M.Sc. MATHEMATICS

I YEAR – I SEMESTER
COURSE CODE: 7MMA1C1

CORE COURSE-I –ALGEBRA– I

Unit I

Group Theory: Definition of a group – Some examples of groups – Some preliminary Lemmas – Subgroups – A counting principle – Normal subgroups and Quotient groups – Homomorphisms – Automorphisms – Cayley's Theorem – Permutation Groups.

Unit II

Another counting Principle – Sylow's Theorem – Direct products

Unit III

Ring Theory: Definition and examples of rings – some special classes of Rings – Homomorphisms.

Unit IV

Ideals and Quotient Rings – More ideals and Quotient Rings – The field of quotients of an Integral Domain

Unit V

Enclidean Rings – A Particular Euclidean Ring – Polynomial Rings – Polynomials over the Rational Field – Polynomial Rings over commutative Rings.

Text Book(s)

I.N.Herstein, Topics in Algebra (2nd Edition) Wiley Eastern Limited, New Delhi, 1975.

Chapter II – 2.1 to 2.13 & Chapter III

Books for Supplementary Reading and Reference:

1. M.Artin, Algebra, Prentice Hall of India, 1991.
2. John B.Fraleigh, A First Course in Abstract Algebra, Addison Wesley, Mass, 1982.
3. D.S.Malik, J.N.Mordeson and M.K.Sen, Fundamentals of Abstract Algebra, McGraw Hill (International Edition), New York, 1997.

♣♣♣♣♣♣♣♣♣♣

course code: 7MMA1C1

core course - I - Algebra-I

Unit-I:-

Group theory: Defn of a group - some examples of groups - some preliminary lemmas - subgroups - A counting principle - Normal subgroups and quotient groups - homomorphism - Automorphism - cayley's thm - permutation groups.

Unit-II:-

Another counting principle - Sylow's theorem - Direct products.

Unit-III:-

Ring theory: Defn and examples of rings - some special classes of rings - homomorphism.

Unit-IV:-

Ideals and quotient rings - more ideals and quotient rings - the field of quotients of an integral domain.

Unit-V:-

Euclidean rings - (A particular Euclidean ring - polynomial rings) - polynomial rings over commutative rings.

Text books:-

I.N. Herstein, Topics in Algebra (2nd edition) Wiley Eastern Limited, New Delhi - 1975

Chapter - II - 2.1 to 2.13 and chapter - III

Books for supplementary reading and references:

1) M. Artin, Algebra, prentice Hall of India 1991

2) John B. Fraleigh, A First course in abstract algebra, Addison Wesley, Mass - 1982

3) D.S. Malik, J.N. Mordeson and M.K. Sen fundamentals of Abstract Algebra,

Unit - I

Group :-

U.Q 2m (2)

Defn :-

A non-empty sets of element G is said to form a group if in G there is defined a binary operation called the product and denoted by (·) such that

i) $a, b \in G \Rightarrow ab \in G$ (closeure)

ii) $a, b, c \in G \Rightarrow a(b \cdot c) = (a \cdot b)c$ (Association)

iii) There exists an element $e \in G$ such that $ae = ea = a$ for all $a \in G$ (the existence of an identity element)

iv) for every $a \in G$ there exists an element $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$ (The existence of inverse in G).

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.

Ex :-

i) Z, Q, R, C are groups under usual addition.

ii) R^*, Q^*, C^* are groups under usual multiplication

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

·	1	−1	i	$-i$
1	1	−1	i	$-i$
−1	−1	1	$-i$	i
i	i	$-i$	−1	1
$-i$	$-i$	i	1	−1

U.Q 2m

Defn : (Abelian group)

A group G is said to be abelian, if for every $a, b \in G$, $ab = ba$.

Ex:- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are abelian groups under usual addition.

$M_2(\mathbb{R})$ is not abelian.

- Thm: 1.1 Lemma 2.3.1 pg no: 33

If G is a group then

2m U.Q i) the identity element of G is unique

ii) Every $a \in G$ has a unique inverse in G.

iii) for every $a \in G$, $(a^{-1})^{-1} = a$.

U.Q 2m iv) for all $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

proof:-

i) Let e and e' be two identity element of G.

Then $ee' = e'$ (e is the identity element of G)

Also $ee' = e$ (e' is the identity element of G)

Hence: $e = e'$

ii) Let a' and a'' be two inverse of a

Hence $aa' = a'a = e$

$aa'' = a''a = e$

$a' = a'e$

$= a'(aa'')$

$= (a'a)a''$

$= ea''$

$a' = a''$

Hence the inverse element of G is unique.

iii) Let $a \in G$,

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

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

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

iv) Let $a, b \in G$

$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}$

$= aea^{-1}$

$= aa^{-1}$

$= e$

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b$$
$$= b^{-1}b$$
$$= e$$

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

Thm: 1.2

In a group the left and right cancellation laws hold that i) $ab = ac \Rightarrow b = c$ ii) $ba = ca \Rightarrow b = c$.

Proof:-

i) $ab = ac \Rightarrow b = c$

$$a^{-1}(ab) = a^{-1}(ac)$$
$$(a^{-1}a)b = (a^{-1}a)c$$
$$eb = ec$$
$$b = c$$

ii) $ba = ca$

$$(ba)a^{-1} = (ca)a^{-1}$$
$$b(aa^{-1}) = c(aa^{-1})$$
$$be = ce$$
$$b = c.$$

Thm: 1.3

Given $a, b \in G$ then the eqn $ax = b$ and $ya = b$ has unique solution for x and y in G.

Proof:-

consider $a^{-1}b \in G$.

Then $a(a^{-1}b) = (aa^{-1})b$

$$= eb$$
$$= b$$

Hence $a^{-1}b$ is the solution of $ax = b$.

Now, to prove the uniqueness

Let x_1 and x_2 be two solution of $ax = b$ then $ax_1 = b$ and $ax_2 = b$.

$$\therefore ax_1 = ax_2$$
$$x_1 = x_2$$

$\therefore x = a^{-1}b$ is the unique solution for $ax = b$.

Similarly,

We can prove that $y = ba^{-1}$ is the

unique solution of the equation $ya=b$.

v.a 2m pgno:37.

Defn:- Subgroup.

A non-empty subset H of group G is called a subgroup of G if H forms a group with respect to the binary operation in G.

Ex:-

1) $(\mathbb{Z},+)$ is a subgroup of $(\mathbb{R},+)$

2) $H=\{1,-1\}$ is a subgroup of $G=\{1,i,-1,-i\}$

pgno:37.

Thm:1.4 2.1.1

A non-empty subset H of the group G is a subgroup of G iff i) $a,b\in H \Rightarrow ab\in H$. ii) $a\in H \Rightarrow a^{-1}\in H$.

Proof:-

Assume H is subgroup of G.

To prove (i) and (ii)

Let H is a subgroup of G.

Then by the defn of subgroup.

(i) and (ii) are satisfied.

conversely,

Assume H is the non-empty subset of G and $a,b\in H \Rightarrow ab\in H$, $a\in H \Rightarrow a^{-1}\in H$.

Then we have to prove that

H is a subgroup of G.

i) $\Rightarrow$ H satisfies closure axiom.

ii) $\Rightarrow$ H satisfies inverse axiom.

and associative law also holds

It is enough to prove that there exist an identity element in H

Let $a\in H \Rightarrow a^{-1}\in H$ by (ii)

$aa^{-1}=e\in H$ by (i)

$\therefore e\in H$.

Hence H is a subgroup of G.

Thm: 1.5 Lemma 2.4.2 (Pgno: 88)
If H is a non-empty finite subset of a group G and H is closed under multiplication. Then H is a subgroup of G.

V.Q 5m (2)

Proof:-

Let $a \in H$.

Since H is closed.

$a, a^2, a^3, \ldots a^n, \ldots$ are all elements of H.

But since H is a finite.

The elements $a, a^2, a^3, \ldots$ cannot all be distinct.

Hence $a^r = a^s$ $r < s$

Then $a^{s-r} = e \in H$.

$a \in H$, we have proved.

That $a^n = e$ for some n.

Hence $a^{n-1}a = e$

$a^{n-1} = a^{-1} \in H$.

$\therefore$ H is a subgroup of G.

Pgno: 43

Defn: Order of the set (group)

Let G be a finite group, then the number of elements in G is called the order of G and is denoted by $|G|$ or $o(G)$.

Order of the element

Let G be a group and let $a \in G$. The least positive integer n (if it exists) such that $a^n = e$ is called the order of a. If there is no positive integer n such that $a^n = e$. Then the order of a is said to be infinite.

Ex:-

1) Let $G = \{1, -1, i, -i\}$

$o(G) = 4$

$o(1) = 1$

$o(-1) = 2$

$o(i) = 4$

$o(-i) = 4$

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

$O(0)=1$, $O(1)=4$, $O(2)=2$, $O(3)=4$.

3) find the order of -1 and 3 in $(Z, +)$

$O(-1)$ is infinite.

$O(3)$ is infinite

Defn:- cyclic group.

Let G be a group. Let $a \in G$. Then $H = \{a^n / n \in Z\}$ is a subgroup of G. H is called the cyclic subgroup of G, generated by a and is denoted by (a).

Let G be a group and let $a \in G$. a is called a generator of G if $(a) = G$.

A group G is cyclic if there exist an element $a \in G$ such that $(a) = G$.

Ex)-

$(Z_8, \oplus)$

$Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

$(0) = \{0\}$

$(1) = \{1, 2, 3, 4, 5, 6, 7, 0\}$

$(2) = \{2, 4, 6, 0\}$

$(3) = \{3, 6, 1, 4, 7, 2, 5, 0\}$

$(4) = \{4, 0\}$

$(5) = \{5, 2, 7, 4, 1, 6, 3, 0\}$

$(6) = \{6, 4, 2, 0\}$

$(7) = \{7, 6, 5, 4, 3, 2, 1, 0\}$

(1), (3), (5), (7) are the generator of the group.

(0) (2) (4) (6) are cyclic subgroup of Z_8

$\therefore (Z_8, \oplus)$ is the cyclic group.

$[(Z_8, \oplus)$

$8 = 4 \times 2$

$= 2^3 \cdot 1$

$\phi(n) = n(1 - 1/p)(1 - 1/q) \ldots$

$\phi(8) = 8(1-1/2)$

$= 8(1/2) = 4$

If n is prime

$\phi(n) = p-1$

To find the 'generator (Relatively prime)]

Thm: 1.6 If H and K are subgroup of a group G. Then $H \cap K$ is also a subgroup of G.

Proof:-

clearly $e \in H \cap K$

Hence $H \cap K \neq \phi$

Now let $a, b \in H \cap K$

Then $a, b \in H$ and $a, b \in K$

Since H and K are subgroup of G.

$ab^{-1} \in H$ and $ab^{-1} \in K$

$\therefore ab^{-1} \in H \cap K$.

Hence $H \cap K$ are subgroup of G.

Note:

The union of two subgroups is a subgroup iff one is contained in other.

Pgno:39 Defn:- Congruence

Let G be a group, H is a subgroup of G, for $a, b \in G$ we say a is congruent to b mod H, we write $a \equiv b \pmod H$ if $ab^{-1} \in H$

Pgno:39 ~~Thm: 1.7~~ Lemma: 2.4.3

Thm: 1.7 The relation $a \equiv b \pmod H$ is a equivalence relation.

proof:-

We have to prove that '$\equiv$' is an equivalence relation.

i) Reflexive:-

Since H is a subgroup of G.

$e \in H$

$aa^{-1} = e$

$aa^{-1} \in H$

$a \equiv a \pmod H$

(ii) Symmetric:

Suppose that $a \equiv b \pmod H$

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

To prove that, $b \equiv a \pmod H$

ie) $ba^{-1} \in H$.

Since H is subgroup of G.

$\Rightarrow (ab^{-1})^{-1} \in H$.

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

$\Rightarrow b \equiv a \pmod H$.

(iii) Transitive:

Suppose that $a \equiv b \pmod H$ and $b \equiv c \pmod H$

ie) $ab^{-1} \in H$ and $bc^{-1} \in H$

To prove that, $a \equiv c \pmod H$

ie) $ac^{-1} \in H$

Let $ab^{-1} \in H$ and $bc^{-1} \in H$

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

$ac^{-1} \in H$

$a \equiv c \pmod H$

Thus the relation $a \equiv b \pmod H$ is an equivalence relation.

Defn:-

If H is a subgroup of G, $a \in G$ then $Ha = \{ha / h \in H\}$. Ha is called right coset of H in G. $aH = \{ah / h \in H\}$ is called the left coset of H in G

Ex:-

In $(Z_8, \oplus)$, $H = \{0, 4\}$ is a subgroup of G. Find the left and right coset of G.

soln:-

$Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

$H = \{0, 4\}$

Right coset:-

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

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

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

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

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

Left coset:-

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

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

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

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

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

The number of left and right coset are 4.

• Defn: Index (pgno:41)

If H is a subgroup of G, the index of H in G is the number of distinct right (left) cosets of H in G. It is denoted by $[G:H]$ or $i_G(H)$

Ex:

In $(Z_8, \oplus)$, $H = \{0,4\}$

$\therefore [G:H] = 4$

$[G:H] \times O(H) = Z_8$

$4 \times 2 = 8$.

• Thm: 1.8 Lemma: 2.4.4 (pgno:40)

For all $a \in G$. $Ha = \{x \in G / a \equiv x \pmod H\}$.

Proof:-

Let $[aJ = \{x \in G / a = x \pmod H\}$

We have to prove that $Ha = [aJ$

Let $b \in Ha \Rightarrow b = ha$ for some $h \in H$

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

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

$\Rightarrow b \equiv a \pmod H$

$a \equiv b \pmod H$

$Ha \subseteq [aJ \rightarrow (1)$

Let $b \in [aJ$ then $b \equiv a \pmod H$

$\therefore ba^{-1} \in H$

$ba^{-1} = h$ for some $h \in H$.

$b = ha \in Ha$

$b \in Ha$

$[aJ \subseteq Ha \rightarrow (2)$

From (1) and (2)

$Ha = [aJ$.

V.Q 5m

(2) Thm: 1.9 (Lagranges thm)

If G is a finite group and H is a subgroup of G then the order of H is a divisor of order of G. $O(H) \mid O(G)$

Proof:-

Let the order of G be n.

Let the order of H is m and $[G:H]=r$

Then the number of left coset of H in G is r.

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.

Corollary:-

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

U.Q. Thm: 1.10 cor: 2.

Pgno: 42

Statement - 8m

Eulers thm (cor: 1)

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

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 $r \in G$

$\therefore r^{\phi(n)} = 1$ (Let G be a group of order n $a \in G \Rightarrow a^n = e$)

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

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

$a^{\phi(n)} \equiv 1 \pmod{n}$ ($\because \equiv$ is transitive)

Page no. 44 Thm: 1.11 (Fermat's thm . cor: 4)

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

Soln:-

Since ϕ is prime

$\phi(p) = p-1$ and

Hence the result follows from Eulers theorem

$\therefore a^{p-1} \equiv 1 \pmod{p}$.

cor: 3 cor: 1

If G is a finite and $a \in G$ the order of a divides order of G. $o(a) \mid o(G)$

proof:-

Let G be a group of order n.

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

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

By the Lagranges thm,

the order of subgroup divides the order of G.

$\therefore$ order of a divides order of G

Page no. 43 cor: 4 cor: 2

If G is a finite group and $a \in G$ then $a^{o(G)} = e$

proof:-

Let $o(G) = n$

Let $o(a) = m$

ie) $a^m = e$

by the above corollary

m divides n.

Hence $n = mq$.

$a^n = a^{mq}$

$\Rightarrow a^n = (a^m)^q$

$\Rightarrow a^n = e^q$

$a^n = e$

$a^{o(G)} = e$ ← (1)

cor:5 If G is a finite group whose order is a prime number p. Then G is a cyclic group.

(or)

Every group of prime order is cyclic.

proof:-

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

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

By cor:3

$o(a)$ is 1 or p

Since $a \neq e$

$o(a) = p$

Hence $G = \langle a \rangle$

Hence G is cyclic group.

Another counting principle:-

If H and K are two subgroups of G. Let $HK = \{x \in G / x = hk, h \in H, k \in K\}$.

pgno:HK

Thm:1.12 Lemma:2.5.1

HK is a subgroup of G iff $HK = KH$.

proof:-

Let HK is a subgroup of G

We claim, $HK = KH$

Let $x \in HK$

Since HK is a subgroup of G.

$\therefore x^{-1} \in HK$

Let $x^{-1} = hk$ where $h \in H$, $k \in K$

$(x^{-1})^{-1} = (hk)^{-1}$

$x = k^{-1}h^{-1}$

Since H and K are subgroup of G.

$h^{-1} \in H$, $k^{-1} \in K$

$\therefore x \in KH$

Hence $HK \subseteq KH \rightarrow (1)$

Now, let $x \in kH$

Then $x = kh$ where $k \in K$ and $h \in H$

$\therefore x^{-1} = (kh)^{-1}$

$= h^{-1}k^{-1} \in HK$

Now since HK is a subgroup, $(x^{-1}) \in HK$.

We have, $x \in HK$.

$\therefore KH \subseteq HK \rightarrow (2)$

From (1) and (2)

we get $HK = kH$

conversely, let $HK = KH$

we claim that

HK is a subgroup of G.

clearly $e \in HK$ and hence $HK \neq \phi$

Let $x, y \in HK$

Then $x = h_1 k_1$ and $y = h_2 k_2$ where $k_1, k_2 \in K_H$ and $h_1, h_2 \in H$.

$xy^{-1} = (h_1 k_1)(h_2 k_2)^{-1}$

$= h_1 k_1 k_2^{-1} h_2^{-1}$

$k_2^{-1} h_2^{-1} \in KH$

since $HK = KH$, $k_2^{-1} h_2^{-1} \in HK$.

$k_2^{-1} h_2^{-1} = h_3 k_3$ where $h_3 \in H$, $k_3 \in K$

$xy^{-1} = h_1 (k_1 h_3) k_3$

$k_1 h_3 \in KH$

since $KH = HK \Rightarrow k_1, h_3 \in HK$

$k_1 h_3 = h_4 k_4$ where $h_4 \in H$ $k_4 \in K$

$xy^{-1} = h_1 h_4 k_4 k_3 \in HK$.

$xy^{-1} \in HK$.

$\therefore HK$ is a subgroup of G

Lemma: 2.4.5

P.T there is a one to one correspondence between the right coset of H.

Proof:-

Let G be a group.

Let H be a subgroup of G.

Let $a, b \in G$.

Let Ha and Hb be two right cosets of H in G.

Forg any $hb \in Hb$ where $h \in H$ $\exists\ ha \in Ha$

This mapping is onto.

Suppose,

$h_1 b = h_2 b$

$\Rightarrow h_1 = h_2$

$\Rightarrow h_1 a = h_2 a$.

Hence mapping is 1-1

Hence there is a one to one correspondence between two right coset of H.

Corollary:1

If G is a finite group and $a \in G$ then $o(a) \mid o(G)$.

Proof:-

Let G be a finite group and $a \in G$

Let $\langle a \rangle$ be a cyclic subgroup of G generated by a

$\langle a \rangle$ consist of elements $e, a, a^2, a^3, \ldots$

Since $a^{o(a)} = e$.

Clearly cyclic subgroup $\langle a \rangle$ of a group G has atmost order of a.

Suppose,

If cyclic subgroup generated by a has more than $o(a)$ elements

then $a^i = a^j$ for some integer $0 \le i < j < o(a)$

then $a^{j-i} = e$, yet $0 < j-i < o(a)$

$\Rightarrow \Leftarrow$ to the defn of order of an element

The cyclic subgroup $\langle a \rangle$ generated by a has $o(a)$ elements

By Lagrange's thm,

$o(\langle a \rangle) \mid o(G)$

$o(a) \mid o(G)$

[Lagrange's thm, Let $|G|$ be a finite group of order n. Let H be a subgroup of G. Then $o(H) \mid o(G)$]

pgno:44 • **cor:5** If G is a finite group whose order is a prime number p then G is a cyclic.

proof:-

Let G be a finite group of prime order p

First we have to prove that,

G has no proper subgroup

Suppose H is a subgroup of G, then by Lagranges thm,

$o(H) \mid o(G)$

$o(H) \mid p$

$o(H) = 1$ or $oH = p$

$\Rightarrow H = \{e\}$ or $H = G$

$\therefore$ G has no proper subgroup

let $a \neq e \in G$

let $H = \langle a \rangle$

Then H is a subgroup of G.

Since G has no proper subgroup.

$H = \{e\}$ or $H = G$.

Since $a \neq e$, $H = G$

G is a cyclic group generated by a.

pgno:44 Hence, any group of prime order is cyclic.

counting principle:-

Let H and K be subgroup of G

$HK = \{hk \mid h \in H, k \in K\}$ and

$KH = \{kh \mid k \in K, h \in H\}$.

centre of a group :-

Let G be a group. Then the centre of G denoted by $Z(G)$ is defined by $Z(G) = \{a \in G \mid ax = xa \ \forall \ x \in G\}$

Thm:-

p.T centre of a group G is a subgroup of G.

proof:-

Let G be any group and then $Z(G) = \{a \in G \mid ax = xa \ \forall \ x \in G\}$ is the centre of G.

To prove that Z is a subgroup of G.

i) let $a, b \in G$

then $ax = xa$

$bx = xb \ \forall \ x \in G$

To Prove that $a \cdot b \in Z$

$(a \cdot b)x = a \cdot (bx)$

$= a \cdot (xb)$

$= (ax) \cdot b$

$= x(a \cdot b)$

$(a \cdot b)x = x(a \cdot b)$

$\Rightarrow a \cdot b \in Z \ \forall \ x \in G$

ii) Let $a \in Z$ then $ax = xa \ \forall \ x \in G$

To prove that

$a^{-1} \in Z$

$ax = xa$

$a^{-1}axa^{-1} = a^{-1}xaa^{-1}$

$xa^{-1} = a^{-1}x$

$\Rightarrow a^{-1} \in Z \ \forall \ x \in G.$

Hence Z is a subgroup of G

$\therefore$ centre of a group G is a subgroup of G.

Normalizer of G:-

Let G be any group and $a \in G$ then $N(a) = \{x \in G / ax = xa\}$ is called the normalizer of G.

Thm:

P.T normalizer of a group G is a subgroup of G.

Proof:-

Let G be any group and $a \in G$.

Then $N(a) = \{x \in G / xa = ax\}$

To prove,

$N(a)$ is a subgroup of G.

clearly $N(a) \neq \phi$

Since, $e \cdot a = a \cdot e$

$\Rightarrow e \in N(a)$

i) Let $x, y \in N(a)$

$\Rightarrow xa = ax$ and $ya = ay$.

$(xy)a = x(ya)$

$= x(ay)$

$= (xa)y$

$= (ax)y$

$(xy)a = a(xy)$

$\Rightarrow xy \in N(a)$

ii) Let $x \in N(a)$

$\Rightarrow xa = ax$

$x^{-1}xax^{-1} = x^{-1}axx^{-1}$

$ax^{-1} = x^{-1}a$

Hence $N(a)$ is a subgroup of G.

$\therefore$ Normalizer of G is a subgroup.

pg no:50 ✓ V.Q 2m (2)

Normal subgroup:-

Let G be any group and N be subgroup of G then N is a normal subgroup of G if for every $g \in G$ and $n \in N$ then $gng^{-1} \in N$.

Another defn:-

Let G be any group and N be subgroup of G then N is a normal subgroup of G iff $gng^{-1} \subset N$ for every $g \in G$.

pg no:50 ✓

Lemma: 2.6.1

P.T, N is a normal subgroup of G iff $gNg^{-1} = N$ for every $g \in G$.

Proof:-

Suppose N is a normal subgroup then by defn,

$$gNg^{-1} \subset N \quad \forall\ g \in G \rightarrow (1)$$

To prove,

$$N \subset gNg^{-1} \quad \forall\ g \in G$$

let $g \in G \Rightarrow g^{-1} \in G$

then by defn of normal subgroup

$g^{-1}N(g^{-1})^{-1} \subset N$ for every $g^{-1} \in G$

$$g^{-1}Ng \subset N$$

$$gg^{-1}Ngg^{-1} \subset gNg^{-1}$$

$$N \subset gNg^{-1} \rightarrow (2)$$

From (1) & (2)

$$gNg^{-1} = N \text{ for every } g \in G.$$

conversely,

suppose $gNg^{-1} = N$ for every $g \in G$

clearly $gNg^{-1} \subset N$.

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

jno:5

Lemma : 2.6.2

P.T a subgroup N of G is a normal subgroup of G iff every left coset N in G is a right coset of N in G.

