18/11/23

CH 14 Rings & Modular Arithmetic

14.1 The ring structure

Def 14 Let R be a non empty set on which we have 2 closed binary operation denoted by "+" and "·"

The $(R, +, \cdot)$ is a ring if for all $a, b, c \in R$, the following conditions are satisfied.

1) $a + b = b + a$ {commutative law for ⊕}

2) $a + (b + c) = (a + b) + c$ { Associative law for ⊕ }

3) ∃ an element $z \in R$ such that Existence of an identity for ⊕

$a + z = z + a = a$

4) For each $a \in R$, ∃ an element $b \in R$ with

$a + b = b + a = z$ { Existence of inverse element }

identity element

5) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ { Associative law of · }

6) $a \cdot (b + c) = a \cdot b + a \cdot c$

$(b + c) \cdot a = b \cdot a + c \cdot a$

} Distributive laws of · over +

Ex 14.1 Is $(Z, +, \cdot)$ is a ring

Let $a, b, c \in Z$

1) $a + b = b + a$; for any integer

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

3) $a + 0 = 0 + a = a$

4) $a + b = 0$

$a = -b$

5) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

6) $a(b + c) = ab + ac$

Ex 14.2 Let $M_2(\mathbb{Z})$ denote the set of all 2×2 matrices with integer entries. In $M_2(\mathbb{Z})$, 2 matrices are equal if their corresponding entries are equal in $\mathbb{Z}$. Here we define $+$ and $\cdot$ by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}$$

Check if $(M_2(\mathbb{Z}), +, \cdot)$ is a ring or not

Soln Let $A, B \in M_2(\mathbb{Z})$

1) $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_2 \end{bmatrix}$, $B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$

$$A+B = \begin{bmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{bmatrix}$$

$$= \begin{bmatrix} a_2+a_1 & b_2+b_1 \\ c_2+c_1 & d_2+d_1 \end{bmatrix}$$

$$= B + A$$

commutative law for $+$ satisfied

2) Let $A, B, C \in M_2(\mathbb{Z})$

3) $A + Z = A$

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$$

$Z = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ ∴ there is an existence for identity for $+$

Ans - yes it is

(a) If $ab = ba \ \forall a, b \in R$, then the ring R is called commutative ring.

(b) The ring R is said to have no proper divisor of zero if for all $a, b \in R$, $ab = 0 \Rightarrow a = 0$ or $b = 0$ { where 0 = additive identity }

i) Eg. $(\mathbb{Z}, +, \cdot)$ has no proper divisor of 0

because

$a \cdot b = 0$ when either $a = 0$ or $b = 0$

ii) $(M_2(\mathbb{Z}), +, \cdot)$ has proper divisor of 0

Eg-

$$\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

(c) If there exists ($\exists$) an element $u \in R$ such that $u \neq 0$ and $ua = au = a \ ; \forall a \in R$ then we call u as a unity or multiplicative identity

Eg for $(\mathbb{Z}, +, \cdot)$

$u = 1 \leftarrow$ Multiplicative identity

$1 \cdot a = a \cdot 1 = a$

22/11/23

Ex-14.3 Consider the set Z with the binary operations $\oplus$ and $\odot$ which are defined by

$x \oplus y = x + y - 1$ and $x \odot y = x + y - xy$

check whether $(Z, \oplus, \odot)$ is a ring or not.

Soln (1) To check $x \oplus y = y \oplus x$

LHS $= x \oplus y = x + y - 1 = y + x - 1 = y \oplus x$

$\Rightarrow$ Commutative property holds.

2) $x \oplus (y \oplus z) = x + (y \oplus z) - 1$

$= x + y + z - 1 = (y \oplus z) + x - 1$

$= (x \oplus y) \oplus z$

holds

$\Rightarrow$

(3) $x \oplus z = x$

$x + z - 1 = x$

$z = 1$

(4) $x \oplus y = 1$

$x + y - 1 = 1$

$x + y = 2$

$y = 2 - x$

(5) $x \odot (y \odot z) = x + (y \odot z) - x(y \odot z)$

$= x + (y + z - yz) - x(y + z - yz) \rightarrow (i)$

$(x \odot y) \odot z = (x + y - xy) \odot z$

$= (x \odot y) + z - (x \odot y) z$

$= x + y - xy + z - (x + y - xy) z \rightarrow (ii)$

$i = ii$

(6) $x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$

Multiplicative unity

$x \odot a = x$

$x + a - ax = x$

$a(1 - x) = 0$

$x \neq 1, \ a = 0$

Def 14.3 Let R be a ring with unity u. If $a \in R$ and $\exists\ b \in R$ such that $ab = ba = u$. Then b is called multiplicative inverse of a and a, b are called unit of R.

