Ch-14 14.1 674-678
679

Def^n: 14.1, 14.2, 14.3, 14.4

Example: 14.1, 14.2, 14.3

Ex: 2, 3, 6, 7, 12, 13

14.2 680-682; 684

Def^n: 14.5

eg: 14.7, 14.8

Theorem: 14.1, 14.2, 3, 4, 5, 6

Ex: 2, 3, 4

Chapter-14

$(R, +, \cdot)$ is ring if $\forall\, a, b, c \in R$ satisfy following condition

(I) Commutative (+) $a+b = b+a$ — where + may not be ordinary addition.

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

(III) $a+z = z+a = a \quad \forall\, a \in R$ — Identity.

(IV) $a+b = b+a = z$. — Inverses.

(V) Associative ($\cdot$) $a\cdot(b\cdot c) = (a\cdot b)\cdot c$

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

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

$(b+c)\cdot a = b\cdot a + c\cdot a$ — Distributive Laws of $\cdot$ over +.

eg: 14.1 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ & $\mathbb{C}$ are rings

additive identity is 0.

additive inverse of $x = -x$.

def^n 14.2 Let $(R, +, \cdot)$ be a ring

(I) If $ab = ba \quad \forall\, a, b \in R$ then R is commutative ring

(II) R has no proper divisors of zero $\forall\, a, b \in R$

$ab = z \Rightarrow a = z$ or $b = z$

(III) $u \in R$, ~~$a \in$~~ $a \neq z$ & $au = ua = a \quad \forall\, a \in R$

(Multiplicative identity / Unity)

proper divisors of a ring = elements whose product is zero element of the ring

ex 14.3 $\oplus$ and $\odot$

$x \oplus y = x + y - 1$ $\quad$ $x \odot y = x + y - xy$.

$\Rightarrow (\mathbb{Z}, \oplus, \odot)$ is a ring.

To proove:

① $x \oplus y = x + y - 1 = y + x - 1 = y \oplus x$. commutative.

② $a \oplus z = z \oplus a = a \quad \forall a \in \mathbb{Z}$

$a + z - 1 = a$

$\Rightarrow z = 1$ ($\therefore$ additive identity for $\oplus$ is z)

③ $a \oplus b = b \oplus a = z$

$a + b - 1 = 1$. $\quad$ $b \oplus a = b + a - 1$

$\Rightarrow a + b = 2$. $\quad = 2 - a + a - 1$

$b = 2 - a$. $\quad = 2 - 1 = 1 = z$.

$\therefore$ satisfied inverses.

④ $a \oplus (b \oplus c) = (a \oplus b) \oplus c$. Associative $\oplus$.

⑤ $a \odot (b \odot c) = (a \odot b) \odot c$ Associative $\odot$

⑥ $a \odot (b \oplus c) = a \odot b \oplus a \odot c$
$(b \oplus c) \odot a = b \odot a \oplus c \odot a$] Distribution.

4). $a \oplus (b \oplus c) = a \oplus (b + c - 1)$
$= a + b + c - 1 - 1$
$= a + b + c - 2$ — eqⁿ ①

$(a \oplus b) \oplus c = (a + b - 1) \oplus c$
$= a + b - 1 + c - 1$
$= a + b + c - 2 = $ eqⁿ ① proved.

(5) $a \odot (b \odot c) = a \odot (b + c - bc)$
$= a + b + c - bc - (ab + ac - abc)$
$= a + b + c - bc - ab - ac + abc$. — eqⁿ (1).

$(a \odot b) \odot c = (a + b - ab) \odot c$
$= (a + b - ab) + c - (a + b - ab)c$
$= a + b - ab + c - ac - bc + abc$
$= a + b + c - bc - ab - ac + abc$.
$=$ eqⁿ (1).

prooved.

(6) $a \odot (b \oplus c) = a \odot (b + c - 1)$
$= a + (b + c - 1) - (b + c - 1)a$
$= a + b + c - 1 - ab - ac + a$.
$= 2a + b + c - ab - ac - 1$. — eqⁿ (1).

$(b \oplus c) \odot a = (b + c - 1) \odot a$.
$= (b + c - 1) + a - (b + c - 1)a$
$= b + c - 1 + a - ab - ac + a$.
$= 2a + b + c - ab - ac - 1$.
$=$ eqⁿ (1).

Prooved.

14.2 conditions proove.

(b) (1) $ab = ba$
$a \odot b = b \odot a$.
$a \odot b = a + b - ab$
$b \odot a = b + a - ba$
)) equal.

