ABSTRACT ALGEBRA

By,

Mrs.Sirin Hasina

ABSTRACT ALGEBRA

Subject code : 7BMA3C1

Syllabus :

Unit - I :

Groups Definition and Examples - Elementary Properties of a group - equivalent definitions of a group - Permutation groups.

Unit - II :

Subgroups - cyclic groups - order of an elements - cosets and lagrange's theorem.

Unit - III :

Normal subgroups and Quotient groups - Isomorphism - Homomorphism.

Unit - IV :

Rings : definition and examples - elementary properties of rings -

Isomorphism – types of rings – characteristics of a ring – sub rings – Ideals – Quotient rings.

Unit – V :

Maximal and Prime Ideals – Homomorphism of rings – field of Quotients of an integral domain – unique factorization domain – Euclidean domain.

Text Book :

S. Arumugam and A. Thanga Pandi Modern Algebra Scitech Publication Pvt. Lt Chennai – 2003.

Unit	Chapter	Section
Unit – I	Chapter – 3	Section 3.1 to 3.4
Unit – II	Chapter – 3	Section 3.5 to 3.8
Unit – III	Chapter – 3	Section 3.9 to 3.11
Unit – IV	Chapter – 4	Section 4.1 to 4.8
Unit – V	Chapter – 4	Section 4.9 to 4.10 4.12 to 4.14

Unit 1

Unit - I :

Groups Definition and Examples - Elementary Properties of a group - equivalent definitions of a group - Permutation groups.

UNIT. 1

sec 3.1 **GROUPS** page 1

2m ☆☆ Definition and Examples :-

Definition :-

A non-empty set G together with a binary operation $*: G \times G \to G$ is called a group, if the following conditions are satisfied

i) $*$ is closed
ie, $a,b \in G \Rightarrow a*b \in G$.

ii) $*$ is associative
ie, $a*(b*c) = (a*b)*c$, $\forall a,b,c \in G$.

iii) there exists an element $e \in G$, such that $a*e = e*a = a$ for all $a \in G$.

iv) For any element in G there exists an element $a' \in G$ such that
$a*a' = a'*a = e$.
a' is called inverse of a.

Examples :-

1) Z, Q, R, C are groups under addition.

Soln :-

i) Closure axiom :-

For all $a, b \in Z \Rightarrow a+b \in Z$ / (Q/R)

$\therefore$ Z is a closure with respect to addition.

ii) Associative axiom :-

Let $a, b, c \in Z$ then

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

$\therefore$ Z is a associative under addition.

iii) Existence of identity :-

$0+a = a+0 = a, \ \forall a \in Z.$

$\therefore$ 0 is the identity element of Z.

iv) Existence of inverse :-

If $a \in Z$, then $-a \in Z$.

$(-a)+a = a+(-a) = 0.$

Hence, the inverse element exists

$\therefore$ Z is a group under addition.

"

2) $C = \{x+iy \,/\, x, y \in R\}$.

(3)

i) Closure axiom :-

For all $a, b \in C$

$a = x_1 + iy_1$

$b = x_2 + iy_2$

$$a+b = (x_1+iy_1) + (x_2+iy_2)$$

$$= \underbrace{(x_1+x_2)}_{x} + i \underbrace{(y_1+y_2)}_{y} \in C.$$

$x + i\,y \in C$

$\therefore$ C is a closure under addition.

ii) Associative axiom :-

Let $a, b, c \in C$.

$a = x_1 + iy_1$

$b = x_2 + iy_2$

$c = x_3 + iy_3$.

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

$$(x_1+iy_1) + [(x_2+iy_2) + x_3 + iy_3] = [(x_1+iy_1 + x_2 + iy_2)] + (x_3+iy_3)$$

$$(x_1+iy_1) + [(x_2+x_3) + i(y_2+y_3)] = [(x_1+x_2) + i(y_1+y_2)] + x_3 + iy_3$$

$(x_1+x_2+x_3)+i(y_1+y_2+y_3) = (x_1+x_2+x_3) +$
$i(y_1+y_2+y_3) \in C.$

$x + iy \in C$

$\therefore C$ is associative under addition.

iii) Existence of identity :-

Let $a, e \in C$.

$a = x+iy$

$e = 0+i0$

$a+e = (x+iy)+(0+i0)$

$= x+iy.$

$e+a = (0+i0)+(x+iy)$

$= x+iy.$

$a+e = e+a \in C.$

$\therefore e$ is the identity element of C.

iv) Existence of inverse :-

Let $a, -a \in C$.

$-a+a$

$a = x+iy$

$-a = -a(x+iy)$

$a+(-a) = (x+iy)-(x+iy)$

$= 0+i0.$

Hence, the identity element exists.

$\therefore C$ is a group under addition.

3) The set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $a, b, c, d \in R$ is a group under matrix addition.

5

soln :-

$$M = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle/ a, b, c, d \in R \right\}.$$

i) Closure axiom :-

let $A, B \in M$

$$A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 3 & 4 \\ 4 & 3 \end{pmatrix}.$$

$$A + B = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} + \begin{pmatrix} 3 & 4 \\ 4 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 4 & 6 \\ 6 & 4 \end{pmatrix} \in M.$$

$\therefore$ M is a closure under addition.

ii) Associative axiom :-

let $A, B, C \in M$.

$$A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 3 & 4 \\ 4 & 3 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}$$

$$A + (B + C) = (A + B) + C$$

(b)

$$A+(B+C)=\begin{pmatrix}1&2\\2&1\end{pmatrix}+\left[\begin{pmatrix}3&4\\4&3\end{pmatrix}+\begin{pmatrix}1&1\\2&2\end{pmatrix}\right].$$

$$=\begin{pmatrix}5&7\\7&5\end{pmatrix}\in M \rightarrow (1)$$

$$(A+B)+C=\left[\begin{pmatrix}1&2\\2&1\end{pmatrix}+\begin{pmatrix}3&4\\4&3\end{pmatrix}\right]+\begin{pmatrix}1&1\\2&2\end{pmatrix}$$

$$=\begin{pmatrix}5&7\\7&5\end{pmatrix}\in M. \rightarrow (2)$$

$\therefore$ (1) = (2)

$\therefore$ M is associative under addition.

iii) Existence of identity :-

Let $A, E \in M$.

$$A=\begin{pmatrix}1&1\\2&2\end{pmatrix} \text{ and } E=\begin{pmatrix}0&0\\0&0\end{pmatrix}$$

$$A+E=E+A=A$$

$$\begin{pmatrix}1&1\\2&2\end{pmatrix}+\begin{pmatrix}0&0\\0&0\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}+\begin{pmatrix}1&1\\2&2\end{pmatrix}$$

$$\begin{pmatrix}1&1\\2&2\end{pmatrix}=\begin{pmatrix}1&1\\2&2\end{pmatrix}\in M.$$

$\therefore$ E is the identity element of M.

iv) Existence of inverse:

Let $A, -A \in M$.

$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ and $-A = -\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$

$A + (-A) = -A + A = E$

$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = -\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$

$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in M$

Hence, the identity element exists.

$\therefore$ M is a group under addition.

//

4) N is not a group under usual addition.

Since there is no element $e \in N$, such that $x + e = x$. But N is a semi group.

5) The set E of all even integers under usual addition is a group.

Soln:

For, $a, b \in E \Rightarrow a + b \in E$

$0 \in E$ is the identity element.

If $a \in E$, $-a \in E$ is the inverse of a.

"

6) Q^* and R^* under usual multiplications are groups.

soln:-

Since 1 is the identity element and the inverse of a is $1/a$.

7) The set of all 2×2 non-singular matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $a, b, c, d \in R$, is a group under matrix multiplication.

soln:-

$$M = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Big| \ a, b, c, d \in R \right\}.$$

i) Closure axiom:-

Let $A, B \in M$.

$$A = \begin{pmatrix} 1 & 2 \\ 4 & 5 \end{pmatrix} \text{ and } B = \begin{pmatrix} 3 & 6 \\ 2 & 1 \end{pmatrix}$$

$$AB = \begin{pmatrix} 1 & 2 \\ 4 & 5 \end{pmatrix} \cdot \begin{pmatrix} 3 & 6 \\ 2 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 3+4 & 6+2 \\ 12+10 & 24+5 \end{pmatrix}$$

$$= \begin{pmatrix} 17 & 8 \\ 22 & 29 \end{pmatrix} \in M.$$

$\therefore$ M is a closure under matrix multiplication.

ii) <u>Associative axiom</u>:

let $A, B, C \in M$

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}$$

$$A(BC) = (AB)C.$$

$$A(BC) = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \left[\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix} \right]$$

$$= \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 1+6 & 2+2 \\ 2+3 & 4+1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 7 & 4 \\ 5 & 5 \end{pmatrix}$$

$$= \begin{pmatrix} 7+10 & 4+10 \\ 21+20 & 12+20 \end{pmatrix}$$

$$= \begin{pmatrix} 17 & 14 \\ 41 & 32 \end{pmatrix} \in M. \rightarrow (1)$$

$$(AB)C = \left[\begin{pmatrix}1 & 2\\3 & 4\end{pmatrix}\begin{pmatrix}1 & 2\\2 & 1\end{pmatrix}\right]\begin{pmatrix}1 & 2\\3 & 1\end{pmatrix}$$

$$= \begin{pmatrix}1+4 & 2+2\\3+8 & 6+4\end{pmatrix}\begin{pmatrix}1 & 2\\3 & 1\end{pmatrix}$$

$$= \begin{pmatrix}5 & 4\\11 & 10\end{pmatrix}\begin{pmatrix}1 & 2\\3 & 1\end{pmatrix}$$

$$= \begin{pmatrix}5+12 & 10+4\\11+30 & 22+10\end{pmatrix}$$

$$= \begin{pmatrix}17 & 14\\41 & 32\end{pmatrix} \in M \rightarrow (2)$$

$(1) = (2)$.

$\therefore$ M is a associative under matrix multiplication.

iii) Existence of identity:-

Let $A, E \in M$.

$$A = \begin{pmatrix}1 & 2\\2 & 1\end{pmatrix} \text{ and } E = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}.$$

$AE = EA = A$

$$AE = \begin{pmatrix}1 & 2\\2 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$$

$$= \begin{pmatrix}1+0 & 0+2\\2+0 & 0+1\end{pmatrix}$$

11

$$= \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \in M \rightarrow (1)$$

$$EA = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \in M. \rightarrow (2)$$

$(1) = (2)$.

$\therefore$ E is the identity element of M.

iv) Existence of inverse :-

Let $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$

$$A^{-1} = \frac{1}{|A|} (\text{adj } A)$$

$$|A| = \begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix}$$

$$= 4 - 6$$

$$= -2$$

$$|A| = -2.$$

$$\text{adj } A = \begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix}$$

$$A^{-1} = -\frac{1}{2}\begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix}$$

$$A^{-1} = \begin{pmatrix} -2 & 1 \\ 3/2 & -1/2 \end{pmatrix}$$

$$AA^{-1} = A^{-1}A = E$$

$$= \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} -2 & 1 \\ 3/2 & -1/2 \end{pmatrix} \quad \begin{pmatrix} -2 & 1 \\ 3/2 & -1/2 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} -2+3 & 1-1 \\ -6+6 & 3-2 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M.$$

Hence, the identity element exists

$\therefore$ M is a group under matrix multiplication.

8) Q^+ is a group under usual multiplication?

13

Soln:-

$$Q^+ = \{ p/q , q \neq 0 \}.$$

i) Closure axiom:-

Let $a, b \in Q^+$.

$$a = 1/x , \quad b = 1/y .$$

$$ab = 1/xy \in Q^+$$

$\therefore Q^+$ is a closure under usual multiplication.

ii) Associative axiom:

Let $a, b, c \in Q^+$

$$a = 1/x , b = 1/y , c = 1/z .$$

$$a(bc) = (ab) c$$

$$1/x (1/yz) = (1/xy) 1/z$$

$$\frac{1}{xyz} = \frac{1}{xyz} \in Q^+$$

$\therefore Q^+$ is a associative under usual multiplication.

(14) iii) Existence of identity :-

let $a, e \in Q^+$

$a = 1/x, \quad e = 1/1.$

$ae = 1/x \cdot 1/1$

$= 1/x \in Q^+$

$\therefore$ e is the identity element of Q^+.

iv) Existence of inverse :-

let $a, a^{-1} \in Q^+$

$a = 1/x, \quad a^{-1} = x/1.$

$a \cdot a^{-1} = 1/x \cdot x/1$

$= 1/1 \in Q^+$

$a \cdot a^{-1} = a^{-1} \cdot a = a$

Hence, the inverse element exists.

$\therefore Q^+$ is the group under usual multiplication.

//

9) $(Z, \cdot)$ is not a group.