Def 14.4 Let R be a commutative ring with unity. Then

(a) R is called an integral domain if R has no proper divisor of zero.

(b) R is called a field if every non-zero element of R is a unit.

20/12/23.

Ex (14.1) Determine whether or not, each of the following sets of no. is a ring under ordinary addition & multiplication.

(a) R = the set of positive integers & zero.

Sol^n This is not a ring as the additive inverse does not exist.

(b) $R = \{kn ;$ k is a fixed +ve integer & $n \in \mathbb{Z}\}$

(1) $\forall\ a, b \in R$

$a + b = b + a$

(2) $\forall\ a, b, c \in R$

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

$\exists\ a = kn$

$kn + z = kn$

u —

⟶ It is a ring

(6) $R = \{ a + b\sqrt{2} \quad ; a, b \in \mathbb{Z} \}$

Sol^n ~~If~~ Yes, it is a ring.

3|1|24. (Ex 14.1)

(6) Define the binary operations $\oplus$ & $\odot$ on $\mathbb{Z}$ by $x \oplus y = x+y$ $x \odot y = x+y-3xy$ for all $x, y \in \mathbb{Z}$. Explain why $(\mathbb{Z}, \oplus, \odot)$ is not a ring.

(1) Closure property

if $x, y \in \mathbb{Z}$

then $x+y-3xy$ & $x+y-7$ both $\in \mathbb{Z}$

(2) Commutative " wrt add^n

$x \oplus y = x+y-3xy = y+x-3yx = y \oplus x$

(3) Associative " w.r.t add^n

$x \oplus (y \oplus z) = x \oplus x + (y \oplus z) - 7$

$= x + (y+z+7) - 7$

$= x+y+z-14$

$= (x \oplus y) \oplus z$

(4) Identity element

~~$x \oplus y$~~ If z is the zero element.

$x \oplus z = x$

$x + z - 7 = x$

$\boxed{z = 7}$ ← exists.

(5) Inverse element

$x \oplus y = z$

$x+y-7 = 7$

$x+y = 14$

$\boxed{y = 14 - x}$ exists

(6) ~~commutative~~ Associative property of ⊙

$$x \odot (y \odot z) = x + (y \odot z) - 3x(y \odot z)$$

$$= x + (y + z - 3yz) - 3x(y + z - 3yz)$$

$$= (x \odot y) \odot z$$

(7) Distributive.

$$x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$$

$$= x \odot (y + z - 7)$$

$$= x + (y + z - 7) - 3x(y + z - 7)$$

$$= 22x + y + z - 3xy - 3xz - 7$$

$$\neq (x \odot y) \oplus (x \odot z)$$

As $x \odot (y \oplus z) \neq (x \odot y) \oplus (x \odot z)$ so

It is not a ring.

Q (120) (b) S.T. $\begin{bmatrix} 1 & 2 \\ 3 & 8 \end{bmatrix}$ is a unit in the ring $M_2(\mathbb{Q})$ but not a unit in $M_2(\mathbb{Z})$

Sol^n $\mathbb{Q} \rightarrow$ rational no.s

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 8 \end{bmatrix} \qquad A^{-1} = \frac{1}{2}\begin{bmatrix} 8 & -2 \\ -3 & 1 \end{bmatrix}$$

$$|A| = 8 - 6 = 2 \qquad = \begin{bmatrix} 4 & -1 \\ -3/2 & 1/2 \end{bmatrix}$$

As all the entries of A^{-1}, are rational nos but not integers so A is a unit in the ring $M_2(\mathbb{Q})$ but not in $M_2(\mathbb{Z})$.

Theorem 14.2.1 In any ring $(R, +, \cdot)$

(a) the zero element $\mathfrak{z}$ is unique &

(b) the additive inverse of each ring element is unique

Theorem 14.2.2 The cancellation laws of addition $\forall\ a, b, c \in R$ holds

(a) $a + b = a + c \Rightarrow b = c$

(b) $b + a = c + a \Rightarrow b = c$

Theorem 14.2.3 For any Ring $(R, +, \cdot)$ and any $a \in R$, $a\mathfrak{z} = \mathfrak{z}a = \mathfrak{z}$

Theorem 14.2.4 Given a ring $(R, +, \cdot)$ for all $a, b \in R$

(a) $-(-a) = a$

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

(c) $(-a)(-b) = ab$

Theorem 14.2.5 For a ring $(R, +, \cdot)$

(a) if R is a unity, then it is unique &

(b) if R has a unity & x is a unit of R then the multiplicative inverse of x is unique.

Theorem 14.2.6 Let ~~R~~ $(R, +, \cdot)$ be a commutative ring with unity. The R is an integral domain iff $\forall\ a, b, c \in R$ where $a \neq \mathfrak{z}$, $ab = ac \Rightarrow b = c$

Ex 14.2

(2) If a, b & c are any elements in a ring $(R, +, \cdot)$ P.T.

