1 Introduction to Rings

Definition 1.1 [Ring (p.245)] A *ring* R is a set with two binary operations, addition (denoted by $a+b$) and multiplication (denoted by ab), such that for all $a, b, c \in R$:

1. $a+b=b+a$.

2. $(a+b)+c=a+(b+c)$.

3. There is an additive identity 0. That is, there is an element $0 \in R$ such that $a+0=a$ for all $a \in R$.

4. There is an element $-a \in R$ such that $a+(-a)=0$.

5. $a(bc)=(ab)c$.

6. $a(b+c)=ab+ac$ and $(b+c)a=ba+ca$.

Hence, a ring is an Abelian group under addition, also having an associative multiplication that is left and right distributive over addition.

- When $ab=ba$ for all $a, b \in R$, R is called *commutative*, or a *commutative ring.*
- A *unity* (or *identity*) in a ring is a nonzero element that is an identity under multiplication.
- An element of a ring with a unity is called a *unit* if it has a multiplicative inverse. When R is a ring $U(R)=\{u \in R \mid \exists v \in R \text{ s.t. } uv=1=vu\}$ forms a group called *the unit group, or the group of units* of R. (Exercise 22)
- When n is a positive integer we write $n \cdot a$ or na for $a+a+\cdots+a$ with n summands. By convention we write $(-n) \cdot a$ for $n(-a)=-(n \cdot a)$ when n is a nonnegative integer. (Exercise 16)

Example 1.1 1. $\boldsymbol{Z}$. $U(\boldsymbol{Z})=\{\pm 1\}$.

2. $\boldsymbol{Z}_n$. $U(\boldsymbol{Z}_n)=\boldsymbol{Z}_n^*=U(n)$.
3. $\boldsymbol{Z}[x]$. $U(\boldsymbol{Z}[x])=\{\pm 1\}$. (Exercise 25)
4. $M_2(\boldsymbol{Z})$. $U(M_2(\boldsymbol{Z}))=\{A \in M_2(\boldsymbol{Z}) \mid \det(A)=\pm 1\}$. (Exercise 20)
5. $2\boldsymbol{Z}$. *No unity.*
6. All continuous real-valued functions f of a real variable such that $f(1)=0$[1]. Binary operations are defined by $(f+g)(x)=f(x)+g(x)$ and $(fg)(x)=f(x)g(x)$. *No unity*
7. Let $R_1, R_2, \ldots, R_n$ be rings. Then the *direct sum* is defined by coordinate wise operation on the set:

$$R_1 \oplus R_2 \oplus \cdots \oplus R_n=\{(a_1, a_2, \ldots, a_n) \mid a_i \in R_i\}.$$

What is $U(R)$? (Exercise 24)

[1]Why do you think we assume this condition?

Proposition 1.1 (Theorem 12.1) [2] *Let R be a ring and $a, b, c \in R$. Then*

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

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

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

(iv) $a(b - c) = ab - ac$ *and* $(b - c)a = ba - ca$[3].

if R has a unity element 1*, then*

(v) $(-1)a = -a$.[4]

(vi) $(-1)(-1) = 1$.

(vii) *If a ring has a unity, it is unique. If a ring element has a multiplicative inverse, it is unique.* (Theorem 12.2, Exercise 5)

Proof. [Exerises]
(i) $a0 = a(0+0) = a0+a0$. Hence $0 = a0+(-a0) = (a0+a0)+(-a0) = a0+(a0+(-a0)) = a0 = 0 = a0$. $0a = 0$ is similar.
(ii) $ab + a(-b) = a(b + (-b)) = a0 = 0$. Since in a group the inverse of each element is unique, $a(-b) = -(ab)$. $(-a)b = -(ab)$ is similar.
(iii) $(-a)(-b) = -((-a)b) = -(-(ab)) = ab$. Note that in general $-(-a) = a$.
(iv) $a(b - c) = a(b + (-c)) = ab + a(-c) = ab + (-ac) = ab - ac$. $(b - c)a = ba - ca$ is similar.
(v) This follows from (ii).
(vi) This follows from (v).
(vii) The proof is same as in the case of a group. ■

Note. A ring need not have a multiplicative identity, and even if it has a multiplicative identity it need not have multiplicative inverses. $ab = ac$ does not imply $b = c$ even if $a \neq 0$. This holds if a is a unit.[5]

For example in $\boldsymbol{Z}_6$, $3 \cdot 4 = 3 \cdot 2 = 0$.

Definition 1.2 [Subring (p.248)] A subset S of a ring R is a *subring* of R if S is itself a ring with the operations of R. $\{0\}$ and R are always subrings and are called the *trivial subrings* of R.

Proposition 1.2 (Theorem 12.3) *A nonempty subset S of a ring R is a subring if S is closed under subtraction and multiplication – that is if $a - b$ and ab are in S, whenever $a, b \in S$.*

Example 1.2 1. $\{0, 2, 4\} \in \boldsymbol{Z}_6$ is a subring. Although 1 is the unity in $\boldsymbol{Z}_6$, 4 is the unity in $\{0, 2, 4\}$.

$$4 \cdot 0 = 0, 4 \cdot 2 = 2, \text{ and } 4 \cdot 4 = 4.$$

[2] If you have not taken Algebra I, please write out your proof confirming which condition in Definition 1.1 is used in each step.
[3] For $a, b \in R$, we write $a - b$ for $a + (-b)$ as in Abelian groups.
[4] There are two meanings of this formula.
[5] Do we always need this condition?

2. $n\boldsymbol{Z}$ is subring of $\boldsymbol{Z}$ for each positive integer n.

3. $\boldsymbol{Z}[i]$, where $i = \sqrt{-1}$[6], is a subring of $\boldsymbol{C}$. $U(\boldsymbol{Z}[i]) = \{\pm 1, \pm i\}$. (Exercise 23)[7]

Further Readings

1. B. Erickson, Orders for Finite Noncommutative Rings, American Mathematical Monthly 73 (1966), 376–377.

2. K. E. Eldridge, Orders for Finite Noncommutative Rings with Unity, American Mathematical Monthly 75 (1968), 512–514.

[6] In this textbook, i is an element in a larger ring such that $i^2 = -1$

[7] $O_d = \boldsymbol{Z}[\sqrt{d}]$ if $d \equiv 2, 3\ (4)$ and $\{\frac{a+b\sqrt{d}}{2} \mid a, b \in \boldsymbol{Z}, a \equiv b\ (2)\}$ otherwise.