Solution:-

15

$1 \in Z$ is the identity element but inverse element is not exists.

$\therefore Z$ is monoid.

10) Let $G = \{e\}$ and $e * e = e$ clearly G is a group.

11) Let $G = \{1, -1\}$ is a group under usual multiplication.

Soln:-

1 is the identity element.

The inverse of each element is itself

$\cdot$	1	-1
1	1	-1
-1	-1	1

Conversely,

let $a^m = e$.

Let $m = nq + r$, where $0 \le r < n$

$$a^m = a^{nq+r}$$

$$= a^{nq} a^r$$

$$= e a^r = a^r$$

$\therefore a^r = e$ and $0 \le r < n$.

Now, since n is the smallest +ve integer.

such that $a^n = e$, we have $r = 0$

Hence $m = nq$.

$\therefore n / m$.

THEOREM : 2.13

Let G be a group and $a, b \in G$,

u.q

then

i) Order of a = Order of a^{-1}

ii) Order of a = Order of $b^{-1}ab$

iii) Order of ab = Order of ba.

Proof:-

i) Let a be an element of order n.

Then $a^n = e$

$$(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$$

Now, if possible let $0 < m < n$ and $(a^{-1})^m = e$.

$\therefore (a^m)^{-1} = e$. Hence $a^m = e$ which contradicts the definition, of the order of a. Thus, n is the least positive integer such that $(a^{-1})^n = e$.

$\therefore$ The order of a^{-1} is n.

ii) We shall first prove that for any positive integer r.

$$(b^{-1}ab)^r = b^{-1}a^r b \quad \rightarrow (1)$$

(1) is trivially true. if $r=1$

Now, suppose that (1) is true for $r=k$.

so that, $(b^{-1}ab)^k = b^{-1}a^k b$.

Then,

$$(b^{-1}ab)^{k+1} = (b^{-1}ab)^k (b^{-1}ab)$$
$$= (b^{-1}a^k b)(b^{-1}ab)$$
$$= b^{-1}a^{k+1}b.$$

Hence by induction (1) is true for all positive integers.

Now, let a be an element of order n.

Then $a^n = e$

$\therefore (b^{-1}ab)^n = (b^{-1}a^n b)$ [by (1)]

$= b^{-1}eb$

$= e$

Now, if possible let $0 < m < n$, and $(b^{-1}ab)^m = e$

$\therefore b^{-1}a^m b = e$. Hence $a^m = e$.

Which contradicts the definition of the order of a. Thus n is the least positive integer such that $(b^{-1}ab)$ is n.

iii) The order of ab = The order $a^{-1}(ab)a$ [by ii]

= The order of ba.

THEOREM : 2.14

Let G be a group and let a be an element of order n in G. Then the order of a^s, where $0 < s < n$, is n/d (n divides d), where d is greatest common divisor [G.C.D] of n and s.

Proof:

Let $(n/d) = k$ and $(s/d) = l$

so that k and l are relatively prime.

Now, $(a^s)^k = a^{sk}$

$= a^{ldk}$ $\Rightarrow s = dl$

$= a^{ln}$ $\Rightarrow dk = n$

$= (a^n)^l = e$

Further if m is any +ve integer such that $(a^s)^m = e$ then

$a^{sm} = e$

since order of a is n.

We have n / sm

$\therefore kd / ldm$

Hence k / lm.

But k and l are relatively prime.

Hence k/m so that $m \geq k$.

Thus k is the least positive integer such that $(a^s)^k = e$

$\therefore$ Order of $a^s = k = n/d$.

Corollary :1

The order of any power of 'a' cannot exceed the order of 'a'.

Corollary :2

Let G be a finite cyclic group of order n generated by an element a. Then a^s generates a cyclic group of order n divides d, where d is 30

G.C.D (Greatest Common Divisor).

Corollary : 3

Let G be a finite cyclic group of order n, generated by an element a. a^s is a generator of G if and only if s and n are relatively prime. Hence, the number of generators of a cyclic group of order n is $\phi(n)$. where $\phi(n)$ is the number of +ve integer less than n and relatively prime to n.

for example,

Consider the group $(Z_{12}, \oplus)$.

$\phi(12) = 4$.

Hence, the group exactly 4 generators and they are 1, 5, 7, 11.

Solved Problems:-

1) If G is a finite group with even number of elements, then G contains atleast one element of order 2.

soln:

a is an element of order $2 \Leftrightarrow a^2 = e$

$\Leftrightarrow a^{-1} = a$

Hence, it is enought to prove that there exists an element different from e in G, whose inverse is itself.

Let $S = \{a \mid a \in G, a \neq a^{-1}\}$

Clearly $a \in S \Rightarrow a^{-1} \in S$ and $a \neq a^{-1}$.

Hence S contains an even number of element.

Also, $e \notin S$

Hence $S \cup \{e\}$ contains an odd number of elements.

Since, the order of the group is even, there exists atleast one element $a \notin S \cup \{e\}$

Clearly $a = a^{-1}$.

2) The order of a permutation P is the L.C.M of the length. if it's disjoint cycle. 32

soln.

Let $P = c_1, c_2, \ldots, c_r$,

where c_i's are mutually disjoint cycle of length l_i.

Now, let $P^m = e$.

Since, the product of disjoint cycle is commutative.

$$e = P^m = (c_1 c_2 \ldots c_r)^m$$

$$= c_1^m c_2^m \ldots c_r^m$$

Now, since, the elements moved by one cycles are left fixed by all the other cycles.

$$c_1^m = c_2^m = \ldots c_r^m = e.$$

Now, $c_1^m = e \Rightarrow l_1/m$.

Since, the order of $c_1 = l_1$

Similarly $l_2, l_3, \ldots, l_r$ divide m.

Thus m is a common multiple of $l_1, l_2, \ldots, l_r$.

$\therefore$ The order of P is the least, such m which is obviously the L.C.M of $l_1, l_2, \ldots l_r$.

Example [for thrm: 2]

1. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 4 & 1 & 2 & 3 \end{pmatrix} = P$

(2 elmts) (4 elmts)

The cycle of $P = (1\ 5)(2\ 7\ 3\ 6)$ (4)

L.C.M $2 \times 2 = 4$

The order of permutation is 4

3) If a is the generator of the cyclic group G. If there exists two unequal integers m and n, such that $a^m = a^n$. Prove that G is a finite group.

Soln:

Since m and n are unequal

We may assume that m greater than n

Hence $m-n$ is a positive integer.

Also, $a^m = a^n$

$a^{m-n} = e$

$\therefore$ order of a is finite.

$\therefore$ $G = \langle a \rangle$ is a finite group.

[By thrm: 2.10]

Cosets And Lagrange's Theorem.

Definition:

Let H be a subgroup of G. Let $a \in G$. Then the set $aH = \{ah / h \in H\}$ is called the left coset of H, defined by a in G.

Similarly $Ha = \{ha / h \in H\}$ is called the right coset of H, defined by a in G.

Example:

1) Let us determine, the left ~~coach~~ cosets of $(5Z, +)$ in $(Z, +)$.

Here, the operation is '+'.

$0 + 5Z = 5Z$ is the left coset

$1 + 5Z = \{1 + 5n / n \in Z\}$

$2 + 5Z = \{2 + 5n / n \in Z\}$

$3 + 5Z = \{3 + 5n / n \in Z\}$

and $4 + 5Z = \{4 + 5n / n \in Z\}$

These are all the left cosets of $(5Z, +)$

2) 35 Consider $(Z_{12}, \oplus)$, then $H = \{0, 4, 8\}$ is a subgroup of G.

$0 + H = \{0, 4, 8\}$ aH

$1 + H = \{1, 5, 9\}$

$2 + H = \{2, 6, 10\}$

$3 + H = \{3, 7, 11\}$

$4 + H = \{4, 8, 0\}$. etc...

There are 4 left cosets.

$H + 0 = \{0, 4, 8\}$ Ha.

$H + 1 = \{1, 5, 9\}$

$H + 2 = \{2, 6, 10\}$

$H + 3 = \{3, 7, 11\}$

$H + 4 = \{4, 8, 0\}$ etc...

There are 4 right cosets.

U.Q

THEOREM: 2.15

Let G be a group and H be a subgroup of G. Then if & only if

i) $a \in H \Rightarrow aH = H$

ii) $aH = bH \Rightarrow a^{-1}b \in H$

iii) $a \in bH \Rightarrow a^{-1} \in Hb^{-1}$

iv) $a \in bH \Rightarrow aH = bH$

Proof :-

i) Let $a \in H$. We claim that $aH = H$

Let $x \in aH$. Then $x = ah$ for some $h \in H$.

Now $a \in H$ and $h \in H \Rightarrow ah = x \in H$

(Since H is a subgroup)

Hence $aH \subseteq H$

Let $x \in H$. Then $\underline{x = a(a^{-1}x)} \in aH$

Hence $H \subseteq aH$. Thus $H = aH$

$x = h$
$= aa^{-1}h$
$= a(a^{-1}h)$ [$x = h$]
$a(a^{-1}x)$

Conversely,

Let $aH = H$. Now $a = ae \in aH$

$\therefore a \in H$

ii) Let $aH = bH$

$\therefore a^{-1}(aH) = a^{-1}(bH)$

$H = \underline{(a^{-1}b)}^{a} H$

$aH = H$

$\therefore \underline{a^{-1}b} \in H$ [by i] $a \in H$

Conversely,

Let $a^{-1}b \in H$

Then $a^{-1}bH = H$ [by i]

$\therefore aa^{-1}bH = aH$

Hence $aH = bH$

iii) Let $a \in bH$.

Then $a = bh$ for some $h \in H$.

$\therefore a^{-1} = (bh)^{-1}$

$= h^{-1}b^{-1} \in Hb^{-1}$

Converse can be similarly proved.

iv) let $a \in bH$

We claim that $aH = bH$

let $x \in aH$

Then $x = ah_1$ for some $h_1 \in H$.

Also,

$a \in bH \Rightarrow a = bh_2$ for some $h_2 \in H \rightarrow$ ①

$\therefore x = (bh_2)h_1$

$= b(h_2 h_1) \in bH$.

$\therefore aH \subseteq bH$.

Now, let $x \in bH$. Then $x = bh_3$ for some $h_3 \in H$

Also, from ①, $b = ah_2^{-1}$

$\therefore x = ah_2^{-1}h_3 \in aH$.

$\therefore bH \subseteq aH$

Hence $aH = bH$

Conversely,

let $aH = bH$

Then,

$a = ae \in aH$

$\therefore a \in bH$

THEOREM: 2.16

Let H be a subgroup of G.

Then, i) any two left cosets of H are either identical or disjoint

ii) Union of all the left cosets of H is G

iii) The number of elements in any left coset aH is the same as the number of element in H) Lgrge Thm.

Proof:

i) Let aH and bH be the two left cosets.

Suppose aH and bH are not disjoint.

We claim that $aH = bH$.

Since aH and bH are not disjoint.

$aH \cap bH \neq \phi$

$\therefore$ There exists an element $c \in aH \cap bH$

$\therefore c \in aH$ and $c \in bH$

$\therefore aH = cH$ and $bH = cH$

[by (iv) of thrm: 2.15]

$\therefore aH = bH$

ii) Let $a \in G$. Then $a = ae \in aH$.

$\therefore$ Every element of G belongs to a left coset of H

$\therefore$ The union of all the left cosets of H is G.

iii) The map $f: H \to aH$ defined by $f(h) = ah$ is clearly a bijection. Hence every left coset has the same number of elements as H.

Note: 1

This theorem show that the collection of all left cosets forms a partition of the group.

Note: 2

The above result is true if we replace left cosets by right cosets. In what follows, the results we prove for left cosets are also true for right cosets.

THEOREM : 2.17

Let H be a subgroup of G. The number of left cosets of H is the same as the number of right cosets of H.

Proof:-

Let L and R respectively denote the set of left and right cosets of H.
We define a map $f : L \to R$ by $f(aH) = Ha^{-1}$.
f is well defined. For $aH = bH \Rightarrow a^{-1}b \in H$
$\Rightarrow a^{-1} \in Hb^{-1}$
$\Rightarrow Ha^{-1} = Hb^{-1}$

f is 1-1 for

$$f(aH) = f(bH)$$
$$\Rightarrow Ha^{-1} = Hb^{-1}$$
$$\Rightarrow a^{-1} \in Hb^{-1}$$
$$\Rightarrow a^{-1} = hb^{-1} \text{ for some } h \in H.$$
$$(a^{-1})^{-1} = (hb^{-1})^{-1}$$
$$\Rightarrow a = bh^{-1} \qquad = (b^{-1})^{-1}h^{-1}$$
$$\Rightarrow a \in bH \qquad = bh^{-1}$$
$$\Rightarrow aH = bH$$

f is onto. For, every right cosets Ha has a pre-image under f namely $a^{-1}H$.