Proof:-

Let N be a subgroup of G.

Suppose, N is a normal subgroup of G.

By the above lemma

for every $g \in G$, $gNg^{-1} = N$

$$gNg^{-1} = N$$

$$gNg^{-1}g = Ng \quad \forall\ g \in G$$

$$gN = Ng$$

Hence every left coset of N in G is a right coset of N in G.

conversely,

Suppose every left coset of N in G is a right coset of N in G.

To prove, N is a normal subgroup of G.

Let $g \in G$.

Then, $g = g \cdot e \in gN$.

$g = e \cdot g \in Ng$.

$\therefore$ g is an element in two distinct right (left) cosets in gN and Ng (left).

But, distinct right cosets have, no common element.

$$gN = Ng \quad \forall\ g \in G$$

$\Rightarrow gNg^{-1} = Ngg^{-1}$

$\Rightarrow gNg^{-1} = N$

$\Rightarrow gNg^{-1} \subset N$ (obviously)

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

clearly $gNg^{-1} \subset N$.

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

pg no: 51

Lemma : 2.6.2

P.T a subgroup N of G is a normal subgroup of G iff every left coset N in G is a right coset of N in G.

Proof:-

Let N be a subgroup of G.

Suppose, N is a normal subgroup of G.

By the above lemma

for every $g \in G$, $gNg^{-1} = N$

$$gNg^{-1} = N$$

$$gNg^{-1}g = Ng \quad \forall\ g \in G$$

$$gN = Ng$$

Hence every left coset of N in G is a right coset of N in G.

conversely,

Suppose every left coset of N in G is a right coset of N in G.

To prove, N is a normal subgroup of G.

Let $g \in G$.

then, $g = g \cdot e \in gN$.

$g = e \cdot g \in Ng$.

$\therefore g$ is an element in two distinct right (left) cosets in gN and Ng (right).

But, distinct right (left) cosets have, no common element.

$gN = Ng \quad \forall\ g \in G$

$\Rightarrow gNg^{-1} = Ngg^{-1}$

$\Rightarrow gNg^{-1} = N$

$\Rightarrow gNg^{-1} \subset N$ (obviously)

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

pg no:57

V.Q (2) mrs

• Lemma : 2.6.3

P.T a subgroup N of G is a normal subgroup of G iff the product of two right cosets of N is again right cosets of N in G.

Proof:-

Let N be subgroup of G.

Suppose N is a normal subgroup of G.

To prove,

the product of two right cosets of N is again a right coset.

Let $a, b \in G$.

Na, Nb be two right cosets of N.

$$Na.Nb = N(aN).b$$
$$= N.Nab.$$
$$= Nab.$$

which is the right coset of N.

conversely,

suppose the product of two right cosets of N, is again a right coset.

To prove,

N is a normal subgroup of G

Let Na, Nb be two cosets of N in G.

Given that,

$$Na.Nb = N.ab$$

where Nab is a right coset of N containing ab

Let $a \in G, n \in N$.

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

Hence, N is a normal subgroup of G.

pblm:-

P.T every subgroup of abelian group is a normal subgroup.

proof:-

$a \cdot b = b \cdot a \quad \forall\ a, b \in G$.

let N be a subgroup of G.

To prove, N is a normal

ie) To prove, $gng^{-1} \in N \quad \forall\ g \in G$

let $g \in G$, $n \in N$.

$gn = ng$

G is abelian

$gng^{-1} = ngg^{-1}$

$gng^{-1} = n \in N$.

$gng^{-1} \in N$.

pg.no:52 N is a normal subgroup of G.

Thm: 2.6.1

If G is a group and N is a normal subgroup of G then G/N is also a group.

proof:-

Let G/N denote the collection of right cosets of N in G.

ie) $G/N = \{Na \mid a \in G\}$

i) let $x, y \in G/N$

For $x = Na$, $y = Nb$ for some $a, b \in G$

$xy = Na \cdot Nb$

$= N(aN)b$

$= N(Na)b$

$xy = NNab$

$xy = Nab$ is a right coset

$\Rightarrow xy \in \frac{G}{N}$.

ii) Associative:-

let $x, y, z \in G/N$

for $x = Na$, $y = Nb$, $z = Nc$ for some $a, b, c \in G$

$$X(YZ) = Na\,(Nb\,Nc)$$
$$= Na\,(Nbc)$$
$$= Na\,(bc)$$
$$= N(ab)c$$
$$= N(ab)\,Nc$$
$$X(YZ) = (XY)Z$$

$\therefore \frac{G}{N}$ is associative

iii) Identity

Consider the element,

$N = Ne \in G/N$

Let $x \in G/N$ for $x = Na$ for some $a \in G$

$$xN = Na \cdot Ne$$
$$= Nae$$
$$= Na$$
$$xN = Na$$
$$xN = x.$$
$$Nx = Ne \cdot Na$$
$$= Nea$$
$$= Na$$
$$Nx = x.$$
$$Nx = xN = x$$

iv) Inverse:-

Suppose $Na \in G/N$ where $a \in G$

This $Na^{-1} \in G/N$ where $a^{-1} \in G$.

$$Na \cdot Na^{-1} = Naa^{-1}$$
$$= Ne$$

Hence, Na^{-1} is the inverse of Na in G/N

Hence, G/N is a group.

Quotient group:-

Let G be any group and N be a normal subgroup of G, then $G/N = \{Na / a \in G\}$ is a group with respect to the product

defined by,

$N_a \cdot N_b = N_{ab}$, $\forall a, b \in G$.

This group G/N is called quotient or factor group of G/N.

pblm:-

P.T every subgroup of a cyclic group is normal.

proof:-

We know that

Every cyclic group is abelian

every subgroup of an abelian group is normal.

Hence, every subgroup of a cyclic group is normal.

Let $G = \langle a \rangle$ is a cyclic group generated by a.

Let $x, y \in G$

$x = a^r$, $y = a^s$ for some r, s is an integers

$$x \cdot y = a^r \cdot a^s$$
$$= a^{r+s}$$
$$= a^{s+r}$$
$$= a^s \cdot a^r$$
$$xy = yx$$

$\therefore G$ is an abelian.

Lemma:

If G is a group and H is a subgroup of index 2 in G then prove that H is a normal subgroup of G.

proof:-

Let G be a group

H is a subgroup of index 2.

Let $a \in G$.

if $a \in H$, then $aH = H$

$Ha = H$

$aH = Ha$

Hence H is a normal.

If $a \notin H$, then $aH \cap H = \phi$ and

$$aH \cup H = G$$

$$\Rightarrow aH = G - H$$

Illy $Ha = G - H$.

Hence H is a normal.

Homomorphism:-

Let G and $\bar{G}$ be two subgroups. then a map $\phi: G \to \bar{G}$ is called a homomorphism if $\phi(ab) = \phi(a) \cdot \phi(b)$ $\forall\ a, b \in G$.

Theorem 2.5.1

If H and K are finite subgroups of a group G of order $O(H)$ and $O(K)$ respectively, then $O(HK) = \frac{O(H) \cdot O(K)}{O(H \cap K)}$.

Proof:-

Case (i)

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

$\therefore O(H \cap K) = 1$.

It is enough if we prove that $O(HK) = O(H) \cdot O(K)$

This is true if $O(H) = 1$.

Reason:

$O(H) = 1 \Rightarrow H = \{e\}$

$HK = \{e\}K$

$O(HK) = O(K)$

$O(HK) = 1 \cdot O(K)$

$O(HK) = O(H) \cdot O(K)$.

Assume the contrary that $O(HK) \neq O(H) \cdot O(K)$

Hence there is duplication of an element in HK

Hence there exists $h_1 k_1$ in HK such that

$h_1k_1 = h_2k_2$ where $h_1, h_2 \in H$ and $k_1, k_2 \in K$ and h_1 and h_2 are distinct.

$h_1k_1 = h_2k_2 \Rightarrow h_2^{-1}h_1k_1k_1^{-1} = h_2^{-1}h_2k_2k_1^{-1}$

$\Rightarrow h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{e\}$.

$\Rightarrow h_2^{-1}h_1 = e$

$\Rightarrow h_1 = h_2 e$.

$\Rightarrow h_1 = h_2$ which is a contradiction

$\therefore O(HK) = O(H) \cdot O(K)$

Case (ii)

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

Since $H \cap K$ is non-empty, take $x \in H \cap K$

consider an element hk in HK.

$hk = he k = h(xx^{-1})k = (hx)(x^{-1}k)$ which is also a member of HK.

Reason $h \in H$, $x \in H \cap K$.
$\Rightarrow h \in H$, $x \in H$
$\Rightarrow hx \in H$
$x \in H \cap K$, $k \in K$.
$x \in K$, $k \in K$
$x^{-1} \in K$, $k \in K$
$\Rightarrow x^{-1}k \in K$

Hence an element hk in HK has a duplication of the form $h(xx^{-1})k$

This is true for all $x \in H \cap K$.

Hence each of $h(xx^{-1})k$ where $x \in H \cap K$ is a duplication of hk.

There may be some more duplications in HK for hk

Any element hk in HK repeats atleast $O(H \cap K)$ times

we shall now prove that hk repeats exactly $O(H \cap K)$ times

Suppose h_1k_1 is any arbitrary duplication of hk.

$hk = h_1k_1$ where $h, h_1 \in H$ and $k, k_1 \in K$.

$h^{-1}hK = h^{-1}h_1K_1$

$K = h^{-1}h_1K_1$

$KK_1^{-1} = h^{-1}h_1K_1K_1^{-1}$.

$KK_1^{-1} = h^{-1}h_1 = u$.

[$KK_1^{-1}=u$ $u\in K$ $h^{-1}h_1=u$ $u\in H$ $u\in H\cap K$

$K_1K_1^{-1}K_1 = uK_1$ $h_1=hu$

$K = uK_1$ $h_1=hu$

$u^{-1}K = K_1$ $h_1=hu$]

Clearly. $u \in H\cap K$

$h_1K_1 = huu^{-1}K \Rightarrow hK = h(uu^{-1})K$.

Any duplication of hK is of the form $hK = h(uu^{-1})K$ where $u \in H\cap K$

Hence every element hk in HK repeats exactly $O(H\cap K)$ times.

Hence the number of distinct elements in HK is given by

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

V.Q 10m ✓

Thm: 2.7.1 Fundamental thm of homomorphism (2)

Let ϕ be a homomorphism of G onto $\bar{G}$ with kernel K. Then $G/K \cong \bar{G}$

Proof:-

Let $g \in G$

$\therefore \phi(g) \in \bar{G}$

Define $\psi : G/K \to \bar{G}$ by $\psi(Kg) = \phi(g)\ \forall\ g \in G$

i) To prove ψ is well defined

Let $Kg_1, Kg_2 \in G/K$.

$Kg_1 = Kg_2 \Rightarrow g \in Kg_2$ [$\because g_1 = eg_1 \in Kg_1 = Kg_2$]

$\Rightarrow g_1 = kg_2$ for some $k \in K$.

$\Rightarrow \phi(g_1) = \phi(kg_2)$ [$\because \phi$ is a homomorphism and hence well defined]

$\Rightarrow \phi(g_1) = \phi(k).\phi(g_2)$

$\Rightarrow \phi(g_1) = \bar{e}\,\phi(g_2)$ [$\because k \in K \Rightarrow \phi(k) = \bar{e}$]

$\Rightarrow \phi(g_1) = \phi(g_2)$

$\Rightarrow \psi(Kg_1) = \psi(Kg_2)$

Hence it is well defined.

ii) To prove: $\psi : G/K \to \bar{G}$ is onto

Let $\bar{g} \in \bar{G}$

since $\phi : G \to \bar{G}$ is onto, there exists $g \in G$ such that $\phi(g) = \bar{g}$

ie) there exists $Kg \in G/K$ such that $\psi(Kg) = \bar{g}$

for any $\bar{g} \in \bar{G}$, there exists $Kg \in G/K$ such that $\psi(Kg) = \bar{g}$

$\therefore \psi$ is onto.

iii) To prove

ψ is a homomorphism.

Let $Kg_1, Kg_2 \in G/K$.

$\psi(Kg_1 \cdot Kg_2) = \psi(Kg_1 g_2)$

$= \phi(g_1 g_2)$ (by defn of ψ)

$= \phi(g_1) \cdot \phi(g_2)$ ($\because \phi$ is a homomorphism)

$= \psi(Kg_1) \cdot \psi(Kg_2)$

$\psi(Kg_1 \cdot Kg_2) = \psi(Kg_1) \cdot \psi(Kg_2) \quad \forall \; Kg_1, Kg_2 \in G/K.$

$\therefore \psi$ is a homomorphism

iv) To prove kernel of ψ = {unit element of G/K}

ie) To prove kernel of ψ = $\{K\}$:

First of all ψ is onto, $\bar{e}$ has atleast one pre-image.

Suppose $Kg \in G/K$ is mapped to $\bar{e}$ under ψ.

ie) $Kg \in G/K$ such that $\psi(Kg) = \bar{e}$

ie) $Kg \in G/K$ such that $\phi(g) = \bar{e}$

$\Rightarrow Kg \in G/K$ & $g \in K$

$\Rightarrow Kg \in G/K \ni : g \in$ Kernel of ϕ

(3) $\Rightarrow Kg \in G/K \ni g \in K$.

$\Rightarrow Kg = K$ [$\because$ K is subgroup and by thm 8.29 (i) in UG book

Let H be a subgroup of a group G 8.29(i) $a \in H \Rightarrow Ha = H$]

Hence K is the only element of G/K mapped to $\bar{e}$ under ψ.

Kernel of $\psi = \{K\}$

ie) Kernel of $\psi = \{$unit element of $G/K\}$

ie) $K_\psi = \{K\}$.

By above corollary, the homomorphism ψ is 1-1.

Hence there exists an isomorphism $\psi : G/K$ onto $\bar{G}$

$\therefore G/K \cong \bar{G}$.

corollary:

A homomorphism ϕ of G into $\bar{G}$ with kernel K_ϕ is an isomorphism of G into $\bar{G} \Leftrightarrow K_\phi = \{e\}$.

ie) already know $K = \{e\} \Leftrightarrow$ homomorphism $\phi : G \to \bar{G}$ is 1-1

ie) $K = \{e\} \Leftrightarrow$ homomorphism $\phi : G \to \bar{G}$ is an isomorphism

Lemma

If $\phi : G \to \bar{G}$ is a homomorphism which is not onto,

$\phi^{-1}(\bar{g}) = \begin{cases} \{\} \text{ if } \bar{g} \text{ has no pre-image} \\ \text{if } \bar{g} \text{ has atleast one pre-image } x \end{cases}$

If $K_\phi = \{e\}$, then $\phi^{-1}(\bar{g}) = \begin{cases} \{\} \text{ if } \bar{g} \text{ has no pre-image} \\ \{x\} \text{ if } \bar{g} \text{ has atleast one pre-image } x. \end{cases}$

$= \begin{cases} \{e\} & \text{if } \bar{g} \text{ has no pre-image.} \\ \{x\} & \text{if } \bar{g} \text{ has atleast one pre image } x. \end{cases}$

If $K=\{e\}$, $\phi^{-1}(\{g\})$ has a maximum of one element.

ie) If $K=\{e\}$, an element $\bar{g} \in \bar{G}$ has a maximum of one pre-image.

ie) If $K=\{e\}$, then homomorphism ϕ is 1-1

$\therefore K=\{e\} \Rightarrow$ homomorphism ϕ is 1-1.

pg no:46 ✓ Q

2m

Corollary 1 to thm: 2.5.1

If H and K are subgroups of G and $O(H) > \sqrt{O(G)}$, $O(K) > \sqrt{O(G)}$, then $H \cap K \neq \{e\}$

proof:-

Since $G \geq HK$, $O(G) \geq O(HK) = \frac{O(H) \cdot O(K)}{O(H \cap K)}$ (By thm 2.5.1)

$> \frac{\sqrt{O(G)} \cdot \sqrt{O(G)}}{O(H \cap K)}$

$\therefore O(G) > \frac{O(G)}{O(H \cap K)}$

$O(H \cap K) > 1$

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

corollary 2 to thm 2.5.1

If the group G is of finite order pq here p and q are prime numbers with $p>q$, then G have atmost one subgroup of order p.

proof:-

Suppose G has two distinct subgroups H, K of order p.

Given $p>q$ ie) $p \cdot p > p \cdot q$ (ie) $p^2 > pq$

(ie) $p > \sqrt{pq} = \sqrt{O(G)}$

Hence $O(H) > \sqrt{O(G)}$ and $O(K) > \sqrt{O(G)}$

By the above corollary $H \cap K \neq \{e\}$

By thm 3.19 in UG Book, If H and K are subgroups of a group G then $H \cap K$ is also a subgroup of G.

We can treat $H \cap K$ as a subgroup of H and also as a subgroup of K.

By note 8 in UG book page 3.30,

Any group of prime order has no proper subgroups.

ie) any group of prime order has only improper subgroup.

Since H is a group of prime order and $H \cap K$ is a subgroup of H, $H \cap K$ must be an improper subgroup H.

$\therefore H \cap K = \{e\}$ or $H \cap K = H$.

Since $H \cap K \neq \{e\}$, $H \cap K = H$.

$\therefore H = H \cap K \subseteq K$

$\therefore H \subseteq K$.

Similarly since K is a group of prime order and $H \cap K$ is a subgroup of K, $H \cap K$ must be an improper subgroup of K.

$\therefore H \cap K = \{e\}$ (or) $H \cap K = K$

Since $H \cap K \neq \{e\}$,

$H \cap K = K$

$K = H \cap K \subseteq H$.

$\therefore K \subseteq H$

Hence $H = K$.

Hence G cannot have two distinct subgroups of order p.

ie) G can have atmost one subgroup of order p.

Quotient group:-

Let G be a group and N is a normal subgroup of G. This group G/N is called the factor group or the quotient group of G by N.

where $G/N = \{Na \mid a \in G\}$

= The set of all right cosets of N in G.

G/N is a group under the operation from $G/N \times G/N \to G/N$ defined by $Na \cdot Nb = Nab$ $\forall a, b \in G$.

Note:

$G/N = \{Na_1, Na_2, \ldots\}$

where $Na_1 \subseteq G$

$Na_2 \subseteq G$

. . .

Hence G/N is a collection of subsets of G.

Thm:-

G/N is a group with respect to the product defined by $Na \cdot Nb = Nab$ $\forall a, b \in G$.

proof:-

i) closure property.

Let $Na, Nb \in G/N$

$Na \cdot Nb = N(aN)b = N(Na)b$ (since N is normal)

$= NN(ab)$

$= Nab$ (since $NN = N$)

$Na \cdot Nb \in G/N$

$\therefore$ closure property is true.

ii) Associative property

Let $Na, Nb, Nc \in G/N$.

$(Na \cdot Nb) \cdot Nc = (Nab) \cdot Nc = N(ab) \cdot c = Na(bc)$

$= (Na)(Nbc) = Na \cdot (Nb \cdot Nc)$

Hence associative property is true.

(iii) Identity

Let $Na \in G/N$.

There exists $Ne \in G/N$ such that

$Na \cdot Ne = Nae = Na$

$Ne \cdot Na = Nea = Na$.

This is true $\forall\ Na \in G/N$.

$\therefore Ne = N$ is the identity element of G/N

iv) Inverse

Let $Na \in G/N$.

There exists $Na^{-1} \in G/N$ such that

$Na \cdot Na^{-1} = Naa^{-1} = Ne = N$

$Na^{-1} \cdot Na = Na^{-1}a = Ne = N$.

Hence inverse of Na is Na^{-1} in G/N.

Hence G/N is a group.

Note:-

$O(G/N)$ = The no. of distinct right cosets of N in G.

= The index of N in G (by index defn)

$= i_G(N)$

$= \frac{O(G)}{O(N)}$ (by corollary to Lagranges thm.)

pblm: 2

Z is a normal subgroup of G.

$Z = \{x \in G \mid xa = ax\ \forall a \in G\}$.

$= \{$The set of all those elements of G which commute with every element of G.

i) $Z \neq \phi$ ($\because e \in Z$ reason: $ea = ae\ \forall\ a \in G$.

ie) e commutes with every element of G)

ii) To prove: $a, b \in Z \Rightarrow ab^{-1} \in Z$.

Let $a, b \in Z$. Hence, a commutes with every element of G.

$(ab)(ab^{-1}) = (ab^{-1})(ab)$ commutes with every element of G.

Hence $ax = xa \ \forall \ x \in G$ & $bx = xb \ \forall \ x \in G$

$bx = xb \Rightarrow b^{-1}(bx)b^{-1} = b^{-1}(xb)b^{-1} \Rightarrow exb^{-1} = b^{-1}xe$

$\Rightarrow xb^{-1} = b^{-1}x$ — (*)

$\therefore (ab^{-1})x = a(b^{-1}x) = a(xb^{-1})$ using (*)

$= (ax)b^{-1} = (xa)b^{-1}$ (since $ax = xa \ \forall \ x \in G$)

$= x(ab^{-1})$.

This is true $\forall \ x \in G$.

Hence ab^{-1} commutes with every element of G.

$\therefore ab^{-1} \in Z$.

from (i) & (ii) Z is a subgroup of G.

(ii) Z is a normal subgroup of G.

To prove that $gxg^{-1} \in Z \ \forall \ g \in G$ and $x \in Z$.

Let $g \in G$ and $x \in Z$.

$x \in Z \Rightarrow xg = gx \ \forall \ g \in G$.

$\Rightarrow gx = xg \ \forall \ g \in G$.

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

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

$\Rightarrow gxg^{-1} = x \in Z$.

Z is a normal subgroup of G.

3) P.T Z is an abelian subgroup of G.

proof

First prove Z is a subgroup. (proof given in previous pblm)

Let $z_1, z_2 \in Z$

we claim $z_1 z_2 = z_2 z_1$

$z_1 \in Z \Rightarrow z_1 a = a z_1 \ \forall a \in G$ — (1)

$\Rightarrow z_1 z_2 = z_2 z_1$ (putting $a = z_2$ in (1))

$\therefore Z$ is abelian

ie) The centre Z of a group G is abelian.

4) If N is a normal subgroup of G and H is any subgroup of G. prove that NH is a subgroup of G.

Proof:-

Since N is normal $\Rightarrow Na = aN \ \forall a \in G$

$\Rightarrow Nh = hN \ \forall h \in H$. since $H \subseteq G$.

Let us prove $NH = HN$.

$x \in HN \Rightarrow x = hn$ for some $h \in H$ and $n \in N$.

$\Rightarrow x \in hN \Rightarrow x \in Nh$ ($\because hN = Nh$)

$\Rightarrow x = n_1 h$ for some $n_1 \in N$

$\Rightarrow x \in NH$

$\therefore HN \subseteq NH$.

Similarly, $x \in NH \Rightarrow x = nh$ where $n \in N, h \in H$.

$\Rightarrow x \in Nh \Rightarrow x \in hN$ ($\because Nh = hN$).

$\Rightarrow x \in hn$ for some $n_1 \in N$.

$\Rightarrow x \in HN$

$\therefore NH \subseteq HN$.

Hence $NH = HN$.

Since $NH = HN$, by lemma 2.5.1, NH is a subgroup of G.

Since $NH = HN$, HN is also a subgroup of G.

V.Q. 2m

5) S.T that the intersection of two normal subgroups of G is a normal subgroup of G.

Soln:- Let H, K be two normal subgroups of G:

By thm 3.19 of UG book, $H \cap K$ is a subgroup of G.

To prove that $H \cap K$ is normal.

Let $g \in G$. Let $n \in H \cap K \Rightarrow n \in H$ & $n \in K$.

$n \in H$ and H is normal $\Rightarrow gng^{-1} \in H$

$n \in K$ and K is normal $\Rightarrow gng^{-1} \in K$.

$\therefore gng^{-1} \in H \cap K$ for any arbitrary $g \in G$ and for any arbitrary $n \in H \cap K$.

$\therefore H \cap K$ is normal.

6) If H is a subgroup of G and N is a normal subgroup of G, S.T $H \cap N$ is a normal subgroup of H and $H \cap N$ need not be normal in G.

soln:- Let H be a subgroup of G.

Let N be a normal subgroup of G.

i) $H \cap N$ is a subgroup of G.

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

ii) Let $g \in H$; $x \in H \cap N$.

claim : $gxg^{-1} \in H \cap N$.

$x \in N$ and $g \in H \Rightarrow x \in N$ and $g \in G$ (∵ $H \subseteq G$)

$\Rightarrow gxg^{-1} \in N$ (∵ N is normal in G)

Also $x \in H$ and $g \in H \Rightarrow gxg^{-1} \in H$ (∵ H is a group)

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

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

Counter ex:- for $H \cap N$ is not normal in G.

