Introduction to Rings

Definitions and Examples

This section of notes roughly follows Sections 7.1–7.3 in Dummit and Foote.

Recall that a group is a set together with a single binary operation, which together satisfy a few modest properties. Loosely speaking, a ring is a set together with two binary operations (called addition and multiplication) that are related via a distributive property.

Definition 1. A **ring** R is a set together with two binary operations $+$ and $\times$ (called **addition** and **multiplication**, respectively) satisfying the following:

(i) $(R,+)$ is an abelian group.

(ii) $\times$ is associative: $(a\times b)\times c = a\times(b\times c)$ for all $a,b,c\in R$.

(iii) The **distributive property** holds: $a\times(b+c) = (a\times b)+(a\times c)$ and $(a+b)\times c = (a\times c)+(b\times c)$ for all $a,b,c\in R$.

Note 2. We make a couple comments about notation.

(1) We write ab in place $a\times b$.

(2) The additive inverse of the ring element $a\in R$ is denoted $-a$.

Theorem 3. Let R be a ring. Then for all $a,b\in R$:

(1) $0a = a0 = 0$

(2) $(-a)b = a(-b) = -(ab)$

(3) $(-a)(-b) = ab$

Definition 4. A ring R is called **commutative** if multiplication is commutative.

Definition 5. A ring R is said to have an **identity** (or called a **ring with 1**) if there is an element $1\in R$ such that $1\times a = a\times 1 = a$ for all $a\in R$.

Theorem 6. If R is a ring with 1, then the multiplicative identity is unique and $-a = (-1)a$.

Question 7. Requiring $(R,+)$ to be a group is fairly natural, but why require $(R,+)$ to be abelian? Here's one reason. Suppose R has a 1. Compute $(1+1)(a+b)$ in two different ways.

Definition 8. A ring R with 1 (with $1\neq 0$) is called a **division ring** if every nonzero element in R has a multiplicative inverse: if $a\in R\setminus\{0\}$, then there exists $b\in R$ such that $ab = ba = 1$.

Definition 9. A commutative division ring is called a **field**.

Definition 10. A nonzero element a in a ring R is called a **zero divisor** if there is a nonzero element $b\in R$ such that either $ab = 0$ or $ba = 0$.

Theorem 11 (Cancellation Law)**.** Assume $a, b, c \in R$ such that a is not a zero divisor. If $ab = ac$, then either $a = 0$ or $b = c$.

Definition 12. Assume R is a ring with 1 with $1 \neq 0$. An element $u \in R$ is called a **unit** in R if u has a multiplicative inverse (i.e., there exists $v \in R$ such that $uv = vu = 1$. The set of units in R is denoted $R^\times$.

Theorem 13. If $R^\times \neq \emptyset$, then $R^\times$ forms a group under multiplication.

Note 14. We make a few observations.

(1) A field is a commutative ring F with identity $1 \neq 0$ in which every nonzero element is a unit, i.e., $F^\times = F \setminus \{0\}$.

(2) Zero divisors can never be units.

(3) Fields never have zero divisors.

Definition 15. A commutative ring with identity $1 \neq 0$ is called an **integral domain** if it has no zero divisors.

Note 16. The Cancellation Law (Theorem 11) holds in integral domains for any three elements.

Corollary 17. Any finite integral domain is a field.

Proof. For any nonzero $a \in R$, define $f_a : R \to R$ via $f_a(x) = ax$. If R is an integral domain, the Cancellation Law forces f_a to be injective. If R is finite, then f_a is also surjective. In this case, there exists $b \in R$ such that $ab = 1$. □

Example 18. Here are some examples of rings. Details left as an exercise.

(1) **Zero Ring**: If $R = \{0\}$, we can turn R into a ring in the obvious way. The zero ring is a finite commutative ring with 1. It is the only ring where the additive and multiplicative identities are equal. The zero ring is not a division ring, not a field, and not an integral domain.

(2) **Trivial Ring:** Given any abelian group R, we can turn R into a ring by defining multiplication via $ab = 0$ for all $a, b \in R$. Trivial rings are commutative rings in which every nonzero element is a zero divisor. Hence a trivial ring is not a division ring, not a field, and not a integral domain.

(3) The integers $\mathbb{Z}$ form a ring under the usual operations of addition and multiplication. The integers form an integral domain, but $\mathbb{Z}$ is not a division ring, and hence not a field.

(4) The rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$ are fields under the usual operations of addition and multiplication.

(5) For $n \geq 1$, the set $\mathbb{Z}_n$ is a commutative ring with 1 under the operations of addition and multiplication mod n. The group of units $\mathbb{Z}_n^\times$ is the set of elements in $\mathbb{Z}_n$ that are relatively prime to n. All other nonzero elements are zero divisors. It turns out that $\mathbb{Z}_n$ forms a finite field iff n is prime.