Hence f is a bijection from L to R. Hence the number of left cosets is the same as the number of right cosets.

Definition :-

Let H be a subgroup of G. The number of distinct left (right) cosets of H in G is called the index of H in G and is denoted by $[G : H]$

~~Remark:~~

Example :-

In $(Z_8, \oplus)$, $H = \{0, 4\}$ is a subgroup. the left cosets of H are

$0 + H = \{0, 4\}$

$1 + H = \{1, 5\}$

$2 + H = \{2, 6\}$

$3 + H = \{3, 7\}$

$\cancel{4 + H = \{4, 0\}}$

These are the 4 distinct left cosets of H.

Hence, the index of the subgroup H is 4.

Note :- 42

$[Z_8 : H] \times |H| = 4 \times 2 = 8 = |Z_8|$

Remark :-

Let H be a subgroup of G. We define a relation in G as follows.

Define $a \sim b \Leftrightarrow a^{-1}b \in H$

Then '$\sim$' is an equivalence relation.

Proof :-

For, $a^{-1}a = e \in H$. Hence $a \sim a$.

Hence $\sim$ is reflexive.

$a \sim b \Rightarrow a^{-1}b \in H \Rightarrow (a^{-1}b)^{-1} \in H$

$\Rightarrow b^{-1}a \in H \Rightarrow b \sim a$

$\therefore a \sim b = b \sim a$

Hence $\sim$ is symmetric.

Now,

$a \sim b$ and $b \sim c \Rightarrow a^{-1}b \in H$ and $b^{-1}c \in H$

$\Rightarrow (a^{-1}b)(b^{-1}c) \in H$

$\Rightarrow a^{-1}c \in H$

$\Rightarrow a \sim c$.

Hence $\sim$ is transitive.

Thus, $\sim$ is an equivalence relation.

Now, we claim that equivalence class, $[a] = aH$.

Let $b \in [a]$. Then $a \sim b$.

$\therefore a^{-1}b \in H$.

$\therefore a^{-1}b = h$ for some $h \in H$.

$b = ah$; Hence $b \in aH$

$\therefore [a] \subseteq aH$

Also,

$b \in aH \Rightarrow b = ah$ for some $h \in H$.

$\Rightarrow a^{-1}b = h \in H$

$\Rightarrow a \sim b$

$\Rightarrow b \in [a]$

Thus, the left cosets of H in G are ~~preciously~~ precisely the equivalence classes determined by $\sim$. Hence, the left cosets form a partition of G. This is a another proof of Theorem: 2.17

Lagrange's Theorem :- 44 [Thrm: 2.18]

or

sm

Let G be a finite group of order n and H be any subgroup of G. Then the order of H divides the order of G.

Proof :-

Let $|H| = m$ (o(H)) and $[G : H] = r$, then the number of distinct left cosets of H in G is r.

[By thrm: 2.16]

these r left cosets are mutually disjoint, they have the same number of elements namely m and their union is G.

$\therefore n = rm$

Hence m divides n ~~(or) $[G : H]$~~ $= \frac{|G|}{|H|}$.

Corallory :-

$$[G : H] = \frac{|G|}{|H|}$$

Note : 1

The converse of lagrange's theorem is not true.

ie) If G is a group of order n and m divides n, then G need not have a subgroup of order m.

Example :-

A_4 is a group of order 12, and it doesn't have a subgroup of order 6.

let $G = \{1, -1, i, -i\}$ is gp of order 4
and $H = \{1, -1\}$ is a subgp of order 2
and the other subset $(i, -i)$ of order 2

But $(i, -i)$ is not a sub gp

Note : 2

(Ex. for Lagrange's theorem) A group G of order 8, cannot have subgroups of order 3, 5, 6 (or) 7 infact any proper subgroup of G must be of order 2 or 4

Note : 3

Any group of prime order has no proper subgroup.

THEOREM : 2.19

The order of any element of a finite group G divides the order of G.

Proof:

Let G be a group of order n.

Let $a \in G$, be an element of order m.

Then the order a is the same as the order of the cyclic group $\langle a \rangle$.

Now, by the lagrange's theorem, the order of the subgroup $\langle a \rangle$ divides the order of G.

Hence, m/n.

THEOREM : 2.20

Every group of prime order is cyclic.

Proof:

Let G be a group of order p, where p is prime.

Let $a \in G$, and $a \neq e$.

[By thrm: 2.18]

order of a divides p.

$\therefore$ Order of a is 1 or p.

Since $a \neq e$, order of a is p.

Hence, $G = \langle a \rangle$ so that G is cyclic.

THEOREM: 2.21

Let G be a group of order n. Let $a \in G$. Then $a^n = e$.

Proof:-

Let the order of a be m.

Then m divides n.

Hence, $n = mq$

$$\therefore a^n = a^{mq}$$

$$= (a^m)^q$$

$$= e^q$$

$$= e$$

$\therefore a^n = e$.

THEOREM: 2.22

EULER'S THEOREM:

If n is any integer and $(a, n) = 1$ then $a^{\phi(n)} \equiv 1 \pmod{n}$

($\phi(n)$ is the number of positive integer less than n relatively prime to n)

Proof:-

Let $G = \{m \mid m < n \text{ and } (m, n) = 1\}$

G is a group under multiplication modulo n. This group of order is $\phi(n)$

Now, let $(a, n) = 1$

Let $a = qn + r, \ 0 \le r < n$.

so that $a \equiv r \pmod{n}$

since $(a, n) = 1$

We have $(n, r) = 1$

so that $r \in G$.

$\therefore r^{\phi(n)} = 1$ (by thm: 2.21)

$\therefore r^{\phi(n)} \equiv 1 \pmod{n}$

Also, $a^{\phi(n)} \equiv r^{\phi(n)} \pmod{n}$

so that $a^{\phi(n)} \equiv 1 \pmod{n}$ [$\because$ '$\equiv$' transitive]

Hence proved.

Unit 3

Unit - III :

Normal subgroups and Quotient groups - Isomorphism - Homomorphism.

Modern Algebra

By,
Mrs M.Sirin Hasina

Unit 3

Unit - iii :

Normal Subgroups and Quotient groups - Isomorphism - Homomorphism.

THEOREM : 2.23

FERMAT's THEOREM :-

Let p be a prime number and a be any integer, relatively prime to p. then, $a^{p-1} \equiv 1 \pmod p$

Proof :-

Since p is prime, $\phi(p) = p-1$ and hence, the result follows from Euler's theorem.

THEOREM : 2.24

A group G has no proper subgroups, iff it is a cyclic group of prime order.

Proof:-

Suppose, G is a group of prime order.

Then, it follows from lagrange's theorem that G has no proper subgroups.

Conversly,

Let G be a group having no proper subgroup.

First we shall prove that G is cyclic.

Suppose G is not cyclic.

let $a \in G$ and $a \neq e$.

Then, the cyclic group $\langle a \rangle$ is a proper subgroup of G, which is a contradiction.

Hence, G is cyclic.

Also G cannot be infinite, for an infinite cyclic group contains a proper subgroup, $\langle a^2 \rangle$.

Hence G must be of finite order say, n.

We claim that, n is prime. If possible let n be a composite number. let $n = pq$ where $p, q > 1$.

Let $a \in G$ be a generator of the group.

Then $\langle a^p \rangle$ is a subgroup of order q and hence is a proper subgroup of G, which is a contradiction.

Hence n is prime.

$\therefore$ G is cyclic group of prime order

Solved Problem :- 5)

1) Let A and B be a subgroups of
5m finite group G, such that A is a
U.Q subgroup of B. Show that

$[G:A] = [G:B][B:A]$

Sol,

$$[G:A] = \frac{|G|}{|A|}$$

$$[G:B] = \frac{|G|}{|B|}$$

$$[B:A] = \frac{|B|}{|A|}$$

R.H.S

$$[G:B]\ [B:A] = \frac{|G|}{|B|}\ \frac{|B|}{|A|}$$

$$= \frac{|G|}{|A|}$$

$$= [G:A]$$

$$= L.H.S$$

Hence proved.

2) Let A and B be two finite subgroups of a group G, such that $|A|$ and $|B|$ have no common divisors. Then show that $A \cap B = \{e\}$.

Soln:

W.K.T:-

$A \cap B$ is a subgroup of A and B.

By lagrange's theorem,

$|A \cap B|$ divides $|A|$ and $|B|$

have no common divisors.

$\therefore |A \cap B| = 1$

Hence $A \cap B = \{e\}$.

3) Let H and k be two subgroups of G of finite index in G. Prove that $H \cap K$ is a subgroup of finite index in G.

Soln:

(By theorem : 2.5)

$H \cap K$ is a subgroup of G.

Let $[G : H] = m$ and $[G : k] = n$.

We claim that for any $a \in G$.

$(H \cap K)a = Ha \cap ka$.

Clearly, $H \cap K \subseteq H$ and K.

$(H \cap K)a \subseteq Ha$ and Ka.

$(H \cap K)a \subseteq Ha \cap Ka \longrightarrow (1)$

Now, let $x \in Ha \cap Ka$.

$\therefore x \in Ha$ and $x \in Ka$.

$\therefore x = ha$ for some $h \in H$ and

$x = ka$ for some $k \in H$.

$\therefore x = ha = ka$

$\therefore h = k$

$\therefore h \in H \cap K$

$\therefore x \in (H \cap K)a$

$\therefore Ha \cap Ka \subseteq (H \cap K)a \longrightarrow (2)$

From (1) & (2), we have,

$(H \cap K)a = Ha \cap Ka$,

$\therefore$ Every right coset of $H \cap K$ in G is the intersection of a right coset of H and a right coset of K.

Also, since $[G:H] = m$, the number of right cosets of H in G is m.

Similarly, the number of right cosets of K in G is n.

Hence the number of right cosets of $H \cap K$ in G is almost mn.

$\therefore [G : H \cap K] \leq mn.$

$\therefore$ $H \cap K$ is a subgroup of finite index in G.

A) Let H and K be two finite subgroups of a group G. Then ~~$|HK|$ or~~ $o(HK) = \frac{|H||K|}{|H \cap K|}$

or $o(HK) = \frac{o(H)\,o(K)}{o(H \cap K)}$

proof:-

Let $L = H \cap K$. Since H and K are subgroups of G, L is also a subgroup of G.

$L \subseteq H$ and K

Now, let $Lx_1, Lx_2, \ldots Lx_m$ be the distinct right cosets of L in K so that

$K = Lx_1 \cup Lx_2 \cup \ldots \cup Lx_m \rightarrow (1)$

and

$m = [K : L] = \frac{|K|}{|L|} = \frac{|K|}{|H \cap K|} \rightarrow (2)$

from (1)

$HK = HLx_1 \cup HLx_2 \cup \ldots \cup HLx_m$

$= Hx_1 \cup Hx_2 \cup \ldots \cup Hx_m$

(since $L \subseteq H$) $\rightarrow (3)$

We claim that the cosets $Hx_1, Hx_2, \ldots, Hx_m$ are distinct.

Suppose $Hx_i = Hx_j$

$\therefore x_i x_j^{-1} \in H$

Also, $x_i, x_j \in K$ and hence $x_i x_j^{-1} \in K$

$\therefore x_i x_j^{-1} \in H \cap K = L$,

Hence, $Lx_i = Lx_j$ which is contradiction.

Since the cosets $Lx_1, Lx_2 \ldots Lx_m$ ~~and~~

& are distinct.

Thus from (3) we have,

$$|HK| = |Hx_1| + |Hx_2| + \cdots + |Hx_m|$$

$$= m|H|$$

$$= \frac{|H||K|}{|H \cap K|} \quad [\text{by } (2)]$$

5) Let H and K be two subgroups of a finite group G such that $|H| > \sqrt{|G|}$ then $H \cap K \neq \{e\}$

Proof:

Suppose $H \cap K = \{e\}$

$$|H \cap K| = 1$$

$$|HK| = \frac{|H||K|}{|H \cap K|} \quad [\text{by prblm: 2}]$$

$$= |H||K|$$

$$> \sqrt{|G|}\ \sqrt{|G|}$$

$= |G|$

$\therefore |HK| > |G|$, which is contradiction.

$\therefore H \cap K \neq \{e\}$.

Unit - 2

Completed.

M. [illegible]

① UNIT - III

left coset = right coset ≠

NORMAL SUBGROUPS AND QUOTIENT GROUP :-

Consider the subgroup $H = \{e, p_3\}$ of S_3. Then $Hp_1 = \{p_1, p_5\}$ and $p_1 H = \{p_1, p_4\}$. Hence $Hp_1 \neq p_1 H$.

Definition :-

A subgroup of H of G is called a normal subgroup of G, if $aH = Ha$, all $a \in G$.

Ex :-

1) In S_3 the subgroup $\{e, p_1, p_2\}$ is normal.