(2) $a \odot u = u \odot a = a$
$= a + u - au = a$
$\Rightarrow u(1 - a) = a - a$
$\Rightarrow u(1 - a) = 0 \cdot \forall a \neq 1 \quad u = 0$ is unity

14.3 Def^n

Let ~~If~~ R is a ring with unity u.
If $a \in R$ $\exists$ $b \in R$ such that $ab = ba = u$ then,
b is multiplicative inverse of a
a is a unit of R.
b is also unit of R.

14.4 Let R be a commutative ring with unity. Then.
a) R is called an integral domain if R has no proper divisors of zero.
b) R is field if every non zero element of R is a unit

Section - 14.2

Theorem 14.1

In any Ring $(R, +, \cdot)$,
a) zero element (z) and additive inverse of each ring is unique.

Theorem 14.2. Cancellation Laws of Addition.
$\forall$ $a, b, c \in R$.
a) $a+b = a+c \Rightarrow b=c$.
b) $b+a = c+a \Rightarrow b=c$.

Theorem 14.3 For any ring $(R, +, \cdot)$ and any $a \in R$,
$az = za = z$.

Theorem 14.4 Given a ring ~~R~~ $(R, +, \cdot)$.
(i) $-(-a) = a$
(ii) $a(-b) = (-a)b = -(ab)$
(iii) $(-a)(-b) = ab$.

Theorem 14.5

For a ring $(R, +, \cdot)$
a) R has unity, it is unique.
b) " ", x is unit of R then the multiplicative inverse of x is unique.

Theorem 14.6

R is a commutative ring with unity.
R is an integral domain if and only if
$\forall\ a, b, c \in R \quad a \neq z$
$ab = ac \Rightarrow b = c.$
commutative ring satisfies cancellation law of multiplication is an integral domain.

def^n 14.5 For a ring $(R, +, \cdot)$, a non empty set S of R is subring of R if $(S, +, \cdot)$ S under the addition and multiplication of R.

example 14.7 For every ring R,
Subsets $\{z\}$ and R are always subrings of R.

14.8 a) set of all even integers is a subring of $(\mathbb{Z}, +, \cdot)$
$\forall\ n \in \mathbb{Z}^{+}\ n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$ subring of $(\mathbb{Z}, +, \cdot)$

b) $(\mathbb{Z}, +, \cdot)$ subring of $(\mathbb{Q}, +, \cdot)$
$(\mathbb{Q}, +, \cdot)$ subring of $(\mathbb{R}, +, \cdot)$
$(\mathbb{R}, +, \cdot)$ subring of $(\mathbb{C}, +, \cdot)$

Chapter - 16 16.1 (745-758)

751

Def^n: 16.1, 16.2, 16.3

Example: 16.1, 16.2, 16.5

Theorem: 16.2, 16.3 (only statements)

Ex No: 1, 3, 8, 10, 15

Chapter - 16

Group

def^n 16.1. A non empty set G equipped with one binary operation o then G is called group. (The following 6 conditions need to be satisfied)

① G is closed for o denoted by (G, o) eg. $a, b \in G$ & $a \circ b \in G$ } closed under o

② Associativity property. $a \circ (b \circ c) = (a \circ b) \circ c$

(N, +), (Z, +) (Z, *) (Q, *) associative

∪ and ∩ are associative. {Union & intersection}

(P(S), ∪)   (P(S), ∩)

(N, −) not associative.

③ Identity element (e) $e \in G$ {G is anyset}

$a \circ e = e \circ a = a$ $a \in G$

Natural numbers:

$2 + 0 = 0 + 2 = 2$ but $0 \notin N$ Hence, N doesn't have additive identity.

$2 \times 1 = 1 \times 2 = 2$ $1 \in N$, N has multiplicative identity.

④ Existence of Inverses.

For addition: Adding inverse to the number gives identity.

$a \circ a^{-1} = \text{identity}$. $a \in G$. $a^{-1} \in G$

if addition.   & multi

$a + a^{-1} = 0$ $a * a^{-1} = 1$.

(Z, +) is a group.

(N, +)
(N, ×)
(Z, ×) } not group.

Abelian group:

The above 4 conditions + 1 more condition
= Abelian group.

Extra condition:

Commutative: $a \circ b = b \circ a \quad \forall a, b \in G$.

Order of group: no. of elements $|G|$.

If $(G, *)$ finite, finite order, finite group.
" " infinite, infinite order, infinite group.

