$ . This is a multiplicative set. The ring of quotients  $R_S$  is usually denoted by  $R_P$  and is called the *localization of  $R$  at  $P$* .
3. As a special case of either example 1 or 2, let  $R$  be an integral domain. Then  $(0)$  is a prime ideal and  $S = R - (0)$  is the set of all non-zero divisors of  $R$ . The localization at  $(0)$  is called the *quotient field* of  $R$ . As the name suggests, it is in fact a field.

**Theorem 3-2.** Let  $S$  be a multiplicative set in a ring  $R$ . Then there exists a bijection between the set of prime ideals of  $R$  whose intersection with  $S$  is empty and the set of prime ideals of  $R_S$ .

*Proof.* If  $0 \in S$ , then both sets are empty. Thus we can assume  $0 \notin S$ . We begin by describing a method of associating an ideal in  $R_S$  with one in  $R$  and vice versa.

If  $A$  is an ideal in  $R$ , define  $AR_S = \{t[a/1] | a \in A, t \in R_S\}$

This is called the *extension of  $A$  to  $R_S$* . On the other hand, if  $B$  is ideal in  $R_S$ , define

$$B \cap R = \varphi^{-1}(B)$$

where  $\varphi : R \rightarrow R_S$  is the natural homomorphism. This is called the *contraction of  $B$  to  $R$* . Note that when  $S$  contains zero divisors,  $\varphi$  is not injective

so that  $R$  cannot be thought of as embedded in  $R_S$ . In this case the contraction is not a genuine intersection. However, the intersection notation is a widely accepted one.

The proof can now be broken down into a sequence of steps.

(a)  $AR_S$  is an ideal of  $R_S$ . For if  $t_1[a_1/1]$  and  $t_2[a_2/1]$  are in  $AR_S$  where  $t_1 = [r_1/s_1]$  and  $t_2 = [r_2/s_2]$ , then

$$\begin{aligned} t_1[a_1/1] - t_2[a_2/1] &= [r_1a_1/s_1] - [r_2a_2/s_2] \\ &= [r_1a_1s_2 - r_2a_2s_1/s_1s_2] = t'[a'/1] \end{aligned}$$

where  $t' = [1/s_1s_2] \in R_S$  and  $a' = r_1a_1s_2 - r_2a_2s_1 \in A$ .

(b) If  $P$  is prime in  $R$  and  $P \cap S = \Phi$ , then  $PR_S$  is prime in  $R_S$ . First of all  $PR_S$  is a proper ideal of  $R_S$ .

For if  $1 \in PR_S$ , then  $[1/1] = [rp/s]$  for some  $r \in R$ ,  $p \in P$ ,  $s \in S$  in which case there exists  $s' \in S$  such that  $s'(s - rp) = 0$ .

That is  $s's = s'rp$ . But  $s's \in S$  and  $s'rp \in P$  so  $P \cap S \neq \Phi$ . Contradiction. Thus  $PR_S$  is proper.

Furthermore if  $[r_1/s_1][r_2/s_2] = [r_1r_2/s_1s_2] \in PR_S$ , say  $[r_1r_2/s_1s_2] = [rp/s]$  for some  $r \in R$ ,  $s \in S$ ,  $p \in P$ , then there exists  $s' \in S$  such that  $s'(r_1r_2s - rps_1s_2) = 0$ . Thus  $s'r_1r_2s = s'rp s_1s_2 \in P$ . But  $s \notin P$ ,  $s' \notin P$  so either  $r_1 \in P$  or  $r_2 \in P$ . Hence either  $[r_1/s_1] \in PR_S$  or  $[r_2/s_2] \in PR_S$ .

(c)  $B \cap R$  is an ideal of  $R$ . If  $b_1, b_2 \in B \cap R$ , then  $\varphi(b_1) = [b_1/1]$  and  $\varphi(b_2) = [b_2/1] \in B$ . Thus  $[b_1/1] - [b_2/1] = [b_1 - b_2/1] = \varphi(b_1 - b_2) \in B$ . Hence  $b_1 - b_2 \in B \cap R$ .

(d) If  $B$  is prime in  $R_S$ , then  $B \cap R$  is prime in  $R$  and  $(B \cap R) \cap S = \Phi$ . For  $ab \in B \cap R$  implies  $[ab/1] = [a/1][b/1] \in B$  whence  $[a/1] \in B$  or  $[b/1] \in B$ , that is,  $a \in B \cap R$  or  $b \in B \cap R$ . Furthermore, if  $s \in (B \cap R) \cap S$ , then  $[s/1] \in B$  so  $[1/s][s/1] = [1/1] \in B$  which implies  $B = R_S$ . Contradiction. Thus  $(B \cap R) \cap S = \Phi$ . In particular,  $1 \notin B \cap R$  so  $B \cap R$  is proper, hence prime.