2) In S_3 the subgroup $\{e, p_3\}$ is not a normal subgroup.

THEOREM : 3.1

Every subgroup of an abelian group is a normal subgroup.

Proof :-

Let G be an abelian group and let H be a subgroup of G. Let $a \in G$.

We claim that,

$$aH = Ha.$$

Let $x \in aH$. Then

$x = ah$ for some $h \in H$.

$x = ha$ (since G is abelian)

$\therefore x \in Ha$. Hence $aH \subseteq Ha$.

Similarly,

$Ha \subseteq aH$.

$\therefore aH = Ha$ and hence H is a normal subgroup of G.

Ex :- Normal subgroup

i) nZ is a normal subgroup of $(Z, +)$

ii) Every subgroup of $(Z_n, \oplus)$ is normal.

iii) Since any cyclic group is abelian any subgroup of cyclic group is normal.

THEOREM: 3.2

no. of cosets

Let H be a subgroup of index 2 in a group G. Then H is a normal subgroup of G.

$\{1, 2, 3, 4, 5\}$

$1\sigma H = \{1, 2\}$

Proof:-

If $a \in H$, then $H = aH = Ha$.

If $a \notin H$, then aH is a left coset different from H.

Hence $H \cap aH = \phi$.

Further, since index of H in G is 2,

$H \cup aH = G$.

Hence $aH = G - H$.

Similarly,

$Ha = G - H$, so that $aH = Ha$.

Hence, H is a normal subgroup of G.

Example:

The alternating group A_n is a subgroup of index 2 in S_n and hence is a normal subgroup of S_n.

THEOREM : 3-3

Let N be a subgroup of G, Then the following are equivalent.

i) N is a normal subgroup of G.

ii) $aNa^{-1} = N$, for all $a \in G$.

iii) $aNa^{-1} \subseteq N$ for all $a \in G$.

iv) $ana^{-1} \in N$ for all $n \in N$ and $a \in G$.

Proof :-

(i) $\Rightarrow$ (ii)

Suppose N is a normal subgroup of G.

$aN = Na$, for all $a \in G$.

$aNa^{-1} = Naa^{-1} = Ne = N$

(ii) $\Rightarrow$ (iii) and (iii) $\Rightarrow$ (iv) are obvious.

(iv) $\Rightarrow$ (i)

Suppose that $ana^{-1} \in N$ for all $n \in N$. and $a \in G$.

We claim that $aN = Na$.

Let $x \in aN$.

$\therefore$ $x = an$ for some $n \in N$.

$\therefore x = (ana^{-1})a \in Na$ $[\because$ since $ana^{-1} \in N]$

$\therefore aN \subseteq Na \rightarrow (1)$

Now let $x \in Na$.

$\therefore x = na$ for some $n \in N$.

$\therefore x = a(a^{-1}na) = a(a^{-1}n(a^{-1})^{-1}) \in aN$

$\therefore Na \subseteq aN \longrightarrow (2)$

from (1) & (2)

We get $Na = aN$

Hence N is a normal subgroup of G.

Solved Problems:-

1) Prove that the intersection of two normal subgroup of a group G is a normal subgroup of G.

Soln:

Let H and K be two normal subgroups of G. Then $H \cap K$ is a subgroup of G.

Now, let $a \in G$ and $x \in H \cap K$.

Then $x \in H$ and $x \in K$.

Since H and K are normal

$axa^{-1} \in H$ and $axa^{-1} \in K$.

Hence $axa^{-1} \in H \cap K$. Thus, $H \cap K$ is a normal subgroup of G.

2) The centre H of a group G is a normal subgroup of G.

Soln:

The centre H of G is given by $H = \{a / a \in G, ax = xa \text{ for all } x \in G\}$.

Now let $x \in H$ and $a \in G$.

Hence $ax = xa$

$\therefore x = axa^{-1} \in H$.

Hence H is a normal subgroup of G.

3) Let H be a subgroup of G. Let $a \in G$. Then aHa^{-1} is a subgroup of G.

Soln.

$e = aea^{-1} \in aHa^{-1}$ and hence $aHa^{-1} \neq \phi$

Now, let $x, y \in aHa^{-1}$

Then $x = ah_1a^{-1}$ and $y = ah_2a^{-1}$.

where $h_1, h_2 \in H$

Now,

$xy^{-1} = (ah_1a^{-1})(ah_2a^{-1})^{-1}$.

$= (ah_1a^{-1})(ah_2^{-1}a^{-1})$

$= a(h_1h_2^{-1})a^{-1} \in aHa^{-1}$.

$\therefore aHa^{-1}$ is a subgroup of G.

4) Show that, if a group G has exactly one subgroup H of given order, then H is a normal subgroup of G.

Soln.

Let the order of H be m.

Let $a \in G$. Then by solved pblm: 3

aHa^{-1} is also a subgroup of G.

We claim that, $|H| = |aHa^{-1}| = m$.

Now,

Consider $f : H \to aHa^{-1}$ defined by $f(h) = aha^{-1}$.

f is 1-1 for,

$f(h_1) = f(h_2) \Rightarrow ah_1a^{-1} = ah_2a^{-1}$

$\Rightarrow h_1 = h_2$

f is onto, for let $x = aha^{-1} \in aHa^{-1}$.

Then $f(h) = x$. Thus f is a bijection.

$|H| = |aHa^{-1}| = m$

But H is the only subgroup of G of order m.

$\therefore aHa^{-1} = H$. Hence $aH = Ha$

$\therefore H$ is a normal subgroup of G.

5) Show that if H and N are subgroups of a group G and N is normal in G, then $H \cap N$ is normal in H. Show by an example that $H \cap N$ need not be normal in G.

Soln.

Let $x \in H \cap N$, and $a \in H$.

We claim that $axa^{-1} \in H \cap N$.

Now, $x \in N$ and $a \in H \Rightarrow axa^{-1} \in N$

[$\because$ N is a normal subgroup]

Also $x \in H$ and $a \in H \Rightarrow axa^{-1} \in H$

[$\because$ H is a group]

Hence $axa^{-1} \in H \cap N$.

$\therefore$ $H \cap N$ is a normal subgroup of H.

The following example show that $H \cap N$ need not be normal in G.

Let $G = S_3$. Take $N = G$ and

$H = \{e, p_5\}$. $\Rightarrow$ Symmetry grp

Now, $H \cap N = H$, which is not normal in G.

6) If H is a subgroup of G and N is a normal subgroup of G then HN is a subgroup of G.

soln.

To prove that HN is a subgroup of G.

It is enough, if we prove that

$HN = NH$ [∵ By thrm : 2.7]

Let $x \in HN$. then $x = hn$, where $h \in H$ and $n \in N$.

$\therefore x \in hN$

But $hN = Nh$ (∵ N is a normal).

$\therefore x \in Nh$

Hence $x = n_1 h$, where $n_1 \in N$.

$\therefore x \in NH$

Hence $HN \subseteq NH$

III'y. $NH \subseteq HN$

$\therefore HN = NH$.

Hence HN is a subgroup of G.

7) M and N are normal subgroups of a group G, such that $M \cap N = \{e\}$. Show that everyelement of M commutes with every element of N.

Soln

Let $a \in M$ ~~ab~~ and $b \in N$.

We claim that $ab = ba$

Consider the element $aba^{-1}b^{-1}$.

Since $a^{-1} \in M$ and M is normal,

$$ba^{-1}b^{-1} \in M.$$

Also, $a \in M$, so that $aba^{-1}b^{-1} \in M$.

Again since $b \in N$ and N is normal.

$$aba^{-1} \in N$$

Also $b^{-1} \in N$, so that $aba^{-1}b^{-1} \in N$

$$\therefore aba^{-1}b^{-1} \in M \cap N = \{e\}$$

$$aba^{-1}b^{-1} = e$$

$$ab = ba.$$

THEOREM: 3.4

A subgroub N of G is normal if and only if, the product two right coset of N is again a right coset of N.

Proof:

~~Let G be a group.~~

Suppose N is a normal subgroup of G.

Then,

$$NaNb = N(aN)b$$

$$= N(Na)b \quad [\because aN = Na]$$

$$= N(Nab)$$

$$= NNab.$$

$$= Nab \quad [\because NN = N]$$

Conversely,

Suppose that the product of two right coset of N is again a right coset of N.

Further $ab = (ea)(eb) \in NaNb$.

Hence $NaNb$ is the right coset containing ab.

$\therefore NaNb = Nab.$

Now, we prove that N is a normal subgroup of G.

let $a \in G$ and $n \in N$

Then,

$$ana^{-1} = eana^{-1} \in NaNa^{-1}$$
$$= Naa^{-1}$$
$$= N$$

$\therefore ana^{-1} \in N$

Hence N is a normal subgroup of G.

THEOREM : 3.5

Let N be a normal subgroup of G. Then G/N is a group under the operation defined by $NaNb = Nab$

Proof :

By the above theorem, the operation given by $NaNb = Nab$ is well defined binary operation in G/N.

Now, let $Na, Nb, Nc \in G/N$.

Then $Na\,(NbNc) = Na(Nbc)$
$$= N\,a(bc)$$
$$= N(ab)c)$$

$= (NaNb)Nc$

$\therefore$ The binary operation is associative. $Ne = N \in G/N$ and

$NaNe = Nae = Na$
$= Nea$
$= NeNa.$

$\therefore Ne$ is the identity element

Also, $NaNa^{-1} = Naa^{-1}$

$= Ne$

$= Na^{-1}a$

$= Na^{-1}Na$

$\therefore Na^{-1}$ is the invase of Na.

$\therefore G/N$ is a group.

Definition :-

Let N be a normal subgroup of

Then the group G/N is called the Quotient group (factor group) of G modulo N.

Example :-

$5Z$ is a normal subgroup of $(Z, +)$.

(15) The Quotient group $\frac{Z}{3Z} = \{3Z+0,$

$3Z+1, 3Z+2\}$.

Hence, $Z/3Z$ is a group of order 3.

HOMOMORPHISM :- [sec. 3.11]

Definition :-

A map f from a group G into a group G' is called a homomorphism if $f(ab) = f(a)f(b)$ for all $a, b \in G$.

Example :-

1) $f(z,+) \rightarrow (z,+)$ defined by

$f(x) = 2x$ is a homomorphism

for, $f(x+y) = 2(x+y)$

$= 2x + 2y$

$f(x+y) = f(x) + f(y)$

$\therefore$ f is a homomorphism.

2) $f : (R^*, \cdot) \rightarrow (R^+, \cdot)$ defined by $f(x) = |x|$

is a homomorphism.

for, $f(xy) = |xy|$

$= |x||y|$

$= f(x) f(y)$

$\therefore$ f is homomorphism.

3) $f : G \to G'$ defined by $f(a) = e'$, where e' is the identity in G' is a trivial homomorphism.

for, $f(ab) = e' e'$

$= f(a) f(b)$

$\therefore$ f is homomorphism.

4) $f : (R \times R, +) \to (R, +)$ given by $f(x, y) = x$ is a homomorphism.

$f((x, y) + (y, z)) = x + y$

$= f(x, y) + f(y, z)$.

$\therefore$ f is a homomorphism.

5) Let G be a group and N is a normal subgroup of G,

$f : G \to G/N$ is given by $f(a) = Na$ is a homomorphism.

$f(ab) = N.ab = NaNb$

$= f(a) f(b)$

$\therefore f$ is a homomorphism.

This f is called "canonical homomorphism" from G to G/N

2m $f : G \rightarrow G/N$"

Definition :-

let $f : G \rightarrow G'$ be a homomorphism.

i) If f is onto, then it is called an "Epimorphism".

ii) If f is 1-1, then it is called a "Monomorphism".

iii) If f is an Epimorphism, then G' is called a "Homomorphic image of G".

iv) A ~~hom~~ homomorphism of a group to itself is called an "endomorphism".

(12)

THEOREM : 3.6

Let $f: G \to G'$ be a homomorphism.

i) $f(e) = e'$.

ii) $f(a^{-1}) = [f(a)]^{-1}$.

iii) If H is a subgroup of G, then $f(H)$ is a subgroup of G'.

iv) If H is ~~a~~ ~~su~~ normal in G, then $f(H)$ is normal in $f(G)$

v) If H' is a subgroup of G', then $f^{-1}(H')$ is a subgroup of G.

vi) If H' is normal in $f(G)$ then $f^{-1}(H')$ is normal in G.) 5m

Proof :-

i) Let $a \in G$.

Then $f(a) = f(ae) = f(a) f(e)$

Hence $f(e) = e'$

ii) $f(a) f(a^{-1}) = f(e) = e'$.

Hence $f(a^{-1}) = [f(a)]^{-1}$

iii) Let H be a subgroup of G.

Since H is non-empty, $f(H)$ is also non-empty.