Let $G = S_3$. Let $N = G$ and $H = \{e, P_3\}$

$\therefore H \cap N = H$.

H is not normal in G.

Reason: there exists $g \in G$ and $h \in H$ such that $ghg^{-1} \in H$.

There exists $P_1 \in G$, $P_3 \in H$ such that $P_1 P_3 P_1^{-1}$

$= P_1 P_3 P_2$

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

$$= \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = P_5 \notin H$$

$e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ $P_1=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$

$P_2=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ $P_3=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$

$P_4=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ $P_5=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$

$\therefore$ HAN is not normal in G.

7) S.T every subgroup of an abelian group is normal.

soln:-

Since G is abelian, $ab=ba$ $\forall$ $a,b \in G$. ——— (1)

Let H be a subgroup of G.

Since $H \subseteq G$,

From (1), $hb=bh$ $\forall$ $h \in H$ and $\forall$ $b \in G$.

$Hb=bH$ $\forall$ $b \in G$.

$\therefore$ H is normal in G.

8) If N and M are normal subgroups of G, P.T NM is also a normal subgroup of G.

soln:-

i) NM is a subgroup of G (by the above pblm 4)

ii) NM is normal.

claim $gxg^{-1} \in NM$ $\forall$ $g \in G$ and $x \in NM$.

Let $g \in G$, $x \in NM$.

$\therefore$ $x=nm$ for some $m \in M$, $n \in N$.

Since N is normal and $n \in N$, $gng^{-1} \in N$.

Since M is normal and $m \in M$, $gmg^{-1} \in M$.

$\therefore$ $(gng^{-1})(gmg^{-1}) \in NM$.

i.e) $gn(g^{-1}g)mg^{-1} \in NM$ (i.e) $gnemg^{-1} \in NM$.

i.e) $gnmg^{-1} \in NM$ (i.e) $g(nm)g^{-1} \in NM$.

i.e) $gxg^{-1} \in NM$ $\forall$ $x \in NM$.

$\therefore$ NM is normal in G.

9) M and N are normal subgroups of a group G such that $M \cap N = \{e\}$. S.T every element of M commutes with every element of N.

Sol^n:- Let $a \in M$ and $b \in N$.

Claim $ab = ba$

Consider $aba^{-1}b^{-1}$

Since $a^{-1} \in M$ and M is normal, $b(a^{-1})b^{-1} \in M$.

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

Since $a \in M$ and $ba^{-1}b^{-1} \in M$, $aba^{-1}b^{-1} \in M$.

Since $b \in N$ and N is normal, $a(b)a^{-1} \in N$.

Since $aba^{-1} \in N$ and $b^{-1} \in N$, $aba^{-1}b^{-1} \in N$.

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

$\therefore aba^{-1}b^{-1} = e \Rightarrow (aba^{-1}b^{-1})b = eb \Rightarrow aba^{-1} = b$.

$\Rightarrow (aba^{-1})a = ba \Rightarrow abe = ba \Rightarrow ab = ba$.

Hence proved.

Homomorphism:

Ex:-

Define $\phi : (G, *) \to (G, *)$ by $\phi(x) = x \ \forall x \in G$

Let $x, y \in G$.

$\phi(x*y) = x*y = \phi(x) * \phi(y) \ \forall x, y \in G$

This ϕ is a homomorphism.

Ex: 2.7.3

Define $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ by $\phi(z) = 2z \ \forall x \in \mathbb{Z}$.

$\phi(x+y) = 2(x+y)$ (by defn of ϕ)

$= 2x + 2y$

$= \phi(x) + \phi(y)$ by defn of ϕ

$\therefore \phi$ is a homomorphism.

Lemma: 2.7.1

Suppose G is a group, N a normal subgroup of G; Define $\phi: G \to G/N$ by $\phi(x) = Nx \ \forall \ x \in G$. Then ϕ is a homomorphism from G onto G/N.

proof:-

Let $a, b \in G$.

$$\phi(a*b) = N(a*b) \quad \text{(by defn of } \phi\text{)}$$
$$= (Na)\cdot(Nb)$$
$$= \phi(a)\cdot\phi(b)$$

$\therefore \phi$ is a homomorphism from G to G/N

This ϕ is onto.

Reason:

Let x be any arbitrary element of G/N.

$\therefore$ There exists $a \in G$ such that $x = Na$

There exists $a \in G$ such that $x = \phi(a)$

$\therefore \phi$ is onto.

Defn:

If $\phi : (G, *) \to (\bar{G}, \circ)$ is a homomorphism the kernel of ϕ denoted by K_ϕ is defined by $K_\phi = \{ x \in G / \phi(x) = \bar{e}$ where $\bar{e}$ is the identity element of $\bar{G} \}$.

Note:-

1) $K_\phi \subseteq G$.

2) $e \in K_\phi$ (Reason is given in the following lemma)

Hence K_ϕ is non-empty.

Lemma: 2.7.2

If ϕ is a homomorphism of $(G, *)$ into $(\bar{G}, \circ)$ the 1) $\phi(e) = \bar{e}$, the unit element of $\bar{G}$

2) $\phi(x^{-1}) = [\phi(x)]^{-1} \ \forall \ x \in G$.

Proof:

1) Let $x \in G$

$\therefore \phi(x) \in \bar{G}$

Since $\bar{e}$ is the unit element of $\bar{G}$,

$$\phi(x) \cdot \bar{e} = \phi(x)$$
$$= \phi(x * e)$$
$$= \phi(x) \cdot \phi(e) \quad (\text{since } \phi \text{ is a homomorphism})$$

$\Rightarrow \phi(x) \cdot \bar{e} = \phi(x) \cdot \phi(e)$

$\Rightarrow \bar{e} = \phi(e)$ (by left cancellation law)

2) By (1), $\bar{e} = \phi(e)$

$$= \phi(x * x^{-1})$$
$$= \phi(x) \cdot \phi(x^{-1}) \quad (\because \phi \text{ is a homomorphism})$$

Premultiplying both sides by $[\phi(x)]^{-1}$

$$[\phi(x)]^{-1} \cdot \bar{e} = \{[\phi(x)]^{-1} \cdot \phi(x)\} \cdot \phi(x^{-1})$$
$$[\phi(x)]^{-1} = \bar{e} \cdot \phi(x^{-1})$$
$$[\phi(x)]^{-1} = \phi(x^{-1})$$

ie) $\phi(x^{-1}) = [\phi(x)]^{-1}$

Hence the result.

Note:-

$K_\phi = \{x \in G \mid \phi(x) = \bar{e}\}$.

W.K.T

$e \in G$ and $\phi(e) = \bar{e}$

$\therefore e \in K_\phi$

$\therefore K_\phi$ is non-empty

Lemma: 2.7.3

If ϕ is a homomorphism of $(G, *)$ into $(\bar{G}, \cdot)$ with kernel K, then K is a normal subgroup

Proof:-

$K = \{x \in G \mid \phi(x) = \bar{e}\}$.

1) W.K.T $e \in G$ and $\phi(e) = \bar{e}$

$\therefore K \neq \{\}$

ii) K is closed under $*$

Let $x, y \in K$

$\therefore \phi(x) = \bar{e}, \phi(y) = \bar{e}$

Since $x, y \in G$, $x * y \in G$

$\phi(x * y) = \phi(x) \cdot \phi(y)$ (since ϕ is a homomorphism)

$= \bar{e} \cdot \bar{e}$

$= \bar{e}$

Hence $x * y \in K$

$\therefore$ K is closed under ~~multiplication~~ $*$

iii) Inverse property

Let $x \in K$

Then $\phi(x) = \bar{e}$

$\phi(x^{-1}) = [\phi(x)]^{-1}$ (By previous lemma)

$= (\bar{e})^{-1}$

$= \bar{e}$

$\therefore x^{-1} \in K$

Hence K satisfies inverse property

From (i), (ii), (iii), K is a subgroup of G.

iv) K is normal

Let $k \in K$, $g \in G$.

$k \in K \subseteq G$, $g \in G$

$\therefore gkg^{-1} \in G$

$\phi(gkg^{-1}) = \phi(g) \cdot \phi(k) \cdot \phi(g^{-1})$ ($\because \phi$ is a homomorphism)

$= \phi(g)\, \bar{e}\, [\phi(g)]^{-1}$ ($\because k \in K$)

$= \phi(g) [\phi(g)]^{-1}$

$= \bar{e}$

$\therefore gkg^{-1} \in K$

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

Lemma: 2.7.4

If ϕ is a homomorphism of G onto $\bar{G}$ with Kernel K, then the set of all inverse images of $\bar{g} \in \bar{G}$ under ϕ in G is given by Kx where x is any particular inverse image of $\bar{g}$ in G.

ie) T.P.T if $\bar{g} \in \bar{G}$ and $\phi(x) = \bar{g}$ [ie x is one inverse image of $\bar{g}$], then Kx = the set of all inverse images of $\bar{g}$ (ie) $\phi(Kx) = \{\bar{g}\}$ or $Kx = \phi^{-1}\{\bar{g}\}$

Proof:-

Let $k \in K$.

$\therefore \phi(k) = \bar{e}$

Let $\bar{g} \in \bar{G}$.

Since ϕ is onto, $\bar{g} \in \bar{G}$ has atleast one pre-image call it as x.

$\therefore \phi(x) = \bar{g}$.

i) Every element of Kx is mapped to $\bar{g}$.

Let kx be any arbitrary element of Kx.

$\phi(kx) = \phi(k) \cdot \phi(x)$ ($\because \phi$ is a homomorphism)

$= \bar{e} \cdot \bar{g} = \bar{g}$

Hence every element of Kx is mapped to $\bar{g}$.

ii) Every element mapped to $\bar{g}$ is a member of Kx.

Let $z \in G$ which is mapped to $\bar{g}$ [ie $\phi(z) = \bar{g}$ $\phi(z) = \phi(x)$ $\because \bar{g} = \phi(x)$]

Subclaim

$zx^{-1} \in K$ ie to prove that $\phi(zx^{-1}) = \bar{e}$

Now, $\phi(zx^{-1}) = \phi(z)\,\phi(x^{-1})$ ($\because \phi$ is homomorphism)

$= \phi(z)[\phi(x)]^{-1}$

$= \phi(z) \cdot [\phi(z)]^{-1}$

$= \bar{e}$

$\therefore zx^{-1} \in K$

$\phi^{-1}\{\bar{g}\} \subseteq Kx \cdot z \in Kx$

$\therefore$ An element mapped to $\bar{g}$ is a member of Kx.

From i) & ii) $Kx = \phi^{-1}(\{g\})$

Hence proved.

Converse is trivially true.

If homomorphism ϕ from G into $\bar{G}$ is 1-1, then $K = \{e\}$

Reason { Already e is mapped to $\bar{e}$
If an element a different from e is taken to $\bar{e}$, then ϕ will not be 1-1

$\therefore$ A homomorphism $\phi: G \to \bar{G}$ is 1-1 $\iff K = \{e\}$.

Isomorphic groups:-

Two groups G, G^* are said to be isomorphic if there exists as 1-1, onto homomorphism from G onto G^*.

we write $G \cong G^*$

Isomorphism:-

A homomorphism ϕ: G into $\bar{G}$ is said to be an isomorphism if ϕ is 1-1.

Note:!

$G \cong G^*$ if there exists an isomorphism from G onto G^*

Note:&

The relation isomorphic is an equivalence relation refer to UG book page 3.3=

Remark:

Lemma 2.7.1 says

G is a group, N is a normal subgroup of G.

Then there exists onto homomorphism $\phi: G \to G/N$
This G/N is called the homomorphic image of G.

By fundamental thm of homomorphism, $\bar{G} \cong G/K$ where K is the kernel of G which is also a normal subgroup of G. For different K, we get different G/K.

ie) There exists a 1-1 correspondence between the set of all normal subgroups of G and the set of all homomorphic images of G.

If G is finite, |set of all normal subgroups|
= |set of all homomorphic images|

$\because$ G is finite, we can talk about cardinality of these sets which are also finite.

Defn:-
A group is said to be simple if it has no non-trivial homomorphic images (ie) if it has no non-trivial normal subgroups.
ie) A group is said to be simple if it has only trivial normal subgroups.

Lemma: 2.7.5
Let ϕ be a homomorphism of G onto $\bar{G}$. Let K be the kernel of ϕ. For any $\bar{H}$, a subgroup of $\bar{G}$, define H by $H = \{x \in G / \phi(x) \in \bar{H}\}$
Then i) H is a subgroup of G (ii) $H \supseteq K$.
iii) $\bar{H}$ is normal in $\bar{G} \Rightarrow$ then H is normal in G.
Moreover, this association sets up a one-to-one mapping from the set of all subgroups of G onto the set of all subgroups of G which contain K.

Proof:-

$\phi : G \to \bar{G}$ is an onto homomorphism.

K = Kernel of ϕ

Let $\bar{H}$ be a subgroup of $\bar{G}$.

i) W.K.T $e \in G$ and $\bar{e} \in \bar{H}$ (∵ H is a subgroup)

$\therefore e \in G$ and $\phi(e) \in \bar{H}$ (∵ $\phi(e) = \bar{e}$)

Hence $e \in H$

$\therefore H \neq \phi$

Let $x, y \in H$.

$\therefore x, y \in G$ and $\phi(x), \phi(y) \in \bar{H}$

$\Rightarrow xy \in G$ and $\phi(x)\phi(y) \in \bar{H}$ (∵ $\bar{H}$ is a subgroup)

$\Rightarrow xy \in G$ and $\phi(xy) \in \bar{H}$ (∵ ϕ is a homomorphism)

$\Rightarrow xy \in H$.

$\therefore H$ is closed.

Let $x \in H \Rightarrow x \in G$ and $\phi(x) \in \bar{H}$

$\Rightarrow x^{-1} \in G$ and $[\phi(x)]^{-1} \in \bar{H}$ (∵ H is a subgroup)

$\Rightarrow x^{-1} \in G$ and $\phi(x^{-1}) \in \bar{H}$ (∵ ϕ is a homomorphism)

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

Hence H satisfies inverse axiom

$\therefore H$ is a subgroup of G.

Proof of iii)

Let $\bar{H}$ be normal.

Claim: H is a normal subgroup of G.

Let $g \in G$ and $h \in H$.

$\therefore \phi(g) \in \bar{G}$ and $\phi(h) \in \bar{H}$

Since $\bar{H}$ is normal in $\bar{G}$, $\phi(g)\phi(h)[\phi(g)]^{-1} \in \bar{H}$

$\therefore \phi(g)\phi(h)\phi(g^{-1}) \in \bar{H}$ (ie) $\phi(ghg^{-1}) \in \bar{H}$ (∵ ϕ is a homomorphism)

Also $ghg^{-1} \in G$.

$ghg^{-1} \in H$ This is true $\forall\, g \in G$ and $h \in H$

$\therefore H$ is normal in G.

Proof of (iii)

$x \in K \Rightarrow x \in G$ and $\phi(x) = \bar{e}$

$\Rightarrow x \in G$ and $\phi(x) = \bar{e} \in \bar{H}$ ($\because \bar{H}$ is a subgroup)

$\Rightarrow x \in H$.

$\therefore K \subseteq H$.

Proof of (iv)

Let L be a subgroup of G and $L \supseteq K$.

Define $\bar{L}$ = The set of all images of elements of L

$= \{\phi(l) \in \bar{G} \mid l \in L\}$

$= \{\bar{x} \in \bar{G} \mid \bar{x} = \phi(l),\ l \in L\}$

claim $\bar{L}$ is a subgroup of $\bar{G}$.

Let $\bar{x}, \bar{y} \in \bar{L}$

$\bar{x} = \phi(l_1)$ and $\bar{y} = \phi(l_2)$ for some $l_1, l_2 \in L$

$\bar{x}\bar{y} = \phi(l_1)\phi(l_2) = \phi(l_1 l_2)$ ($\because \phi$ is a homomorphism)

$\in \bar{L}$ ($l_1, l_2 \in L$, L being a subgroup)

Let $\bar{x} \in \bar{L}$. $\therefore \bar{x} = \phi(l)$ for some $l \in L$.

$\bar{x}^{-1} = [\phi(l)]^{-1} = \phi(l^{-1})$ [$\because \phi$ is a homomorphism]

$\in \bar{L}$ ($\because l^{-1} \in L$, L being a subgroup)

$\therefore \bar{x}^{-1} \in \bar{L}$

Hence $\bar{L}$ is a subgroup of $\bar{G}$

Let $T = \{x \in G \mid \phi(x) \in \bar{L}\} = \phi^{-1}(\bar{L})$

claim $L = T$

Let $l \in L$

Since $L \subseteq G$, $l \in G$ and $\phi(l) \in \bar{L}$

$\Rightarrow l \in T$ (by defn of T)

$\therefore L \subseteq T$ ——— (1)

Let $x \in T$, $\therefore \phi(x) \in \bar{L}$

~~What are the elements present in $\bar{L}$?~~ any only the images of elements of)

$\therefore \phi(x) = \phi(l)$ for some $l \in L$.

$\Rightarrow \phi(x)[\phi(l)]^{-1} = \phi(l)[\phi(l)]^{-1}$

$\Rightarrow \phi(x)[\phi(l)]^{-1} \in \bar{e}$

$\Rightarrow \phi(x)\,\phi(l^{-1}) = \bar{e}$ ($\because \phi$ is a homomorphism)

$\Rightarrow \phi(xl^{-1}) = \bar{e}$ ($\because \phi$ is a homomorphism)

$\Rightarrow xl^{-1} \in K \Rightarrow xl^{-1} \in K \subseteq L \Rightarrow xl^{-1} \in L$

$\Rightarrow x \in Ll$

($xl^{-1} \in L \Rightarrow xl^{-1} = l_1$ for some $l_1 \in L$

$\Rightarrow xl^{-1}l = l_1 l \Rightarrow xe = l_1 l$

$\Rightarrow x = l_1 l \Rightarrow x \in Ll$)

$\Rightarrow x \in L$ ($\because l \in L$)

[$a \in H \Rightarrow H = Ha$ Assume $a \in H$. T.P.T $H \subseteq Ha$.

pf $k \in H \Rightarrow k = (ka^{-1})a \in Ha$ ($\because k \in H, a \in H \Rightarrow ka^{-1} \in H$)

$k \in Ha \Rightarrow k = ha \in H$ ($\because h \in H$ & $a \in H$)]

$\therefore x \in T \Rightarrow x \in L$

Hence $T \subseteq L \rightarrow (2)$

From (1) & (2), $T = L$.

There exists a 1-1 correspondence from the set of all subgroups of $\bar{G}$ onto the set of all subgroups of G which contains K.

Hence proved.

Second isomorphism thm (Correspondence thm)

Thm: 2.7.6

Let ϕ be a homomorphism of G onto $\bar{G}$ with kernel K and let $\bar{N}$ be a normal subgroup of $\bar{G}$. Let $N = \{x \in G \mid \phi(x) \in \bar{N}\}$. Then $G/N \cong \bar{G}/\bar{N}$. Equivalently, $G/N = \frac{G/K}{N/K}$

Proof:-

We have already proved.

$\bar{N}$ is a normal subgroup of $\bar{G} \Rightarrow N$ is a normal subgroup of G and $N \supseteq K$.

(Write proof) (pages 21 & 22 in this notes) (proof of (i), (ii), (iii))

$\therefore G/N$ is a group.

Define a map $\psi: G \to \bar{G}/\bar{N}$ by $\psi(g) = \bar{N}(g)$ $\forall\ g \in G$.

To prove that $\psi: G \to \bar{G}/\bar{N}$ is onto.

Let $\bar{N}\bar{g} \in \bar{G}/\bar{N}$. Here $\bar{g} \in \bar{G}$

Since $\phi: G \to \bar{G}$ is an onto map & since $\bar{g} \in \bar{G}$, there exists $g \in G$ such that $\phi(g) = \bar{g}$

$\therefore \psi(g) = \bar{N}\phi(g)$ (by defn of ψ)

$= \bar{N}\bar{g}$.

$\therefore$ For any element $\bar{N}\bar{g}$ in $\bar{G}/\bar{N}$, there exists $g \in G$ such that $\psi(g) = \bar{N}\bar{g}$

$\therefore \psi$ is an onto map.

To prove that:

$\psi: G \to \bar{G}/\bar{N}$ is a homomorphism

Let $g_1, g_2 \in G$.

$\psi(g_1 g_2) = \bar{N}\phi(g_1 g_2) = \bar{N}\phi(g_1)\cdot\phi(g_2)$ ($\because \phi$ is a homomorphism)

$= [\bar{N}\phi(g_1)][\bar{N}\phi(g_2)]$

[$Hab = Ha \cdot Hb$ if H is a normal subgroup

Here $\bar{N}$ is a normal subgroup]

$= \psi(g_1)\cdot\psi(g_2)$

$\therefore \psi(g_1 g_2) = \psi(g_1)\cdot\psi(g_2)\ \forall\ g_1, g_2 \in G$.

ψ is a homomorphism

Find the Kernel of ψ.

Let Kernel of $\psi = T$.

claim: $T = N$

$t \in T \Rightarrow \psi(t) =$ identity element of $(\bar{G}/\bar{N}) \Rightarrow \psi(t) = \bar{N}\bar{e}$

$\Rightarrow \bar{N}\phi(t) = \bar{N}$ (by defn of ψ).

$\Rightarrow \phi(t) \in \bar{N}$ (N is a subgroup $Na = N \Rightarrow a \in N$ pf $a = ea \in Na = N \Rightarrow a \in N$)

$\Rightarrow t \in N$ (by defn of $\bar{N}$)

$\Rightarrow T \subseteq N \to (1)$

$t \in N \Rightarrow \phi(t) \in \bar{N}$ (by defn of $\bar{N}$)

$\Rightarrow \bar{N}\phi(t) = \bar{N}$ (If N is any group $Na = N \Leftrightarrow a \in N$)

$\Rightarrow \psi(t) = \overline{N} \Rightarrow \psi(t) = \overline{N}\,\overline{e} \Rightarrow \psi(t) =$ identity element of $G/\overline{N}$.

$\Rightarrow t \in$ Kernel of ψ

$\Rightarrow t \in T \quad \because t \in N \Rightarrow t \in T$

$\therefore N \subseteq T \longrightarrow (2)$

From (1) & (2), $N = T$

So, we have proved that $\psi: G \to \overline{G}/\overline{N}$ is an onto homomorphism with kernel N.

By the fundamental thm of homomorphism, we get $G/N \cong \overline{G}/\overline{N}$ [Recall: $G/$kernel of $\psi \cong$ co-domain]

Note: If $\phi: G \to \overline{G}$ is an onto homomorphism with kernel K then $G/K \cong \overline{G}$.

Here $\psi: G \to \overline{G}/\overline{N}$ is an onto homomorphism with kernel K then $G/N \cong \overline{G}/\overline{N}$.

The homomorphism $\phi: G$ onto $\overline{G}$, when elements of N only are considered, induces a homomorphism of N onto $\overline{N}$ with kernel K since N contains K.

ie) Restricted fn $\phi_N: N \to \overline{N}$ is an onto homomorphism with kernel K.

By fundamental thm of homomorphism,

$N/K \cong \overline{N}$ ie) $\overline{N} \cong N/K$.

Now, $G/N \cong \overline{G}/\overline{N}$ & $\overline{G} \cong G/K$, $\overline{N} \cong N/K$ $\Rightarrow G/N \cong (G/K)/(N/K)$

Cauchy's theorem for abelian groups (Application)

Suppose G is a finite abelian group and $p \mid o(G)$ where p is a prime number. Then there exists an element $a \neq e$ in $G \Rightarrow a^p = e$.

Proof:-

Let us prove this thm by induction on $o(G)$

Step: I

Suppose $o(G)=1$

$\therefore G = \{e\}$

There is no prime p dividing 1.

Hence there is no prime p $p \mid o(G)$.

$\therefore$ when hypothesis is not satisfied, we need not prove the result. There is nothing to prove.

$\therefore$ Result is vacuously true in this case.

Step: II

Assume that the statement is true for all those abelian groups K of orders less than $o(G)$ with $p \mid o(K)$ where p is a prime number.

Step: III

Let us prove the statement for finite abelian group satisfying $p \mid o(G)$ where p is a prime number.

case (i) Let G have no proper subgroups.

Then G must be a cyclic group of prime order (ie) G is a cyclic group and $o(G)$ is prime.

$p \mid o(G)$ and $o(G)$ is prime $\Rightarrow p = o(G)$

(Reason: A prime number cannot divide another prime number)

$\therefore G$ has certainly $p-1$ elements other than e.