(e) It remains only to show that this pairing is actually a bijection between the two sets in question. This is left as exercise for the reader.  $\square$

**Definition 3-2.** An element  $r$  in a ring  $\Lambda$  (not necessarily commutative) is called a *unit* if there exists  $s \in \Lambda$  such that  $rs = 1 = sr$ .

**Theorem 3-3.** The following statements are equivalent :

- (1) The set of nonunits of  $R$  form an ideal.
- (2)  $R$  has a unique maximal ideal.

*Proof.* (1) implies (2). Let  $M$  be the ideal of nonunits. If  $x \notin M$ , then  $x$  is a unit so  $R = (x) \subseteq (x, M) \subseteq R$ . Thus  $(x, M) = R$  which implies  $M$  is maximal. Now suppose  $\mathfrak{M}$  is any maximal ideal of  $R$ . Then  $\mathfrak{M}$  consists solely of nonunits. Thus  $\mathfrak{M} \subseteq M \subseteq R$  which implies  $\mathfrak{M} = M$ .

(2) implies (1). We first show that any proper ideal of  $R$  is contained in at least one maximal ideal. To do this we will use Zorn's lemma. Let  $A$  be a proper ideal of  $R$  and consider

$$\delta = \{B \mid B \text{ is an ideal of } R \text{ satisfying } A \subseteq B \subset R\}$$

$\delta$  is not empty since  $A$  is in  $\delta$ . Furthermore, if  $B_i, i \in I$ , is a chain in  $\delta$ , then  $B = \cup_{i \in I} B_i$  is again in  $\delta$ . For certainly  $A \subseteq B$  and if  $B = R$ , then  $1 \in B$ , in which case  $1 \in B_i$  for some  $i$ . Thus  $B_i = R$  contradicting the assumption that  $B_i$  is in  $\delta$ .  $B$  is an upper bound for the chain so  $\delta$  is an inductive set. By Zorn's lemma, let  $M$  be a maximal element of  $\delta$ . If  $x \in R, x \notin M$ , then  $M \subset (x, M) \subseteq R$ . By the choice of  $M$ , it must be that  $(x, M)$  is not in  $\delta$ , that is,  $(x, M) = R$ . Thus  $M$  is a maximal ideal of  $R$  which contains  $A$ .

Now Let  $\mathfrak{M}$  denote the maximal ideal of  $R$  and  $M$  the set of nonunits of  $R$ . Clearly  $\mathfrak{M} \subseteq M$  since  $\mathfrak{M}$  consists solely of nonunits. On the other hand, if  $x \in M$ , then  $(x)$  subseteq  $\mathfrak{M}$  since  $\mathfrak{M}$  is the only maximal ideal. In particular,  $x \in \mathfrak{M}$  so  $M \subseteq \mathfrak{M}$ . Therefore  $M = \mathfrak{M}$  and so  $M$  is an ideal.  $\square$

**Definition 3-3.** Let ring satisfying either (hence both) of the above conditions is called a *local ring*.

**Theorem 3-4.** Let  $P$  be a prime ideal of  $R$ . Then  $R_P$  is a local ring with unique maximal ideal  $PR_P$ .

*Proof.* By Theorem 3-2, the only prime ideals of  $R_P$  are of the form  $QR_P$  where  $Q$  is a prime ideal of  $R$  and  $Q \cap (R - P) = \Phi$ , that is,  $Q \subseteq P$ . Thus  $QR_P \subseteq PR_P$ . Since maximal ideals are prime,  $PR_P$  must be the only maximal ideal of  $R_P$ .  $\square$

**Theorem 3-5.** Let  $P$  be a prime ideal of  $R$ . Then  $R_P/PR_P$  is isomorphic to the quotient field of  $R/P$ .

*Proof.* Recall that the quotient field of an integral domain is just the localization at the prime ideal 0. Define a map

$$\rho : (R/P)_0 \rightarrow R_P/PR_P \text{ by}$$

$$\rho([\tilde{r}/\tilde{s}]) = \overline{[r/s]}$$

where  $\varphi : R \rightarrow R/P$  sends  $r \rightarrow \tilde{r}$ ,  $\psi : R_P \rightarrow R_P/PR_P$  sends  $t \rightarrow \bar{t}$ , and  $[\ ]$  has the usual meaning of the class of an element in a ring of quotients. We must show that  $\rho$  is well-defined and an isomorphism.

(a)  $\rho$  is well - defined. Suppose  $[\tilde{r}_1/\tilde{s}_1] = [\tilde{r}_2/\tilde{s}_2]$ . Then there exists  $\tilde{r} \neq 0$  in  $R/P$  such that  $\tilde{r}(\tilde{r}_1\tilde{s}_2 - \tilde{r}_2\tilde{s}_1) = 0$ . That is, there exists  $r \in R - P$  such that  $r(r_1s_2 - r_2s_1) \in P$ . Thus  $r_1s_2 - r_2s_1 \in P$  which implies  $[r_1s_2 - r_2s_1/s_1s_2] \in PR_P$ . Therefore  $\overline{[r_1s_2 - r_2s_1/s_1s_2]} = 0$ , that is  $\overline{[r_1/s_1]} = \overline{[r_2/s_2]}$ .