Now, let $x, y \in f(H)$

Then $x = f(a)$ and $y = f(b)$ where $a, b \in H$.

$\therefore xy^{-1} = f(a)[f(b)]^{-1}$

$= f(a) f(b^{-1})$

$= f(ab^{-1})$

Now, since H is a subgroup of G,

$ab^{-1} \in H$.

$\therefore xy^{-1} = f(ab^{-1}) \in f(H)$

$\therefore f(H)$ is a subgroup of G'

iv) Let H be a normal in G. Let $x \in f(H)$

and $y \in f(G)$.

We claim that $yxy^{-1} \in f(H)$.

Now, $x = f(a)$ and $y = f(b)$, where

$a \in H$ and $b \in G$.

Since H is normal in G, $bab^{-1} \in H$.

$\therefore f(bab^{-1}) \in f(H)$

$\therefore f(b) f(a) f(b^{-1}) \in f(H)$

$\therefore yxy^{-1} \in f(H)$. Hence $f(H)$ is

normal in $f(G)$.

v) Since $f(e) = e' \in H'$;

$e \in f^{-1}(H')$ and hence $f^{-1}(H') \neq \phi$

Now, let $a, b \in f^{-1}(H')$.

Then $f(a), f(b) \in H'$.

$\therefore f(a)[f(b)^{-1}] \in H'$

$\therefore f(ab^{-1}) \in H'$ ie, $ab^{-1} \in f^{-1}(H')$

Hence, $f^{-1}(H')$ is a subgroup of G.

vi) Let $x \in f^{-1}(H')$ and $a \in G$.

Then $f(x) \in H'$ and $f(a) \in f(G)$

Since H' is normal in $f(G)$

$f(a) f(x) [f(a)]^{-1} \in H'$.

$\therefore f(axa^{-1}) \in H'$.

Hence $axa^{-1} \in f^{-1}(H')$

Thus, $f^{-1}(H')$ is normal in G.

Example :- {Ker f}

1) Consider the homomorphism $f:(Z,+) \to (Z_n, \oplus)$ which is given in the beginning of this section.

Let $K = \{x / x \in Z, f(x) = 0\}$

Clearly, $K = nZ$, which is a normal subgroup of Z.

2) Consider the homomorphism. 21

$f : (R^*, \cdot) \to (R^+, \cdot)$ which is given

by $f(x) = |x|$.

let $k = \{ x \mid x \in R^*, f(x) = 1 \}$

Clearly, $k = \{1, -1\}$ which is a normal subgroup of $(R^*, \cdot)$

Definition:-

Let $f : G \to G'$ be a homomorphism. Let $K = \{ x \mid x \in G, f(x) = e' \}$. Then k is called the kernel of f and denoted by $\ker f$.

THEOREM : 3.7

Let $f : G \to G'$ be a homomorphism. Then ~~then~~ the kernel k of f is a normal subgroup of G.

Proof:-

since $f(e) = e'$, $e \in k$ and

hence, $k \neq \phi$.

Now, let $x, y \in k$

Then $f(x) = e'$, $f(y) = e'$

$f(xy^{-1}) = f(xy^{-1})$

$$= f(x)\, f(y^{-1})$$

$$= f(x)\, [f(y)]^{-1}$$

$$= e'\,(e')^{-1}$$

$$= e'$$

Thus, $xy^{-1} \in k$.

Hence k is a subgroup of G.

Now, let $x \in k$, and $a \in G$.

Then $f(axa^{-1}) = f(a)\, f(x)\, f(a^{-1})$

$$= f(a)\, e\, [f(a)]^{-1}$$

$$= f(a)\, [f(a)]^{-1}$$

$$= e.$$

$\therefore axa^{-1} \in k$

Hence k is a normal subgroup of G

UNIT - III

FUNDAMENTAL THEOREM OF HOMOMORPHISM

Theorem : 3.8

Let $f : G \to G'$ be a epimorphism let k be a kernel of f. Then $G/k \cong G'$.

Proof:-

Define $\phi : G/k \to G'$ by $\phi(ka) = f(a)$

Step (i)

ϕ is well defined.

Let $ka = kb$.

Then $b \in ka$

Hence $b \in ka$

Now $f(b) = f(ka) = f(k) f(a)$

$= e' f(a)$

$= f(a)$

$\phi(kb) = f(b) = f(a) = \phi(ka)$

Stepe (ii)

ϕ is 1-1

for $\phi(ka) = \phi(kb)$

$\Rightarrow f(a) = f(b)$

$\Rightarrow f(a)\,[f(b)]^{-1} = e'$

$\Rightarrow f(a)\,f(b^{-1}) = e'$

$\Rightarrow f(ab^{-1}) = e'$

$\Rightarrow ab^{-1} \in k$

$\Rightarrow a \in kb$

$\Rightarrow ka = kb$

Step (iii)

ϕ is onto

Let $a' \in G'$

Since f is onto, there exists $a \in G$ such that $f(a) = a'$

Hence $\phi(ka) = f(a) = a'$.

Step (iv):

ϕ is a homomorphism.

$\phi(ka\,kb) = \phi(kab)$

$= f(ab)$

$= f(a)\,f(b)$

$= \phi(ka)\,\phi(kb)$

Thus, ϕ is an homomorphism from G/K onto G'.

$$\therefore G/K \cong G'$$

Solved Problems:-

1) Let $f: G \rightarrow G'$ be a homomorphism. Then f is 1-1 iff $\ker f = \{e\}$.

Soln.

Obviously f is 1-1 $\Rightarrow \ker f = \{e\}$

Conversely, Let $\ker f = \{e\}$

To prove that f is 1-1

$$f(x) = f(y)$$

$$f(xy^{-1}) = e'$$

$$xy^{-1} \in \ker f$$

$$xy^{-1} = e'$$

$$x = y.$$

Hence f is 1-1

(26)

2) Let G be any group and H be the centre of G. Then $G/H \cong I(G)$, the group of inner automorphism of G.

<u>Soln:</u>

Consider $f : G \to I(G)$ defined by

$f(a) = \phi_a$

$f(ab) = \phi_{ab} = \phi_a \circ \phi_b = f(a) f(b)$

Hence f is homomorphism.

Clearly f is onto.

Now, we claim that $\ker f = H$

$a \in \ker f \Leftrightarrow f(a) = \phi_e$

$\Leftrightarrow \phi_a = \phi_e$

$\Leftrightarrow \phi_a(x) = x$ for all $x \in G$

$\Leftrightarrow axa^{-1} = x$ for all $x \in G$

$\Leftrightarrow ax = xa$ for all $x \in G$

$\Leftrightarrow a \in H$.

Hence $\ker f = H$

$\therefore$ By the fundamental theorem of homomorphism $G/H \cong I(G)$.

3) Show that $R^* / \{1, -1\} \cong R^+$.

<u>soln</u>

Consider $f : R^* \to R^+$ defined by

$$f(x) = |x|$$

Clearly f is an epimorphism and

$\ker f = \{1, -1\}$

Hence by the fundamental theorem of homomorphism.

$$R^* / \{1, -1\} \cong R^+.$$

4) Any homomorphism image of a cyclic group is cyclic.

<u>soln.</u>

Let G be a cyclic group and $f : G \to G'$ be an epimorphism.

Let a be a generator of G. Then $f(a)$ is a generator of G'.

Hence G' is cyclic.

5) Show that the map $f : (\mathbb{C}, +) \to (\mathbb{R}, +)$
28 defined by $f(x+iy) = y$ is an epimorphism and $\ker f = \mathbb{R}$. Deduce that $\mathbb{C}/\mathbb{R} \cong \mathbb{R}$.

Soln.

Let $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$

Then $z_1 + z_2 = (x_1 + x_2) + i(y_1 + y_2)$

$$f(z_1 + z_2) = y_1 + y_2 = f(z_1) + f(z_2)$$

Hence f is a homomorphism.

Clearly f is onto.

Now,

$$\ker f = \{x + iy \mid f(x+iy) = 0\}$$
$$= \{x + iy \mid y = 0\}$$
$$= \mathbb{R}$$

By the fundamental theorem of homomorphism $\mathbb{C}/\mathbb{R} \cong \mathbb{R}$.

Q9

ISOMORPHISM :-

a thm
4 pblm

Definition :-

Let G and G' be two groups.

A map $f : G \to G'$ is called an isomorphism, if

i) f is bijection

ii) $f(xy) = f(x) f(y)$ for all $x, y \in G$.

$f(ab) = f(a) \cdot f(b)$

Two groups G and G' are said to be isomorphic. If there exists an isomorphism $f : G \to G'$. If two groups G and G' are isomorphic we write $G \cong G'$.

If $f: G \to G'$ is an isomorphism we say that G is isomorphic to G' & we write $G \cong G'$

THEOREM: 3.9

Isomorphism is an equivalence relation among groups.

Proof :-

For any group G, $i_G : G \to G$ is clearly an isomorphism.

39 Hence $G \cong G$. Therefore the relation is reflexive.

Now, let $G \cong G'$ and let $f: G \to G'$ be an isomorphism.

Then f is a bijection.

$\therefore f^{-1}: G' \to G$ is also a bijection.

Now, let $x', y' \in G'$

Let $f^{-1}(x') = x$ and $f^{-1}(y') = y$

$f(b(y))$ Then $f(x) = x'$ and $f(y) = y'$

$f(xy) = f(x) f(y) = x'y'$

$f^{-1}(x'y') = xy = f^{-1}(x') f^{-1}(y')$

Hence f^{-1} is a isomorphism.

Thus $G' \cong G$ and hence the relation is symmetric

Now, let $G \cong G'$ and $G' \cong G''$ and $g: G \to G''$

Since f and g are bijection

g / ~~et~~ $g \circ f : G \to G''$ is also a bijection.

Now, let $x, y \in G$, then

(31)

$(g \circ f)(xy) = g[f(xy)]$

$= g[f(x) f(y)]$

[$\because$ Since f is an isomorphism]

$= g[f(x)]\, g[f(y)]$

($\because$ g is an isomorphism)

$= (g \circ f)(x)\, (g \circ f)(y)$

Hence $g \circ f$ is an isomorphism.

Thus $G \cong G''$ and hence the relation is transitive.

$\therefore$ Isomorphism is an equivalence relation among groups.

Example :-

1) $(Z, +) \cong (2Z, +)$

Consider $f : Z \to 2Z$ given by $f(x) = 2x$.

Clearly f is a bijection.

$f(x+y) = 2(x+y)$

$= 2x + 2y$

$= f(x) + f(y)$

Hence f is an isomorphism.

2) let $G = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in R^* \right\}$

G is a group under matrix multiplication.

We claim that $G \cong (R^*, \cdot)$

Consider $f : G \to R^*$ given by,

$f\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = a$

let $A = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$

$B = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}$

$AB = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix}$

$\therefore f(AB) = ab = f(A)\, f(B)$

Hence f is an isomorphism.

3) $(R, +) \cong (R^+, \cdot)$

Consider $f : R \to R^+$ given by $f(x) = e^x$

Clearly f is a bijection.

$\therefore f(x+y) = e^{x+y} \to ①$

$= e^x \cdot e^y \quad ① = ②$

$= f(x) \cdot f(y)$

$e^x \cdot e^y = e^{x+y} \to ②$

$\therefore f$ is an isomorphism.

4) $G = R - \{-1\}$ is a group under $*$ defined by $a*b = a+b+ab$

We claim that $G \cong (R^*, \cdot)$

Consider $f : G \to R^*$ given by,

$f(x) = x+1$

Clearly f is a bijection.

$f(x*y) = f(x+y+xy)$

$= x+y+xy+1$

$= (x+1)(y+1)$

$\therefore f$ is an isomorphism.

5) $(Z_n, \oplus)$ is a group.

Let G denote the set of all n^{th} roots of unity. G is a group under usual multiplication.

We claim that $(Z_n, \oplus) \cong G$.

Consider $f : Z_n \to G$ given by

~~$f(m) = \omega_m, \omega^n$~~

~~Where $\omega = \omega$~~

$f(m) = \omega^m$, where $\omega = \cos(2\pi/n) + \sin(2\pi/n)$

Clearly f is a bijection.

Let $a, b \in Z_n$.

Let $a+b = qn + r$, where $0 \leq r \leq n$.

then $a \oplus b = r$

$$f(a \oplus b) = \omega^r \longrightarrow (1)$$

Also,

$$f(a) f(b) = \omega^a \omega^b = \omega^{a+b}$$

$$= \omega^{qn+r}$$

$$= \omega^{qn} \cdot \omega^r = \omega^r \rightarrow (2)$$

From (1) & (2)

$$f(a \oplus b) = f(a) f(b)$$

$\therefore f$ is an Isomorphism.

