CHAPTER 6

Rings

Consider the set $\mathbb{Z}$ of integers and the operation addition and multiplication. We already note that $(\mathbb{Z}, +)$ forms an abelian group. We also take the following for granted:

(i) For every $x, y \in \mathbb{Z}$, $xy \in \mathbb{Z}$.
(ii) For every $x, y, z \in \mathbb{Z}$, $(xy)z = x(yz)$.
(iii) For every $x, y, z \in \mathbb{Z}$, $x(y + z) = xy + xz$.
(iv) For every $x, y, z \in \mathbb{Z}$, $(x + y)z = xz + yz$.

Consider now the set $\mathcal{M}_{2,2}(\mathbb{R})$ of 2×2 matrices with entries in $\mathbb{R}$. We already note that $\mathcal{M}_{2,2}(\mathbb{R})$ forms an abelian group under matrix addition. We also take the following for granted:

(i) For every $A, B \in \mathcal{M}_{2,2}(\mathbb{R})$, $AB \in \mathcal{M}_{2,2}(\mathbb{R})$.
(ii) For every $A, B, C \in \mathcal{M}_{2,2}(\mathbb{R})$, $(AB)C = A(BC)$.
(iii) For every $A, B, C \in \mathcal{M}_{2,2}(\mathbb{R})$, $A(B + C) = AB + AC$.
(iv) For every $A, B, C \in \mathcal{M}_{2,2}(\mathbb{R})$, $(A + B)C = AC + BC$.

There are many more examples of sets and operations which have properties analogous to the above. This apparent similarity leads us to consider an abstract object which will incorporate all these individual cases as examples. We say that all these examples have a ring structure.

6.1. Formal Definition

DEFINITION. A set R, together with two binary operations $+$ (addition) and $\cdot$ (multiplication), is said to form a ring, denoted by $(R, +, \cdot)$, if the following properties are satisfied:

(R1–5) (Abelian group) $(R, +)$ is an abelian group.
(R6) (Closure) For every $x, y \in R$, $x \cdot y \in R$.
(R7) (Associativity) For every $x, y, z \in R$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
(R8) (Left distribution) For every $x, y, z \in R$, $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.
(R9) (Right distribution) For every $x, y, z \in R$, $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$.

REMARKS. (1) We usually omit the symbol $\cdot$ and simply write xy for $x \cdot y$. Also the operation $+$ is usually understood, so that we refer to a ring R instead of to a ring $(R, +, \cdot)$.
(2) We also omit brackets and write $xy + xz$ instead of $(xy) + (xz)$.
(3) We denote by 0 the additive identity and by $-x$ the additive inverse of an element x.

EXAMPLES. (1) $\mathbb{Z}$, $\mathbb{R}$, $\{0\}$ and $\mathcal{M}_{2,2}(\mathbb{R})$ are all rings.
(2) For every $n \in \mathbb{N} \setminus \{1\}$, the set $\mathbb{Z}_n$, together with addition and multiplication modulo n, forms a ring.

6.2. Elementary Properties

There are a few simple consequences which can be easily deduced from the definition of a ring.

PROPOSITION 6.1. *Suppose that R is a ring, and that $x, y \in R$. Then*

(i) $0x = x0 = 0$;

(ii) $(-x)y = x(-y) = -(xy)$; *and*
(iii) $(-x)(-y) = xy$.

PROOF. (i) Note that $0x + xx = (0 + x)x = xx = 0 + xx$ in view of (R6), (G1), (R9) and (G3). It follows that $0x = 0$ in view of right cancellation for groups. The proof of $x0 = 0$ is similar.

(ii) Note that $(-x)y + xy = ((-x) + x)y = 0y = 0$ in view of (R6), (G1), (R9), (G4) and (i). By the uniqueness of the additive inverse, we must have $(-x)y = -(xy)$. The proof of $x(-y) = -(xy)$ is similar.

(iii) Note that $(-x)(-y) = -(x(-y)) = x(-(-y))$ in view of (ii). Since R is a group under addition, we must have $-(-y) = y$. The result follows. ◯

6.3. Subrings

DEFINITION. Suppose that R is a ring, and that $S \subseteq R$. Then we say that S is a subring of R if S, under the same binary operations addition and multiplication, forms a ring.

THEOREM 6.2. *Suppose that R is a ring, and that S is a non-empty subset of R. Then S is a subring of R if the following conditions are satisfied:*

(SR) *For every $x, y \in S$, $xy \in S$.*
(SG) *For every $x, y \in S$, $x + (-y) \in S$.*

PROOF. Clearly S forms an abelian group under addition, in view of (SG) and Theorem 1.5. On the other hand, (R6) is simply (SR). (R7)–(R9) clearly hold in S, since they hold in R and S is a subset of R. ◯

EXAMPLES. (1) Let $S = \{3n : n \in \mathbb{Z}\}$. Then S is a subring of $\mathbb{Z}$.
(2) Let $S = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$. Then S is a subring of $\mathbb{R}$.

6.4. Further Properties

DEFINITION. Suppose that R is a ring. A non-zero element $x \in R$ is said to be a zero divisor of R if there exists a non-zero element $y \in R$ such that $xy = 0$.

EXAMPLE. In $\mathbb{Z}_4$, the element 2 is a zero divisor, for $2 \cdot 2 = 0$ in $\mathbb{Z}_4$.

DEFINITION. A ring R is said to be commutative if the following extra property is satisfied:

(RC) For every $x, y \in R$, $xy = yx$.