(b)  $\rho$  is ring homomorphism. This verification is left as an exercise for the reader.

(c) Suppose  $[\tilde{r}_1/\tilde{s}_1] \in \ker \rho$ . Then  $[r_1/s_1] \in PR_P$ . Thus there exist elements  $p \in P, r \in R, s \in R - P$  such that  $[r_1/s_1] = [rp/s]$ , whence there exists  $s' \in R - P$  such that  $s'sr_1 = s'rps_1 \in P$ . But  $s \notin P, s' \notin P$  so  $r_1 \in P$ . Therefore  $\tilde{r}_1 = 0$  and so  $[\tilde{r}_1/\tilde{s}_1] = 0$ . Hence  $\rho$  is injective. It is immediate from the definition that  $\rho$  is surjective, hence an isomorphism.  $\square$

### Exercise.

**3-1.** Prove that the complement of a union of prime ideals in a ring  $R$  is multiplicative set.

**3-2.** Let  $k$  be a field,  $a \in k$ , and set

$$M_a = \{f(X) \in k[X] \mid f(a) \neq 0\}.$$

Show that  $M_a$  is a multiplicative set in the ring  $k[X]$ . More generally, let  $V$  be any collection of  $n$  - tuples  $(a) = (a_1, \dots, a_n)$  in  $k^n$  and set

$$M_V = \{f(X_1, \dots, X_n) \in k[X_1, \dots, X_n] \mid f(a) \neq 0 \text{ for all } (a) \in V\}.$$

Show that  $M_V$  is a multiplicative set in  $k[X_1, \dots, X_n]$ .

**3-3.** Prove that the quotient field of  $\mathbb{Z}[i]$ , the Gaussian integers, is isomorphic to  $\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$ .

**3-4.** Describe the total ring of quotients of  $\mathbb{Z}_n$ .

**3-5.** Complete the proofs of Theorem 3 - 2(e) and Theorem 3 - 5(b).

**3-6.** Prove that the set of units of a ring form a group under multiplication.

**3-7.** First all units in the following rings :

- (a)  $\mathbb{Z}[i]$
- (b)  $k[X]$
- (c)  $\mathbb{Z}_n$
- (d)  $M_2(\mathbb{R})$

**3-8.** Let  $R$  be an integral domain with quotient field  $K$ ,  $S$  a multiplicative set in  $R$ ,  $0 \notin S$ . Prove that  $R_S$  is an integral domain and that the quotient field of  $R_S$  is  $K$ .

**3-9.** Let  $S$  be a multiplicative subset of a ring  $R$ ,  $0 \notin S$ . Let  $P$  be a maximal element in the set of ideals whose intersection with  $S$  is empty. ( Show by Zorn's lemma that there exists such an ideal.) Prove that  $P$  is a prime ideal.

**3-10.** Let  $R$  be a ring in which every nonzero prime ideal is maximal. Prove that  $PR_P$  is the only nonzero prime ideal of  $R_P$  where  $P \neq 0$  is a prime ideal of  $R$ .

## Chapter 4

# UNIQUE FACTORIZATION DOMAINS

In this chapter we will employ the technique of localization developed in the previous chapter to capture some well known results about unique factorization domains, namely Theorems 4-6, 4-7, and 4-8. We begin the chapter with a special class of these rings called Euclidean domains. Once again, all rings are commutative.

**Definition 4-1.** An integral domain  $R$  is called a *Euclidean domain* if there exists a function  $d:R \rightarrow \mathbb{Z}$  satisfying

- (1)  $d(a) > d(0)$  for all  $0 \neq a \in R$ ;
- (2) For any  $a, b \in R, b \neq 0$ , there exist elements  $q, r \in R$  such that  $a = qb + r$  with  $d(r) < d(b)$

**Examples.**

1. Let  $R = \mathbb{Z}$  and  $d(a) = |a|$ , ordinary absolute value. The elements  $q$  and  $r$  are what are usually called the quotient and remainder upon division of  $a$  by  $b$ .
2. Let  $R = k[X]$  for a field  $k$  and set  $d(f(X)) =$ the degree of the polynomial  $f(X)$  if  $f(X) \neq 0$  and  $d(0) = -1$

**Theorem 4-1.** Every Euclidean domain is a principal ideal domain.

*Proof.* Let  $(R, d)$  be a Euclidean domain and  $B$  an ideal in  $R$ . If  $B$  is the zero ideal, then  $B = (0)$  and so is principal. Otherwise consider the non empty subset  $X$  of  $\mathbb{Z}$  given by  $X = \{d(a) | a \in B, a \neq 0\}$ . By property (1) of the function

$d, x > d(0)$  for all  $x \in X$ . Thus  $X$  is a nonempty subset of  $\mathbb{Z}$  which is bounded from below. Hence  $X$  has a minimal element. Let  $0 \neq b \in B$  be such that  $d(b)$  is a minimal element of  $X$ . We want to show that  $B = (b)$ .