THEOREM : 3.10

Let $f : G \to G'$ be an Isomorphism. Then

i) $f(e) = e'$, where e and e' are the identity element of G and G' respectively. ie) in an isomorphism, identity is mapped onto identity.

ii) $f(a^{-1}) = [f(a)]^{-1}$.

Proof:-

i) To prove that $f(e) = e'$.

It is enough, if we prove that,

$$a' f(e) = f(e) a' = a' \text{ for all } a' \in G'.$$

Let $a' \in G'$

since $f : G \to G'$ is a bijection, there exists ~~such that~~ $a \in G$ such that $f(a) = a'$.

$$\begin{aligned} a' f(e) &= f(a) f(e) \\ &= f(ae) \\ &= f(a) \\ &= a' \end{aligned}$$

Similarly $f(e)a' = a'$.

$\therefore f(e) = e'$.

ii) It is enough to prove that

$$f(a)f(a^{-1}) = f(a^{-1})f(a)$$

$$= e'$$

Now, $f(a)f(a^{-1}) = f(aa^{-1})$

$= f(e)$

$= e'$.

Also, $f(a^{-1})f(a) = f(a^{-1}a)$

$= f(e)$

$= e'$.

$\therefore f(a)f(a^{-1}) = f(a^{-1})f(a) = e'$

$\therefore f(a^{-1}) = [f(a)]^{-1}$.

THEOREM : 3.11

Let $f : G \to G'$ be an isomorphism. If G is abelian, then G' is also abelian

Proof :-

Let $a', b' \in G'$, then there exists $a, b \in G$, such that $f(a) = a'$ and $f(b) = b'$.

$$a'b' = f(a) f(b)$$
$$= f(ab)$$
$$= f(ba)$$
$$= b'a'.$$

$\therefore a'b' = b'a'$.

Hence. G' is abelian.

THEOREM: 3.12

Let $f : G \to G'$ be an Isomorphism. Let $a \in G$ then the $o(a) = o[f(a)]$, ie) isomorphism preserves the order of each element in a group

Proof :-

Suppose, the order of a is n, then n is the least ~~posive~~ positive integer such that $a^n = e$

$$[f(a)]^n = f(a) \dots f(a)$$

($f(a)$ written n times)

$$= f(a^n)$$

($\because f$ is an isomorphism)

$$= f(e)$$

$$= e'$$

Now, if possible let m be a +ve integer such that $0 < m < n$ and $[f(a)]^m = e'$, then

$f(a^m) = [f(a)]^m = e'$

But $f(e) = e'$

since f is 1-1, we have $a^m = e$ which contradicts the definition of the order of a.

$\therefore n$ is the least +ve integer such that $[f(a)]^n = e'$.

$\therefore$ The order of $f(a)$ is n.

THEOREM: 3.13

Let $f : G \to G'$ be an isomorphism, if G is cyclic, then G' is also a cyclic.

Proof:-

Let ~~A~~ a be a generator of the group G.

We shall prove that $f(a)$ is the generator of the group G'.

Let $x' \in G'$. Since f is a bijection, there exists $x \in G$ such that $f(x) = x'$

Now, since $G = \langle a \rangle$, $x = a^n$ for some integer n.

Hence $x' = f(x) = f(a^n) = [f(a)]^n$.

Since $x' \in G'$ is arbitrary every element of G' is of the form $[f(a)]^n$.

So that $G' = \langle f(a) \rangle$.

Hence G' is cyclic.

Solved Problems:-

1) ~~R~~ Show that $(R^*, \cdot)$ is not isomorphic to $(R, +)$.

Soln:

In $(R, +)$, every element other than 0 is of infinite order.

But, in $(R^*, \cdot)$ there exists an element ~~of~~ other than, one of finite order.

for example,

-1 is of order 2 in $(R^*, \cdot)$

Hence, we cannot find an isomorphism from $(R^*, \cdot)$ to $(R, +)$.

[By thm: 3.12]

2) Show that $(Z_4, \oplus)$ is not isomorphic to V_4.

$V \to Z_2 \times Z_2$

Soln

In Z_4, 1 is an element of order 4. But in V_4 every element other than e is of order 2.

Hence, the two groups are not isomorphic.

3) If G is a group and G' is a set with a binary opereation and there exists a 1-1 mapping $f : G \xrightarrow{\text{onto}} G'$, such that $f(ab) = f(a)f(b)$ for all $a, b \in G$, then show that G' is also a group.

<u>soln.</u>

Let $a', b', c' \in G'$

Since $f : G \to G'$ is a bijection, there exists $a, b, c \in G$ such that $f(a) = a'$; $f(b) = b'$; $f(c) = c'$

Since G is a group, $(ab)c = a(bc)$

$\therefore f[(ab)c] = f[a(bc)]$

$\therefore f(ab)f(c) = f(a)f(bc)$ by hypothesis.

$\therefore [f(a)f(b)]f(c) = f(a)[f(b)f(c)]$

$\therefore (a'b')c' = a'(b'c')$

$\therefore$ The binary operation in G' is associative.

Now, let $e \in G$ be the identity element.

Let $a' \in G'$. Since $f: G \to G'$ is a bijection, there exists $a \in G$ such that $f(a) = a'$.

Now $ae = ea = a$

$\therefore f(ae) = f(ea) = f(a)$

$\therefore f(a)f(e) = f(e)f(a) = f(a)$

$a'f(e) = f(e)a' = a'$.

$\therefore f(e)$ is ~~the~~ identity in G'.

Let $a' \in G'$. Since $f: G \to G'$ is a bijection, there exists $a \in G$ such that $f(a) = a'$.

Now, $aa^{-1} = a^{-1}a = e$

$f(aa^{-1}) = f(a^{-1}a) = f(e)$

$f(a)f(a^{-1}) = f(a^{-1})f(a) = f(e)$

$a'f(a^{-1}) = f(a^{-1})a' = f(e)$

$\therefore f(a^{-1})$ is the inverse of a' in G'.

Hence G' is a group.

Unit 4

Unit - IV :

Rings : definition and examples - elementary properties of rings -

Isomorphism - types of rings - characteristics of a ring - sub rings - Ideals - Quotient rings.

Modern Algebra

By,
Mrs M.Sirin Hasina

Unit 4

Unit - IV :

Rings : definition and examples -
elementary properties of rings -

Isomorphism - types of rings - characteristics of a ring - subrings - Ideals - Quotient rings.

Unit - IV

Rings:-

A non-empty set R together with two binary operations denoted by "+" and "." and called addition and Multiplication which satisfy the following axioms is called ring.

conditions:

(i) $(R, +)$ is an abelian group.

(ii) "." is an associative binary operation on R.

distributive law

(iii) $a\cdot(b+c) = a\cdot b + a\cdot c$ and $(a+b)c = a\cdot c + b\cdot c$ for all $a, b, c \in R$.

Examples:-

1) In $R \times R$ we define $(a,b)+(c,d) = (a+c, b+d)$ and $(a,b)\cdot(c,d) = (ac, bd)$

Soln:-

Here $(R \times R, +)$ is an abelian group.

The identity is $(0,0)$ and the inverse of (a,b) is $(-a,-b)$.

Further, $(a,b)\cdot[(c,d)+(e,f)] = (a,b)[c+e, d+f]$

$$= (ac, bd) + (ae, bf)$$

$$= (a,b)(c,d) + (a,b)(e,f)$$

Similarly,

$$[(a,b)+(c,d)](e,f) = [a+c, b+d](e,f)$$

$$= (ae+ce, bf+df)$$

$$= (ae, bf) + (ce, df)$$

$$= (a,b)(e,f) + (c,d)(e,f)$$

---

② $(Z_n, \oplus, \odot)$ is a ring.

Proof:-

We know that $(Z_n, \oplus)$ is an abelian group and $\odot$ is an associative binary operation.

We now prove the distributive laws

Let $a, b, c \in Z_n$.

Then $b \oplus c \equiv (b+c) \pmod n$

Hence $(a \odot (b+c)) \equiv a(b+c) \pmod n$

Also, $a \odot b \equiv ab \pmod n$ and

$a \odot c \equiv ac \pmod n$ so that,

$(a \odot b) \oplus (a \odot c) \equiv (ab + ac) \pmod n$

$\therefore a \odot (b \oplus c) \equiv a(b+c)$

$\because a \odot (b \oplus c)$ and $(a \odot b) \oplus (a \odot c) \in Z_n$

we have,

$$a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$$

Similarly.

$$(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$$

Hence $(Z_n, \oplus, \odot)$ is a ring.

Elementry properties of rings.

Thm: 4.1

Let R be a Ring and $a, b \in R$.

2m Exam

Then (i) $0a = a0 = 0$

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

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

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

proof:

(i) $a0 = a(0+0)$

$\cancel{a0} = a0 + a0$

$\cancel{0 = a0}$

$\therefore \boxed{a0 = 0}$ (by cancellation law)

Similarly, $\boxed{0a = 0}$

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

$$a(-b) + (ab) = a(-b+b)$$
$$= a0$$
$$= 0$$

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

Similarly,

$$(-a)b + ab = b(-a+a)$$
$$= b0 = 0$$

$$\therefore \boxed{(-a)b = -(ab)}$$

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

By (ii), $(-a)(-b) = -[a(-b)]$ by (ii)

$$= -(-ab)$$
$$= ab.$$

(iv) $a(b-c) = a[b + (-c)]$

$$= ab + a(-c)$$
$$= ab - ac.$$

Problem: 1

7 4 5m & 2m 4 7

If R is a ring such that $a^2 = a \ \forall \ a \in R$. prove that

(i) $a + a = 0$

(ii) $a + b = 0 \Rightarrow a = b$

(iii) $ab = ba$.

Proof:-

(i) $a+a=0$

$a+a = a^2+a^2$

$= (aa)+(aa)$

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

$= a(a+a)+a(a+a)$

$= aa+aa+aa+aa$

$a+a = (a+a)+(a+a)$

[since $a^2=a$]

Hence $\boxed{a+a=0}$

(ii) Let $a+b=0$ [By (i)]

$a+b = a+a$

$b = a+a-a$

$\boxed{b=a}$

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

TP $ab=ba$

(iii) $a+b = (a+b)(a+b)$ $(\because a^2=a)$

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

$= aa+ab+ba+bb$

$= a^2+ab+ba+b^2$

$a+b = a+ab+ba+b$

$(a+b) = (a+b)+(ab+ba)$

Hence, $ab+ba=0$, So that (ii)

$[\because a+b=0 \Rightarrow a=b]$

$ab+ba=0$

$(ab)=ba$

Problem : 2

The set R of all matrices of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ where $a, b \in R$ is a ring under matrix addition & matrix multiplication

Proof:-

let $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ & $B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \in R$

Then, $A+B = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$

$= \begin{pmatrix} a+c & b+d \\ -(b+d) & (a+c) \end{pmatrix} \in R.$

$AB = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$

$= \begin{pmatrix} ac-bd & ad+bc \\ -(bc+ad) & -(bd+ac) \end{pmatrix}$

clearly matrix addition is commutative and associative.

$\therefore \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in R$ is the zero element

$\begin{pmatrix} -a & -b \\ b & a \end{pmatrix}$ is the inverse of the matrix.

$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$

Further, matrix multiplication is associative and the distributive laws are valid for 2×2 matrixes

Hence R is a ring.

Commutative:-

A ring R is said to be commutative. $\boxed{ab = ba}$ for all $a, b \in R$.

Ring with identity:-

Let R be a ring We say that R is a ring with identity if there exists an element $1 \in R$ such $a1 = 1a = a$ for all $a \in R$

Thm : 4.8:-

In a ring with identity element is unique.

Proof:-

Let $1, 1'$ be Multiplicative Identity

Then $1 \cdot 1' = 1$ (consider $1'$ as identity) and $1 \cdot 1' = 1'$ (consider 1 as identity)

Hence the identity element is unique

Unit :-

Let R be a ring with identity

An element $u \in R$ is called a Unit in R if it has a Multiplicative inverse in R

The Multiplicative inverse of u is denoted by u^{-1}

$u \in R$

$a \in R$

$\boxed{aa^{-1} = a}$ a^{-1}

$\boxed{aa^{-1} = 1}$ ring

$\boxed{aa^{-1} = 1 \in U}$

Boolean ring :-

A Ring R is called a Boolean ring if $\boxed{a^2 = a}$ for all $a \in R$.

Examples.

$(P(S), \Delta, \cap)$ is a boolean ring.

prnf

Isomorphism :- of Ring :-

Let $(R, +)$ and ~~(R', Δ)~~ $(R', +, \cdot)$ be two ring. A bijection $f : R \to R'$ is called an isomorphism. If , further, matrix multiplication is associative and the distributive laws are valid for 2×2 matrixes

Hence R is a ring.

Commutative:-

A ring R is said to be commutative $\boxed{ab = ba}$ for all $a, b \in R$.