(6) The set of even integers $2\mathbb{Z}$ forms a commutative ring under the usual operations of addition and multiplication. However, $2\mathbb{Z}$ does not have a 1, and hence cannot be a division ring nor a field nor an integral domain.

(7) **Polynomial Ring:** Fix a commutative ring R. Let $R[x]$ denote the set of polynomials in the variable x with coefficients in R. Then $R[x]$ is a commutative ring with 1. The units of $R[x]$ are exactly the units of R (if there are any). So, $R[x]$ is never a division ring nor a field. However, if R is an integral domain, then so is $R[x]$.

(8) **Matrix Ring:** Fix a ring R and let n be a positive integer. Let $M_n(R)$ be the set of $n \times n$ matrices with entries from R. Then $M_n(R)$ forms a ring under ordinary matrix addition and multiplication. If R is nontrivial and $n \geq 2$, then $M_n(R)$ always has zero divisors and $M_n(R)$ is not commutative even if R is. If R has a 1, then the matrix with 1's down the diagonal and 0's elsewhere is the multiplicative identity in $M_n(R)$. In this case, the group of units is the set of invertible $n \times n$ matrices, denoted $GL_n(R)$ and called the **general linear group of degree n over R.**

(9) **Quadratic Field:** Define $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. It turns out that $\mathbb{Q}(\sqrt{2})$ is a field. In fact, we can replace 2 with any rational number that is not a perfect square in $\mathbb{Q}$.

(10) **Hamilton Quaternions:** Define $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}, i, j, k \in Q_8\}$ Then $\mathbb{H}$ forms a ring, where addition is definite componentwise in i, j, and k and multiplication is defined by expanding products and the simplifying using the relations of Q_8. It turns out that $\mathbb{H}$ is a non-commutative ring with 1.

Definition 19. A **subring** of a ring R is a subgroup of R that is closed under multiplication.

Note 20. The property "is a subring" is clearly transitive. To show that a subset S of a ring R is a subring, it suffices to show that $S \neq \emptyset$, S is closed under subtraction, and S is closed under multiplication.

Example 21. Here are a few quick examples.

(1) $\mathbb{Z}$ is a subring of $\mathbb{Q}$, which is a subring of $\mathbb{R}$, which in turn is a subring of $\mathbb{C}$.

(2) $2\mathbb{Z}$ is a subring of $\mathbb{Z}$.

(3) The set $\mathbb{Z}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{Q}(\sqrt{2})$.

(4) The ring R is a subring of $R[x]$ if we identify R with set of constant functions.

(5) The set of polynomials with zero constant term in $R[x]$ is a subring of $R[x]$.

(6) $\mathbb{Z}[x]$ is a subring of $\mathbb{Q}[x]$.

(7) $\mathbb{Z}_n$ is *not* a subring of $\mathbb{Z}$.

Definition 22. Let R and S be rings. A **ring homomorphism** is a map $\phi : R \to S$ satisfying

(i) $\phi(a + b) = \phi(a) + \phi(b)$

(ii) $\phi(ab) = \phi(a)\phi(b)$

for all $a, b \in R$. The **kernel** of ϕ is defined via $\ker(\phi) = \{a \in R \mid \phi(a) = 0\}$. If ϕ is a bijection, then ϕ is called an **isomorphism**, in which case, we say that R and S are **isomorphic rings** and write $R \cong S$.

Example 23.

(1) For $n \in \mathbb{Z}$, define $\phi_n : \mathbb{Z} \to \mathbb{Z}$ via $\phi_n(x) = nx$. We see that $\phi_n(x + y) = n(x + y) = nx + ny = \phi_n(x) + \phi_n(y)$. However, $\phi_n(xy) = n(xy)$ while $\phi_n(x)\phi_n(y) = (nx)(ny) = n^2xy$. It follows that ϕ_n is a ring homomorphism exactly when $n \in \{0, 1\}$.

(2) Define $\phi : \mathbb{Q}[x] \to \mathbb{Q}$ via $\phi(p(x)) = p(0)$ (called **evaluation at 0**). It turns out that ϕ is a ring homomorphism, where $\ker(\phi)$ is the set of polynomials with 0 constant term.

Theorem 24. Let $\phi : R \to S$ be a ring homomorphism.

(1) $\phi(R)$ is a subring of S.

(2) $\ker(\phi)$ is a subring of R.

In fact, we can say something even stronger about the kernel of a ring homomorphism, which will lead us to the notion of an **ideal**.

Theorem 25. Let $\phi : R \to S$ be a ring homomorphism. If $\alpha \in \ker(\phi)$ and $r \in R$, then $\alpha r, r\alpha \in \ker(\phi)$. That is, $\ker(\phi)$ is closed under multiplication by elements of R.