We need to find one $a \neq e$ in G satisfying

$a^p = e$

Here each of the $p-1$ elements other than e satisfies our requirement

Let $a \neq e$ be in G. Then $a^p = a^{o(G)} = e$.

case (ii) Let G have a proper subgroup. call it as N.

$\therefore o(N) < o(G)$.

Subcase A:
Let $p \mid o(N)$
Since G is abelian, N is also abelian (Note: subgroup of any abelian group is abelian)
Hence $o(N) < o(G)$ & $p \mid o(N)$
Induction hypothesis can be applied for N in the place of K in step II.

By induction hypothesis there exists an element $b \neq e$ in N such that $b^p = e$.

Since $N \leq G$, this $b \in G$.
There exists an element $b \neq e$ in G such that $b^p = e$.
Theorem is proved in this case

Subcase B
Let $p \nmid o(N)$.
Since G is abelian, N is a normal subgroup of G (by pblm 7)
$\therefore G/N$ is an abelian group (by pblm 10 gvn later)
$o(G/N) = \frac{o(G)}{o(N)}$ (by a note grn in 9th page of this material)
$< o(G)$ ($\because o(N) > 1$ as N is a proper subgroup)
Given that $p \mid o(G)$ (i.e) $p \mid \left[\frac{o(G)}{o(N)} \cdot o(N)\right]$
$\Rightarrow p \mid \left[\frac{o(G)}{o(N)}\right]$ [By thm in number theory
If p is prime, $p \mid ab$ & $p \nmid a$
$\Rightarrow p \mid b$]
(since $p \nmid o(N)$)
We have found out an abelian group G/N with $o(G/N) < 1$ and $p \mid o(G/N)$.
Induction hypothesis can be applied for G/N in the place of G/N in step II.

~~By induction hypothesis can be applied~~

~~for G/N in~~

By induction hypothesis, there exists an element $Nb\ (\neq Ne)$ in G/N $\ni : (Nb)^p = N$.

ie) There exists $b \notin N \ni : b^{p} = e$ where $c = b^{o(N)}$

Claim $c \in G$.

$b \in G \Rightarrow b^{o(N)} \in G \Rightarrow c \in G$.

Claim $c \neq e$

Assume the contrary that $c = e$ (ie) $b^{o(N)} = e$.

$\therefore N[b^{o(N)}] = Ne$ ie) $N[b^{o(N)}] = N$

$\Rightarrow (Nb)^{o(N)} = Ne$ ($\because N$ is normal)

$\therefore (Nb)^p = N$ and $(Nb)^{o(N)} = N$.

$[N(b^2) = N(b \cdot b) = Nb \cdot Nb$ as $N(ab) = Na \cdot Nb$ By defn of $\cdot$ on the elements of $G/N]$

Also p does not divide $o(N)$

Moreover, p is prime,

Combining these 4, we get $Ne = N$

$\therefore b \in N$ [by Thm 3.29(i)]

which is a contradiction to the fact that $b \notin N$

$\therefore c \neq e$.

Hence there exist $c (\neq e)$ in $G \ni : c^p = e$

Hence the result.

Pblm: 10 If G is abelian and N is a normal subgroup of G then G/N is abelian.

proof:-

Let Na, Nb be any two arbitrary elements of G/N.

$Na \cdot Nb = N(a \cdot N)b = N(Na)b = NN(ab) = Nab$

$= Nba$ (∵ G1 is abelian)

$= NN(ba) = N(bN)a = Nb \cdot Na$

∴ G1/N is abelian.

Application: 2 Sylow's thm for abelian groups

If G1 is an abelian group of order $o(G_1)$ and if p is a prime number such that $p^\alpha \mid o(G_1)$, $p^{\alpha+1} \nmid o(G_1)$, then G1 has a subgroup of order p^α.

Proof:-

If $\alpha = 0$, the hypotheses are $p^0 \mid o(G_1)$, $p^1 \nmid o(G_1)$

Anyway, G1 has a subgroup $\{e\}$ of order $p^0 = 1$

Let $\alpha \neq 0$. Assume the hypotheses of the theorem.

$p^\alpha \mid o(G_1) \Rightarrow p \mid o(G_1)$

Since G1 is finite abelian and $p \mid o(G_1)$, by cauchy's thm for abelian groups, ∃ an element $a (\neq e)$ in G1 ∋ $a^p = e$.

Define $S = \{x \in G_1 \mid x^{p^n} = e$ for some integer $n\}$

note that $e \in S$

This $a (\neq e)$ in G1 belongs to S since $a^p = e \Rightarrow a^{p^1} = e$

$\therefore S \neq \{e\}$ (Note that $a, e \in S$)

Claim S is a subgroup of G

Since G is finite, it is enough if we prove only the closure axiom for S.

(By thm 3.18 in UG1 book finite, non-empty, closure ⇒ subgroup)

Let $x, y \in S$

$x^{p^n} = e$, $y^{p^m} = e$ for some integers m, n

$(xy)^{p^{m+n}} = x^{p^{m+n}} \cdot y^{p^{m+n}}$ ($\because$ G is abelian)

[Note: $(ab)^n = a^n b^n$]

$= x^{p^m \cdot p^n} \cdot y^{p^m \cdot p^n}$

$= (x^{p^m})^{p^n} (y^{p^m})^{p^n}$

$= e^{p^n} \cdot e^{p^n}$

$= e \cdot e$

$\therefore (xy)^{p^{m+n}} = e \Rightarrow xy \in S$

S is finite, non-empty satisfying closure axiom,

S is a subgroup [S is finite Reason G has order o(S) & hence finite]

Any number is either 1 or product of prime powers

$\therefore o(S) = 1$ or product of prime powers

Claim $o(S) = p^\beta$ where $0 \le \beta \le \alpha$.

Let some prime q different from p divide o(S), G is finite abelian $\Rightarrow$ S is finite abelian

Since S is finite abelian and $q \mid o(S)$

By cauchy's theorem for finite abelian groups,

$\exists$ an element $c \in S \ni : c \neq e$ and $c^q = e$

Since $c \in S$, $e^{p^n} = e$ for some integer n

Since p and q are primes and since $q \neq p$,

g.c.d of p^n and q is 1 (ie) $(p^n, q) = 1$

$\therefore \exists$ integers $\lambda, \mu \ni : \lambda q + \mu p^n = 1$

$c = c^1 = c^{\lambda q + \mu p^n} = e^{\lambda q} \cdot c^{\mu p^n} = (c^q)^\lambda (c^{p^n})^\mu$

$= e^\lambda e^\mu = e$

$\therefore c = e$.

Which is a contradiction to the fact that $c \neq e$

∴ The only prime factor of the number $o(s)$ is p.

$\therefore o(s) = p^\beta$ where $0 \le \beta$

By Lagranges thm, since s is a subgroup of G, $o(s) \mid o(G)$

ie) $p^\beta \mid o(G)$

From hypothesis, the highest power of p dividing $o(G)$ is α

$\therefore$ Here $\beta \le \alpha$

$\therefore o(s) = p^\beta$ where $0 \le \beta \le \alpha$

Claim $\beta \neq 0$

If $\beta = 0$, $o(s) = p^0 = 1 \Rightarrow s$ has only one element which is a contradiction to the fact that $s \neq \{e\}$ $\therefore 1 \le \beta \le \alpha$.

claim $\beta = \alpha$.

Assume the contrary that $\beta < \alpha$

consider G/s.

We know that $o(G/s) = \frac{o(G)}{o(s)}$

Since $p^\alpha \mid o(G)$ & $p^\beta = o(s)$, $o(G) = ip^\alpha$

& $\phi(s) = p^\beta$.

$\frac{o(G)}{o(s)} = ip^{\alpha-\beta}$ where $\alpha - \beta > 0$ (ie) $\alpha - \beta \ge 1$

$\therefore p \mid (ip^{\alpha-\beta})$

$\therefore p \mid \frac{o(G)}{o(s)}$

$\therefore p \mid o(G/s)$

Since G is finite abelian, G/s is also finite abelian.

Hence by cauchy theorem for abelian groups, $\exists$ an element $sx \in G/s$ $\ni$ $sx \neq$ identity element of G/s

$(sx)^p = s$

Since S is normal,

$(Sx)^p = Sx^p$

i.e) $S = Sx^p$

$Sx^{p^1} = S \Rightarrow x^{p^1} \in S$ [By Thm 3.29 (i)]

$\Rightarrow (x^{p^1})^{o(S)} = e$

$\Rightarrow (x^{p^1})^{p^\beta} = e$ [$\because o(S) = p^\beta$]

$\Rightarrow x^{p^1 \cdot p^\beta} = e \Rightarrow x^{p^{(1+\beta)}} = e \Rightarrow x \in S$ (by defn of S)

$\Rightarrow Sx = S$

$\Rightarrow Sx =$ identity element of G/S

which is a contradiction to the fact that $Sx \neq$ identity of G/S.

$\therefore \beta < \alpha$ is wrong

$\therefore \beta = \alpha$

Hence $o(S) = p^\beta \Rightarrow o(S) = p^\alpha$

S is the required subgroup of G of order p^α.

Corollary:

If G is abelian of order $o(G)$ and $p^\alpha | o(G)$, $p^{\alpha+1} \nmid o(G)$, then there is a unique subgroup of G of order p^α.

proof:-

Suppose there are two distinct subgroups T, S of same order p^α.

$\therefore T \neq S$, $o(T) = o(S) = p^\alpha$.

Since G is abelian, $ST = TS$.

$\therefore ST$ is a subgroup of G (by lemma 2.5.1)

$$o(ST) = \frac{p^\alpha \cdot p^\alpha}{o(S \cap T)} = \frac{p^\alpha \cdot p^\alpha}{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}}$$

$$o(ST) = p^\alpha$$

$$O(ST) = \frac{O(S)\,O(T)}{O(S\cap T)} = \frac{p^\alpha p^\alpha}{O(S\cap T)} > p^\alpha \cdot 1$$

$$O(ST) > p^\alpha$$

$S \neq T$, c

$\Rightarrow (S = T)^c$

$\Rightarrow (S \subseteq T \text{ and } T \subseteq S)^c$

$\Rightarrow S \supset T$ or $T \supset S$

$\Rightarrow S\cap T = T \subset S$ or $S\cap T = S \subset T$

$\Rightarrow S\cap T \subset S$ or $S\cap T \subset T$.

$\Rightarrow O(S\cap T) < O(S) = p^\alpha$ or $O(S\cap T) < O(T) = p^\alpha$.

$\Rightarrow O(S\cap T) < p^\alpha$ or $O(S\cap T) < p^\alpha \Rightarrow \frac{p^\alpha}{O(S\cap T)} > 1$

ie) $p^\gamma = O(ST) > p^\alpha$

ie) $p^\gamma > p^\alpha$

ie) $\gamma > \alpha$

$\therefore O(ST) = p^\gamma$ where $\gamma > \alpha$.

Since ST is a subgroup of G_1,

By Lagrange's thm, $O(ST) \mid O(G_1)$

ie) $p^\gamma \mid O(G_1)$. the fact that α is the largest power of p which divides $O(G_1)$.

Hence $\exists$ a unique subgroup of order p^α.

Remark:-

The above corollary fails if G_1 is not abelian.

Proof:-

consider $S_3 = \{e, P_1, P_2, P_3, P_4, P_5\}$ where

$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$,

$P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

We can easily prove $H_1=\{e, p_3\}$, $H_2=\{e, p_4\}$, $H_3=\{e, p_5\}$ are subgroups.

$$p_3^{-1}=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}^{-1}=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=p_3$$

$\circ$	e	p_3
e	e	p_3
p_3	p_3	e

$$p_4^{-1}=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}^{-1}=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=p_4$$

$\circ$	e	p_4
e	e	p_4
p_4	p_4	e

$$p_5^{-1}=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}^{-1}=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=p_5$$

$$p_3^2=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=e$$

$$p_4^2=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=e$$

$$p_5^2=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=e$$

$\circ$	e	p_5
e	e	p_5
p_5	p_5	e

S_3 is non-abelian Reason

$$p_2p_4=\begin{pmatrix}1&2&3\end{pmatrix}\begin{pmatrix}1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3\end{pmatrix}$$

$$p_4p_2=\begin{pmatrix}1&2&3\end{pmatrix}\begin{pmatrix}1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3\end{pmatrix}$$

$p_2p_4 \neq p_4p_2$.

Put $p=2, \alpha=1$ in the Statement of the thm

$p^\alpha = 2^1$ divides $b=O(S_3)$

$p^{\alpha+1}=2^2$ does not divide $b=O(S_3)$

$\left.\begin{array}{l} p^\alpha \mid O(S_3) \\ p^{\alpha+1} \nmid O(S_3) \end{array}\right\}$

S_3 has 3 distinct subgroups of order $p^\alpha=2$.

$\therefore$ The corollary fails for non-abelian group.

(1) Cayley's theorem

Thm: 2.9.1

Every group is isomorphic to a subgroup of $B(S)$ for some appropriate S where $B(S)$ = The set of all bijections from S to S.

Proof:-

Let G be a group.

We will prove this theorem with G in the place of appropriate S.

ie) $G_1 \cong$ a subgroup of $B(G_1)$ where $B(G_1)$ = The set of all bijections from G_1 onto itself.

Let G' = The set of all bijections $t_g : G \to G$ defined by $t_g(x) = xg \ \forall \ x \in G$.

Let us prove $G \cong G'$

I) a) t_g is well-defined

Let x_1, x_2 be any two arbitrary elements of G.

$x_1 = x_2 \Rightarrow x_1 g = x_2 g \Rightarrow t_g(x_1) = t_g(x_2)$

b) t_g is 1-1

Let x_1, x_2 be any two arbitrary elements of G.

$t_g(x_1) = t_g(x_2) \Rightarrow x_1 g = x_2 g \Rightarrow x_1 = x_2$ [By right cancellation]

c) $t_g : G \to G$ is onto

$b \in G$, then $\exists\ bg^{-1} \in G \ni : t_g(bg^{-1}) = (bg^{-1})g = be = b$

II) $(B(G), \circ)$ is a group

III) $G' \subseteq B(G)$

IV) $(G', \circ)$ is a group. Hence $(G', \circ)$ is a subgroup of $(B(G), \circ)$

a) Let $t_{g_1}, t_{g_2} \in G'$

To prove that $t_{g_1} \circ t_{g_2} \in G'$

Clearly $t_{g_1} \circ t_{g_2}$ is a bijection from G to G

$(t_{g_1} \circ t_{g_2})x = t_{g_2}(t_{g_1}(x)) = t_{g_2}(xg_1) = (xg_1)g_2$

$= x(g_1 g_2) = t_{g_1 g_2}(x)$

This is true $\forall\ x \in G$.

$\therefore t_{g_1} \circ t_{g_2} = t_{g_1 \cdot g_2} \in G'$ (Since $g_1, g_2 \in G$)

b(ii) Associativity is true on the elements of $B(G)$. Hence associativity is true on the elements of its ~~subgroups~~ subset G_1.

c) $\exists\ t_e \in G_1' \ni : t_e \circ t_g = t_e = t_g \circ t_e$.

pf $(t_e \circ t_g)x = t_g(t_e(x)) = t_g(xe) = t_g(x)$

$(t_g \circ t_e)x = t_e(t_g(x)) = t_e(xg) = xge = xg = t_g(x)$

$\therefore t_e \circ t_g = t_g = t_g \circ t_e$

d) If $g \in G_1$, then $g^{-1} \in G_1'$.

If $t_g \in G_1'$, then $\exists\ t_{g^{-1}} \in G_1'$ such that

$(t_g \circ t_{g^{-1}})x = t_{g^{-1}}(t_g(x)) = t_{g^{-1}}(xg) = (xg)g^{-1} = x(gg^{-1})$

$= xe = t_e(x)$.

$(t_{g^{-1}} \circ t_g)x = t_g(t_{g^{-1}}(x)) = t_g(xg^{-1}) = (xg^{-1})g = x(g^{-1}g)$

$= xe = t_e(x)$

$\therefore \exists\ t_{g^{-1}} \in G_1' \ni : t_{g^{-1}} \circ t_g = t_g \circ t_{g^{-1}} = t_e$.

$\therefore (G_1', \circ)$ is a subgroup of $B(G_1)$

Define $\psi : G_1 \to B(G_1)$ by $\psi(g) = t_g \ \forall\ g \in G_1$.

claim: ψ is a homomorphism

Let $g_1, g_2 \in G_1$.

$\psi(g_1 g_2) = t_{g_1 g_2}$; $\psi(g_1)\psi(g_2) = t_{g_1} \circ t_{g_2}$

Let us prove $t_{g_1 g_2} = t_{g_1} \circ t_{g_2}$ so that $\psi(g_1 g_2) = \psi(g_1)\psi(g_2)$ ——— (*)

To prove (*), we have to prove $t_{g_1 g_2}(x) = (t_{g_1} \circ t_{g_2})(x)$ $\forall\ x \in G$.

L.H.S $= t_{g_1 g_2}(x) = xg_1 g_2$

R.H.S $= (t_{g_1} \circ t_{g_2})(x) = t_{g_2}(t_{g_1}(x)) = t_{g_2}(xg_1) = xg_1 g_2$

L.H.S $\neq$ R.H.S

$\therefore \psi$ is a homomorphism.

claim ψ is 1-1

It is enough to prove that kernel of $\psi = \{e\}$

Let $g \in$ kernel of ψ

$\therefore x(g) =$ identity element of $B(G)$ ie) $t_g = t_e$

$t_g(x) = t_e(x) \quad \forall x \in G$.

$xg = xe \quad \forall x \in G$

$\Rightarrow g = e$

$\therefore \ker \psi = \{e\}$

$\therefore \psi$ is 1-1

claim $\psi: G \to G'$ is onto

Let $t_g \in G'$. $\exists g \in G \ni t_g \in G'$

Hence $\psi: G \to G'$ is onto.

$\therefore G \cong G'$ where G' is a subgroup of $B(G)$

Hence proved.

Thm: 2.9.2

If G is a group, H a subgroup of G, and S is the set of all right cosets of H in G, then there is a homomorphism θ of G into $B(S)$ and the kernel of θ is the largest normal subgroup of G which is contained in H.

Proof:-

$S = \{Hx \mid x \in G\}$

Let $g \in G$. Define $t_g: S \to S$ by $t_g(Hx) = Hxg \quad \forall Hx \in S$.

claim $t_g: S \to S$ is well defined

$Hx = Hy \Rightarrow x \in Hy$

$\Rightarrow x = hy$

$\Rightarrow xg = hyg$

$\Rightarrow xg \in Hyg$

$\Rightarrow Hxg = Hyg$

$\Rightarrow t_g(Hx) = t_g(Hy)$

$\therefore t_g$ is well-defined.

claim: t_g is 1-1

Let $Hx_1, Hx_2 \in S$

$t_g(Hx_1) = t_g(Hx_2)$

$\Rightarrow Hx_1 g = Hx_2 g$

$\Rightarrow x_1 g \in Hx_2 g$

$\Rightarrow x_1 g = hx_2 g, \; h \in H$

$\Rightarrow x_1 = hx_2 \Rightarrow x_1 \in Hx_2 \Rightarrow Hx_1 = Hx_2$

$\therefore t_g$ is 1-1

claim: $t_g : S \to S$ is onto.

Let $Hx \in S$. $\exists \; Hxg^{-1} \ni : t_g(Hxg^{-1}) = (Hxg^{-1})g =$

$Hxe = Hx$

Hence t_g is onto.

$\therefore t_g \in B(S)$

II) $(B(S), o)$ is a group

III) Define $G' =$ The set of bijections $t_g : S \to S$ defined by $t_g(Hx) = Hxg \;\; \forall \; Hx \in S$

$G' \subseteq B(S)$

IV) Define a map $\theta : G \to B(S)$ by $\theta(g) = t_g \;\; \forall \; g \in G$

claim: θ is a homomorphism.

To prove that

$$\theta(g_1 g_2) = \theta(g_1)\theta(g_2)$$

i.e) To prove that

$$t_{g_1 g_2} = t_{g_1} \circ t_{g_2}$$

i.e) To prove that

$$t_{g_1 g_2}(Hx) = (t_{g_1} \circ t_{g_2})(Hx) \;\; \forall \; Hx \in S$$

Now, $(t_{g_1} \circ t_{g_2})(Hx) = t_{g_2}(t_{g_1}(Hx)) = t_{g_2}(Hxg_1)$

$= (Hxg_1g_2) = t_{g_1g_2}(Hx)$.

$\therefore \theta$ is a homomorphism

claim: $\ker\theta = \{b \in G \mid Hgb = Hg \ \forall g \in G\}$

Let $b \in \ker\theta$:

$\therefore \theta(b)$ = identity element of $B(S)$

ie) $t_b = t_e$

ie) $t_b(Hg) = t_e(Hg) \ \forall \ Hg \in S$.

$\Rightarrow Hgb = Hge \ \forall \ Hg \in S \Rightarrow Hgb = Hg \ \forall g \in G$

$\Rightarrow b \in \{b \in G \mid Hgb = Hg \ \forall g \in G\}$

$\therefore \ker\theta \subseteq \{b \in G \mid Hgb = Hg \ \forall g \in G\}$

Now, $b \in \{b \in G \mid Hgb = Hg \ \forall g \in G\}$

$\Rightarrow Hgb = Hg \ \forall g \in G \Rightarrow Hgb = Hge \ \forall Hg \in S$

$\Rightarrow t_b(Hg) = t_e(Hg) \ \forall \ Hg \in S \Rightarrow t_b = t_e \Rightarrow \theta(b) =$ identity element of $B(S)$

$\Rightarrow b \in \ker\theta$.

$\therefore \{b \in G \mid Hgb = Hg \ \forall g \in G\} = \ker\theta$.

claim: $\ker\theta \subseteq H$

$b \in \ker\theta \Rightarrow Hgb = Hg \ \forall g \in G$

$\Rightarrow Heb = He \Rightarrow Hb = H \Rightarrow b \in H$.

$\therefore \ker\theta \subseteq H$.

By thm 3.56 in UG book, kernel of a homomorphism is always a normal subgroup

$\therefore$ Kernel θ is the normal subgroup of G.

To prove that

$\ker\theta$ is the largest normal subgroup $\leq H$.

Let N be any normal subgroup contained in H.

To prove that: $N \subseteq \ker\theta$.

Let $n \in N$. Let $g \in G$

Since N is normal, $gng^{-1} \in N \subseteq H \ \forall\ g \in G$ and $\forall\ n \in N$.

$gng^{-1} \in H \ \forall\ g \in G$

$\Rightarrow gng^{-1} = h$ for some $h \in H$ and $\forall\ g \in G$

$\Rightarrow gn = hg \ \forall\ g \in G$

$\Rightarrow gn \in Hg \ \forall\ g \in G$

$\Rightarrow Hgn = Hg \ \forall\ g \in G$

$\Rightarrow n \in \{b \in G \mid Hgb = Hg \ \forall\ g \in G\}$

$\Rightarrow n \in \ker\theta$

$\therefore N \subseteq \ker\theta$

Hence $\ker\theta$ is the largest normal subgroup of G which is contained in H.

Remark

If H has no normal subgroup of G other than $\{e\}$ in it, then $\ker\theta = \{e\}$

Recall: A homomorphism θ is 1-1 $\Leftrightarrow \ker\theta = \{e\}$

$\therefore \theta$ is 1-1

$\theta : G \to B(S)$ is 1-1 homomorphism

$\theta : G \to \theta(G)$ is 1-1, onto, homomorphism ie) $G \cong \theta(G)$

which is cayley's theorem.

Remark:

Suppose that a finite G has a subgroup H whose $i(H)$ satisfies $\underline{i(H)} < o(G)$

ie) $|B(S)| < O(G)$ where S is the set of all distinct right cosets of H in G.

Then the homomorphism

$\theta : G \to B(S)$ cannot be 1-1

Reason

If $\theta : G \to B(S)$ is a 1-1 and homomorphism, then $\theta : G \to \theta(G)$ is a bijective homomorphism

$\therefore G \cong \theta(G)$

$O(G) = O(\theta(G))$

$|B(S)| < O(G) = O(\theta(G))$ ie) $|B(S)| < |\theta(G)|$ which is not possible since $\theta(G)$ is a subgroup of $B(S)$

Hence homomorphism $\theta : G \to B(S)$ is not 1-1

$\therefore \ker \theta \neq \{e\}$

By thm 2.9.2, $\ker \theta$ is the largest normal subgroup of G contained in H.

$\therefore$ The largest normal subgroup of G contained in H is $\neq \{e\}$

ie) $\{e\}$ is not the largest normal subgroup of G in H.