Ring with identity:- (

Let R be a ring we say that R is a ring with identity if there exists an element $1 \in R$ such $a1 = 1a = a$ for all $a \in R$.

Thm : 1.2:-

In a ring with identity element is unique.

Proof:-

Let $1, 1'$ be Multiplicative

Identity

Then $1 \cdot 1' = 1$ (consider $1'$ as identity) and $1 \cdot 1' = 1'$ (consider 1 as identity)

Hence the identity element is unique.

Unit :-

Let R be a ring with identity. An element $u \in R$ is called a Unit in R if it has a multiplicative inverse in R.

$u \in R$
$1 \in R$

The Multiplicative inverse of u is denoted by u^{-1}

$\boxed{aa^{-1} = e}$ grp
$\boxed{aa^{-1} = 1}$ ring
$\boxed{aa^{-1} = 1 \in U}$

Boolean ring :-

A Ring R is called a Boolean ring if $\boxed{a^2 = a}$ for all $a \in R$.

Examples.

$(P(S), \Delta, \cap)$ is a boolean ring.

Isomorphism :- of Ring :-

Let $(R, +)$ and ~~(R', Δ)~~ $(R', +, \cdot)$ be two ring. A bijection $f : R \to R'$ is called an isomorphism. If,

(i) $f(a+b) = f(a) + f(b)$

(ii) $f(ab) = f(a) \cdot f(b) \ \forall \ a, b \in R$.

If $f : R \to R'$ is an isomorphism. we say that R is isomorphic to R' and we write $R \cong R'$.

Thm: 4.3

Let R be a ring with identity the set of all units R is a group under Multiplication.

proof:

Let U denote the set of all units in R.

$U \subset R$ $\quad$ $0 \neq 1$

clearly $1 \in U$, let $a, b \in U$.

Hence $a^{-1} b^{-1}$ exists in R.

Now, $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}$

$= a 1 a^{-1}$

$= 1$

similarly $(b^{-1}a^{-1}) ab = 1$.

Hence $ab \in U$

Also, $(a^{-1})^{-1} = a$ and hence

$a \in U \Rightarrow a^{-1} \in U$.

Hence U is a group under multiplication

Skew field (or) Division ring :-

(Let R be a ring with identity element R is called a skew field (or) a divison ring if every non-zero element in R is a unit.)

(ie) for every non-zero element $a \in R$.

there exists a multiplicative inverse $a^{-1} \in R$ Such that $\boxed{aa^{-1} = a^{-1}a = 1}$.

Thus in a skew field the non-zero elements from a group under multiplication.

Field:-

A commutative skew field is called a field.

In other words a field is a system $(F, +, \cdot)$ satisfied the following conditions

(i) $(F,+)$ is an abelian group

(ii) $(F-\{0\},\cdot)$ is an abelian group

(iii) $a\cdot(b+c) = a\cdot b + a\cdot c$ for all $a,b,c \in F$

Thm: 11:

In a skew field R.

(i) $ax = ay$, $a \neq 0 \Rightarrow x = y$ } cancellation
(ii) $xa = ya$, $a \neq 0 \Rightarrow x = y$ } laws in ring

(iii) $ax = 0 \Longleftrightarrow a = 0$ (or) $x = 0$.

Proof:-

(i) Let $ax = ay$ and $a \neq 0$.

Since R is a skew field there Exists $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$.

Hence $ax = ay$.

$$a^{-1}(ax) = a^{-1}(ay)$$

$$(a^{-1}a)x = (a^{-1}a)y$$

$$\boxed{x = y}.$$

(ii) Let $xa = ya$ and $a \neq 0$.

We claim that, $x = y$.

Since R is a skew field there Exists $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$

Hence $xa = ya$.

$$(xa)a^{-1} = (ya)a^{-1}$$

$$\boxed{x = y}$$

(iii) If $a = 0$, (or) $x = 0$, then clearly $ax = 0$,

conversely, let $ax = 0$ and $a \neq 0$.

$$\therefore ax = a0$$

$$\boxed{x = 0} \quad [\text{by (i)}]$$

Zero divisor:- $(ab \neq 0)$

Let R be a ring. A non-zero element $a \in R$ is said to be a zero divisor if there exist a non-zero element $b \in R$ such that $ab = 0$ (or) $ba = 0$.

Examples:-

In the ring of matrics $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ $\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$ are zero-divisor, since.

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Thm : 4.5 :

A ring R has non zero divisors iff cancellation laws is valid in R.

Proof:-

Let R be a ring without zero divisor.

Let $ax = ay$ and $a \neq 0$.

$\therefore ax - ay = 0$.

Hence $a(x-y) = 0$ and $a \neq 0$.

$\therefore x - y = 0$ (Since R has no zero divisor)

$\boxed{\therefore x = y}$

Thus cancellation laws is valid in R.

Conversely,

Let the cancellation law be valid in R.

Let $ab = 0$ and $a \neq 0$

Then $ab = 0 = a0$

Hence by cancellation law $b = 0$

$\therefore$ R has no zero-divisors

Thm: 4.6:-

Any unit in R cannot be a zero divisors.

Proof:-

Let $a \in R$ be a unit.

Then $ab = 0$

$a^{-1}(ab) = 0$

$\boxed{b = 0}$

$\boxed{aa^{-1} = 1}$

Similarly.

$ba = 0$ $(ba)a^{-1} = 0$

$\boxed{b = 0}$

Hence R cannot be a zero divisor.

Integral domain:-

A commutative ring with identity having no zero divisors is called in Integral domain.

$(+)(\times)$ $(+)$ 2m

This is in an integral domain. $ab = 0$. Either $a = 0$ (or) $b = 0$ (or) Equivalently $ab = 0$ & $a \neq 0 \Rightarrow b = 0$ (or) $a \neq 0$ & $b \neq 0 \Rightarrow ab \neq 0$.

Scanned by TapScanner

Thm 4.7:

Z_n is an integral domain iff n is prime.

<u>Proof</u>:-

Let Z_n is an integral domain.

We claim that n is prime.

Suppose, n is not prime.

Then $n = pq$ where $1 < p < n$ and $1 < q < n$

clearly $p \odot q = 0$.

Hence p and q are zero divisors

$\therefore$ Z_n is an not integral domain

which contradiction.

Hence n is prime

Converseley,

Suppose n is prime

Let $a, b \in Z_n$.

Then $a \odot b = 0$

$\Rightarrow ab = qn$ where $q \in Z_n$

$\Rightarrow n / ab$

$\Rightarrow n/a$ (or) n/b (since n is prime)

$\therefore a = 0$ (or) $b = 0$.

$\therefore Z_n$ has no zero divisors.

Also Z_n is commutative ring with identity.

Hence Z_n is an integral domain.

<u>thm : 4.8</u>.

Any field F is an integral domain.

<u>proof</u>:-

It is enough if we prove that F has no zero divisor.

Let $a, b \in F$, $ab = 0$ and $a \neq 0$.

Since F is a field a^{-1} exists

Now,

$ab = 0$

$a^{-1}(ab) = 0$ $\quad (aa^{-1}) = 1$

$b = 0$

$\therefore$ F has no zero divisors

Hence, F is an integral domain.

Thm: 4.9:-

let R be a commutative ring with identity 1. Then R is an integral domain iff the set of non-zero element in R is closed under multiplication.

proof:

let R be an integral domain

let $a, b \in R - \{0\}$

since R has no zero-divisors $ab \neq 0$

so that $R - \{0\}$ is closed under multiplication.

conversely,

suppose $R - \{0\}$ is closed under multiplication.

Then the product of any two non-zero elements is a non-zero elements.

Hence R has no zero-divisors so that R is an integral domain.

Thm : 4.11

Any finite integral domain is a field

Proof:-

Let R be a finite integral domain.

We need only to prove that every non-zero element in R has a multiplicative inverse.

let $a \in R$ and $a \neq 0$.

let $R = \{0, 1, a_1, a_2, \ldots a_n\}$

consider $\{a1, aa_1, aa_2, \ldots aa_n\}$

By thm 4.9 all these elements are non-zero and all these elements are distinct.

Hence $aa_i = 1$ for some $a_i \in R$

Since R is commutative, $aa_i = a_i a = 1$

So that $a_i = a^{-1}$.

Hence R is a field.

<u>Problem:-</u>

Prove that the only idempotent elements of an integral domain are 0 and 1

<u>Proof:-</u>

let R be an integral domain

let $a \in R$ be an idempotent element.

Then $a^2 = a$. So that $a^2 - a = a(a-1) = 0$

Since R has no zero-divisors.

$a(a-1) = 0$

$a = 0$ (or) $a - 1 = 0$

Hence, $\boxed{a=0}$ (or) $\boxed{a=1}$

Hence 0 and 1 are the only idempotent elements of R.

Scanned by TapScanner

Characteristic of a ring:-

Let R be a ring. If there exists a positive integer n such that $na = 0$, for all $a \in R$ then the least such positive integer is called the characteristic of the ring R. If no such positive Integer exists then the ring is said to be of characteristic zero.

Thm: 4.15:-

The characteristic of an integral domain D is either 0 or a prime number.

Proof:-

If the characteristic of D is 0 then there is nothing to prove.

If not be the characteristic of D be n.

If n is not prime, let $n = pq$

where $1 < p < n$ and $1 < q < n$

Since characteristic of D is n

we have $n \cdot 1 = 0$.

Hence $n \cdot 1 = pq \cdot 1$

$= (p \cdot 1)(q \cdot 1)$

$= 0$.

Since D is an integral domain either

$p \cdot 1 = 0$ (or) $q \cdot 1 = 0$.

Since p, q are both less than n, this contradicts the definition of the characteristic of D.

Hence n is a prime number.

Subrings:-

A non-empty subset of a ring $(R, +, \cdot)$ is called a subring if S itself is a ring under the same operations as in R.

Scanned by TapScanner

Thm : 4.17:

A non-empty subset S of a ring R is a subring iff $a, b \in S \Rightarrow a-b \in S$ and $ab \in S$

Proof:-

Let S, be a subring of R.

Then $(S, +)$ is a sub group of $(R, +)$

Hence $a, b \in S \Rightarrow a-b \in S$.

Also, Since S itself is a ring $ab \in S$

Conversely,

Let S be a non-empty subset of R such that $a, b \in S \Rightarrow a-b \in S$ and $ab \in S$.

Then $(S, +)$ is a Subgroup of $(R, +)$

Also, S is called under multiplication

The associative and distributive laws are consequences of the corresponding laws in R.

Hence S is a subring.

Ideals:-

Let R be a ring. A non-empty subset of R is called a left ideal of R if:

(i) $a, b \in I \Rightarrow a - b \in I$.

(ii) $a \in I$ and $r \in R \Rightarrow ra \in I$

I is called a right ideal of R if

(i) $a, b \in I \Longrightarrow a - b \in I$.

(ii) $a \in I$ and $r \in R \Rightarrow ar \in I$

I is called an ideal of R if I is both a left ideal and a right ideal.

Thm: 4.20:-

Let R be ring with identity

1. If I is an ideal of R and $1 \in I$. Then $I = R$.

Proof:-

Obviously, $I \subseteq R$.

Now, let $r \in R$.

Since $1 \in I$, $r \cdot 1 = r \in I$

Thus $R \subseteq I$.

Hence $R = I$

Thm : 4.21 :-

Let F be a any field. Then the only ideal of F are $\{0\}$ and F.

Proof:-

Let I be an ideal of F.

Suppose $I \neq \{0\}$.

we shall prove that $I = F$.

since $I \neq \{0\}$, there exists an element $a \in I$ such that $a \neq 0$.

since F is a field a has a Multiplicative inverse $a^{-1} \in F$.

Now, $a \in I$ and $a^{-1} \in F \Rightarrow aa^{-1} = 1 \in I$

Hence by thm 4.2,

$I = F$.

Scanned by TapScanner

Thm: 4.23:-

Let R be a ring and I be a subgroup of $(R,+)$. The multiplication in R/I given by $(I+a)(I+b) = I+ab$ is well defined iff I is an Ideal of R.

Proof:-

Let I be an ideal of R.

To prove multiplication is well defined.

Let $I+a_1 = I+a$ & $I+b_1 = I+b$

Then $a_1 \in I+a$ & $b_1 \in I+b$.

$\therefore$ $a_1 = i_1 + a$ and $b_1 = i_2 + b$ where $i_1, i_2 \in I$.

Hence $a_1 b_1 = (i_1 + a)(i_2 + b)$.

$= i_1 i_2 + i_1 b + a i_2 + ab$.

Now, since I is an ideal we have $i_1 i_2$, $i_1 b$, $a i_2 \in I$

Scanned by TapScanner

Hence, $a_1 b_1 = i_3 + ab$ where

$i_3 = i_1 i_2 + i_1 b + a i_2 \in I$

$\therefore$ $a_1 b_1 \in I + ab$.