Suppose  $a \in B$ . Then there exist elements  $q$  and  $r$  in  $R$  such that  $a = qb + r$  with  $d(r) < d(b)$ . Since  $a \in B, qb \in B$ , we have  $r = a - qb \in B$ . But  $d(r) < d(b)$  contradicts the choice of  $b$  unless  $r = 0$ . Hence  $a = qb$  and  $B = (d)$ . Therefore every ideal of  $R$  is principal.  $\square$

**Definition 4-2.** A ring  $R$  is said to satisfy the *ascending chain condition* if every strictly ascending chain of ideals of  $R, A_1 \subset A_2 \subset A_3 \subset \dots$  is finite. Equivalently if for every infinite chain of ideals  $A_1 \subseteq A_2 \subseteq \dots$ , there exists an integer  $k$  such that  $A_i = A_k$  for  $i > k$ .

**Definition 4-3.** A ring  $R$  is said to satisfy the *maximum condition* if every nonempty collection of ideals of  $R$  has a maximal element, that is, an ideal which is properly contained in no ideal of the collection.

**Theorem 4-2.** A ring  $R$  satisfies the ascending chain condition if and only if  $R$  satisfies the maximum condition.

*Proof.* If  $R$  does not satisfy the ascending chain condition, there exists an infinite strictly ascending chain of ideals  $\{A_i\}$ . The collection of these ideals has no maximal element.

If  $R$  does not satisfy the ascending chain condition, let  $\mathfrak{A}$  be a nonempty collection of ideals. Let  $A_1 \in \mathfrak{A}$ . If  $A_1$  is maximal, we are done. Otherwise, there exists  $A_2 \in \mathfrak{A}$  such that  $A_1 \subset A_2$ . If  $A_2$  is maximal, we are done. Otherwise, continue the process. Since  $R$  satisfies the ascending chain condition, this process must stop. When it does, we have a maximal element in  $\mathfrak{A}$ . To say that a ring satisfies the ascending chain condition for principal ideals has the obvious meaning, that is, replace “ideal” by “principal ideal” in Definition 4-2.  $\square$

**Definition 4-4.** Let  $R$  be a domain. A nonunit  $p \in R$  is called *irreducible* if  $p = ab$  implies either  $a$  or  $b$  is a unit in  $R$ .

**Definition 4-5.** An integral domain  $R$  is called a *unique factorization domain* if every nonzero nonunit of  $R$  can be written uniquely as a finite product of irreducibles. More precisely,

- (1) If  $a \neq 0$  is a nonunit, then  $a = p_1 p_2 \cdots p_r$  where each  $p_i$  is irreducible.
- (2) If  $p_1 \cdots p_r = q_1 \cdots q_s$  (all  $p_i$  and  $q_j$  irreducible) then  $r = s$  and there exists a permutation  $\pi$  of  $\{1, 2, \dots, r\}$  such that  $p_i = u_i q_{\pi(i)}$  for some units  $u_i$ .

**Definition 4-6.** A nonzero element  $p \in R$  is called a *prime* if  $(p)$  is a prime ideal of  $R$ .

**Note.**

1. Every prime is irreducible. For if  $p$  is prime and  $p = ab$ , then  $ab \in (p)$  so either  $a \in (p)$  or  $b \in (p)$ . If  $a \in (p)$ , then  $a = rp$  for some  $r \in R$ . Thus  $p = ab = rpb$ , that is,  $1 = rb$  so  $b$  is a unit in  $R$ .
2. Not every irreducible is prime. Consider the ring  $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$  where the operations are the usual ones for complex numbers. In this ring,  $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ . All of these elements are irreducible, but none is prime.

**Theorem 4-3.** A domain  $R$  is a unique factorization domain if and only if every nonzero nonunit of  $R$  can be written as a finite product of prime elements.

*Proof.* Assume  $R$  is a unique factorization domain. It suffices to show that every irreducible element of  $R$  is prime. Let  $p$  be irreducible and suppose  $ab \in (p)$ , that is,  $ab = rp$  for some  $r \in R$ . Write  $a, b, r$  as products of irreducibles, say  $a = p_1 p_2 \cdots p_\alpha$ ,  $b = q_1 q_2 \cdots q_\beta$ ,  $r = p'_1 p'_2 \cdots p'_\rho$ . Then  $p_1 p_2 \cdots p_\alpha q_1 q_2 \cdots q_\beta = p'_1 p'_2 \cdots p'_\rho p$ . By uniqueness  $p = up_i$  for some  $i$ ,  $1 \leq i \leq \alpha$  or  $p = vq_j$  for some  $j$ ,  $1 \leq j \leq \beta$ ,  $u$  and  $v$  units. In one case  $a \in (p)$ , in the other  $b \in (p)$ . Therefore  $(p)$  is a prime ideal so  $p$  is a prime element.