Hence H has a non-trivial normal subgroup of G.

Hence G has a non-trivial normal subgroup of G.

$\therefore G$ is not simple.

Hence G is not simple when $[i(H)] < O(G)$

Lemma: 2.9.1

If G is a finite group and $H \neq G$ is a subgroup of G such that $O(G) \nmid [i(H)]$ then H must contain a non-trivial normal subgroup of G. In particular, G cannot be simple

Proof:-

Assume G is a finite group; $H \neq G$ is a subgroup of G $\ni$: $O(G) \nmid [G:H]$

Then B(S) can have no subgroup of order O(G)

[Reason if B(S) has a subgroup P with order O(G), by Lagrange's thm, $O(P) \mid O(B(S)) \Rightarrow O(G) \mid O(B(S))$ [$\because O(P) = O(G)$]

$\Rightarrow O(G) \mid [G:H] \Rightarrow \Leftarrow$ to the hypothesis]

Hence B(S) can have no subgroup of order O(G)

Hence B(S) can have no subgroup is isomorphic to G

i.e) No subgroup of $B(S) \cong G$.

But B(S) contains $\theta(G)$ as its subgroup

Hence $\theta(G) \cong G$

Homomorphism $\theta: G \to \theta(G)$ is onto already

$\therefore \theta: G \to \theta(G)$ is not 1-1

$\therefore \ker \theta \neq \{e\}$

W.K.T $\ker \theta$ is the largest normal subgroup of G $\subseteq$ in H.

$\therefore \ker \theta$ is a non-trivial normal subgroup of G $\subseteq$ in H.

$\therefore$ G is not simple.

V.Q 2m

Automorphism:- (1)

An isomorphism of G onto G is called automorphism.

Ex:

The map $f: R^* \to R^*$ defined by $f(a) = a^{-1}$ is an automorphism.

proof :-

Clearly f is a bijection

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

$= b^{-1}a^{-1}$

$= a^{-1}b^{-1}$

$f(a) = f(a) f(b)$

f is an automorphism

Ex:

Let G_1 be a group $a \in G_1$, $\phi \in a$ $\phi_a : G_1 \to G_1$ is defined by $\phi_a(x) = axa^{-1}$ is an automorphism of G_1

proof:-

For $x, y \in G_1$ then $\phi_a(x) = \phi_a(y)$

$axa^{-1} = aya^{-1}$

$x = y$

ϕ_a is $1-1$

Hence $a^{-1}xa$ is the pre-image of x under ϕ_a.

Also $\phi_a(xy) = axya^{-1} = ax^{-1}yx^{-1}$

$= axaa^{-1}ya^{-1}$

$= (axa^{-1})(aya^{-1})$

$\phi_a(xy) = \phi_a(x)\,\phi_a(y)$

ϕ_a is an automorphism and is an inner automorphism.

Inner automorphism:

The automorphism $\phi_a : G \to G$ is defined by $\phi_a(x) = axa^{-1}$ is called an inner automorphism of the group G_1.

The set of all automorphism of G_1 is denoted by $Aut\,g'$ and the set of all inner automorphism of G_1 is denoted by $'I(G)'$

Thm: 1.24 21.8.21

$I(G) \cong G/Z$ where $I(G)$ is the group of inner automorphism of G and Z is the centre of G.

Proof:-

Given G is group, $g \in G$

Define $T_g : G \to G$ by $xT_g = g^{-1}xg \quad \forall x \in G$.

claim 1:

T_g is an automorphism.

Let $x, y \in G$ be arbitrary.

Then, $(xy)T_g = g^{-1}(xy)g = (g^{-1}xg)(g^{-1}yg)$

$= (xT_g)(yT_g)$

T_g is a homomorphism

T_g is 1-1

Suppose $xT_g = yT_g$

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

$g(g^{-1}xg)g^{-1} = g(g^{-1}yg)g^{-1}$

$(gg^{-1})x(gg^{-1}) = (gg^{-1})y(gg^{-1})$

$x = y$

$\therefore T_g$ is 1-1

T_g is onto,

Take any element $z \in G$, $g \in G$

$T_g(gzg^{-1}) = g^{-1}(gzg^{-1})g = (g^{-1}g)z(g^{-1}g)$

$= z$

T_g is onto.

Hence T_g is an automorphism which is called the inner automorphism

Take $I(G) \cong \{T_g \in A(G) / g \in G\}$

claim 2:

$I(G)$ is a subgroup of $A(G)$

Clearly $I(G) \neq 0$

Let $T_g, T_h \in I(G)$, where $g, h \in G$.

Then $x(T_g T_h) = (xT_g)T_h = h^{-1}(xT_g)h$

$= h^{-1}(g^{-1}xg)h$

$= (h^{-1}g^{-1})x(gh)$

$= (gh)^{-1}x(gh)$

(A)

$x(T_g T_h) = xT_{gh}$

$T_g T_h = T_{gh}$

Let $T_g \in I(G_1)$

$\Rightarrow g \in G_1$

$\Rightarrow g^{-1} \in G_1$

$\Rightarrow T_{g^{-1}} \in I(G_1)$

Now, $T_g \cdot T_{g^{-1}} = T_{gg^{-1}} = T_e = I$

$T_{g^{-1}} T_g = T_{g^{-1}g} = T_e = I$.

$T_{g^{-1}}$ is the inverse of T_g.

$T_{g^{-1}} \in x(G_1) \Rightarrow (T_g)^{-1} \in I(G_1)$

Hence $I(G_1)$ is a subgroup of $A(G)$.

Claim:3

To prove $I(G_1) \cong G_1/Z$

Define $\psi : G_1 \to I(G_1)$ by $\psi(g) = T_g$

To prove, $k\psi = Z$.

Z is the centre of G_1

The centre Z of a group G_1 is defined by,

$Z = \{x \in G_1 / zx = xz \ \forall \ x \in G_1\}$

Let $\alpha \in k_\psi$

$\alpha \in G_1$ there exist $\psi(\alpha) = T_\alpha$

$T_\alpha = I$

$xT_\alpha = xI$

$\alpha^{-1}x\alpha = x$

$x\alpha = \alpha x$

$k_\psi \subset Z$ ——— (1)

Let $\alpha \in Z$ be arbitrary

$\Rightarrow \alpha x = x\alpha \ \forall \ x \in G_1$

$\Rightarrow \alpha^{-1}x\alpha = x \ \forall x \in G_1$

$x(T_\alpha) = xI \quad \forall\ x \in G$.

$T_\alpha = I$

(5) $\psi = I$

$\alpha \in K_\psi$

$Z \subseteq K_\psi$ — (2)

From (1) & (2)

$Z = K_\psi$

ψ is a homomorphism

Let $g, h \in G$ be arbitrary

Then $gh \in G \Rightarrow T_{gh} = T_g \cdot T_h = \psi_g \cdot \psi_h \quad \forall\ h, g \in G$.

ψ is onto

Take any element $T_g \in I(G)$

$\because g \in G$,

$\psi_g = T_g$.

$\psi : G \to I(G)$ be an onto homomorphism with kernel Z

$K_\psi = Z$ [By fundamental thm of homomorphism]

$\Rightarrow I(G) \cong G/Z$

Hence proved

U.Q

10m.

Thm: 1.25 (Cayley's thm)

(2) Every group is isomorphic to a subgroup of $A(S)$ for some appropriate S.

proof:-

Let G be a group

To prove that $G \cong A(S)$

put $S = G \Rightarrow G \cong A(G)$

claim 1:

If $g \in G$ define $T_g : G \to G$ by $xT_g = xg$ $\forall\ x \in G$ then $T_g \in A(S)$

sub claim i):

T_g is 1-1

Let $x, y \in G$

$x T_g = y T_g$

$xg = yg$

$x = y$

T_g is $1-1$

(6)

Sub claim ii)

T_g is onto

If $y \in G$ then $y = y(g^{-1}g) = (yg^{-1})g = (yg^{-1})T_g$

T_g maps S onto itself

$T_g \in A(S)$

Sub claim iii)

T_g is a homomorphism

If $g, h \in G$ for $x \in S$

$x T_{gh} = x(gh) = (xg)h = (xg)T_h = (xT_g)T_h$

$x T_{gh} = x T_g T_h$

$T_{gh} = T_g T_h$.

Claim 2:

$G \cong A(S)$

Define $\psi : G \to A(S)$ such that $\psi(g) = T_g \ \forall \ g \in G$.

Subclaim i)

ψ is well defined.

If $g, h \in G$

suppose $g = h$

$T_g = T_h$

$\psi(g) = \psi(h)$

ψ is well defined.

Subclaim ii)

$\psi(g) = \psi(h)$

$T_g = T_h$

$xT_g = xT_h \Rightarrow xg = xh$

$\Rightarrow g = h$.

$\therefore \psi$ is $1-1$

Subclaim iii)

ψ is homomorphism.

Let $g, h \in G$

$\Rightarrow T_g, T_h \in A(S)$

$\psi(gh) = T_{gh} = T_g \cdot T_h = \psi(g)\,\psi(h)$

$\psi(gh) = \psi(g)\,\psi(h)$

ψ is homomorphism.

clearly,

ψ is an isomorphism of G onto $A(S)$.

Thm: 1.26

If G is a group. H is a subgroup of G and S is the set of all right cosets of H in G. Then there is a homomorphism $\theta(G)$ into $A(S)$ and (i.the kernel of θ is the largest normal subgroup of G which is contained in H.

Proof:-

Let G be a group

H is a subgroup of G.

Let S be the set whose elements are the right coset of H in G.

ie) $S = \{Hg / g \in G\}$

Define $f_g : S \to S$ such that $f_g(Hx) = Hxg \;\forall\, Hx \in S$

Claim i)

i) f_g is 1-1

Suppose $f_g(Hx) = f_g(Hy)$

$Hxg = Hyg$ where $Hx, Hy \in S$

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

$(Hx)gg^{-1} = Hy(gg^{-1})$

$Hx = Hy$

$x = y$.

ii) f_g is onto

Take any element $x \in G$

(8)

$Hx \in S$

$Hxg \in S$

$Hxg = f_g(Hx)$

f_g is onto.

iii) f_g is homomorphism

Take $Hx \in S$

$f_g f_h(Hx) = (Hxg)h = f_h(Hxg)$

$= f_h(f_g(Hx))$

$= f_h f_g(Hx)$

$\therefore f_{gh} = f_g f_h$.

Then f_g is 1-1 and onto homomorphism

$f_g \in A(S)$

claim 2:

i) θ is homomorphism ii) $K\theta = K$ iii) $K \subseteq H$.

iv) K is the largest subgroup of G which is contained in H.

for i)

Define $\theta : G \to A(G)$ by $\theta(g) = f_g \ \forall \ g \in G$.

Let $g, h \in G$

Then $\theta(gh) = f_{gh} = f_g \cdot f_h = \theta_g \cdot \theta_h$

θ is homomorphism.

for ii)

Let $K = \{g \in \theta / Hxg = Hx, \ \forall \ x \in G\}$

Let $g \in K\theta$

$\Rightarrow g \in G$ such that $\theta(g) = I$

$\Rightarrow g \in G$ such that $f_g = I$

$\Rightarrow g \in G$ such that $f_g(Hx) = I(Hx)$

$\Rightarrow g \in G$ such that $Hxg = Hx \quad [\because g \in K]$

$\therefore K\theta = K$.

for iii)

$K = K\theta$ (Kernel of θ)

Let $g \in K$

$\Rightarrow y \in G$ such that $Hxy = Hx \quad \forall x \in G$

$\Rightarrow y \in G$ such that $Hey = He \quad \forall e \in G$

(9) $\therefore Hy = H$

$K \leq H$.

K is a normal subgroup of G which is contained in H. [By thm 1.1.9]

for iv)

Let N is a normal subgroup of G contained in H.

claim: $N \leq K$.

Let $\alpha \in N \Rightarrow \alpha^{-1} \in N$

Let $\alpha^{-1} \in N \Rightarrow x \in G$

$\Rightarrow x\alpha^{-1}x^{-1} \in N$

$\Rightarrow x\alpha^{-1}x^{-1} \in N \leq H$.

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

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

$\Rightarrow Hx\alpha^{-1} = Hx \quad \forall x \in G$

$\alpha \in K$

$N \leq K$.

Hence K is the largest subgroup of G which is contained in H.

Defn: permutation

Let A be a finite set. A bijection from A to itself is called a permutation.

Ex:

If $A = \{1, 2, 3, 4\}$, $f: A \to A$ is given by $f(1) = 2$, $f(2) = 1$, $f(3) = 4$, $f(4) = 3$ is a permutation of A.

We can write this permutation

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

Symmetric group:-

Let A be a finite set containing n elements. The set of all permutation of A is clearly group under the composition of functions.

This group is called a symmetric group of degree n and is denoted by S_n.

(6) The order of $S_n = n!$

Ex:-

1) $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ find $\alpha\beta$ and α^{-1}

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

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

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

2) Find the cycle of permutation

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

$$= (1\ 2\ 3\ 7\ 6)(4\ 5)$$

3) S.T $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix}$ where θ consist of elements $(1,2,3,4,5,6)$

The orbit of $1 = (1,2)$
The orbit of $2 = (2,1)$
The orbit of $3 = (3)$
The orbit of $4 = (4,5,6)$
The orbit of $5 = (5,6,4)$
The orbit of $6 = (6,4,5)$

The cycle of θ is $(1\ 2)(3)(4\ 5\ 6)$.

Defn: Disjoint cycle

Two cycles are said to be disjoint if they have no symbols in common.

Transposition:-

A cycle of length two is called a transposition.

Ex:

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

$$= (1\ 3)(1\ 5)(2\ 4).$$

Defn:

Even permutation:-

A permutation $\theta \in S_n$ is said to be an even permutation if it can be represented as a product of an even number of transposition.

Odd permutation:-

A permutation $\theta \in S_n$ is said to be an odd permutation if it can be represented as a product of an odd number of transposition.

Ex:-

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

$$= (1\ 3\ 5)(2\ 4) = (1\ 3)(1\ 5)(2\ 4)$$

no of transposition $= 3$

ϕ is an odd permutation.

Thm: 1.27

Every permutation is a product of its cycle (or) Every permutation is a product of disjoint cycles.

proof:-

Let p be a given permutation of the set $S = \{1, 2, \ldots, n\}$

Let $a_1 \in S$

Let $p(a_1) = a_2$, $p(a_2) = a_3$

Since S is finite

Hence, there exist a positive integer r such that $1 \leq r < n$ and $p(a_r) = a_1$

Let $c = (a_1, a_2 \ldots a_r)$

If $r=n$ then $p=c$

If $r<n$

Let b_1 be the symbol in S such that

$b_1 \notin (a_1, a_2, \ldots, a_r)$

$d = (b_1, b_2, \ldots, b_s)$

clearly the cycles c and d are disjoint

If $r+s=n$

$p = cd$

If $r+s<n$

we repeat the above process to obtain more cycles until all the symbols appears in one of the cycles.

∴ We get a decomposition of P into disjoint cycles.

Thm: 1.28

Every permutation is a product of two cycles (transpositions)

Proof:-

consider the m cycles $(a_1\ a_2 \ldots a_m)$

It can be decomposed into $(a_1\ a_2)(a_1\ a_3)\ldots(a_1\ a_m)$

Since any permutation is the product of disjoint cycles.

Each cycle is a product of transposition.

But the decomposition is not a unique.

∴ m cycle can be written as product of two cycles is more than one way.

for ex:

consider $(1\ 2\ 3)$ we can write this cycle as a product of another two cycles

$(1\ 2)(1\ 3) = (3\ 1)(3\ 2)$

∴ every permutations is product of two cycles

Result:-

The product of two even permutation is an even permutation.

The product of two odd permutation is an even permutation.

The product of an even permutation and an odd permutation is an odd permutation.

The inverse of an even permutation is an even permutation.

The inverse of an odd permutation is an odd permutation.

Defn: Alternating group.

The group A_n of all even permutation is S_n is called the alternating group of n.

Note:-

Let A_n be the set of all even permutation is S_n, then A_n is a group containing $\frac{n!}{2}$ permutations.

Thm: 1.29

S_n has a normal subgroup of index 2 of the alternating group A_n consisting of all even permutation.

Proof:-

Let S_n be the set of all permutation.

Then S_n is a group with respect to permutation multiplication.

Let A_n be the subset of S_n consisting of all even permutations.

Claim 1:

A_n is a subgroup of S_n.

Let $f, g \in A_n$

$\Rightarrow f, g$ are even permutation

$\Rightarrow fg$ is also an even permutation

$\Rightarrow fg \in A_n$

(14)

Let $f \in A_n$

$\Rightarrow f$ is an even permutation.

$\Rightarrow f^{-1}$ is also an even permutation.

$\Rightarrow f^{-1} \in A_n$

Hence A_n is a subgroup of S_n.

Claim 2:-

A_n is a normal subgroup of S_n with index 2.

Let $W = \{1, -1\}$.

Then W is a group with respect to multiplication.

Define $\phi : S_n \to W$ such that,

$$\phi(s_n) = \begin{cases} 1 & \text{if } b \text{ is even} \\ -1 & \text{if } b \text{ is odd.} \end{cases}$$

Then ϕ is a homomorphism of S_n onto W with $K\phi = A_n$

$\Rightarrow A_n$ is a normal subgroup of S_n

$$\frac{S_n}{A_n} \cong W.$$

$$O(W) = 2$$

$$O\left(\frac{S_n}{A_n}\right) = 2$$

$$\frac{O(S_n)}{O(A_n)} = 2 \Rightarrow \frac{n!}{O(A_n)} = 2$$

$$O(A_n) = \frac{n!}{2}.$$

Thm: 1.30 Thm: 2.8.1

If G is a group then $A(G)$ is set of all automorphism of G is also a group.

Proof:-

Given G is a group.

$A(G) = \{T / T : G \to G\}$ is set of all automorphism of G.

(14) To prove that, $A(G_1)$ is a group.

ie) To prove that, $A(G_1)$ is a group with respect to the composition of mapping defined by $x(T_1 T_2) = (xT_1)T_2$ where $x \in G_1$, $T_1, T_2 \in A(G_1)$

i) closure:

Let $T_1, T_2 \in A(G_1)$

Let $x, y \in G_1$.

then $xy(T_1 T_2) = (xy)T_1)T_2 = (xT_1)(yT_1)T_2$

$= (x(T_1 T_2)) \cdot (y(T_1 T_2))$

$T_1, T_2 \in A(G_1) \Rightarrow T_1 T_2 \in A(G_1)$

ii) Associative:

Let $T_1, T_2, T_3 \in A(G_1)$

$x((T_1)(T_2 T_3)) = (xT_1)T_2 T_3 = x(T_1 T_2)T_3$

$T_1(T_2 T_3) = (T_1 T_2)T_3$

iii) Existence of identity:-

Define $I : G_1 \to G_1$, $I(x) = x \ \forall \ x \in G_1$.

Let $T, I \in A(G_1)$ such that,

$x(IT) = (xI)T = xT$

$x(TI) = (xI)T = xT$

$\therefore IT = TI = T$

iv) Existence of Inverse:-

Let $T, T^{-1} \in A(G_1)$

$(xT)T^{-1} = x(TT^{-1}) = xI = x.$

$(xT^{-1})T = x(T^{-1}T) = xI = x.$

$TT^{-1} = T^{-1}T = I$

$A(G_1)$ is a group.

Unit - II

Another counting principle:

U.Q. 2m (3)

Defn: conjugate:

If $a, b \in G_1$ then b is said to be a conjugate of a in G_1. If there exist an element $c \in G_1$ such that $b = c^{-1}ac$.

It can be write $a \sim b$.

U.Q. 2m 15m

Thm:

Conjugancy is an equivalence relation on G_1.

Proof:-

Given G_1 is a group.

To prove, $\sim$ is an equivalence relation

i) Reflexive:

Let $a \in G_1$ be arbitrary.

Then $a = e^{-1}ae$ where e is identity element in G_1 $\Rightarrow a \sim a$.

ii) Symmetric:

Let $a, b \in G_1$ be arbitrary.

Suppose $a \sim b$ then

$b = x^{-1}ax$ for some $x \in G_1$

Hence $a = (x^{-1})^{-1} b x^{-1} = (x^{-1})^{-1}(x^{-1}ax)x^{-1}$

$= ((x^{-1})^{-1} \cdot x^{-1}) a (x x^{-1}) = e^{-1}ae$.

$= a$.

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

Let $y = x^{-1} \Rightarrow a = y^{-1}by$

$\therefore b \sim a$..

hence $a \sim b \Rightarrow b \sim a$.

iii) Transitive:

Let $a, b, c \in G_1$ be arbitrary.

Suppose $a \sim b$ and $b \sim c$.

$b = x^{-1}ax$ and $c = y^{-1}by$

Since $c = y^{-1}by = y^{-1}(x^{-1}ax)y$

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

Take $x = xy$

$c = z^{-1}az$

$\therefore a \sim c$

Hence $a \sim b$ and $b \sim c \Rightarrow a \sim c$.

$\therefore$ conjugancy is an equivalence relation.

Defn: Equivalence class

For $a \in G$. Let $C(a) = \{x \in G / a \sim x\}$ $C(a)$, the equivalence class of a in G under the relation $\sim$ is called the conjugate class of a in G.

Defn: Normalizer

If $a \in G$ then $N(a)$ the normalizer of a in G is the set $N(a) = \{x \in G / xa = ax\}$.

Thm 2.2

$N(a)$ is a subgroup of G.

proof:-

claim: $N(a)$ is a subgroup of G.

subclaim i) $N(a) \neq \phi$, $N(a) \subseteq G$.

ii) $x, y \in N(a) \Rightarrow xy \in N(a)$

iii) $x \in N(a) \Rightarrow x^{-1} \in N(a)$

for i)

clearly $ea = ae = a$

$\Rightarrow e \in N(a)$

$\Rightarrow Na \neq \phi$

Let $x \in N(a)$

$\Rightarrow x \in G$ such that $xa = ax$

$\therefore N(a) \subseteq G$.

For ii)

Let $x, y \in N(a)$

$\Rightarrow x, y \in G$ such that $ax = xa$, $ay = ya$

Let $(xy)a = x(ya) = x(ay) = (xa)y = (ax)y$

$(xy)a = a(xy)$

$\therefore xy \in N(a)$

For iii)

Let $x \in N(a)$

$\Rightarrow x \in G$ such that $ax = xa$.

$x^{-1} \in G$ such that $x^{-1}a = x^{-1}ae$

$= (x^{-1}a)(xx^{-1})$

$= x^{-1}(ax)x^{-1}$

$= x^{-1}(xa)x^{-1}$

$= (x^{-1}x)(ax^{-1})$

$= ax^{-1}$

$x^{-1}a = ax^{-1}$

$x^{-1} \in N(a)$

$\therefore N(a)$ is a subgroup of G.

Remark:-

$O(G) = \Sigma c_a$ where $c_a = O(C(a))$ [The conjugate class of a in G, $C(a)$, consists exactly of all the elements $x^{-1}ax$ as x ranges over G.

c_a measure the number of distinct $x^{-1}ax$'s].

Thm 2.3

If G is a finite group then $c_a = \frac{O(G)}{O(N(a))}$.

In another words the number of elements conjugate to 'a' in G is the index of the normalizer of 'a' in G.

Given G is a finite group and $a \in G$

We have $N(a) = \{x \in G / xa = ax\}$

and $C(a) = \{y \in G / a \sim y\}$

Now, we know that $O(C(a)) = Ca$.

Denote $M = \{N(a)x / x \in G\}$

$= \{$right coset of $N(a)$ in $G\}$

Define $f : M \to C(a)$ such that

$f(N(a)x) = x^{-1}ax \quad \forall \; x \in G$.

To prove f is 1-1 and onto.

i) f is well defined:

$\Rightarrow N(a)x = N(a)y$.

$\Rightarrow N(a)xy^{-1} = N(a)$

$\Rightarrow xy^{-1} \in N(a)$

$\Rightarrow a(xy^{-1}) = (xy^{-1})a$

$\Rightarrow x^{-1}a(xy^{-1})y = x^{-1}(xy^{-1})ay$

$\Rightarrow (x^{-1}ax)(y^{-1}y) = (x^{-1}x)(y^{-1}ay)$

$\Rightarrow (x^{-1}ax)e = e(y^{-1}ay)$

$\Rightarrow f(N(a)x) = f(N(a)y)$.

ii) f is 1-1

$f(N(a)x) = f(N(a)y)$

$\Rightarrow (x^{-1}ax) = (y^{-1}ay)$

$(x^{-1}ax)e = e(y^{-1}ay)$

$\Rightarrow (x^{-1}ax)(y^{-1}y) = (xx^{-1})(y^{-1}ay)$

$\Rightarrow x^{-1}a(xy^{-1})y = x^{-1}(xy^{-1})ay$.

