Chapter 12 Introduction to Rings

Definition A ring is a set with two binary operations: addition $a+b$ and multiplication ab satisfying

(R1) $(R, +)$ is an Abelian group with identity 0, and inverse $-a$ for $a \in R$.

(R2) $(ab)c = a(bc)$ for any $a, b, c \in R$.

(R3) $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$ for any $a, b, c \in R$.

Remark A ring may not have unity (multiplicative identity).

The multiplication may not be commutative. If it does, we say that R is **commutative**.

Examples $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Z}_n$, $M_2(\mathbb{Z})$, $\mathbb{Z}[x]$, external direct product $R_1 \oplus R_2$, the set of real-valued functions f such that $f(1) = 0$.

Basic results

Theorem 12.1-2 Let a, b, c, be elements of a ring R. Then

1. $a0 = 0a = 0$. [Proof. $0 + 0a = 0a = (0 + 0)a = 0a + 0a$.]
2. $a(-b) = (-a)b = -(ab)$.

   [Proof. $a(-b) + ab = a(-b + b) = a0 = 0 = -(ab) + ab$.]
3. $(-a)(-b) = ab$. [Proof. $(-a)(-b) + (-ab) = 0$.
4. $a(b - c) = ab - ac$ and $(b - c)a = ba - ca$.

   Suppose R has a unity 1.
5. The unity is unique. [Proof. $1 = 11' = 1'$.]
6. $(-1)a = -a$ [Proof. $(-1)a = -(1a) = -a$.]
7. $(-1)(-1) = 1$.
8. Every $a \in R$ has none or a unique multiplicative inverse.

[Proof. If $1a = a1 = a = 1'a = a1'$ for all $a \in R$, then $1 = 11' = 1'$.

Subrings

Definition A subset S of a ring R if $(S, +, \cdot)$ is a ring.

Theorem 12.3 A non-empty subset S of a ring R is a subring if and only if S is closed under subtraction and multiplication, i.e., $a - b, ab \in S$ for any $a, b \in S$.

Example $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$;

$\mathbb{Z}[x] \subseteq \mathbb{Q}[x] \subseteq \mathbb{R}[x] \subseteq \mathbb{C}[x]$;

$M_2(\mathbb{Z}) \subseteq M_2(\mathbb{Q}) \subseteq M_2(\mathbb{R}) \subseteq M_2(\mathbb{C})$;

$\mathbb{Z}[i]$.

Chapter 13 Integral Domains

Definitions (a) A nonzero element a in a commutative ring R is a zero divisor if there is a nonzero element b such that $ab = 0$.

(b) An integral domain is a communtative ring with unity and no zero-divisors.

(c) A field is a commutative ring R such that $(R^*, \cdot)$ is a group.

Examples $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Z}_n$, $M_2(\mathbb{Z})$, $\mathbb{Z}[x]$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Z}_3[i]$, external direct product $R_1 \oplus R_2$.

Theorem 13.1 If $a \in R$ is not a zero divisor and $ab = ac$, then $b = c$. Consequently, if R is an integral domain and $a \in R$ is nonzero such that $ab = ac$, then $b = c$.

Theorem 13.2 A finite integral domain is a field.

Corollary If p is a prime, then $\mathbb{Z}_p$ is a field.

Definition If there is $x \in R$ such that $nx = x + \cdots + x \neq 0$ for any $n \in \mathbb{N}$, then we say that R has has characteristic 0.

Otherwise, we can let n be the smallest positive integer such that $0 = nx = x + \cdots + x$ (n times) for every $x \in R$; we say that R has characteristic n.

Notation Denote by char$R$ the characteristic of R.

Theorem 13.3-4 If R has unity 1, then char$R = n$ if $|1| = n$ in $(R, +)$. If R is an integral domain, then char$R$ is zero or prime.