Now assume every nonunit can be written as a finite product of primes. Since primes are irreducible, it suffices to show the expression is unique. Suppose  $p_1 \cdots p_r = q_1 \cdots q_s$  where all  $p_i, q_j$  are primes. Then  $p_1$  divides  $q_j$  for some  $j$ , say  $j = 1$  (relabel if necessary). Hence  $q_1 = u_1 p_1$  where  $u_1$  is a unit. After cancellation  $p_2 \cdots p_r = u_1 q_2 \cdots q_s$ . Proceeding by induction, the uniqueness follows.  $\square$

**Theorem 4-4.** Let  $S$  be the multiplicative set generated by 1 and all primes in the domain  $R$ . Then  $R$  is a unique factorization domain if and only if  $R_S$  is a field.

*Proof.* Assume  $R$  is a unique factorization domain. Then every nonzero nonunit of  $R$  is in  $S$ . But in  $R_S$ , elements of  $S$  become units. Hence every nonzero element of  $R_S$  is a unit, that is,  $R_S$  is a field.

Suppose  $R$  is not a unique factorization domain and  $a \in R$  is nonzero nonunit which cannot be written as a finite product of primes, that is,  $a \notin S$ . Clearly then  $(a) \cap S = \Phi$ . For if  $ba$  is a finite product of primes,  $a$  must be also. Thus  $0 \neq (a)R_S \neq R_S$ , that is, the ideal generated by  $[a/1]$  in  $R_S$  is nonzero and proper. Therefore  $R_S$  is not a field since it has a nonzero proper ideal.  $\square$

**Theorem 4-5.** Let  $R$  be a domain with the ascending chain condition on principal ideals. Let  $M$  be a multiplicative set generated by 1 and prime elements (not necessarily all prime elements). If  $R_M$  is a unique factorization domain, then  $R$  is a unique factorization domain.

*Proof.* Let  $S$  be the multiplicative set generated by 1 and all primes in  $R$  and let  $T$  be the multiplicative set generated by  $[1/1]$  and all primes in  $R_M$ . We will accomplish the proof by a series of reductions.

- (a) Since  $R_M$  is by hypothesis a unique factorization domain, Theorem 4-4 states that  $(R_M)_T$  is a field. Again by Theorem 4-4,  $R$  is a unique factorization domain if and only if  $R_S$  is a field. Thus it suffices to prove  $R_S = (R_M)_T$ .
- (b)  $R_S \subseteq (R_M)_T$ . For let  $x = [r/s] \in R_S$ . Write  $s = ms'$  where  $m$  is a product of generators of  $M$  and  $s'$  involves no generators of  $M$ . Then  $x = [r/m][1/s']$  where clearly  $[r/m] \in (R_M)_T$ . Thus it suffices to show that  $[1/s'] \in (R_M)_T$ . Furthermore it suffices to show that  $[1/p] \in (R_M)_T$  where  $p$  is a prime of  $R$  and not one of the generators of  $M$ , since  $[1/s']$  is just a product of such elements. Now  $(p)$  is a prime ideal of  $R$ . If  $(0) \cap M \neq \Phi$ , then  $rp \in M$  for some  $r \in R$ . Thus  $[1/rp] \in R_M$  so  $[1/p] = [r/1][1/rp] \in R_M \subseteq (R_M)_T$  and we are done. Otherwise  $(p) \cap M = \Phi$  in which case  $[p/1]$  generates a prime ideal in  $R_M$ . That is,  $[p/1]$  is a prime element in  $R_M$ , hence in  $T$ . Thus  $[[1/1]/[p/1]] = [1/p] \in (R_M)_T$ . This shows that  $R_S \subseteq (R_M)_T$ .
- (c) The next claim is that in order to show  $(R_M)_T \subseteq R_S$ , it suffices to prove the following statement: if  $x \in R$  and  $[x/1]$  is a prime in  $R_M$ , then  $x \in S$ . For a typical element of  $(R_M)_T$  can be written as  $[z/t]$  where  $z \in R_M$ ,  $t \in T$  and  $t = [x_1/1][x_2/1] \cdots [x_k/1]$  where  $x_1, \dots, x_k \in R$  and  $[x_1/1] \cdots [x_k/1]$  are prime in  $R_M$ . Our statement would then say that  $x_1, \dots, x_k \in S$ . Thus  $[1/t] \in R_S$ . This verifies the claim.
- (d) If  $x \in R$  and  $[x/1]$  is a prime in  $R_M$ , then  $x \in S$ . Assume the contrary, that is, there exists an element  $x \in R_S$  such that  $[x/1]$  is prime in  $R_M$ . Let  $\delta = \{x \in R \mid x \in R - S \text{ and } [x/1] \text{ is prime in } R_M\}$ . By hypothesis  $\delta$  is nonempty and by the ascending chain condition on principal ideals, there exists a maximal element in  $\delta$ . Call it  $(y)$ .

