Plan

- Section 18. Rings and Fields

Definition 18.1. A ring $(R, +, \cdot)$ is a set R with two binary operations addition $+$ and multiplication $\cdot$ such that the following axioms are satisfied:

(1). $(R, +)$ is an abelian group.
(2). Multiplication $\cdot$ is associative.
(3). For all $a, b, c \in R$, the left distributive law and the right distributive las hold:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

Example. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, and $(\mathbb{C}, +, \cdot)$ are rings.

It is customary to write $a \cdot b$ as ab.

Since $(R, +)$ is a group, its identity element is denoted by 0 and the inverse of a is denoted by $-a$. 0 is called the **additive identity**.

Example. Let $C[1,6]$ be the space of all continuous functions on the interval $1 \leq x \leq 6$. We have add and multiply two continuous functions, and the results are still continuous functions, so $C[1,6]$ has addition and multiplication. It is easy to see that the three axioms in the definition of the ring are satisfied for $(C[1,6], +, \cdot)$. So $(C[1,6], +, \cdot)$ is a ring.

Example. Recall the modular n addition gives the abelian group $(\mathbb{Z}_n, +)$,

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

We can introduce the modular multiplication $\cdot$ on $\mathbb{Z}_n$:

$$i \cdot j = \text{usual multiplication ij modular } n$$

Then $(\mathbb{Z}_n, +, \cdot)$ is a ring.

Example. In the ring $(\mathbb{Z}_9, +, \cdot)$,

$$\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$$

$$3 + 4 = 7, \;\; 6 + 7 = 13 = 4, \;\; 3 + 8 = 11 = 2$$

$$3 \cdot 4 = 12 = 3, \;\; 6 \cdot 7 = 42 = 6, \;\; 3 \cdot 7 = 21 = 3$$

In all the above examples, we have

$$ab = ba.$$

Definition. A ring $(R, +, \cdot)$ is called a **commutative ring** if the multiplication $\cdot$ is commutative, that is,

$$a \cdot b = b \cdot a \quad \text{for all} \quad a, b \in R.$$

$(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $C[1, 6]$, $(\mathbb{Z}_n, +, \cdot)$ are all commutative rings.

Example. Let $M_2(\mathbb{R})$ be the set of all 2×2 matrices with real number entries, $M_2(\mathbb{R})$ has matrix addition $+$ and matrix multiplication $\cdot$. It is easy to see that $(M_2(\mathbb{R}), +, \cdot)$ is a ring. This ring is **not** a commutative ring, as $AB \neq BA$ in general.

For all $n \geq 2$, let $M_n(\mathbb{R})$ be the set of all $n \times n$ matrices with real number entries, $(M_n(\mathbb{R}), +, \cdot)$ is a ring. This ring is **not** commutative ring,

Example. If $R_1, R_2, \ldots, R_n$ are rings, we can form the set $R_1 \times R_2 \times \cdots \times R_n$. An element in $R_1 \times R_2 \times \cdots \times R_n$ is a n-tuple

$$(r_1, r_2, \ldots, r_n), \quad r_1 \in R_1, r_2 \in R_2, \ldots, r_n \in R_n$$

We define the component-wise addition and the component-wise multiplication on $R_1 \times R_2 \times \cdots \times R_n$ as follows:

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

$$(a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_n) = (a_1 \cdot b_1, a_2 \cdot b_2, \ldots, a_n \cdot b_n)$$

Then $(R_1 \times R_2 \times \cdots \times R_n, +, \cdot)$ is a ring, which is called the **direct product** of rings R_i.

Let n be a positive integer, we will write

$$a + a + \cdots + a \qquad n \text{ copies of } a$$

as na.
and write

$$(-a) + (-a) + \cdots + (-a) \qquad n \text{ copies of } -a$$

as $-na$

We will often write a ring $(R, +, \cdot)$ simply as R, with the understanding that it has $+$ and $\cdot$.

Theorem 18.8. If R is a ring with additive identity 0, then for any $a, b \in R$, we have

(1) $0a = a0 = 0$.
(2) $a(-b) = (-a)b = -(ab)$.
(3) $(-a)(-b) = ab$.

Definition 18.9. For rings R and R', a map $\phi : R \to R'$ is a **homomorphism** if the following two conditions are satisfied for all $a, b \in R$:

(1) $\phi(a + b) = \phi(a) + \phi(b)$.

(2) $\phi(ab) = \phi(a)\phi(b)$.

Example. The map $\phi : \mathbb{Z} \to \mathbb{Z}_3$ given by

$$\phi(n) = \begin{cases} 0, & \text{if } n \text{ has remainder } 0 \text{ divided by } 3 \\ 1, & \text{if } n \text{ has remainder } 1 \text{ divided by } 3 \\ 2, & \text{if } n \text{ has remainder } 2 \text{ divided by } 3 \end{cases}$$

ϕ is a homomorphism.

More generally, we have

Example. The map $\phi : \mathbb{Z} \to \mathbb{Z}_n$ given by

$$\phi(a) = a \mod n$$

is a homomorphism.

To distinguish homomorphisms for rings from homomorphisms for groups, sometimes we use the phrase "**ring homomorphism**" or "**group homomorphism**".

Example. $\phi : \mathbb{R} \to M_2(\mathbb{R})$ given by

$$\phi(a) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

is a ring homomorphism.

Example. $\phi : \mathbb{C} \to M_2(\mathbb{R})$ given by

$$\phi(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

is a ring homomorphism.

Definition 18.12. An **isomorphism** $\phi : R \to R'$ from a ring R to a ring R' is a homomorphism that is one-to-one and onto. The rings R and R' are then said to be isomorphic.

The end