Q8) $(ab)^2 = a^2 b^2 \quad \forall a, b \in G$.

C1: Let $a, b \in G \Rightarrow (ab)^2 = a^2 b^2 \in G$
Closure is satisfied

C2: ~~Let a, b, c ∈ G~~

$$(ab)^2 = (ab)(ab)$$
$$= a(ba)b$$
$$= a(ab)b$$
$$= a^2 b^2$$

prooved.

OR

$$a \circ b = b \circ a$$
$$\Rightarrow a \circ a \circ b = a \circ b \circ a$$
$$\Rightarrow a^2 b = aba$$
$$\Rightarrow a^2 b \circ b = abab$$
$$\Rightarrow a^2 b^2 = abab = a(ba)b = (ab)(ab)$$
$$= (ab)^2$$

eg. 16.5 Let $G = (Z_6, +)$.
$H = \{0, 2, 4\}$.

$+$	0	2	4
0	$0+_6 0 = 0$	$0+2 = 2$	$0+4 = 4$
2	$0+_6 2 = 2$	$2+2 = 4$	$2+4 = 6 \% 6 = 0$
4	$0+_6 4 = 4$	$4+_6 2 = 6\%6 = 0$	$4+4 = 8\%6 = 2$

C1. $(H, +)$ is closed under $+$ as every element $\in H$.

C2. Associativity:

$(0+2)+4 = 0+(2+4)$
$= 2+4 \quad = 0+6$
$= 6\%6 = 0. \quad = 6\%6 = 0.$
✓

C3: Identity: $0+0=0$.
$0+2=2$
$0+4=4$.
Hence $e=0$.

C4: Inverse: $0+0=0$.
$2+4=0$.
$4+2=0$.
Hence, inverse exists for every element.

C5: Commutative.
$0+2 = 2+0$.
$= 2 \quad = 2$ Hence, commutative.

def^n 16.3 Subgroup.

$H \subseteq G$ if H is a group under the binary opt of G.

$a, b \in H \Rightarrow ab \in H$.

$(\mathbb{Z}, +)$ subgp. $(\mathbb{Q}, +)$ sub gp $(\mathbb{R}, +)$ Additive.

$(\mathbb{Z}, \cdot)$ is not sub gp $(\mathbb{Q}, \cdot)$

Theorem 16.2 $H \subseteq G$ which is non empty.
H subgroup of G iff
(I) $\forall a, b \in H$, $ab \in H$. (finite set)
(II) $\forall a \in H$, $a^{-1} \in H$.

Theorem 16.3 If G is a group.
$\phi \neq H \subseteq G$.
H is finite then H is subgroup of G
iff H is closed under the binary opt^n of G.

Q10) G is abelian iff $\forall a, b \in G$
$(ab)^{-1} = a^{-1}b^{-1}$

$(a^{-1}b^{-1}) = (ab)^{-1}$
$\Rightarrow a^{-1}b^{-1} = b^{-1}a^{-1}$
$\Rightarrow ba^{-1}b^{-1} = bb^{-1}a^{-1}$
$\Rightarrow ba^{-1}b^{-1} = a^{-1}$
$\Rightarrow ba^{-1}b^{-1}b = a^{-1}b$.
$\Rightarrow ba^{-1} = a^{-1}b$
$\Rightarrow ba^{-1}a = a^{-1}ba$.
$\Rightarrow b = a^{-1}ba$
$\Rightarrow ab = aa^{-1}ba$.
$\Rightarrow ab = ba$ prooved. commutative.

Q15) G is a group.

$H = \{a \in G \mid ag = ga \ \forall \ g \in G\}$

C1: Let $a_1, a_2 \in H$.

$a_1 g = g a_1$.

$\Rightarrow a_1 g g^{-1} = g a_1 g^{-1}$

$\Rightarrow a_1 = g a_1 g^{-1}$

$\therefore a_2 = g a_2 g^{-1}$

$a_1 \cdot a_2 = g a_1 g^{-1} g a_2 g^{-1}$

$= g a_1 a_2 g^{-1} \in G$.

$\therefore$ closure is satisfied.

C(ii) $g \in G$. and $x \in H$.

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

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

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

$\Rightarrow g x^{-1} = x^{-1} g$, ~~and~~ hence $x^{-1} \in H$.

If $x, y \in H$, then $xg = gx$ and $yg = gy$.

$(xy)g = x(yg)$

$\Rightarrow x(gy) = (xg)y = (gx)y = g(xy)$

$\therefore xy \in H$.

Hence, H is a subgroup.