The next claim is that  $[y/1]R_M \cap R = (y)$ . Suppose that  $[y/1][r/m] \in R$  for some  $r \in R$ ,  $m \in M$ . That is,  $m$  divides  $yr$ . We want to show that  $m$  divides  $r$ . If  $p$  is a prime (in  $R$ ) factor of  $m$  and  $p$  divides  $y$ , then  $y = pz$  for some  $z \in R$ . Clearly  $z \notin S$  for  $z \in S$  would imply  $y \in S$ . Furthermore  $[z/1]R_M = [y/p]R_M = [y/1]R_M$  so  $[z/1]$  is prime in  $R_M$ . Hence  $(z)$  is in  $\delta$  and by the choice of  $(y)$ ,  $(z) = (y)$ . Thus  $z = ay$  for some  $a$  in  $R$  from which  $y = pz = pay$ . Therefore  $pa = 1$  making  $p$  a unit and contradicting  $p$  a prime. Thus no prime factor of  $m$  divides  $y$ , hence  $m$  divides  $r$ . This gives the inclusion  $[y/1]R_M \cap R \subseteq (y)$ . The reverse inclusion is immediate and the claim is established.

Finally we conclude from the claim and Theorem 3-2 that  $y$  is a prime in  $R$ . This immediately contradicts  $y \notin S$  and completes the proof of the theorem.  $\square$

**Theorem 4-6.** Every principal ideal domain is a unique factorization domain.

*Proof.* Let  $R$  be a principal ideal domain and  $S$  the multiplicative set generated by 1 and all primes in  $R$ . If  $R_S$  is not a field, let  $0 \neq A \subset R_S$  be a maximal ideal in  $R_S$ .

Then  $A$  is a prime ideal of  $R_S$  so  $A \cap R$  is a prime ideal of  $R$ . But  $A \cap R = (r)$  for some  $r \in R$ , whence  $r$  is prime in  $R$ . Thus  $r \in S$ . But this implies  $A = (A \cap R)R_S = [r/1]R_S = R_S$ , contradicting the choice of  $A$ . Thus  $R_S$  is a field and by Theorem 4-4,  $R$  is a unique factorization domain.  $\square$

**Corollary 4-1.** Every Euclidean domain is a unique factorization domain.

**Lemma 4-1.**

- (1) If  $R$  is a domain, then  $R[X]$  is a domain.
- (2) If  $R$  satisfies the ascending chain condition for principal ideals, so does  $R[X]$ .

*Proof.* (1) Obvious.

- (2) Consider  $(f_1(X)) \subseteq (f_2(X)) \subseteq \dots$ . Then  $\deg f_1(X) \geq \deg f_2(X) \geq \dots$ . This must end at some nonnegative integer. Suppose  $\deg f_i(X) = \deg f_k(X)$  for all  $i \geq k$ . Then  $(f_k) \subseteq (f_{k+1})(X)$  implies  $f_k(X) = af_{k+1}(X)$  for some  $a \in R$ .

Let  $a_i$  be the leading coefficient of  $f_i(X)$ . Then  $(a_k) \subseteq (a_{k+1}) \subseteq \dots$ . Thus there exists  $N$  such that  $(a_j) = (a_t)$  for  $j, t \geq N$ . Suppose  $j > t > n$ . Then  $f_j(X)$  divides  $f_t(X)$ , that is,  $f_t(X) = af_j(X)$ . Therefore  $a_t = aa_j$ . But  $(a_t) = (a_j)$  so  $a$  is a unit in  $R$ . Therefore  $(f_t(X)) = (f_j(X))$ .  $\square$

**Theorem 4-7.** If  $R$  is a unique factorization domain, then  $R[X]$  is a unique factorization domain.

*Proof.* Note that for any ideal  $A$  of  $R$ ,  $(R/A)[X] \approx R[X]/AR[X]$ . Therefore if  $P$  is a prime ideal in  $R$ , then  $PR[X]$  is a prime ideal in  $R[X]$ . So if  $p$  is a prime element in  $R$ , it is also a prime element in  $R[X]$ . Let  $S$  be the multiplicative set generated by prime elements in  $R$ .

Then  $(R[X])_S = R_S[X]$ . But  $R_S$  is a field so  $R_S[X]$  is a principal ideal domain. Then by Theorem 4-6,  $R_S[X]$  is a unique factorization domain, whence by Theorem 4-5 and the above lemma,  $R[X]$  is a unique factorization domain.  $\square$

**Note.** We have used here the fact that a unique factorization domain satisfies the ascending chain condition on principal ideals. This follows immediately by considering the factorization of the generators of the ideals in a chain.

**Corollary 4-2.** If  $R$  is a unique factorization domain, then  $R[X_1, \dots, X_n]$  is a unique factorization domain.