DEFINITION. Suppose that R is a ring. An element $1 \in R$ is said to be a unity in R if $1 \neq 0$ and $x1 = 1x = x$ for every $x \in R$.

EXAMPLE. $\mathbb{Z}_4$ is a commutative ring with unity 1.

DEFINITION. A ring R is said to be an integral domain if the following three properties are satisfied:

(ID1) R is a commutative ring.
(ID2) R contains a unity element.
(ID3) R has no zero divisors.

EXAMPLE. Let $n \in \mathbb{N} \setminus \{1\}$. Then $\mathbb{Z}_n$ is an integral domain if and only if n is prime. To see this, suppose that n is a prime. Write $n = p$. Then $x, y \in \{1, 2, \ldots, p-1\}$ for all non-zero elements $x, y \in \mathbb{Z}_p$, so we cannot have $p \mid xy$ in $\mathbb{Z}$, for otherwise $p \mid x$ or $p \mid y$ in $\mathbb{Z}$, a contradiction. It follows that $xy \neq 0$ in $\mathbb{Z}_p$. Suppose now that n is not a prime. Then $n = xy$ in $\mathbb{Z}$ for some $x, y \in \{2, 3, \ldots, n-1\}$, so that $xy = 0$ in $\mathbb{Z}_n$.

DEFINITION. A ring R is said to be a field if the following three properties are satisfied:

(F1) R is a commutative ring.
(F2) R contains a unity element 1.
(F3) For every non-zero element $x \in R$, there exists an element $x^{-1} \in R$ such that $x^{-1}x = 1$.

To show that a field is an integral domain, we have the following simple result.

PROPOSITION 6.3. *Suppose that R is a commutative ring, and that $x \in R$. Suppose further that there exists an element $x^{-1} \in R$ such that $x^{-1}x = 1$. Then x is not a zero divisor.*

PROOF. Suppose that $xy = 0$. Then $x^{-1}(xy) = 0$ by Proposition 6.1(i). On the other hand, it follows from our assumption, (R7) and the definition of 1 that $x^{-1}(xy) = (x^{-1}x)y = 1y = y$, whence $y = 0$. ◯

EXAMPLE. Let $n \in \mathbb{N} \setminus \{1\}$. Then $\mathbb{Z}_n$ is a field if and only if n is prime. To see this, suppose that n is a not a prime. Then we have already shown that $\mathbb{Z}_n$ has zero divisors, and so cannot be a field in view of (F3) and Proposition 6.3. On the other hand, if n is a prime, then writing $n = p$, we know that any congruence $yx \equiv 1 \pmod{p}$ in $\mathbb{Z}$ is soluble for $y \in \mathbb{Z}$. It follows that x has multiplicative inverse in $\mathbb{Z}_p$.

The last part of our example can also be justified by the following result.

PROPOSITION 6.4. *Every finite integral domain is a field.*

REMARK. $\mathbb{Z}$ is an integral domain but not a field.

PROOF OF THEOREM 6.4. Suppose that R is a finite integral domain. Write $R = \{x_1, \ldots, x_k\}$, where $k \in \mathbb{N}$. Let $x \in R$ be non-zero, and consider the set

$$\mathcal{S} = \{x_1x, \ldots, x_kx\}.$$

Note that for every $j = 1, \ldots, k$, we have $x_jx \neq 0$, for otherwise x is a zero divisor. On the other hand, for every $i, j = 1, \ldots, k$, we have $x_ix \neq x_jx$, for otherwise it follows from Proposition 6.1(ii) that $x_ix = -(x_jx) = (-x_j)x$, and so $(x_i + (-x_j))x = 0$. Since R has no zero divisors, it follows that either $x = 0$ or $x_i = x_j$, a contradiction. Hence we conclude that

$$\mathcal{S} = \{x_1, \ldots, x_k\}.$$

Note now that $1 \in \mathcal{S}$. It follows that there exists precisely one $j = 1, \ldots, k$ such that $x_jx = 1$. ◯

The idea of the proof can also be used to prove the following result.

PROPOSITION 6.5. *Suppose that R is an integral domain, and that $a, x, y \in R$. Suppose further that $a \neq 0$. Then*

(i) (Left cancellation) *if $ax = ay$, then $x = y$; and*
(ii) (Right cancellation) *if $xa = ya$, then $x = y$.*

Problems for Chapter 6

1. Suppose that R is a ring, and that $a \in R$. Prove that $S = \{ax : x \in R\}$ is a subring of R.
2. Suppose that R is a ring, and that $a \in R$. Prove that $S = \{x \in R : ax = 0\}$ is a subring of R.
3. Suppose that R is a ring, and that S and T are subrings of R.
   (i) Prove that $S \cap T$ is a subring of R.
   (ii) Is $S \cup T$ is a subring of R? Justify your assertion.
4. Suppose that S is a subring of $\mathbb{R}$. Show that the set $\mathcal{M}_{2,2}(S)$ of 2×2 matrices with entries in S is a subring of $\mathcal{M}_{2,2}(\mathbb{R})$.
5. Suppose that R is an integral domain, and that $a, b \in R$ with $a \neq 0$.
   (i) Show that there is at most one $x \in R$ satisfying $ax + b = 0$.
   (ii) Comment on the case when R is a field.
6. Show that there is no field of 6 elements.
7. For every $n \in \mathbb{N} \setminus \{1\}$, determine all the invertible elements and zero divisors of the ring $\mathbb{Z}_n$.
8. Show that the subring $\{0, 2, 4, 6, 8\}$ of $\mathbb{Z}_{10}$ has unity.
   [*Comment*: This example shows that a unity in a subring need not be the unity in the ring.]