$(G,*)$

Chapter 12 Introduction to Rings $(R,+,\cdot)$ $(R,*_1,*_2)$

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 $f(1) = 0$.

Example $(\mathbb{Z},+,\cdot)$ — an commutative ring with unity 1.

$(2\mathbb{Z},+,\cdot)$ — an commutative ring with no unity.

because for any $a \in 2\mathbb{Z}$.

Case 1 if $a=0$, then $ax = 0 \neq x$ for any nonzero $x \in 2\mathbb{Z}$

Case 2 if $a \neq 0$ then $|ax| > |x|$.

$\therefore$ a is not a unity.

$\mathbb{Z}/k\mathbb{Z} \cong \mathbb{Z}_k$

$(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ are commutative ring with unity 1.

$(\mathbb{Z}_n,+,\cdot)$ $+,\cdot \pmod n$

is a commutative ring with unity $[1]$.

Example $M_2(\mathbb{Z}_2) = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{Z}_2\right\}$ has $2^4 = 16$ elements.

is a non-commutative ring with unity I_2. $I_2\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} I_2 = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$A = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ $AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ $BA = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$

Example $M_2(2\mathbb{Z})$ is non-commutative $A = \begin{bmatrix} 0 & 0 \\ 2 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix}$ $AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ $BA = \begin{bmatrix} 0 & 0 \\ 4 & 0 \end{bmatrix}$.

has no unity. $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$

Example $\mathbb{Z}[x] = \left\{ a_0 + a_1 x + \cdots + a_n x^n : n \in \{0,1,2,\cdots\},\ a_0, \cdots, a_n \in \mathbb{Z},\ a_n \neq 0 \text{ if } n > 0 \right\}$.

$f(x) = a_0 + \cdots + a_n x^n$, $g(x) = b_0 + \cdots + b_m x^m$.

Then $f(x) + g(x) = (a_0 + b_0) + \cdots + (a_k + b_k) x^k$.

where $k \le \max(m,n)$, and $a_j = 0$ if $j > n$, $b_j = 0$ if $j > m$

$f(x)g(x) = a_0 b_0 + (a_1 b_0 + b_1 a_0)x + (a_2 b_0 + a_1 b_1 + a_0 b_2)x^2 + \cdots$

$= \sum_{k=0}^{m+n} c_k x^k$, $c_k = a_k b_0 + a_{k-1} b_1 + \cdots + a_0 b_k$

$= \sum_{i+j=k} a_i b_j$.

(R1) One can check $(\mathbb{Z}[x], +)$ is an Abelian group ✓

(R2) $[f(x) + g(x)]h(x) = f(x)h(x) + g(x)h(x)$

(R3) $(f(x)g(x))h(x) = f(x)(g(x)h(x))$

$(f(x) + g(x))x^k c_k = f(x)x^k c_k + g(x)x^k c_k$ $\forall k = 0, 1, 2, \cdots$.

Then $(f(x) + g(x))(h_0 + h_1 x + \cdots + h_r x^r)$

$= f(x)(h_0 + h_1 x + \cdots + h_r x^r) + g(x)(h_0 + h_1 x + \cdots + h_r x^r)$.

Unity $\theta(x) = 1$ satisfies.

$\theta(x) f(x) = f(x)\theta(x) = f(x)$ $\forall f(x) \in \mathbb{Z}[x]$.

$f(x)^{-1}$ exists if and only if $f(x) = 1$ or $f(x) = -1$.

Proof: If $f(x) = 1$ or -1, then $f(x)^{-1} = f(x)$

If $f(x) \notin \{1, -1\}$, then $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ with $a_0 \neq 1, -1$ (*) or $n > 0$

Suppose $g(x) = b_0 + \cdots + b_m x^m$ is the inverse of $f(x)$. Then $g(x) \neq 0$. Then $(a_0 + \cdots + a_n x^n)(b_0 + \cdots + b_m x^m) = 1$.

