

Topics in Ring Theory

Jacob Barshay

Contents

1 Preliminary Terminology and Examples	3
*	

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 $a \leq c$, 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 Λ on which are defined two binary operations $+$ and \cdot satisfying the following conditions :

- (1) Λ 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 Λ ;
- (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) and (6) is called a *ring with unit* ;
- (c) (5) and (7) is called a *commutative ring with unit* ;
- (d) (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 Λ and Λ' 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. Δ , 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 Δ , 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 Δ 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 α , 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 Λ 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 Λ . C is called the *center* of Λ .

1-6. Let Λ be a ring and let Γ denote the set $\mathbb{Z} \times \Lambda$. Define operations in Γ 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 Λ . Similarly for nx . Show that Γ is a ring with unit element $(1, 0)$. Furthermore, Γ is commutative if and only if Λ is commutative. Finally, consider the map $\varphi : \Lambda \rightarrow \Gamma$ given by $\varphi(x) = (0, x)$. Prove that φ is a monomorphism and that if Λ possesses a unit element, φ 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.