$\Rightarrow a(xy^{-1}) = (xy^{-1})a$

$\Rightarrow xy^{-1} \in N(a)$

$\Rightarrow N(a)xy^{-1} = N(a)$

$\Rightarrow N(a)(x) = N(a)(y)$

For any $x^{-1}ax \in C(a)$

There exist $N(a)$ & $x \in M$ such that $f(N(a)x) = x^{-1}ax$ from that

$$O(C(a)) = O(M)$$

= Number of right coset of $N(a)$ in G

= Index of $N(a)$ in G.

$$= \frac{O(G)}{O(N(a))}$$

$$\therefore C_a = \frac{O(G)}{O(N(a))}$$

Corollary:-

$$O(G) = \sum \frac{O(G)}{O(N(a))}$$ where this sum runs over one element a in each conjugate class.

proof:-

We know that $\bigcup_{a \in G} C(a)$

Now, we take $O(G) = \sum_{a \in G} O(C(a)) = \sum_{a \in G} C_a$.

If G is a finite group then $C_a = \frac{O(G)}{O(N(a))}$

$$\therefore C_a = \frac{O(G)}{O(N(a))}$$

Hence $$O(G) = \sum \frac{O(G)}{O(N(a))}$$

This equation is called conjugate class equation in G.

U.R
gm

Defn: centre

The centre $Z(G)$ of a group G is set of all $a \in G$ such that $ax = xa \ \forall x \in G$

i) $a \in Z$ iff $N(a) = G_1$

ii) If G_1 is finite $a \in Z$ i.f.f $o(N(a)) = o(G_1)$

proof:-

Let $N(a) = \{x \in G_1 / ax = xa\}$

and $Z(a) = \{a \in G_1, ax = xa \text{ for } x \in G_1\}$

Assume that $a \in Z$.

To prove that $N(a) = G_1$.

Since $N(a)$ is a subgroup of G_1.

$\therefore N(a) \leq G_1 \rightarrow (1)$.

By the defn of centre

Take $y \in G_1$, $a \in Z$.

$\Rightarrow ay = ya$

$\Rightarrow y \in N(a)$

$\therefore G_1 \leq N(a) \rightarrow (2)$

From (1) and (2) $G_1 = N(a)$

conversely,

Assume that $N(a) = G_1$

To prove $a \in Z$.

Since $N(a) = G_1$

$\Rightarrow G_1 \leq N(a)$

For any $y \in N(a)$

$\Rightarrow ay = ya \ \forall \ y \in G_1$

$\Rightarrow a \in Z$.

ii) Assume G_1 is finite group

$a \in Z$.

From i) $a \in Z \iff N(a) = G_1$

Since G_1 is a finite group $\iff o(N(a)) = o(G_1)$.

Remark:-

If G is a finite group and z be the centre of G then the class eqn of G can be written as $o(G) = o(z) + \sum_{a \in z} \frac{o(G)}{o(N(G))}$ where the $\sum$ runs over one element in each conjugate class containing more than one element.

(4) Repeated ques.

Thm: 2.5

$o(G) = p^n$ where p is prime number

$Z(G) \neq \{e\}$

Proof:-

To prove $Z(G) \neq \{e\}$

Let $a \in G$, then $N(a)$ is a subgroup of G.

By Lagrange's thm, order of $N(a)$ is the divisor of $o(G)$

Since $o(G) = p^n$

$o(N(a)) = p^{na}$ $\quad 0 \leq na \leq n$.

By the class eqn

$$o(G) = \sum \frac{o(G)}{o(N(a))}$$

$$\Rightarrow p^n = \sum_{na \leq n} p^n / p^{na}.$$

$$\Rightarrow p^n = \sum_{na=n} p^n / p^{na} + \sum_{na<n} p^n / p^{na} \rightarrow (1)$$

Let $a \in z \Leftrightarrow o(N(a)) = o(G)$

$\Leftrightarrow p^{na} = p^n$

$\Leftrightarrow na = n.$

From (1)

$\Rightarrow p^n = \sum 1 + \sum_{na<n} p^n / p^{na}$ $\quad [\because p^n / p^{na} = 1]$

$= o(z) + \sum_{na<n} p^n / p^{na}$

$$p^n = x + \sum_{na<n} p^n/p^{na}$$

$$x = p^n - \sum_{na<n} p^n/p^{na} \rightarrow (2)$$

Since R.H.S of eqn (2) is divisible by p

$\Rightarrow$ x is divisible by p

$\Rightarrow x > 1$ [$\because$ p is a prime]

$\Rightarrow x \neq \{e\}$

Hence proved.

Corollary:

If $O(G) = p^2$ where p is a prime number then G is abelian.

proof:-

Given $O(G) = p^2$, p is prime.

To prove G is abelian

claim that: $Z(G) = G$

Since $O(G) = p^2$

We know that $Z(G) \neq \{e\}$

$Z(G)$ is a subgroup of G.

$\therefore O(Z(G))$ is a divisor of p^2

The possibilities of $O(Z(G))$ are $1, p, p^2$

By the above thm, $Z(G) \neq \{e\}$.

$O(Z(G)) > 1$

$\therefore O(Z(G)) = 1$ is impossible.

$O(Z(G)) = p$ or p^2.

Suppose $O(Z(G)) = p^2$

$O(Z(G)) = O(G)$

$Z(G) = G$

$\therefore$ G is abelian

Suppose $O(Z(G)) = p$.

Let $a \in G$, $a \notin Z(G)$.

then $N(a)$ is a subgroup of G.

$Z(G) \subset N(a)$

$\therefore a \in N(a)$

So that $O(N(a)) > p$.

By the Lagranges thm:

$O(N(a)) / O(G) = p^2$

The only possibilities must be equal to p^2

$O(N(a)) = p^2$

$O(N(a)) = O(G)$

$N(a) = G$.

$a \in Z(G)$

which is contradiction.

Thus $O(Z(G)) = p$ is impossible.

The only possibilities of $O(Z(G)) = p^2$.

Hence $Z(G) = G$.

$\therefore$ G is abelian.

(*) Thm: 2.6 Cauchy thm

If p is a prime number and $p / O(G)$ then G has an element of order p.

Proof:-

We have to find an element $a \neq e \in G$. satisfying $a^p = e$.

To prove, its existence we proceed by induction on $O(G)$.

Let us assume that; the thm to be true for all groups T such that

that $p / o(w)$

Then by our induction hypothesis, there exist an element of order p in w.

Let us assume that p is not a divisor of the order of any proper subgroup of G.

In particular,

If $a \notin z(G)$

since $N(a) \neq G$

$p \nmid o(N(a))$

Let us write the class equation

$$o(G) = o(z(G)) + \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}$$

Since $p / o(G)$, $p \nmid o(N(a))$

$$\Rightarrow p / \frac{o(G)}{o(N(a))}$$

$$\Rightarrow p / \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}$$

Since $p / o(G)$, $p \nmid o(N(a))$

$$\Rightarrow p / \frac{o(G)}{o(N(a))}$$

$$\Rightarrow p / \sum_{Na \neq G} \frac{o(G)}{o(N(a))}$$

Since $p / o(G)$, $p / \left(o(G) - \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}\right) = o(z(G))$

$\Rightarrow p$ divides $o(z)$

But $z(G)$ is a subgroup of G whose order is divisible by p.

(7) But our assumption, p is not a divisor of order of any proper subgroup of G.

So that, $Z(G)$ cannot be a proper subgroup of G.

ie) $Z(G)$ is a improper subgroup of G

$\therefore Z(G) = G$

$\therefore G$ is abelian.

By cauchy theorem of abelian group (write statement)

$\therefore G$ has an element of order p.

Defn: sylow thm

A subgroup of G order p^m where $p^m / o(G)$ and $p^{m+1} \nmid o(G)$ is called a p-sylow subgroup of G.

Remark:-

Let $n(k)$ is defined by $p^{n(k)} / p^{(k)}!$

but $p^{n(k+1)} \nmid p^{(k)}!$

ie) $n(k)$ = power p which divides $(p^{(k)})!$

Thm: 8.7

$n(k) = 1 + p + \cdots + p^{k-1}$

proof:-

We know that, $n(k)$ is defined by $p^{n(k)} / p^{(k)}!$

but $p^{n(k+1)} \nmid p^{(k)}!$

ie) $n(k)$ = power p which divides $(p^k)!$

If $k = 1$

then, $(p^k)! = p^1! = 1 \cdot 2 \cdots (p-1)p$

$\Rightarrow p^1 / p^1 \Rightarrow p^2 \nmid p!$

Hence $n(1)=1$.

$n(k)$ must be the power of p which divides $p(2p)(3p)\cdots(p^{k-1}p)$

Now $n(k)$ = powers of p which divides $(p^k)!$

= powers of p which divides $p(2p)(3p)\cdots(p^{k-1}p)$

= powers of p which divides $p^{p^{k-1}}(1\,2\cdots p^{k-1})$

= powers of p which divides $p^{p^{k-1}}+(p^{k-1})!$

$= p^{k-1}$ + power of p which divides $(p^{k-1})!$

$\therefore n(k) = p^{k-1} + n(k-1)$

$n(k) - n(k-1) = p^{k-1}$

Similarly $n(k-1) - n(k-2) = p^{k-2}$

$\vdots$

$n(2) - n(1) = p$

$\therefore n(1)=1$

Adding these we get

$n(k) = 1+p+p^2+\cdots+p^{k-1}$

Defn: Equivalence

Let G_1 be a group A, B subgroup of G_1 If $x, y \in G_1$ define $x \sim y$ if $y = axb$ for some $a \in A$, $b \in B$.

Thm 2.8

Let A and B be the two subgroup of G_1 the relation defined by $x \sim y$ if $y = axb$ for some $a \in A$, $b \in B$ and $x, y \in G_1$. To prove that $\sim$ is an equivalence.

Proof:-

Let $x \in G_1$ be an arbitrary element

Then i) $x = exe \quad \forall\ e \in A,\ e \in B$.

$\therefore x \sim x$.

(9)

ii) $y = axb \quad \forall\ a \in A,\ b \in B,\ x, y \in G$.

$a^{-1}yb^{-1} = a^{-1}(axb)b^{-1}$

$a^{-1}yb^{-1} = (a^{-1}a)\,x\,(bb^{-1}) = x$.

$x = a^{-1}yb^{-1} \ \forall\ a^{-1} \in A,\ b^{-1} \in B,\ x, y \in G$.

[A, B is a subgroup of G]

iii) $x \sim y,\ y \sim z \Rightarrow x \sim z$

$x \sim y \Rightarrow y = axb \quad \forall\ a \in A,\ b \in B \quad x, y \in G$

$y \sim z \Rightarrow z = cyd \quad \forall\ c \in A,\ d \in B,\ z \in G$

$z = c\,(axb)\,d$.

$= (ca)\,x\,(bd) \quad \forall\ ca \in A,\ bd \in B,\ x \in G$.

[$\because$ A, B is a subgroup of G]

$\Rightarrow x \sim z$

$\therefore x \sim y,\ y \sim z \Rightarrow x \sim z$.

The relation is an equivalence relation.

Thm: 2.9

If A, B are finite subgroup of G then $O(AxB) = \frac{O(A)O(B)}{O(A \cap xBx^{-1})}$. Given that A and B of two finite subgroup of G.

Given that A and B of two finite subgroup of G.

To prove $O(AxB) = \frac{O(A)\,O(B)}{O(A \cap xBx^{-1})}$

consider the function

$f : AxB \to AxBx^{-1}$ by $f(axb) = axbx^{-1}$

i) f is well defined

$axb = cxd$

$axbx^{-1} = cxdx^{-1}$

(10)

$f(axb) = f(cxd)$

$\therefore f$ is well-defined.

ii) f is 1-1

$f(axb) = f(cxd)$

$axbx^{-1} = cxdx^{-1}$

$axb = cxd$

f is 1-1

iii) f is onto

For any element $axbx^{-1} \in AxBx^{-1}$

There exist an element

$axb \in AxB$ such that

$f(axb) = axbx^{-1}$

$\therefore f$ is onto

Hence f is bijection

$\therefore$ The two sets AxB and $AxBx^{-1}$ are equivalent.

$$O(AxB) = O(AxBx^{-1})$$

Since xBx^{-1} is a subgroup of G_1 of order $O(B)$

$$O(AxB) = O(AxBx^{-1})$$

[If H and K are finite subgroup of G_1 of orders $O(H)$ and $O(K)$ respectively then

$$O(HK) = \frac{O(H)O(K)}{O(H \cap K)}]$$

$$O(AxB) = O(AxBx^{-1}) = \frac{O(A)O(xBx^{-1})}{O(A \cap xBx^{-1})}$$

$$O(AxB) = \frac{O(A)O(B)}{O(AxBx^{-1})}$$

Hence proved.

Thm: 2.10

Let G be a finite group and suppose that G is a subgroup of the finite group M. Suppose further that M has a p-sylow subgroup Q. then G has a p-sylow subgroup P in fact $P = G \cap xQx^{-1}$ for some $x \in M$.

proof:-

Let G is a subgroup of M.

Suppose that $p^m / o(M)$, $p^{m+1} \nmid o(M)$

Since M has a p-sylow subgroup Q of order p^m.

ie) $o(Q) = p^m$

Let $o(G) = \pm p^n$ where $p \nmid \pm$.

claim:

Let G has a p-sylow subgroup of order p^n consider the double coset decomposition of M given by G and Q.

$$M = UGxQ$$

[If A, B are finite subgroup of G, then $o(AxB) = \frac{o(A)o(B)}{o(A \cap xBx^{-1})}$ Given that A and B of two finite subgroup of G].

$$o(GxQ) = \frac{o(G)o(Q)}{o(G \cap xQx^{-1})}$$

$$= \frac{p^n \pm p^m}{o(G \cap xQx^{-1})}$$

since $G \cap xQx^{-1}$ is a subgroup of xQx^{-1} Its order is p^{mx}

then $O(G \times Q) = \frac{p^n \pm p^m}{p^m}$

(12)

$= \pm p^{m+n-mx}$ is divisible by p^{m+1}

ie) $p^{m+1} / O(G \times Q)$

$\Rightarrow p^{m+1} / O(M)$

which is contradiction to $p^m / O(M)$

$p^{m+1} \not| O(M)$

$\therefore mx = n$ for some $x \in M$.

$O(G \cap x Q x^{-1}) = p^n$.

Since $G \cap x Q x^{-1} = P$ is a subgroup of G and has order p^n.

Thm 2.11 Second part of sylow's thm.

If G is a finite group, p is a prime and $p^n / O(G)$ but $p^{n+1} \not| O(G)$. then any two subgroups of G of order p^n are conjugate.

proof:- Let A and B be two subgroups of G each of order p^n ~~each of order p^n~~.

ie) $O(A) = O(B) = p^n$.

We want to prove that $A = xBx^{-1}$.

Decompose G into double cosets of A and B.

$$G = \cup AxB$$

$$O(G) = \sum_{x \in G} O(AxB)$$

By thm,

[If A, B are finite subgroups of G then $O(AxB) = \frac{O(A)O(B)}{O(A \cap xBx^{-1})}$ ~~Given that A and B are two finite subgroups of G~~]

If $A \neq xBx^{-1}$ for every $x \in G$, then $O(AxB) = p^m$ where $m < n$ thus

$$O(A\times B) = \frac{O(A)\,O(B)}{p^m} = \frac{p^{2n}}{p^m}$$

(13)

$$= p^{2n-m}$$

$\because\ 2n-m > n$

$2n-m \geq n+1$

$p^{2n-m} \geq p^{n+1}$]

ie) $p^{n+1} / O(A\times B)$ for every x.

Since $O(G) = \sum_{x\in G} O(A\times B)$

$\therefore\ p^{n+1} / O(G)$

which is contradiction to $p^n / O(G)$

$p^{n+1} \nmid O(G)$

$\therefore\ A = xBx^{-1}$ for some $x \in G$.

Thus any two subgroup of G of order p^n are conjugate

Note:-

If H is a subset of G then N(H) is a normalizer of G is defined by $N(H) = \{x\in G / xHx^{-1} = H\}$

Thm: 2.12

The number of p-sylow subgroup in G equals $O(G)/O(N(p))$ where p is any p-sylow subgroup of G. In particular this number is a divisor of $O(G)$

proof:-

Let L be the set of all p-sylow subgroups of G.

ie) $L = \{xpx^{-1} / x\in G\}$

Let $K = G/N(p) = \{N(p)x / x\in G\}$

Define $f: L\to K$ such that

$f(xpx^{-1}) = N(p)x^{-1}$ $\forall\ x\in G$.

claim: f is well-defined.

Let $xpx^{-1} = ypy^{-1}$. $[xpx^{-1}, ypx^{-1} \in L]$

$\Rightarrow y^{-1}xpx^{-1}x = y^{-1}ypy^{-1}x$

(11) $\Rightarrow (y^{-1}x)p = p(y^{-1}x)$

Since $y^{-1}x \in N(p)$ and $N(p)$ is a subgroup of G_1.

$\Rightarrow (y^{-1}x)^{-1} \in N(p)$

$\Rightarrow x^{-1}y \in N(p)$

$\Rightarrow N(p)x^{-1} = N(p)y^{-1}$

$f(xpx^{-1}) = f(ypy^{-1})$

f is well defined.

claim: f is 1-1

let $f(xpx^{-1}) = f(ypy^{-1})$

$\Rightarrow N(p)x^{-1} = N(p)y^{-1}$

$\Rightarrow (y^{-1}x)^{-1} \in N(p)$

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

$\Rightarrow xx^{-1}ypy^{-1} = xpx^{-1}yy^{-1}$

$ypy^{-1} = xpx^{-1}$

$\therefore f$ is 1-1

claim: f is onto

Given $N(p)x \in K$, there exist an element $x^{-1}p(x^{-1})^{-1} \in L$ such that $f(x^{-1}p(x^{-1})^{-1}) = N(pxx^{-1})^{-1}$

$= N(p)x$

$\therefore f$ is onto

$O(L) = O(K)$

$\Rightarrow O(L) = \frac{O(G_1)}{O(N(p))}$

$S_p = \frac{O(G_1)}{O(N(p))}$

$\Rightarrow O(N(p)) = \frac{O(G_1)}{S_p}$

Thm: 2.13 Third part of Sylow's thm.

(15) U.Q. 3m Statement 10 m

The number of p-sylow subgroup in G, for a given prime, is of the form $1+kp$

proof:-

Let P be a p-sylow subgroup of G.

Let $o(P)=p^n$ where $p^n / o(G)$ and $p^{n+1} \nmid o(G)$

Now, decompose G into double cosets of P and P.

$$\text{Thus } G = \cup (PxP)$$

$$o(G) = \sum_{x \in G} o(PxP)$$

$$= \sum_{x \in N(P)} o(PxP) + \sum_{x \notin N(P)} o(PxP) \rightarrow (1)$$

By thm 2.9 we know that

$$o(PxP) = \frac{o(P)\,o(P)}{o(P \cap xPx^{-1})} = \frac{o(P)^2}{o(P \cap xPx^{-1})}$$

If $P \cap xPx^{-1} \neq P$ then $p^{n+1} / o(PxP)$ where $o(P)=p^n$

Now, consider $\sum_{x \in N(P)} o(PxP)$

If $x \in N(P)$ then $PxP = P(Px) = P^2x = Px$.

$$\therefore o(PxP) = o(Px) = o(N(P))$$

Now consider $\sum_{x \notin N(P)} o(PxP)$

If $x \notin N(P)$ then $p^{n+1} / \sum_{x \notin N(P)} o(PxP)$

$\Rightarrow \sum_{x \notin N(P)} o(PxP) = u \cdot p^{n+1}$ where u is an integer.

Now, then (1) becomes

$$o(G) = o(N(P)) + u \cdot p^{n+1}$$

[÷ o(N(P))]

$$\frac{o(G)}{o(N(P))} = 1 + \frac{u \cdot p^{n+1}}{o(N(P))} \quad — (2)$$

Now, $o(N(P)) / o(G)$ [By Lagrange's thm]

since $N(P)$ is a subgroup of G

Hence $p^{n+1} u / o(N(P))$ is an integer

Also, since $p^{n+1} \nmid o(G)$, p^{n+1} cannot divide $o(N(p))$

But, then $p^{n+1}.u / o(N(p))$ must be divide by p.

So we can write $p^{n+1}.u / o(N(p))$ as kp where k is an integer.

ie) $kp = p^{n+1}.u / o(N(p))$

$$o(G)/o(N(p)) = 1 + kp$$

$\therefore$ $o(G)/o(N(p))$ is the number of p-sylow subgroup of G.

Q. Thm: 2.14 First part of sylow thm.

If p is a prime number and $p^{\alpha} / o(G)$ then G has a subgroup of order p^{α}.

proof:-

Let p be a prime number and $p^{\alpha} / o(G)$

To prove, G has a subgroup of order p^{α}

We prove the theorem by induction on $o(G)$

Suppose $o(G) = 2$

then the only possible prime number which divide 2.

$\therefore$ The theorem is true for $o(G) = 2$.

$\therefore$ G has a subgroup of order 2.

We assume that the theorem is true for all the groups of order $< o(G)$

case(i) If H is a subgroup of G and $H \neq G$ and $p^{\alpha} / o(H)$

$\Rightarrow$ H has a subgroup T of order p^{α}

$\Longrightarrow$ G has a subgroup T of order p^{α}

[$\because T \subset H \subset G \Rightarrow T \subset G$]

case(ii)

Suppose H is a subgroup of G $H \neq G$ and $p \not| o(H)$

In particular,

If $a \in G$ then $N(a) = \{x \in G / xa = ax\}$ is a subgroup of G.

Moreover if $a \notin z$, $N(a) \neq G$

The class equation of G is $o(G)$

$$\Rightarrow \sum \frac{o(G)}{o(N(a))}$$

$$o(G) = \sum_{a \in z} \frac{o(G)}{o(N(a))} + \sum_{a \notin z} \frac{o(G)}{o(N(a))}$$

$$= \sum_{N(a)=G} \frac{o(G)}{o(N(a))} + \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}$$

$$o(G) = o(z) + \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}$$

$$o(z) = o(G) - \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}$$

Since $p \not| o(H)$, $p \not| o(N(a))$

$$p \Big/ \sum_{a \notin z} \frac{o(G)}{o(N(a))}$$

$$p / o(G) - \sum_{a \notin z} \frac{o(G)}{o(N(a))}$$

$$p / z = o(z)$$

$$p / o(z)$$

By cauchy's theorem

z has an element $b \neq e$ of order p

Let $B = \langle b \rangle$

The subgroup of G generated by b.

B is of order of p.

Moreover, since $b \in z$, B must

(18)

$\bar{G} = G/B$

Since G is finite

$$o(\bar{G}) = o(G/B) = \frac{o(G)}{o(B)}$$

$$o(\bar{G}) = \frac{o(G)}{p} \quad [\because o(\bar{G}) = n/p]$$

By Induction hypothesis,

$\bar{G}$ has a subgroup of $\bar{P}$ of order $p^{\alpha-1}$

$$\because p^{\alpha}/o(G) \to p^{\alpha}/n \Rightarrow p^{\alpha}/p/n/p$$

$$= p^{\alpha-1}/o(G), \text{ But } p^{\alpha} \nmid o(G)]$$

$$\therefore p^{\alpha}/o(G)$$

$$o(G) = p^{\alpha}k$$

$$\Rightarrow p^{\alpha}/p \,/\, p^{\alpha}/p \cdot k \Rightarrow p^{\alpha-1}/p^{\alpha-1} \cdot k.$$

Let $P = \{x \in G / xB \in \bar{P}\}$

By cauchy's theorem P is a subgroup of G.

Claim:

$$\bar{P} \cong P/B$$

Define $\phi : P \to \bar{P}$ by $\phi(x) = xB \; \forall \; x \in P$.

We have to prove that ϕ is onto homomorphism with Kernel B.

i) ϕ is well defined.

Let $x, y \in P$ be a arbitrary element

Now, $x = y$

$\Rightarrow e = x^{-1}y, \; x^{-1}y = e \in B.$

$\Rightarrow x^{-1}y \in B, \; xB = yB$

$\Rightarrow \phi(x) = \phi(y)$

$\Rightarrow \phi$ is well defined.

ii) ϕ is onto.

Let $xB \in \bar{P}$ be an element in $\bar{P}$

$\Rightarrow x \in P$

by the definition of P

$\Rightarrow \phi(x) = xB$

(9) For any $xB \in \bar{P}$, there exists an element such that $\phi(x) = xB$

$\therefore \phi$ is onto.