Then $f(x)g(x)$ has degree $n + m > 0$ if $n = 0$, $f(x) = a_0 \in \{1, -1\}$

Example. Let R_1, R_2 be rings.

$$R_1 \oplus R_2 = \{(r_1, r_2) : r_1 \in R_1, r_2 \in R_2\}.$$

Define.
$$(r_1, r_2) + (s_1, s_2) = (r_1 +_1 s_1, r_2 +_2 s_2)$$
$$(r_1, r_2) \cdot (s_1, s_2) = (r_1 s_1, r_2 s_2)$$
} form a ring.

Example: $\mathbb{Z}_n[x] \oplus M_2(\mathbb{R})$.

$$= \{(f(x), A) : f(x) \in \mathbb{Z}_n[x],\ A \in M_2(\mathbb{R})\}$$

$$(f(x), A) + (g(x), B) = (f(x) + g(x), A + B)$$
$$(f(x), A) \cdot (g(x), B) = (f(x) \cdot g(x), AB).$$

Example

$(\mathbb{R}^n, +, \cdot)$ is NOT a ring

$+$: vector addition

$\cdot$: scalar multiplication is not from $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$.

Example

$(\mathbb{R}^n, +, \cdot)$ is NOT a ring if $n > 1$.

$+$: vector addition

$\cdot$: inner product is not binary unless $n = 1$

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = x_1 y_1 + \cdots + x_n y_n$$

$e^2 = e$

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 $(b - c)a = ba - ca$.

$(-a)[-b + b] = [-a][0] = 0$

$\therefore (-a)(-b) = ab$

Suppose R has a unity 1.

5. The unity is unique. [Proof. $1 = 11' = 1'$.] and if $1'$ is another unity
6. $(-1)a = -a$ [Proof. $(-1)a = -(1a) = -a$.]
7. $(-1)(-1) = 1$. $= -(-1)$
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 $1 = 11' = 1'$.~~

Suppose $aa' = 1 = a'a$

and $a\hat{a} = 1 = \hat{a}a$

Then $a' = a'(a\hat{a}) = (a'a)\hat{a} = \hat{a}$.

Example $\mathbb{R}[x]$ with unity $Q(x) = 1$.

$f(x) \in \mathbb{R}[x]$

has inverse (multiplicative) if and only if

$f(x) = a_0$ with $a_0 \neq 0$.

$f(x)^{-1} = \frac{1}{a_0}$

Subrings

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

If S is a subset of R where $(R,+,\cdot)$ is a ring, and $(S,+,\cdot)$ is a ring, then S is a ~~subset~~ subring of R

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 $a, b \in S$.

Take care of (R1) binary

Remarks (R2) "$(ab)c = a(bc)$ is true for $a,b,c \in R$" will ensure the same property in S.

(R3) $a(b+c) = ab + ac$, $(b+c)a = ba + ca$ ✓✓✓ in S.

~~Inherited~~ ensured by property in R

~~$(N, +, \cdot)$~~

Example.

$(\mathbb{Z}, +, \cdot)$ is a $(\mathbb{Z}[x], +, \cdot)$ $(M_n(\mathbb{Z}), +, \cdot)$

$(\mathbb{Q}, +, \cdot)$ $(\mathbb{Q}[x], +, \cdot)$ $(M_n(\mathbb{Q}), +, \cdot)$

$(\mathbb{R}, +, \cdot)$ $(\mathbb{R}[x], +, \cdot)$ $(M_n(\mathbb{R}), +, \cdot)$

$(\mathbb{C}, +, \cdot)$ $(\mathbb{C}[x], +, \cdot)$ $(M_n(\mathbb{C}), +, \cdot)$

$D_n(\mathbb{Z}[x]) \to T_n \to M_n$

$D_n(\mathbb{Q}[x]) \to T \to M_n$

$D_n(\mathbb{R}[x]) \to \to M_n$

$D_n(\mathbb{C}[x]) \to$

$(D_n(\mathbb{Z}), +, \cdot) \to (T_n(\mathbb{Z}), +, \cdot)$

$(D_n(\mathbb{Q}), +, \cdot)$ $(T_n(\mathbb{Q}), +, \cdot)$

$(D_n(\mathbb{R}), +, \cdot)$ $(T_n(\mathbb{R}), +, \cdot)$

$(D_n(\mathbb{C}), +, \cdot)$ $(T_n(\mathbb{C}), +, \cdot)$

$M_m(M_n)$