Ring Theory.

Alec Zabel-Mena

October 24, 2022

Contents

Chapter 1

Rings.

1.1 Definitions and Examples.

Definition. A **ring** R is a set together with two binary operations $+ : (a, b) \to a + b$ and $\cdot : (a, b) \to ab$ called **additon** and **multiplication** such that:

(1) R is an Abelian group over $+$, where we denote the identity element as 0 and the inverse of each $a \in R$ as $-a$.

(2) R is closed under $\cdot$ and $\cdot$ is associative. That is, $ab \in R$ whenever $a, b \in R$ and $a(bc) = (ab)c$.

(3) $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

If $ab = ba$ for all $a, b \in R$, then we call R **commutative**. If there exists an element $1 \in R$ such that $a_1 = 1a = R$, then we call R a ring with **unit**.

Definition. A ring R with identity $1 \neq 0$ is called a **division ring** if for all $a \in R$, where $a \neq 0$, there exists a $b \in R$ such that $ab = ba = 1$. We call a commutative division ring a **field**.

Example 1.1. Let R be an abelian group under an operation $+$, define the operation $\cdot$ by $(a, b) \to ab = 0$ for all $a, b \in R$. Then R is a ring under $+$ and $\cdot$, called the **trivial ring**. If $R = \langle e \rangle$, the trivial group, then we call R the **zero ring**.

(2) The integers $\mathbb{Z}$ form a ring under the usual addition and muiltiplication.

(3) The sets of rational numbers $\mathbb{Q}$ and the set of real numbers $\mathbb{R}$ are rings under their usual addition and multiplication; in fact, they are fields. The complex numbers $\mathbb{C}$ also form a field under complex addition and complex multiplication, where

$$+ : (a + ib, c + id) \to (a + c) + i(b + d)$$
$$\cdot : (a + ib, c + id) \to (ac - bd) + i(ad + bc)$$

(4) The factor group of integers modulo n, $\mathbb{Z}/_{n\mathbb{Z}}$ is a commutative ring under addition modulo n, and multiplication modulo n, $\mathbb{Z}/_{n\mathbb{Z}}$ has unit $1 \mod n$. $\mathbb{Z}/_{n\mathbb{Z}}$ forms a field if, and only if $n = p^r$, where p is a prime.

(5) We define the **real quaternions** to be the set $\mathbb{H} = \{a + ib_jc_kd : a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = -1 \text{ and } ij = k, jk = i, \text{ and } ki = j\}$. $\mathbb{H}$ is a ring under addition and multiplication are defined for all $x = a + ib + jc + kd$ and $y = e + if + jg + kh$ to be:

$$+(x, y) : \to x + y = (a + e) + i(b + f) + j(c + g) + k(d + h)$$
$$\cdot(x, y) : \to xy = (a + ib + jc + kd)(e + if + jg + kh)$$

(6) Let A be a ring and R the set of all maps $f : X \to A$. Then R forms a ring under function addition $f + g(x) = f(x) + g(x)$ and function multiplication $fg(x) = f(x)g(x)$. Notice that R is commutative if, and only if A is, moreover, R has unit if, and only if A has unit.

(7) We say a realvalued function $f : \mathbb{R} \to \mathbb{R}$ has **compact support** if there exist $a, b \in \mathbb{R}$ such that $f(x) = 0$ for all $x \notin [a, b]$. The set of all functions with compact support forms a ring without unit under function addition and function multiplication.

(8) Let $X, Y \subseteq \mathbb{R}$. We denote the set of all continuous functions $f : X \to Y$ by $C(X, Y)$. Then $C(X, Y)$ forms a commutative ring with unit under function addition and function multiplication.

Lemma 1.1.1. *Let R be a ring. Then the following are true for all $a, b \in R$.*

(1) $0a = a0 = 0$.

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

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

(4) If R has unit $1 \neq 0$, then 1 is unique and $-a = (-1)a$.

Proof. (1) Notice $0a = (0 + 0)a = 0a + 0a$, so that $0a = 0$. Likewise, $a0 = 0$ by the same reasoning.

(2) Notice that $b - b = 0$, so $a(b - b) = ab + a(-b) = 0$, so that $a(-b) = -(ab)$. The same argument with $(a - a)b$ gives $(-a)b = -(ab)$.

(3) By the inverse laws of addition in R, we have $-(a(-b)) = -(-(ab))$, so that $(-a)(-b) = ab$.

(4) Suppose R has unit $1 \neq 0$, and suppose there is an element $2 \in R$ for which $2a = a2 = a$ for all $a \in R$. Then we have that $1 \cdot 2 = 1$ and $1 \cdot 2 = 2$, making $1 = 2$; so 1 is unique. Now, we have that $a + (-a) = 0$, so that $1(a + (-a)) = 1a + 1(-a) = 1a + (-a) = 0$ So $(-a) = -(1a) = (-1)a$ by (2).

■

Definition. Let R be a ring. We call an element $a \in R$ a **zero divisor** if $a \neq 0$ and there exists an element $b \neq 0$ such that $ab = 0$. Similarly, we call $a \in R$ a **unit** if there is a $b \in R$ for which $ab = ba = 1$.

Example 1.2. Notice if R is a ring with unit 1, then 1 is a unit of R by definition.