(ii) ϕ is homomorphism

Let $x, y \in P$.

Since P is a subgroup

$\Rightarrow xy \in P$

Now, $\phi(xy) = xy \cdot B$

Since B is normal

$\phi(xy) = xByB$

$\phi(xy) = \phi(x)\phi(y)$

ϕ is homomorphism.

Kernel $\phi = B$.

It is enough to prove that

$x \in \ker \phi \Leftrightarrow x \in B$.

So that $\phi(x)$ is the identity element in $\bar{P}$

$\Leftrightarrow x \in P$ such that $\phi(x) = B$

$\Leftrightarrow x \in P$ such that $xB = B$.

$\Leftrightarrow x \in P$ such that $x \in B$

$x \in \ker \phi \Leftrightarrow x \in B$.

By fundamental thm of homomorphism

$\bar{P} \cong P/B$

$\Rightarrow O(\bar{P}) = O(P/B)$

$\Rightarrow p^{\alpha-1} = O(P)/O(B)$

$\Rightarrow p^{\alpha-1} = \frac{O(P)}{p}$

$\Rightarrow p^{\alpha-1} p = O(P)$

$O(P) = p^{\alpha}$

$\Rightarrow G$ has a subgroup of order p^{α}.

G has a required subgroup of order $p^{\alpha-1}$

$\left|\frac{P}{B}\right| = p^{\alpha-1}$

$\Rightarrow |P| = p^{\alpha-1}|B| = p^{\alpha-1} p \quad [\because \langle b \rangle = B]$

$= p^{\alpha}$ and $p \subseteq G_1$

$\therefore G_1$ has a subgroup of order p^{α}

Direct products

Let $G_1, G_2, \ldots, G_n$ be any n group. Let $G = G_1 \times G_2 \times \ldots \times G_n = \{(g_1, g_2, \ldots, g_n) / g_x \in G_i\}$ be the set of all ordered n-tuples we can also say that the cartesian product of $G_1, G_2, \ldots, G_n$.

Define a product in G $(g_1, g_2, \ldots, g_n) \times (g_1', g_2', \ldots, g_n') = g_1 g_1', g_2 g_2', \ldots, g_n g_n'$ [ie) component wise multiplication]

Then G is a group in which $(e_1, e_2, \ldots, e_n)$ is the unit element where each e_i is the unit element of G_i and $(g_1, g_2, \ldots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})$

We call this group G the external direct product of $G_1, G_2, \ldots, G_n$.

Defn: Internal direct product

Let G be a group and $N_1, N_2, \ldots, N_n$ are normal subgroup of G such that

i) $G = N_1 N_2 \ldots N_n$

ii) Given $g \in G$ then $g = m_1 m_2 \ldots m_n \in N_i$ in a unique way. Then G is the internal direct product of $N_1, N_2, \ldots, N_n$

Thm: 2.15

Suppose that G is the internal direct product of $N_1, N_2, \ldots, N_n$ then for $i \neq j$ $N_i \cap N_j = \{e\}$ and of $a \in N_i$, $b \in N_j$ then $ab = ba$.

proof:-

Let $G = N_1 N_2$.

claim i) $N_i \cap N_j = \{e\}$

ii) $ab = ba$ if $a \in N_i$, $b \in N_j$

(21)

Suppose $x \in N_i \cap N_j$

then $x \in N_i$ and $x \in N_j$

Since $x \in N_j$

then we can write x as

$$x = e_1, \ldots e_i, e_{i+1}, \ldots, e_{j-1}, \ldots, e_{j+1} \ldots e_n$$

where $e_t = e$

Viewing x as an element in N_i

Similarly we can write every element in particular x has a unique representation in the form $m_1, m_2, \ldots, m_n$ where $m_i \in N_n$

Since two composition of x must coincide

$$x = e_i = e_j = e$$

$$N_i \cap N_j = \{e\} \quad \forall \; i \neq j$$

claim(ii) $ab = ba$

Since $a \in N_i$, $b \in N_j$ and $i \neq j$

$\Rightarrow aba^{-1} \in N_i$

$\Rightarrow aba^{-1}b^{-1} \in N_i \rightarrow (1)$

Also, $a^{-1} \in N_j \Rightarrow ba^{-1}b^{-1} \in N_j$

$$aba^{-1}b^{-1} \in N_j \rightarrow (2)$$

From (1) and (2)

$$aba^{-1}b^{-1} \in N_i \cap N_j$$

$$aba^{-1}b^{-1} \in N_i \cap N_j = \{e\} \text{ [by i]}$$

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

$\Rightarrow ab = ba$

Hence proved.

Remark:

In $G = G_1 \times G_2 \times \ldots \times G_n$

Let $\overline{G_i} = \{e_1, e_2, \ldots, e_{i-1}, e_i, e_{i+1}, \ldots e_n\}$

then $\overline{G_i}$ is a normal subgroup of G and is isomorphic to G_i moreover $G = \overline{G_1}, \overline{G_2}, \ldots \overline{G_n}$

and every $g \in G$ has a unique decomposition $g = \bar{g}_1, \bar{g}_2, \ldots, \bar{g}_n$ where $\bar{g}_i \in G_i$, $i = 1, 2, \ldots, n$.

22 Thm: 2.16

Let G be a group and suppose that G is the internal direct product of $N_1, N_2, \ldots, N_n$. Let $T = N_1 \times N_2 \times \ldots \times N$ then G and T are isomorphic.

Proof:-

Define a map $\psi : T \to G$ by

$$\psi(a_1, a_2, \ldots, a_n) = a_1 a_2 \ldots a_n$$

claim (i)

ψ is homomorphism

Let $x, y \in T$

$x = (a_1, a_2, \ldots, a_n)$ and $y = (b_1, b_2, \ldots, b_n)$ where $a_i, b_i \in N_i \quad \forall i = 1, 2, \ldots, n$

$$xy = a_1 b_1, a_2 b_2, \ldots, a_n b_n$$

Now,

$$\psi(xy) = \psi(a_1 b_1, a_2 b_2, \ldots, a_n b_n)$$
$$= a_1 b_1 a_2 b_2 \ldots a_n b_n$$
$$= (a_1 a_2 \ldots a_n)(b_1 b_2 \ldots b_n)$$
$$\psi(xy) = \psi(x)\psi(y)$$

claim ii)

ψ is 1-1

Let $\psi(a_1, a_2, \ldots, a_n) = \psi(b_1, b_2, \ldots, b_n)$

$$a_1, a_2, \ldots a_n = b_1, b_2, \ldots, b_n.$$

Since any element in G expressed as a unique way $a_i = b_i \quad \forall i$

$\therefore \psi$ is 1-1

claim iii)

ψ is onto

For given $(a_1, a_2, \ldots, a_n) \in G$

There exists an element $(a_1, a_2, \ldots, a_n)$ such

that $\psi(a_1, a_2, \ldots, a_n) = (a_1, a_2, \ldots, a_n)$

ψ is onto

Hence G and T are isomorphic.

Unit - III

Definition: Ring Theory

Ring

A non-empty set R together with two binary operation denoted by '+' and '.' are called addition and multiplication which satisfies the following axiom is called Ring

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

ii) $(R,\cdot)$ is an associative binary operation

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

[Distributive laws]

Example:-

$(Z,+,\cdot)$, $(Q,+,\cdot)$, $(R,+,\cdot)$, $(C,+,\cdot)$ are all rings

Definition: Commutative Ring

A ring R is said to be commutative if $ab=ba$ for all $a,b \in R$

Ex: 1) Z, Q, R are all commutative

2) $M_2(R)$ is a non-commutative ring

Definition: Ring with Identity

Let R be a ring we say that R is a ring with identity if there exist an element $1 \in R$ such that $a\cdot 1 = 1\cdot a = a$ for all $a \in R$

Definition: 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}

Definition: Division Ring

Let R be a ring with identity element in R is called a Skew field (or) division ring if every non-zero element in R is unit

ie) For every non-zero element $a \in R$ there exist a multiplicative inverse $a^{-1} \in R$ such that

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

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

$a(-b) + ab = a(-b+b) = a \cdot 0 = 0$

$a(-b) + ab = 0$

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

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

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

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

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

$= ab$

(iv) Suppose that R has unit element 1.

$(-1)a = -a$

$(-1)a + a = a(-1+1) = a(0)$

$= 0$

$(-1)a + a = 0$

$(-1)a = -a$

(v) $(-1)(-1) = 1$

by (iii) $(-1)(-1) = -(1(-1)) = -(-1)$

$= 1$

The Pigeon hole principle

If n objects are distributed over m places and if $n > m$ the some places receives atleast two object

---

Theorem 3-2

Any field is an integral domain

Proof:-

Given. F is a field

To proove,

F is an integral domain

ie) To prove F has no zero divisor

Let $a, b \in F$ and $a \neq 0$

Since F is a field and a^{-1} exist

Now, $ab = 0 \Rightarrow a^{-1}(ab) = 0$

$\Rightarrow b = 0$

$\therefore$ F has no zero divisor

Hence F is an integral domain

Theorem 3.3

A finite integral domain is a field

Proof:-

An integral domain is a commutative ring such that $ab=0$ iff atleast one of a or b is zero

A field is a commutative ring with unit element in which every non-zero element has a multiplicative inverse.

Let D be finite integral domain

To Prove:

i) D has a unit element 1 such that $a \cdot 1 = a$ For every $a \in D$

ii) For every element $a \neq 0 \in D$ produce an element $b \in D$ such that $ab = 1$

Let $x_1, x_2, \ldots x_n$ be all the element in D

Suppose that $a \neq 0 \in D$

Consider the element $x_1a, x_2a, \ldots x_na$ they are all in D.

Now, we have to prove they are all distinct

Suppose $x_i a = x_j a \quad \forall\ i \neq j$

then $x_i a = x_j a$

$x_i a - x_j a = 0$

$\Rightarrow (x_i - x_j).a = 0$

Since D is an Integral domain $a \neq 0$

we have, $x_i - x_j = 0$

$x_i = x_j$.

which is contradiction to $i \neq j$

$x_1a, x_2a, \ldots x_na$ are in distinct element in D

By the pigeonhole principle

there must be account for all element of D

(i.e) every element $y \in D$, y can be written as $x_i = a$ for some x_i

Since $a \in D$

$a = x_i \cdot a$

$a = a x_i$

$y = x_i a$

$y \cdot x_i = x_i \cdot x_i a$

$y \cdot x_i = x_i a$

$a = x_{i_0} a$ For some $x_{i_0} \in D$

Since D is commutative

$$a = x_{i_0} a = a x_{i_0}$$

Now to prove x_{i_0} is unit element in D.

If $y \in D$

then $y = x_i a$

$$y x_{i_0} = x_i a x_{i_0} = x_i (a x_{i_0})$$

$$= x_i a$$

$$y x_{i_0} = y$$

Thus x_{i_0} is a unit element for D and we write it is 1 Now $1 \in D$

ie) there exist $b \in D$ such that $b \cdot a = 1$

$\Rightarrow ab = 1$

∴ every non-zero element in D has multiplicative inverse

Hence D is a field

Theorem 3.4

If P is a prime number then J_p, the ring of integer mod p is a field

Proof:- Let J_p be the ring of integer mod p

∴ J_p is a finite set

To prove: J_p is a field

It is enough to prove that J_p is an integral Domain

Clearly, the ring of integers J_p is commutative.

Now to prove J_p has no-zero divisor

Let $a, b \in J_p$ and $ab \equiv 0 \pmod p$

$\Rightarrow p / ab$

since p is a prime number

p / a (or) p / b

$\Rightarrow a \equiv 0 \pmod p$ or $b \equiv 0 \pmod p$

either p / a or p / b in J_p

∴ J_p has no zero divisor.

By the above theorem 3.3

[A finite integral Domain is a field]

$\therefore J_p$ is field

Definition: Characteristic zero

An integral domain D is said to be a characteristic zero if the relation $ma = 0$ where $a \neq 0 \in D$ and where m is an integer, can hold only if $m = 0$

Ex: Z_6 is a ring of characteristic 6

Finite characteristic

An integral domain D is said to be of finite characteristic if there exist a positive integer m such that $ma = 0 \ \forall a \in D$

Homomorphism of Ring

Let R and R' be two rings $\phi : R \to R'$ is called a homomorphism if i) $\phi(ab) = \phi(a)\phi(b)$

ii) $\phi(a+b) = \phi(a) + \phi(b) \ \forall a, b \in R$

Definition: Ring kernel of ϕ

Let $\phi : R \to R'$ be a homomorphism then the kernel of ϕ, $I(\phi)$ is the set of all elements $a \in R$ such that $\phi(a) = 0$ the zero element of R'

ie) $I(\phi) = \{ a \in R / \phi(a) = 0$, 0 is the identity element of $R' \}$] seminar 1

(X) VQ

Theorem: 3.5

(i) ϕ is a homomorphism of R into R' with kernel $I(\phi)$, then $I(\phi)$ is a subgroup of R under addition.

(ii) If $a \in I(\phi)$ and $r \in R$ then $a \cdot r$ and ra in $I(\phi)$

Proof: To prove, $I(\phi)$ is a subgroup of R under addition

$I(\phi)$ is a subset of R

By the definition, $I(\phi)$ is a subgroup of R

Now to prove

(I) (i) $a, b \in I(\phi) \Rightarrow a+b \in I(\phi)$

(ii) $a \in I(\phi) \Rightarrow -a \in I(\phi)$

(i) Let $a, b \in I(\phi)$

$\phi(a+b) = \phi(a) + \phi(b) = 0+0$

$\phi(a+b) = 0$

$\therefore a+b \in I(\phi)$

(ii) $\phi(-a) = -\phi(a) = 0$ $\quad a \in I(\phi)$

$\Rightarrow -a \in I(\phi)$

$\therefore I(\phi)$ is a subgroup under addition

(II) Let $a \in I(\phi)$ and $r \in R$

To prove, ar, ra are in $I(\phi)$

$\phi(ar) = \phi(a)\phi(r) = 0\,\phi(r)$

$= 0$

$\therefore ar \in I(\phi)$ and $\phi(ra) = \phi(r) \cdot \phi(a) =$

$\phi(r) \cdot 0$

$= 0$

$\therefore ra \in I(\phi)$

Hence ar and $ra \in I(\phi)$

Definition :- Isomorphism

A homomorphism of R into R' is said to be an Isomorphism if it is a 1-1 mapping

Definition :- Isomorphic

Two rings are said to be Isomorphic if there is an Isomorphism of one onto the other

Theorem 3.6 Theorem 3.20 and corollary

The homomorphism ϕ of R into R' is an isomorphism iff $I(\phi) = (0)$ or $\{0\}$

Proof: Let $\phi : R \to R'$ be a homomorphism

TO prove, $I(\phi) = \{0\}$

Let $I(\phi) = \{a \in R \mid \phi(a) = 0\}$

Let $x \in I(\phi)$

$\Rightarrow \phi(x) = 0$

$\Rightarrow \phi(x) = \phi(0)$

$\Rightarrow x = 0$

$\therefore I(\phi) = 0$

To prove ϕ is 1-1

Suppose $\phi(x) = \phi(y)$

$\phi(x) - \phi(y) = 0$

$\phi(x) + \phi(-y) = 0$

$\phi(x-y) = 0$

$x-y \in \ker \phi$

$x-y = 0$ $\quad [\because I(\phi) = \{0\}]$

$x = y$

$\therefore \phi$ is 1-1

Unit - 4

Ideal and quotient Ring

Defn:-

A non empty set U of R is said to be ideal of R.

(i) U is a subgroup of R under addition.

(ii) for every $u \in U$, $r \in R$, both ur and ru are in U.

Example:

$2z$ is an ideal of z (or).

nz is an ideal of z.

let $a, b \in 2z$ then $a-b \in 2z$.

let $a \in 2z$ and $b \in 2z$.

Then a, b is an even.

Then $2z$ is an ideal of z.

Lemma 3.4.1

If U is an ideal of R, then R/U is a ring and is a homomorphic image of R.

proof:

let U be an ideal of R.

U is a subgroup of R under addition.

(i) R/U is a ring.

let $R/U = \{U+a \mid a \in R\}$ and '+' and '.' are defined as follows.

$(U+a)+(U+b) = U+(a+b)$.

(ii) $(u+a)(u+b) = u+ab$.

To prove R/U is an abelian group under addition.

(i) closure:-

'+' is a binary operation

'+' is a closure.

(ii) Associative:-

Let $U+a, U+b, U+c \in R/U$.

$$(U+a)+[(U+b)+(U+c)] = U+a+[U+(b+c)]$$

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

$$= U+[(a+b)+c]$$

$$= [U+(a+b)]+[U+c]$$

$$= [(U+a)+(U+b)]+U+c$$

R/U is associative.

(iii) Identity:-

Let $U+a \in R/U$

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

$U+0$ is the identity of R/U.

(iv) Inverse:-

$a \neq 0 \in R$
$\exists\ b \neq 0 \in R \ni ab=1$
$Ra = \text{ring} \in R$

For $U+a \in R/U$.

$\exists\ U+(-a) \ni$:

$$(U+a)+(U+(-a)) = U+(a+(-a))$$

$$= U+0.$$

$(U+(-a))$ is inverse of $U+a$.

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

$= (U+b)+(U+a)$.

R|U is an abelian group under addition.

multiplication is associative,

closure

'.' is a closure.

Associative:-

$(U+a)[(U+b)(U+c)] = (U+a)[U+(bc]$

$= U+(abc]$.

$= [U+(ab)]\,[U+c)$

$= [(U+a)(U+b)](U+c)$.

R|U is a ring.

TO prove :- R|U is a homomorphism.

Let $\phi : R \to R|U$ is defined by $\phi(a) = U+a$.

(i) $\phi(a+b) = U+(a+b) = (U+a)+(U+b) = \phi(a)+\phi(b)$.

(ii) $\phi(ab) = U+(ab) = (U+a)(U+b) = \phi(a).\phi(b)$.

ϕ is a homomorphism.

R|U is a homomorphism image of R.

Lemma 3.5.1.

Let R be a commutative ring with element those only ideals are (0) and R itself then R is a field

proof:-

Given R be a commutative ring.

with unit element whose only ideals are

(0) and R itself.

To prove: R is a field.

For any $a \neq 0 \in R$.

If ∃ an element $b \neq 0 \in R$ such that $ab = 1$

$Ra = \{ra \mid r \in R\}$.

we claim that, Ra is a field of R.

we have to show that.

Ra is a ideal of R.

Ra is a subgroup under addition.

If $u \in Ra$ and $r \in R$ then $ru \in Ra$.

Let $u, v \in Ra$.

$u = r_1 a$ and $v = r_2 a$ for some $r_1, r_2 \in R$.

$u + v = (r_1 a) + (r_2 a) = (r_1 + r_2) a \in Ra$.

iii),

$-u = -(r_1, a) = (-r_1) a \in Ra$.

hence Ra is a additive subgroup of R.

If $r \in R$, $u \in Ra$.

$ru = r(r_1 a) = (rr_1) a \in Ra$.

Ra is an ideal of R.

$Ra = (0)$ or $Ra = R$.

since $a \neq 0 \Rightarrow a = 1 \cdot a \in Ra$

$Ra \neq 0$

$Ra = R$.

Every element of R is a multiple of a by.

In particular $1 \in R$.

So $1 = a.b$ for some $b \in R$.

Hence R is a field.

Maximum ideal:-

An ideal $M \neq R$ is a ring R is said to be a maximum ideal of R. If whenever U is an ideal R such that $M \subset U \subset R$, either $R = U$ (or) $M = U$.

If p is a prime number. Then $p = p$ is a maximal ideal of R.

Theorem 3.5.1.

If R is commutative ring with element and is an ideal of R. Then M is a maximal ideal of R, R/M is a field.

Proof:

Given R is a commutative ring. with unit element and M is an ideal of R.

Suppose R/M is a field.

To prove:-

M is a maximal ideal of R.

We know that any field of $\mathbb{F}$ has only. two ideals (0) and itself.

Hence R/M is a field.

By Theorem,

... rings and ϕ be a

homomorphism of R onto R' with kernal U.
Then R' is isomorphic to R/U.
moreover there is one to one correspondence
between the set of ideals of R' and set
of ideals of R which contains U.

This correspondence can be achieved
by this associating with ideal W' in
R'.

The ideal W in R defined by.
$W = \{x \in R \mid \phi(x) \in W'\}$ with W so defined
R/W is isomorphic to R'/W'.

R/M has two ideals {0} and R/M can
there is 1-1 correspondence between.
the set of ideals of R/M and the
set of ideal of R which contains M
M ∈ R
0 ∈ R/M

This ideals M of R correspondence
M ∈ R 0 ∈ R/M
to ideal (0) of R/M. The ideal R of R
correspondence to the ideal R/M of R/M.

conversely.

Hence M is a maximal ideal of R.
suppose M is maximal ideal of R.

To prove:
R/M is a field.
since M is a maximal ideal of R.
By the correspondence mentioned above
has the two ideals (0) and R/M.

since R is commutative ring with unit element

By previous theorem. (4.2)

R/M is a field.

Theorem 4.4.

Every integral domain can be imbedded in a field.

proof:

Stage (i).

Let D be an integral domain.

Let $S = \{(a,b) \mid a,b \in D \text{ and } b \neq 0\}$.

Two element (a,b) and (c,d) are declared to be equivalent iff $ad = bc$.

If (a,b) is equivalent to (c,d) we write.

$(a,b) \sim (c,d)$.

Lemma 1:-

'$\sim$' is an equivalence relation on S. Thus relation $\sim$ is an equivalence relation.

proof:-

Let $(a,b) \in S$.

To prove $\sim$ is reflexive.

Since . is a commutative.

$ab = ba$.

$(a,b) \sim (b,a)$.

Hence $\sim$ is reflexive.

symmetric

Now, $(a,b) \sim (c,d) \Rightarrow ad = bc$

$\Rightarrow cb = da$.

$\Rightarrow (c,d) \sim (a,b)$

Hence $\sim$ is symmetric,

transitive

now, let $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$

now to prove that.

$(a,b) \sim (e,f)$.

we must prove that $af = be$.

$(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$.

$\Rightarrow ad = bc$ and $cf = de$,

f b.

multiply by 'f'.

$adf = bcf$. and $bcf = bde$.

$adf = bde$.

$afd = bed$.

$af = be \Rightarrow (a,b) \sim (e,f)$

Hence $\sim$ is transitive.

Hence $\sim$ is an equivalence relation.

Consider the equivalence class containing (a,b).

let it be denoted by a/b.

let $F = \{a/b \mid (a,b) \in \mathbb{Z} \times \mathbb{Z}, b \neq 0\}$.

Stage (ii)

let $a/b, c/d \in F$.

we now define,

$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ and $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.

since F is an integral domain $b_1 d \neq 0$.

we have $bd \neq 0$.

$\frac{ad+bc}{bd}$ and $\frac{ac}{bd} \in F$.

Lemma 2.1

Addition and multiplication defined above are well defined.

proof:

Let $(a_1, b_1) \in a/b$ and $(c_1, d_1) \in c/d$.

$(a_1, b_1) = (a, b)$ and $(c_1, d_1) = (c, d)$.

$a_1 b = b_1 a$ and $c_1 d = d_1 c$ $\longrightarrow$ (1).

(*) dd_1

$a_1 bdd_1 = b_1 add_1$ and $c_1 d b b_1 = d_1 c b b_1$.

$(a_1 d_1 + b_1 c_1) bd = (ad + bc) b_1 d_1$.

$$\frac{ad+bc}{bd} = \frac{a_1 d_1 + b_1 c_1}{b_1 d_1}$$

$(ac, bd) \sim (a_1, c_1, b_1, d_1)$

$$\frac{a}{b} + \frac{c}{d} = \frac{a_1}{b_1} + \frac{c_1}{d_1}.$$

Addition is well defined

~~$(a+b, b-a) = (c+c, d, d)$~~

also from (1). $a_1 b c_1 d = b_1 a d_1 c$.

$(ac, bd) \sim (a_1, c_1, b_1, d_1)$ (a_1, c_1, b_1, d_1)

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a_1}{b_1} \cdot \frac{c_1}{d_1}.$$

Lemma 3.

Stage (iii)

F is a field with the addition and multiplication are defined above.

proof:

It can be easily verified that.

addition is commutative and associative.

$\frac{0}{1}$ is the zero of F and

unit-V

Euclidean Ring

Definition. Euclidean Ring.