**Corollary 4-3.** If  $k$  is a field,  $k[X_1, \dots, X_n]$  is a unique factorization domain.

**Note.** Not every unique factorization domain is a principal ideal domain. For example,  $k[X_1, \dots, X_n]$ ,  $n \geq 2$ .

**Definition 4-7.** If  $a = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$  and  $b = p_1^{\beta_1} \cdots p_t^{\beta_t}$  are prime factorizations of  $a$  and  $b$  in the unique factorization domain  $R$  where  $\alpha_i \geq 0, \beta_j \geq 0$ , then  $d = \prod_{i=1}^t p_i^{\min(\alpha_i, \beta_i)}$  is called a *greatest common divisor* (g.c.d) of  $a$  and  $b$ . It is unique up to multiplication by a unit.

**Definition 4-8.** Let  $R$  be a unique factorization domain and  $f(X) = a_0 + a_1X + \cdots + a_nX^n \in R[X]$ . Then the *content* of  $f = c(f) = g.c.d.(a_0, \dots, a_n)$ . If  $c(f) = 1$ ,  $f$  is called a *primitive polynomial*.

**Theorem 4-8.** (Gauss lemma) Let  $R$  be a unique factorization domain with quotient field  $K$ . If  $f(X) \in R[X]$  is irreducible over  $R[X]$ , then it is irreducible over  $K[X]$ .

*Proof.* Suppose  $f(X) = G(X)H(X)$  where  $G(X), H(X) \in K[X]$ . Set  $G(X) = g(X)/d$  and  $H(X) = h(X)/e$  where  $d$  and  $e$  are the least common denominators of the coefficients of  $G$  and  $H$ , respectively, and  $g(X), h(X) \in R[X]$ . Set  $p(X) = g(X)/c(g)$  so that  $p(X)$  is a primitive polynomial in  $R[X]$ . Then  $\deg f(X) = c(g)h(X)p(X)$ . But  $R[X]$  is a unique factorization domain, primes in  $R$  are primes in  $R[X]$ , and  $p(X)$  is primitive. Therefore  $de$  divides  $c(g)h(X)$  so  $f(X)$  factors over  $R[X]$ .  $\square$

### Exercise.

**4-1.** Let  $R$  be a Euclidean domain,  $a \in R$ . Prove that  $a$  is a unit in  $R$  if and only if  $d(a) = d(1)$ .

**4-2.** Prove that every prime ideal in a Euclidean domain is maximal. Show by example, that this is false for unique factorization domains.

**4-3.** Define  $d : \mathbb{Z} \rightarrow \mathbb{Z}$  by  $d(a + bi) = a^2 + b^2$ . Prove that this function gives  $\mathbb{Z}[i]$  the structure of a Euclidean domain.

**4-4.** (Factor Theorem) Let  $k$  be a field,  $a \in k$  a root of  $f(X) = 0$  where  $f(X) \in k[X]$ . Prove that  $X - a$  divides  $f(X)$ .

**4-5.** Prove that  $\mathbb{Z}[X]$  is not a principal ideal domain.

**4-6.** Prove that in a principal ideal domain, every ideal is a unique product of prime ideals.

**4-7.** Prove the remark following Theorem 4-7, that is, every unique factorization domain satisfies the ascending chain condition on principal ideals.

**4-8.** (Eisenstein's Criterion) Let  $f(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$  and suppose  $p$  is a prime number such that  $p$  divides  $a_i$  for  $i = 0, 1, \dots, n-1$ ,  $p$  does not divide  $a_n$ , and  $p^2$  does not divide  $a_0$ . Prove that  $f(X)$  is irreducible in  $\mathbb{Q}[X]$ .

**4-9.** Let  $p$  be a prime number. Prove that  $f(X) = 1 + x + x^2 + \cdots + X^{p-1} = X^p - 1/X - 1$  is irreducible in  $\mathbb{Q}[X]$ . (Hint: If  $f(X)$  factors, so does  $f(X+1)$ . Substitute  $X+1$  for  $X$  and apply Eisenstein's Criterion.)

**4-10.** A ring  $\Lambda$  is called *regular* if for any  $a \in \Lambda$ , there exists  $b \in \Lambda$  such that  $aba = a$ . Suppose  $\Lambda$ . Prove each of the following:

- (a) Every non-zero divisor of  $\Lambda$  is a unit.
- (b) Every prime ideal of  $\Lambda$  is maximal.
- (c) Every principal left ideal of  $\Lambda$  is generated by an element  $e$  satisfying  $e^2 = e$ .



## Chapter 5

# MODULES AND EXACT SEQUENCES



## Chapter 6

# NOETHERIAN RINGS AND MODULES



## Chapter 7

# DEDEKIND DOMAINS

In view of the introductory remarks to Chapter 6 and the results obtained in that chapter, we are still left with the question of describing a class of rings in which every ideal can be written (preferably uniquely) as a product of prime ideals. Since Noetherian rings yield a partial result in this direction, by replacing "product" with "intersection" and "prime" with "primary", we might expect a subclass of Noetherian rings to be the sought after type. In this chapter we characterize these rings called Dedekind domains.