Definition. Let R be a ring. We call the set of all units in R the **group of units** and denote it R^*

Lemma 1.1.2. *Let R be a ring with unit $1 \neq 0$. Then the group of units $R^\times$ forms a group.*

Proof. Let $a, b \in R$ be units in R. Then there are $c, d \in R$ for which $ac = ca = 1$ and $bd = db = 1$. Consider then ab. Then $ab(dc) = a(bd)c = ac = 1$ and $(dc)ab = d(ca)b = db = 1$ so that ab is also a unit in R. Moreover R^* inherits the associativity of $\cdot$ and 1 serves as the identity element of R^*. Lastly, if $a \in R^*$ is a unit there is a $b \in R$ for which $ab = ba = 1$. This also makes b a unit in R, and the inverse of a. ■

Corollary. *a is a zero divisor if, and only if it is not a unit.*

Proof. Suppose that $a \neq 0$ is a zero divisor. Then there is a $b \in R$ such that $b \neq 0$ and $ab = 0$. Then for any $v \in R$, $v(ab) = (va)b = 0$ so that a cannot be a unit. On the other hand let a be a unit, and $ab = 0$ for some $b \neq 0$. Then there is a $v \in R$ for which $v(ab) = (va)b = 1b = b = 0$. Then $b = 0$ which is a contradiction. ■

Corollary. *If R is a field, then it has no zero divisors.*

Proof. Notice by definition of a field, every element is a unit, except for 0. ■

Example 1.3.
(1) $\mathbb{Z}$ has no zero divisors, and has as units the elements -1 and 1.

(2) For any $n \in \mathbb{Z}^+$, the units of $\mathbb{Z}/n\mathbb{Z}$ are all elements $a \mod n$ such that $(a, n) = 1$. That is $\mathbb{Z}/n\mathbb{Z}^* = U(\mathbb{Z}/n\mathbb{Z})$; recall that $U(\mathbb{Z}/n\mathbb{Z})$ is called the unit group, or group of units of $\mathbb{Z}/n\mathbb{Z}$.

(3) Let $D \in \mathbb{Q}$ be squarefree. Define $\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} : a, b \in \mathbb{Q}\}$. Then $\mathbb{Q}(\sqrt{D})$ is a field called the **quadratic field** under the operations

$$
\begin{aligned}
+ &: (a + b\sqrt{D}, c + d\sqrt{D}) \to (a + c) + (b + d)\sqrt{D} \\
&\cdot((a + b\sqrt{D}, c + d\sqrt{D})) \to (ac - bdD) + (ad - bc)\sqrt{D}
\end{aligned}
$$

Since $\mathbb{Q}(\sqrt{D})$ is a field, every element is a unit.

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

Lemma 1.1.3. *Let R be a ring, and a not a zero divisor. Then if $ab = ac$, then either $a = 0$, or $b = c$.*

Proof. Notice that $ab = ac$ implies $ab - ac = a(b - c) = 0$. Since a is not a zero divisor, either $a = 0$ or $b - c = 0$. ∎

Corollary. *Any finite integral domain is a field.*

Proof. Let R be a finite integral domain and consider the map on R, by $x \to ax$. By above, this map is 1–1, moreover since R is finite, it is also onto. So there is a $b \in R$ for which $ab = 1$, making a a unit. Since a is abitrarily chosen, this makes R a field. ∎

Corollary. *If R is a field it is a (not necessarily finite) integral domain.*

Example 1.4. We have that fields are integral domains, and finite integral domains are fields. However, notice that not every integral domain need be a field. $\mathbb{Z}$ is an integral domain that is not a field. Moreover, so are the real quaternions $\mathbb{H}$.

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

Example 1.5. (1) We have the following sequence of subgrings $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

(2) The factor group $\mathbb{Z}/n\mathbb{Z}$ is not a subgring of $\mathbb{Z}$, well the multiplication and addition of $\mathbb{Z}$ is different from that of $\mathbb{Z}/n\mathbb{Z}$.

(3) The set $\mathbb{Z} + i\mathbb{Z} + j\mathbb{Z} + k\mathbb{Z} \subseteq \mathbb{H}$ is a subring of $\mathbb{H}$.

(4) If F is a field, then any subring of F is also an integral domain by inheretence.

(5) The set $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} : a, b \in \mathbb{Z}\}$ is a subring of the quadratic field $\mathbb{Q}(\sqrt{D})$. Moreover if $D \equiv 1 \mod 4$, then the set

$$\mathbb{Z}[\frac{1+\sqrt{D}}{2}] = \{a + b\frac{1+\sqrt{D}}{2} : a, b \in \mathbb{Z}\}$$

is also a subgring of $\mathbb{Q}(\sqrt{D})$. We call the subgring $\mathbb{Z}[\omega]$, where

$$\omega = \begin{cases} \sqrt{D}, \text{ if } D \not\equiv 1 \mod 4 \\ \frac{1+\sqrt{D}}{2}, \text{ if D} \equiv 1 \mod 4 \end{cases}$$

the **ring of integers** in the quadratic field. When $D = -1$, we get the ring $\mathbb{Z}[i]$, with $i^2 = -1$ and call it the **Gaussian integers**. Notice then that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$; in fact, it is field in $\mathbb{C}$.

Bibliography

[1] D. Dummit, *Abstract algebra.* Hoboken, NJ: John Wiley & Sons, Inc, 2004.

[2] I. N. Herstein, *Topics in algebra.* New York: Wiley, 1975.