(a) $a(b-c) = ab-(ac)$

$= ab - ac$

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

$= ba - ca$

Proof

(a) $a(b-c) = a(b+(-c))$

$= ab + a(-c)$

$= ab + (-ac)$

$= ab - (ac)$

$= ab - ac$

(b) $(b-c)a$

$= (b+(-c))a$

$= b$.

HW Q (3)

(4) P.T. a unit is a ring R cannot be a proper divisor of zero.

Let ~~If~~ $ab = 3$ ⟶ (i)

where $a \neq 3$ & $b \neq 3$ ⟶ (ii)

if the above 2 cases satisfy then, it has proper divisor of zero.

Let u be a unity of R & let x be unit.

Hence there is an element y s.t. $xy = yx = u$

If ~~xxx~~ $xw = 3$; (3 is zero of R)

$y(xw) = y3 = z$ &

$y(xw) = (yx)w = uw = w$

$w = \{\}$, so x is not a proper divisor of zero.

6/1/24. # Ch 16 - Group Theory

Def^n 6.1 Group Theory

1) Closure Property
2) Associative property
3) Identity element exists
4) Inverse " "

} If these 4 properties satisfy then Z is called a group.

Eg - $(Z, +, *)$: Is a group
$(R, +)$: "
$(Q, +)$: "
$(C, +)$: "

↳ w.r.t add^n Z, R, Q, C are group

> If $a * b = b * a$
> then the group is called abelian group or commutative

Def^n 16.2 For every group G, the no. of elements in G is called the order of G & is denoted by $|G|$

Eg 16.2 $(Z_n, +)$
↳ modulus set of n

$Z_n = \{0, 1, 2, \cdots, n-1\}$

Find the order of Z_4 & inverse of each elemen in Z_4

sol^n Order of ~~Z~~ $(Z_4, +)$ is 4

$Z_4 = \{0, 1, 2, 3\}$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

← operation of Z_4 (+) with all its elements.

★ Inverse element of x = after operation with which element x becomes "0"

Inverse of 0 = 0
" " 1 = 3
" " 2 = 2
" " 3 = 1

Def 16.3 Let G be a group & $\phi \neq H \subseteq G$ (non empty set). If H is a group under the binary operation of G then we call H is a subgroup of G.

Theorem 16.2 If H is a non-empty subset of a group G then H is a subgroup of G if & only if

(a) for all $a, b \in H$, $ab \in H$ { closure property holds of multiplication }

(b) for all $a \in H$, $a^{-1} \in H$

Theorem 16.3 If G is a group & $\phi \neq H \subseteq G$, with H is finite then H is a subgroup of G iff H is closed under the binary operation of G.

Exercise 16.1

① For each of the following sets, determine whether or not the set is a group under the stated binary operation.

(a) $\{-1, 1\}$ wrt multiplication

i) closure property

$$-1 \times 1 = -1 \in G$$

ii) Associative property holds

iii) $-1 \times 1 = -1$

$1 \times 1 = 1$

1 is the identity element.

iv) $(-1) \times (-1) = 1$

-1 is the inverse of -1

1 is " " 1

(b) $\{-1, 1\}$ wrt add^n

i) $-1 + 1 = 0 \notin G$

closure property doesn't hold

(d) $\{10n, n \in Z\}$ under add^n

$G = \{10n, n \in Z\}$

$a, b \in G$, $a + b \in G$

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

Holds.

HW Ex 16.1, e, f

g is the set $\mathbb{Z}$ is not a group under Subtraction ?

Sol^n

(1) $a, b \in \mathbb{Z}$ $\Rightarrow a - b \in \mathbb{Z}$ Closure property holds.

(2) $1, 2, 3 \in \mathbb{Z}$ $\Rightarrow (1-2) - 3 = -4$

$1 - (2-3) = 2$

Associative property doesn't hold

(13) If G is a group let $H = \{ a \in G, ag = ga \; \forall g \in G \}$ P.T, H is a subgroup of G.

Sol^n Let $e \in G$ is the identity element in G.

$\forall a \in G$, $ea = ae$ that means

$e \in H$, so H is non-empty $\longrightarrow$ (i)

(ii) Let $x, y \in H$

$$(xy)g = x(yg) = x(gy) = (xg)y$$
$$= (gx)y = g(xy)$$

$\Rightarrow x, y \in H$

Closure property satisfies.

(iii) $xy \in H$

$x \in H$

$xg^{-1} = g^{-1}x$

$\Rightarrow (xg^{-1})^{-1} = (g^{-1}x)^{-1}$

$gx^{-1} = x^{-1}g$

$\Rightarrow x^{-1} \in H$