Hence, $I + ab = I + a_1 b_1$

conversely,

suppose that the multiplication in R/I given by $(I+a)(I+b) = I + ab$ is well defined.

To prove,

I is an ideal of R.

let $i \in I$ and $r \in R$.

we have to prove that $ir, ri \in I$

Now, $I + ir = (I+i)(I+r)$

$= (I+0)(I+r)$

$= I + 0r$

$= I$

$\therefore$ $ir \in I$

$|||^{ly}$

$ri \in I$

Hence I is an ideal.

Unit 5

Unit - V :

Maximal and Prime Ideals - Homomorphism of rings - field of Quotients of an integral domain - unique factorization domain - Euclidean domain.

Modern Algebra

By,

Mrs M.Sirin Hasina

Unit 5

Unit - V :

Maximal and Prime Ideals – Homomorphism of rings – field of Quotients of an integral domain – unique factorization domain – Euclidean domain.

Unit - V

Maximal and prime ideals

Definition :

Let R be a ring. An ideal $M \neq R$ is said to be a maximal ideal of R if whenever U is an ideal of R such that $M \subseteq U \subseteq R$ then either $U = M$ or $U = R$. That is there is no proper ideal of R properly containing M.

Prime Ideal:

Let R be a commutative ring. An ideal $P \neq R$ is called a prime ideal if $ab \in P \Rightarrow$ either $a \in P$ or $b \in P$.

Example:

(3) is a prime ideal of $\mathbb{Z}$ for, $ab \in (3) \Rightarrow ab = 3n$ for some integer n.

$$ab \in (3) \Rightarrow ab = 3n$$
$$\Rightarrow 3/ab$$
$$\Rightarrow 3/a \text{ or } 3/b$$
$$\Rightarrow a \in (3) \text{ (or) } b \in (3)$$

$\therefore$ (3) is a prime ideal

———— / ————

Example : (maximum ideal)

Let p be any prime. Then (p) is maximal ideal in $\mathbb{Z}$.

Let U be any ideal of $\mathbb{Z}$ such that $(p) \subseteq U$

Since every ideal of $\mathbb{Z}$ is a principal ideal $U = (n)$ for some $n \in \mathbb{Z}$.

Now. $\boxed{p \in (p) \subseteq U \Rightarrow p \in U = (n)}$

$\therefore$ $p = nm$ for some integer m.

Since p is prime either $n = 1$ or $n = p$

Suppose $n = 1$. Then $U = \mathbb{Z}$

Suppose $n = p$. Then $U = (p)$

$\therefore$ There is no proper ideal of $\mathbb{Z}$ properly containg (p).

Hence (p) is a maximal ideal in $\mathbb{Z}$.

Theorem : 4.24

Let R be a commutative ring with identity. An ideal M of R is maximal iff R/M is a field.

Proof:

Let M be a maximal ideal in R. Since R is a commutative ring with identity and $M \neq R$, R/M is also a commutative ring with identity.

Now, let $M+a$ be a non-zero element in R/M such that $a \notin M$.

We shall now prove that $M+a$ has Multiplicative inverse in R/M.

Let $U = \{ra+m / r \in R \text{ and } m \in M\}$

We claim that U is an ideal of R.

$(r_1a+m_1) - (r_2a+m_2) = (r_1-r_2)a + (m_1-m_2) \in U$.

Also $r(r_1a+m_1) = (rr_1)a + rm_1 \in U$ $\quad (\because rm_1 \in M)$

$\therefore U$ is an ideal of R.

Now, let $m \in M$. Then $m = 0a + m \in U$

$\therefore M \subseteq U$

$\therefore U$ is an ideal of R properly containing M.

But M is a maximal ideal of R.

$\therefore U = R$. Hence $1 \in U$

$\therefore 1 = ba + m$ for some $b \in R$.

Now,

$$M+1 = M+ba+M = M+ba \quad (\because m \in M)$$

$$= (M+b)(M+a)$$

Hence $M+b$ is the inverse of $M+a$.

Thus every non-zero element of R/M has a inverse.

Hence R/M is a field.

Conversely,

Suppose R/M is a field.

Let U be any ideal of R properly containing M

$\therefore$ There exists an element $a \in U$ such that $a \notin M$.

$\therefore$ $M+a$ is non-zero element of R/M.

Since R/M is a field $M+a$ has an inverse, say $M+b$

$\therefore$ $(M+a)(M+b) = M+1$

$M+ab = M+1$

$\therefore$ $1-ab \in M$.

But $M \subseteq U$. Hence $1-ab \in U$

Also $a \in U \Rightarrow ab \in U$

$\therefore$ $1 = (1-ab)+ab \in U$. Thus $1 \in U$

$\therefore$ $U = R$. Thus there is no proper ideal of R properly containg M.

Hence M is a Maximal Ideal in R.

Theorem 4.25

Let R be any commutative rings with identity. Let P be an ideal of R. Then P is a prime ideal $\Leftrightarrow$ R/P is an integral domain.

proof:

Let p be a prime ideal. Since R is commutative ring with identity an $M \neq R$, R/M is also a commutative ring with identity.

Now, $(p+a)(p+b) = p+0$

$\Rightarrow p+ab = p$

$\Rightarrow ab \in p$

$\Rightarrow a \in p$ or $b \in p$ (since p is a prime ideal)

$\Rightarrow p+a = p$ or $p+b = p$

Thus R/p has no zero divisors.

$\therefore R/p$ is integral domain.

Conversely, suppose R/p is an integral domain.

We claim that p is a prime ideal of R

Let $ab \in p$.

Then $p+ab = p$

$\therefore (p+a)(p+b) = p$

$\therefore p+a = p$ (or) $p+b = p$

(since R/p has no zero-divisors)

$\therefore \boxed{a \in p \text{ or } b \in p}$

$\therefore p$ is a prime ideal of R.

Homomorphism Rings:

Let R and R' be rings. A function $f : R \to R'$ is called a homomorphism, if

i) $f(a+b) = f(a) + f(b)$ and

ii) $f(ab) = f(a) \cdot f(b) \ \forall \ a, b \in R$.

If f is 1-1, then is called a monomorphism. If f is onto, then is called an epimorphism. A homomorphism of a ring onto itself is called an endomorphism.

Example:-

Let R be a ring and I be an ideal of R. Then $\phi : R \to R/I$ defined by $\phi(x) = I + x$ is a ring homomorphism. ϕ is called the natural homomorphism.

$$\begin{aligned} \phi(x+y) &= I + (x+y) \\ &= (I+x) + (I+y) \\ &= \phi(x) + \phi(y) \end{aligned}$$

$$\begin{aligned} \phi(xy) &= I + xy \\ &= (I+x)(I+y) \\ &= \phi(x)\,\phi(y) \end{aligned}$$

Hence ϕ is a ring homomorphism.

Theorem 1.28

Fundamental theorem of homomorphism.

Let R and R' be rings and $f: R \to R'$ be an epimorphism. Let k be the kernel of f. Then $R/K \approx R'$.

proof:

Define $\phi: R/K \to R'$ by $\phi(K+a) = f(a)$

and $\phi[(K+a)(K+b)] = \phi(K+ab)$

$= f(ab)$

$= f(a) \cdot f(b)$

(since f is homomorphism)

$= \phi(K+a)\, \phi(K+b)$

Hence ϕ is an isomorphism.

Hence $R/K \simeq R'$.

Field of quotients :-

The field F which any integral domain D can be embedded in a field F and every element of F can be expressed as a quotient of two elements of D, is called the field of quotients of D.

Theorem : 4.30

The field of quotients F of an integral domain D is the smallest field containing D. (ie) If F' is any other field containing D then F' contains a subfield isomorphic to F.

proof:

Let $a, b \in D$ and $b \neq 0$.

Then $a, b \in F'$ and since F' is a field $ab^{-1} \in F'$

Now, let F be the quotient field of D.

We define $f : F \to F'$ by $f(a/b) = ab^{-1}$

f is well defined.

For let $(a_1, b_1) \sim (a, b)$

Then $a_1 b = b_1 a$.

Hence $a_1 b_1^{-1} = ab^{-1}$

f is 1-1, Since $f(a/b) = f(c/d)$

$\Rightarrow ab^{-1} = cd^{-1}$

$\Rightarrow ad = cb$

$\Rightarrow a/b = c/d$.

Now, let $a/b, c/d \in F$

Then $f[(a/b) + (c/d)] = f[(ad + bc)/bd]$

$= (ad + bc)(bd)^{-1}$

$= (ad + bc) d^{-1} b^{-1}$

$= ab^{-1} + cd^{-1}$

$= f(a/b) + f(c/d)$

Also $f[(a/b)(c/d)] = f[(ac)/(bd)]$

$= (ac)(bd)^{-1}$

$= acd^{-1}b^{-1}$

$= ab^{-1} \cdot cd^{-1}$

$= f(a/b) \cdot f(c/d)$

Thus F is homomorphically embedded in F'.

Ordered Integral domain:

An integral domain D is called an ordered integral domain if D contains a subset, S with the following properties.

i) $a, b \in S \Rightarrow a+b \in S$

ii) $a, b \in S \Rightarrow ab \in S$

For each element $a \in D$, exactly one of the following holds.

$a = 0$, $a \in S$, $-a \in S$

The elements of S are called positive elements and the non-zero elements of D which are not in S are called negative elements.

Scanned by TapScanner

Unique factorization domain :-

An integral domain R is said to be unique factorization domain (U.F.D) if

i) any non-zero element in R which is not a unit can be expressed as the product of a finite number of prime elements.

ii) the factorization in (i) is unique up to the order and associates of the prime elements

i.e) If $a = p_1 p_2 \ldots\ldots p_r = q_1 q_2 \cdots q_s$ where the p_i's and q_j's are prime elements then $r = s$ and each p_i is an associate of some q_j.

Eucliden domain :-

Let R be a commutative rings without zero-divisors R is called an Eucliden domain or an Euclidean Ring if for every non-zero element $a \in R$. there is defined a non-negative integer $d(a)$ satisfying the following conditions.

i) For any two non-zero elements $a, b \in R$
$d(a) \leq d(ab)$.

ii) for any two non-zeros elements $a, b \in R$ there exists $q, r \in R$ such that $a = qb + r$. where either $r = 0$ (or) $d(r) < d(b)$.

Theorem 4.31:

Any Euclidean domain R has an identity element.

proof:

Since R is an ideal of R, there exists $c \in R$ such that $R = cR$

$\therefore$ Every element of R is a multiple of c.

In particular $c = ec$ for some $e \in R$.

Now,

let $x \in R$

Then $x = cy$ for some $y \in R$

$$\begin{aligned} \therefore ex &= e(cy) \\ &= (ec)y \\ &= cy \\ &= x \end{aligned}$$

$\therefore$ e is the required identity element.

Theorem : 4.32.

Let R be an Euclidean domain. Let a and b be two non-zero elements of R.

Then (i) b is not a unit in $R \Rightarrow d(a) < d(ab)$

(ii) b is a unit in $R \Rightarrow d(a) = d(ab)$

proof:

i) Suppose b is not a unit in R.

By defn of Euclidean domain there exists elements $q, r \in R$ such that

$$a = q(ab) + r \quad \text{——— ①}$$

where either $r = 0$ (or) $d(r) < d(ab)$

Now,

Suppose $r = 0$ then $a = q(ab)$

$$\therefore a - q(ab) = 0$$

$$a(1 - qb) = 0$$

Now, R has no zero-divisors and $a \neq 0$

$$\therefore 1 - qb = 0$$

Hence $\boxed{qb = 1}$

$\therefore$ b is a unit in R which is contradiction

$\therefore r \neq 0$. Hence $d(r) < d(ab)$ ——— ②

Now,

$$r = a(1 - qb) \quad (\text{by ①})$$

$$\therefore d(r) = d[a(1 - qb)]$$

$$\geq d(a) \quad \text{——— ③}$$

$$\therefore d(a) \leq d(r) < d(ab) \quad (\text{by ②})$$

$$\therefore d(a) < d(ab)$$

iii) Suppose b is unit in R

Now, $d(a) \leq d(ab)$

Also, $d(a) = d[(ab)b^{-1}] \geq d(ab)$

$\therefore d(a) \geq d(ab)$

$\therefore d(a) = d(ab)$

Theorem : 4.40

Let a be a non-zero element of an Euclidean domain R. Then a is a unit in R iff $d(a) = d(1)$

proof:-

Suppose a is a unit in R.

$\therefore d(a) = d(aa^{-1})$ (by thm 4.39)

$= d(1)$

Conversely,

let $d(a) = d(1)$

Suppose a is not a unit in R.

Then $d(1a) > d(1)$ (by thm 4.39)

$\therefore d(a) > d(1)$ which is contradiction.

$\therefore a$ is unit in R.

The End