**Definition 7-1.** Let  $R$  be an integral domain with quotient field  $K$ . An  $R$ -module  $0 \neq B \subseteq K$  is called a *fractionary ideal* if there exists  $d \neq 0$  in  $R$  such that  $B \neq d^{-1}R$ .

*Note.* 1. If  $B$  is a fractionary ideal, then  $B = d^{-1}A$  where  $A$  is an ordinary ideal of  $R$ . Namely,  $A = \{x \in R \mid d^{-1}x \in B\}$ .

2. Every ordinary ideal  $0 \neq A \subseteq R$  is a fractionary ideal by taking  $d = 1$ . These will now be called *integral ideals*.

3. The addition, multiplication, intersection, and quotient of fractionary ideals can be defined as they were for integral ideals in Chapter 2. The relationship among these operations carry over to fractionary ideals.

4. The ideal  $R$  acts as a unit in the multiplication of fractionary ideals.

5. If  $M$  is a  $R$ -module and  $B$  is a fractionary ideal of  $R$ , then  $BM = \{\sum_{finite} b_i m_i \mid b_i \in B, m_i \in M\}$ . Since  $B \subseteq K = R_0$  each summand  $b_i m_i$  is an element of  $M_0$  and the addition should be interpreted as taking place in  $M_0$ . Thus  $BM$  is a certain  $R$ -submodule of  $M_0$ .

**Definition 7-2.** A fractionary ideal  $A$  is called *invertible* if there exists a fractionary ideal  $A^{-1}$  such that  $AA^{-1} = R$ .

**Theorem 7-1.** If a fractionary ideal  $A$  is invertible, then  $A^{-1} = (R : A) = \{x \in K \mid xA \subseteq R\}$ . In particular,  $A^{-1}$  is unique.

*Proof.* Suppose  $AA^{-1} = R$ . Then  $A' \subseteq (R : A)$ . On the other hand,  $(R : A) = (R : A)R = (R : A)AA' \subseteq RA' = A'$  so  $A' = (R : A)$ .

**Theorem 7-2.** If every integral ideal of  $R$  is invertible, then every fractionary ideal is invertible.

*Proof.* Let  $B$  be a fractionary ideal. Then  $B = d^{-1}A$ , where  $A$  is an integral ideal. If  $A^{-1}$  is the inverse of  $A$ , then  $dA^{-1}$  is the inverse of  $B$  so  $B$  is invertible.

**Theorem 7-3.** Let  $R$  be an integral domain in which every ideal is a unique product of prime ideals and  $P$  an invertible integral prime ideal of  $R$ . Then  $P$  is maximal.

*Proof.* Let  $a \in R - P$  and set  $B = (P, a)$ ,  $C = (P, a^2)$  and  $D = (P^2, a)$ . We want to show  $B = R$ . Since  $P$  is invertible, this is equivalent to showing  $PB = P$ . Let  $B = \prod_{i=1}^s P_i$  and  $C = \prod_{j=1}^t Q_j$  be the prime factorizations of  $B$  and  $C$ . Set  $\bar{R} = R/P$  and  $\bar{I} = I/P$  for any ideal  $I$  of  $R$ . Then

$$\prod_{i=1}^s \bar{P}_i^2 = \bar{B}^2 = \bar{C} = \prod_{j=1}^t \bar{Q}_j.$$

By unique factorization in  $\bar{R}$ ,  $t = 2s$  and by relabeling, we can assume that  $\bar{Q}_{2i} = \bar{Q}_{2i-1} = \bar{P}_i$  for  $i = 1, \dots, s$ . Thus  $\bar{Q}_{2i} = \bar{Q}_{2i-1} = \bar{P}_i$  for  $i = 1, \dots, s$ , so  $\bar{B}^2 = \bar{C}$ . Therefore  $P \subseteq C = B^2 \subseteq D$ . If  $x \in P$ ,  $x = y + ra$  for some  $y \in P^2$ ,  $r \in R$ . Then  $ra = x - y \in P$  and  $a \notin P$  so  $r \in P$ . Therefore  $P \subseteq (P^2, Pa) = PB$ . The inclusion  $PB \subseteq P$  is obvious and so  $PB = P$ .

**Theorem 7-4.** Let  $R$  be a local principal ideal domain with maximal ideal  $\mathfrak{m}$

## Chapter 8

# ARTIN RINGS AND MODULES

In this chapter and the following chapter  $\lambda$  will denote an arbitrary ring with unit element, not necessarily commutative.

**Lemma 8-1.** Let  $A$  be a left ideal of a ring  $\lambda$  such that every element of the set  $1 + A = \{1 + a \mid a \in A\}$  has a left inverse in  $\lambda$ . Then every element of  $1 + A$  is a unit in  $\lambda$ .

*Proof.*

□



## Chapter 9

# SEMISIMPLE RINGS