An integral Domain R is said to be Euclidean ring if every $a \neq 0$ in R there is defined a non-negative integer $d(a)$ such that

i) For all $a, b \in R$ both non-zero $d(a) \leq d(ab)$

ii) For any $a, b \in R$ both non-zero there exists $t, r \in R$ such that $a = tb + r$

where either $r = 0$. (Or) $d(r) < d(b)$

Theorem: 5.1

Let R be an Euclidean ring and let A be an Ideal of R. then there exist an element $a_0 \in A$ such that A consist exactly of all $a_0 x$ as x ranges multiple of x over R.

Proof:- Given R is an Euclidean Ring.

A is ideal of R.

To prove, $A = \{a_0 x / x \in R\}$ for some $a_0 \in A$

(case(i)) Suppose $A = \{0\}$

$\Rightarrow a_0 = 0$

$\Rightarrow A = \{a_0 x / x \in R\}$ where $a_0 = 0$

(case(ii)) Suppose $A \neq \{0\}$

$\Rightarrow$ there exist $a \in A$ such that $a \neq 0$

Take $a_0 \in A$ such that $d(a_0)$ is minimal $\rightarrow$ (1)

Now, we have $a, a_0 \in A$

$\Rightarrow a, a_0 \in R$

By the Property of an Euclidean ring

there exist $t, r \in R$ such that $a = a_0 t + r \rightarrow$ (2)

where either $r = 0$ or $d(r) < d(a_0)$

$\Rightarrow t a_0 \in A$ [$\because$ A is an ideal of R]

$a \in A \quad t a_0 \in A$

$\Rightarrow a - t a_0 \in A$ [using (2)]

$\Rightarrow r \in A$

Suppose $r \neq 0$

then $d(r) < d(a_0)$

which is contradiction [$\because d(a_0)$ is minimal]

$r = 0$

(2) $\Rightarrow a = t a_0 + 0$

$a = t a_0$

Hence $A = \{a_0 x / x \in R\}$ for some $a_0 \in A$

Definition: Principal Ideal Ring

An Integral domain R with unit element is a Principal Ideal ring, if every ideal A in R is of the form $A = (a)$ for some $a \in R$

Corollary:

A Euclidean Ring possess a unit element

Proof: Let R be an Euclidean ring:

$R = u_0 c$ for some $u_0 \in R$ for every $c \in R$ is a multiple of u_0

then particular $u_0 \in R$

$u_0 = u_0 c$ for some $c \in R$

Let $a \in R$

$a = x \cdot u_0$ For some $x \in R$

$ac = (x u_0) c$

$ac = x (u_0 c)$

$ac = x u_0$

$ac = a$

$\therefore c$ is the unit element

Hence the Euclidean ring possesses a unit element

Definition: Divide

If $a \neq 0$ and b are in a commutative ring R then a is said to divide b if there exist $c \in R$ such that $b = ac$

Remark:

i) If a/b, b/c then a/c

ii) If a/b, a/c then $a/b \pm c$

iii) If a/b then $a/bx \ \forall x \in R$.

Proof: (i) If a/b then by definition there exist $x \in R$ such that $b = ax \rightarrow (1)$

If b/c then by defn there exist $y \in R$ such that $c = by$ (by (1))

$= (ax)y$

$= (xa)y$

$= x(ay)$

$= x(ya)$

$= (xy)a$

$c = za$

ii) If a/b then by defn there exist $x \in R$ such that

$b = ax \rightarrow (1)$

If a/c then by defn there exist $y \in R$ such that

$c = ay \rightarrow (2)$ Adding (1) and (2)

$b + c = ax + ay$

$= a(x+y)$

From this we can say $a/b+c \rightarrow (3)$

similarly (1) - (2)

$b - c = a(x-y)$

$= a/b-c \rightarrow (4)$

From (3) and (4)

$a/b \pm c$

(iii) Given a/b then by definition there exist $x \in$ such that $b = ax$

multiple of both sides x

$bx = ax^2$, $x \in R$ $x^2 \in R$

From this we can say a/bx

Definition :- Greatest common divisor

If $a, b \in R$ then $d \in R$ is said to be a greatest common divisor of a and b if

i) d/a and d/b

ii) whenever c/a and c/b then c/d

We shall use the notation $d = (a, b)$ to denote that d is the greatest common divisor of a and b.

Theorem : 5.2

Let R be a Euclidean ring then any two element a and b in R have a greatest common divisor d. Moreover $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$

Proof: Let A be the set of all elements $ra+sb$ where r, s range over R.

We claim that A is an ideal

For $x, y \in A$

Therefore $x = r_1 a + s_1 b$

$y = r_2 a + s_2 b$

and so $x \pm y = (r_1 \pm r_2) a + (s_1 \pm s_2) b_2 \in A$

Thirdly For any $u \in R$

$ux = u(r_1 a + s_1 b)$

$= (ur_1) a + (us_1) b \in A$

Since A is an ideal of R

[By theorem. Let R be a Euclidean ring and Let A be a ideal of R then there exist an element $a_0 \in A$ such that A consist exactly of all $a_0 x$ as x ranges over R]

There exist an element $d \in A$ such that every element in A is a multiple

By defn of the fact that

$d \in A$ and that every element of A is of the form $ra + sb$

$d = \lambda a + \mu b$ for some $\lambda, \mu \in R$

we know that,

R has a unit element 1

Thus $a = 1 \cdot a + 0 \cdot b \in A$

$b = 0 \cdot a + 1 \cdot b \in A$

These are both multiple of d

hence d/a and d/b

Suppose Finally that c/a and c/b

then $c/\lambda a$ and $c/\mu b$

So that c certainly divides $\lambda a + \mu b = d$

$\therefore d$ has all the required

greatest common divisor

Defn:- Unit

Let R be a commutative ring with unit element. An element $a \in R$ is a unit in R if there exist an element $b \in R$ such that $ab = 1$

Theorem: 5.3

Let R be an Integral domain with unit element and suppose that for $a, b \in R$ both a/b and b/a are true. then $a = ub$ where u is unit in R

Proof: Since $a/b \Rightarrow b = xa \rightarrow ①$

$b/a \Rightarrow a = ub \rightarrow ②$

$b = xa = x(ub)$

$b = (xu)b$

$xu = 1$

$\therefore u$ is a unit in R

$a = ub$

$a = u(xa)$

$a = (ux)a$

$ux = 1$

$\therefore u$ is a unit in R

$\therefore a = ub$

$\therefore u$ is a unit in R

Defn: Associative

Let R be a commutative Ring with unit element two elements a and b said to be associative if $b = ua$ for some unit u in R

Theorem 5.4

Let R be a Euclidean Ring and $a, b \in R$ if $b \neq 0$ is not a unit in R then $d(a) < d(ab)$.

proof:- Let us consider the ideal A of R

(15) A = ideal generator by a

$A = (a)$

$= \{xa / x \in R\}$

By the defn of Euclidean Ring (i). condition for a $d(a) \leq d(ab)$ $\forall x \neq 0$ in R

Thus d value of a is minimum for the d value of element in A.

Let us consider the ab in A.

ie) $ab \in A$

If $d(a) = d(ab)$.

we have d value of ab is minimal with regard ideal A.

Every element in A is a multiple of ab

In particular,

Since $a \in A \Rightarrow a$ must be a multiple of ab

$a = abx$, $x \in R$

$a = a(bx)$

$\frac{a}{a} = bx$

$1 = bx$

R is an integral domain we have $bx = 1$

[By theorem,

Let R be an integral domain with unit element and suppose that $a, b \in R$ both a/b and b/a true then $a = ub$ where u is a unit in R]

b is unit in R

which is contradiction to b is not a unit in R

$d(a) = d(ab)$ is impossible

Hence $d(a) < d(ab)$.

Prime Element

Definition

In the Euclidean Ring R a non unit π is to be a prime element of R if whenever $\pi = ab$ a, b are in R then one a (or) b is a unit R

Theorem 5.5

Let R be a Euclidean then every element in R is either a unit in R or can be written as a product of a finite number of prime element

Proof:

To Prove the theorem by induction on d(a)

If $a = 1$

$d(a) = d(1)$

Then a is a unit element in R

Let us assume that for all element x in R

$d(x) < d(a)$

If a is a prime number in R

There is nothing to prove

suppose that

$a = bc$ where neither b or c is a unit in R

$d(a) < d(ab)$

$d(b) < d(bc)$ [by definition]

$< d(a)$

$d(b) < d(a)$

$d(c) < d(bc)$

$< d(a)$

$d(c) < d(a)$

Thus by our assumption hypothesis b and c can be written as product of finite number of prime elements of R

$b = \pi_1, \pi_2, \pi_3, \ldots, \pi_n$

$c = \pi_1', \pi_2', \pi_3', \ldots \pi_m'$

Where π and π' are prime elements in R

Consequently

$a = bc = \pi_1 \pi_2 \pi_3 \cdots \pi_n \pi_1' \pi_2' \pi_3' \cdots \pi_m' \cdots$

Hence, It has been factorized as the product of a finite number of element

Hence Proved.

Seminar

Definition (1) — particular Euclidean Ring

Samira

Let $J[i]$ denote the set of all complex number of the form $a+ib$ where a and b are integer under the usual addition and multiplication of the complex number $J[i]$ forms integral domain is called the domain of Gaussian integers

Note:

A function $d(x)$ defined for every non zero element in $J[i]$

i) $d(x)$ is non-negative for every $x \neq 0$ in $J[i]$

ii) $d(x) \leq d(xy)$ for every $y \neq 0$ in $J[i]$

iii) given $u, v \in J[i]$ there exist $t, r \in J[i]$ such that $v = tu + r$ where $r = 0$ (or) $d(r) < d(u)$

Proof:

We have to introduce a function $d(x)$ for every non-zero element in $J[i]$

(i) $d(x)$ is the non-negative integer for every $x \neq 0$ in $J[i]$

Let us define a function d, as follows

Let $x = a+ib$ be a non-zero element in $J[i]$

define $d(x) = a^2 + b^2$

By define d we have $d(x)$ is non-negative integer in face if $x \neq 0$ in $J[i]$

we have, $d(x) \geq 1$

∴ condition (i) is satisfied.

ii) For any two complex number not necessary

$$d(xy) = d(x)d(y)$$

Let $x = a+ib$; $y = c+id$

where a, b, c, d are integers

$$xy = (a+ib)(c+id)$$

$$= ac + iad + ibc - bd$$

$$= (ac-bd) + i(ad+bc)$$

$$d(xy) = (ac-bd)^2 + (ad+bc)^2$$

$$= a^2c^2 + b^2d^2 - 2acbd + a^2d^2 + b^2c^2 + 2ad$$

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

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

$$d(xy) = d(x)d(y) \rightarrow (1)$$

In particular if $x, y \in J[i]$

we have $d(xy) = d(x)d(y)$

Also if $y \neq 0$ in $J[i]$ then $d(y) \geq 1$

$$d(x) = d(x) \cdot 1$$

$$\leq d(x) \cdot d(y)$$

$$d(x) \leq d(xy)$$

Condition (ii) is satisfied

We have to Prove (iii) condition for a given $x, y \neq$ in $J[i]$

There exist $t, r \in J[i]$ such that $y = tx + r$ where $r = 0$ (or) $d(r) < d(x)$ (1)

Theorem: 5.6

$J[i]$ is an Euclidean Ring

Proof:

We have to consider this special case.

Given $x, y \in J[i]$ there exists $t, r \in J[i]$ such that $y = tx + r$ where $r = 0$ (or) $d(r) < d(x)$

y is arbitrary in $J[i]$ and x is an (ordinary) positive integer n

Since $y \in J[i]$

(19) We have $y = a + ib$ where a and $b \in Z$

By the division algorithm for the integer a, b, n there exist a positive integer u, v such that $a = un + u_1$, $b = vn + v_1$, where u_1 and v_1 are integers satisfying $|u_1| \leq \frac{1}{2}n$ and $|v_1| \leq \frac{1}{2}n$

Let $t = u + iv$ and $r = u_1 + iv_1$

$$y = a + ib$$
$$= (un + u_1) + i(vn + v_1)$$

Also
$$= n(u + iv) + (u_1 + iv_1)$$

$$d(r) = d(u_1 + iv_1)$$
$$= u_1^2 + v_1^2$$
$$\leq n^2/4 + n^2/4$$
$$= 2n^2/4$$
$$= n^2/2 < n^2$$
$$d(r) < d(n)$$

In this case $y = tn + r$ where $r = 0$ (or) $d(r) < d(n)$

Let us consider the general case $x \neq 0$ and y be two arbitrary elements in $J[i]$

Then $x\bar{x}$ is an arbitrary positive integer n where $\bar{x}$ is the complex conjugate of x

Applying the case to the element $y\bar{x}$ and n There exists an elements $t, r \in J[i]$ such that $y\bar{x} = tn + r$ with $r = 0$ (or) $d(r) < d(n)$

Putting into this relation $n = x\bar{x}$

Now, $y = tx \neq 0$

$$r = y\bar{x} - tn.$$
$$r = y\bar{x} - t(x\bar{x})$$
$$d(r) < d(n)$$

$\Rightarrow d(y\bar{x} - t(x\bar{x})) < d(x\bar{x})$

$\Rightarrow d[(y - tx)\bar{x}] < d(x)\, d(\bar{x})$

$d(y - tx)\, d(\bar{x}) < d(x) d(\bar{x})$

since $x \neq 0$

$d(\bar{x})$ is positive integer

$d(y - tx) < d(x)$

$\Rightarrow r_0 = y - tx$

Put $y = tx + r_0$

Then t and r_0 are in $J[i]$ and we have

either $d(r_0) \leq d(x)$ (or) $r_0 = 0$

$y = tx + r_0$ with $r = 0$ (or) $d(r_0) <$

Hence $J[i]$ is Euclidean Ring.

Theorem : 5-7

Let p be a prime integer and suppose that fo some integer c relatively prime to p. we can fi integers x and y such that $x^2 + y^2 = cp$ then p can be written as the sum of square of two int that is there exists integer a and b such that $p = a^2 + b^2$

Proof :- The ring of integer is a subring of $J[i]$

suppose that the integer p is also a prime eleme of $J[i]$ Since $cp = x^2 + y^2 = (x + iy)(x - iy)$

By theorem 5-5

If π is a prime element in the Euclidean ring R nd π / ab where $a, b \in R$

Then π divides atleast one of a (or) b

$p / (x + iy)$ (or) $(x - iy)$ in $J[i]$

But if $p / x + iy$

Then $(x+yi) = p(u+vi)$

which would say that $x = pu$ and $y = pv$. so that p also ~~called~~ would divide $x-yi$

(21) But then $p^2 / (x+yi)(x-yi) = cp$

$\therefore p^2 / cp$

$\therefore p/c$ which is $\Rightarrow\Leftarrow$ to $(c,p)=1$

IIIly. If $p/(x-yi)$

Then p is not a prime element in $J[i]$

Let $p = (a+bi)(g+di)$

Where $a+bi$ and $g+di$ are in $J[i]$ and where neither $a+bi$ nor $g+di$ is a unit in $J[i]$

But this means that neither $a^2+b^2=1$ nor $g^2+d^2=1$ From $p=(a+bi)(g+di)$ it follows easily that $\bar{p} = (a-bi)(g-di)$

Thus $p^2 = (a+bi)(g+di)(a-bi)(g-di)$

$p^2 = (a^2+b^2)(g^2+d^2)$

$\therefore (a^2+b^2) / p^2$

By cauchy theorem

p or p^2

so, $a^2+b^2 = 1$

$a^2+b^2 \neq 1$

Since $a+bi$ is not a unit in $J[i]$

$a^2+b^2 \neq p^2$

$\therefore$ otherwise $g^2+d^2=1$

Which is $\Rightarrow\Leftarrow$ to $g+di$ is not a unit in $J[i]$

Thus only possibility left is that $a^2+b^2=p$

Theorem 5-8.

If p is a prime number of the form $4n+1$ then we can solve the congruence $x^2 \equiv -1 \pmod{p}$

proof.

Let $p = 4n+1$

$p-1 = 4n$

$\frac{P-1}{2} = 2n$

Let $x = 1 \cdot 2 \cdot 3 \cdots \frac{P-1}{2} \rightarrow ①$

Since $P-1 = 4n$ is an even number then even number of form n the product of x

$x = (-1)(-2) \cdots (-(\frac{P-1}{2}))$

Clearly $P/P = P/P-k+k$

$= P/(P-k)-(-k)$

$= P-k \equiv -k \pmod P$

Since $a \equiv b \pmod p$ iff $P/a-b$

Now $x = (-1)(-2) \cdots (-(\frac{P-1}{2}))$

$x = (P-1)(P-2) \cdots (P-(\frac{P-1}{2})) \rightarrow ②$

From ① and ②

$x \cdot x = 1 \cdot 2 \cdots (\frac{P-1}{2})(\frac{P+1}{2}) \cdots (P-1)$

$= (P-1)!$

$x^2 \equiv (-1) \pmod p$

Theorem : 5.9 Fermat is Theorem

If P is a prime number of the form $4n+1$, then $P = a^2+b^2$ for some integer a and b

Proof:

By theorem 5.8. $x^2 \equiv -1 \pmod p$

There exist an x such that

$x^2 \equiv (-1) \pmod p \rightarrow ①$

We can choose x so that $0 \leq x \leq P-1$, $x \leq P/2$

Let $x > P/2$

then $y = P-x$

$y^2 = (P-x)^2 = P^2 + x^2 - 2Px$

$y^2 - x^2 = P^2 - 2Px$

$= P(P-2x) \rightarrow ②$

Clearly P/P

$\Rightarrow P/P(P-2x)$

$\Rightarrow p / y^2 - x^2$

$y^2 \equiv x^2 \pmod p$ [by ②]

(23)

$y^2 \equiv -1 \pmod p$ (by ①)

Also, $x > p/2$

$-x < -p/2$

$p - x < p - p/2$

$p - x < p/2$

$y < p/2$

Which is not possible

Assume that

$x \leq p/2$ and $x^2 \equiv -1 \pmod p$

$x^2 + 1 \equiv 0 \pmod p$

$\Rightarrow p / (x^2+1)$

$(x^2+1) = cp$

cp is an integer

Now, $cp = x^2 + 1 \leq (p/2)^2 + 1$

$\leq p^2/4 + 1$

$cp \leq p^2$

$c \leq p$

$\Rightarrow p \not| c$

c and p is relatively prime

We know that, [by theorem 5.E]

If p is relatively prime to some integer then $p = a^2 + b^2$ where $a, b \in Z$.

Definition:

Polynomial Ring:

Let R be a ring. A polynomial $F[x]$ with co-efficien in a real number is defined to be an expression of the form $a_0 + a_1 x + \cdots + a_n x^n$ where n is positive integer and $a_0, a_1, \ldots a_n \in R$ the set of all polynomial with coefficient in R denoted by $R[x]$.

Definition: Polynomial Multiplication.

If $p(x) = a_0 + a_1 x + \cdots + a_m x^m$

$q(x) = b_0 + b_1 x + \cdots + b_n x^n$ and are in

$p(x) \cdot q(x) = c_0 + c_1 x + \cdots + c_k x^k$

where $c_t = a_t b_0 + a_{t-1} b_1 + \cdots + a_0 b_t$

Definition: Polynomial Addition.

If $p(x) = a_0 + a_1 x + \cdots + a_m x^m$

$q(x) = b_0 + b_1 x + \cdots + b_n x^n$ and are both $F[x]$. then $p(x) + q(x) = c_0 + c_1 x + \cdots + c_t x^k$

For each $c = a_i + b_i$

Example: $p(x) = 1 + x - x^2$ $q(x) = 2 + x^2 + x^3$

$p(x) \cdot q(x) = (1 + x - x^2)(2 + x^2 + x^3)$

$= 2 + x^2 + x^3 + 2x + x^3 + x^4 - 2x^2 - x^4 - x^5$

$= 2 - x^2 + 2x^3 + 2x - x^5$

$= -x^5 + 2x^3 - x^2 + 2x + 2$

$\Rightarrow 2 + 2x - x^2 + 2x^3 - x^5$

Definition: Degree of Polynomial

If $f(x) = a_0 + a_1 x + \cdots + a_n x^n \neq 0$ and $a_n \neq 0$ the degree of $f(x)$ written as $\deg f(x)$ is n a polynomial is a constant if its degree is 0

Theorem 5.10

If $f(x), g(x)$ are two non-zero elements of $F(x)$. then $\deg (f(x) g(x)) = \deg f(x) + \deg g(x)$

Proof: Let $f(x) = a_0 + a_1 x + \cdots + a_m x^m$

$a_m \neq 0$, $a_i = 0 \quad \forall i > m$

$g(x) = b_0 + b_1 x + \cdots + b_n x^n$

$b_n \neq 0$; $b_j = 0 \quad \forall j > n$

$\deg f(x) = m$

$\deg g(x) = n$

by definition

Now, $f(x) g(x) = c_0 + c_1 x + \cdots + c_k x^k$

Where $c_t = a_0 b_t + a_1 b_{t-1} + \cdots + a_{t-1} b_1 + a_t b_0$

ie) To prove $c_{m+n} \neq 0$ and $c_i = 0 \ \forall \ i > m+n$

Now, $c_{m+n} = a_0 b_{m+n} + a_1 b_{m+n-1} + \cdots + a_{m-1} b_{n+1} + a_m b_n$

Where $a_m \neq 0$, $b_n \neq 0$

$c_{m+n} = a_m b_n \neq 0$

$\Rightarrow a_j \ b_{i-j} = 0$

$\Rightarrow c_{j+i-j} = 0$

$c_i = 0 \quad \forall \ i > m+n$

$\deg [f(x) g(x)] = m+n$

$\deg [f(x) g(x)] = \deg f(x) + \deg g(x)$

Corollary:

If $f(x), g(x)$ are non-zero element in $F[x]$ then $\deg f(x) \leq [\deg f(x) g(x)]$

Proof: If $f(x), g(x)$ are non-zero element

$\deg [f(x) g(x)] = \deg f(x) + \deg g(x)$

but $\deg g(x) \geq 0$

$\deg [f(x) g(x)] \geq \deg f(x)$

$\deg f(x) \leq \deg [f(x), g(x)]$

Theorem: 5.11 — **Division Algorithm**

Given two polynomial $f(x)$ and $g(x) \neq 0$ in $F[x]$ then $f(x) = t(x) g(x) + r(x)$ where $r(x) = 0$ (or) $\deg r(x) < \deg g(x)$

Proof: Case (i) Suppose $\deg f(x) < \deg g(x)$

Take $t(x) = 0 \quad r(x) = f(x)$

$f(x) = t(x) g(x) + r(x)$

$= 0 \times g(x) + f(x)$

Where $\deg f(x) < \deg g(x)$ or $f(x) = 0$

case (ii)

Suppose $\deg f(x) \geq \deg g(x)$

Let $f(x) = a_0 + a_1 x + \cdots + a_m x^m$, $a_m \neq 0$

$\deg f(x) = m$

$g(x) = b_0 + b_1 x + \cdots + b_n x^n \quad b_n \neq 0$

$\deg g(x) = n$

$m \geq n$

Let $f_1(x) = f(x) - \left(\frac{a_m}{b_n}\right) x^{m-n} g(x) \rightarrow (1)$

$\deg f_1(x) \leq m-1$

$\deg f_1(x) < \deg g(x)$

So by induction on the degree of $f(x)$. we may assume by case (i) — There exist $t_1(x)\ r(x) \in f(x)$

$$f_1(x) = t_1(x)\, g(x) + r(x) \longrightarrow (2)$$

Where $r(x) = 0$ (or) $\deg r(x) < \deg g(x)$

But then

$$f(x) - \left(\frac{a_m}{b_n}\right) x^{m-n} g(x) = t_1(x)\, g(x) + r(x)$$

$$f(x) = \left[\left(t_1(x) + \left(\frac{a_m}{b_n} x^{m-n}\right)\right) g(x)\right] + r(x)$$

$$f(x) = t(x)\, g(x) + r(x)$$

Where either $r(x) = 0$ (or) $\deg r(x) < \deg g(x)$)

Corollary:- $F[x]$ is an integral domain

Proof:- The function $\deg f(x)$ defined for all $f(x) \neq 0$ in $F[x]$ satisfies

i) $\deg f(x)$ is an non-negative integer.

ii) $\deg f(x) \leq \deg (f(x)\, g(x))$

In order for $F[x]$ to be Euclidean ring with the degree acting as a function of Euclidean ring as still need that given $f(x), g(x) \in F[x]$

There exists $t(x)\ r(x)$ in $F[x]$ such that

$\therefore f(x) = t(x)\, g(x) + r(x)$

where either $r(x) = 0$ (or) $\deg r(x) < \deg g(x)$

$r(x) = f(x)$ no zero divisor
$r(x) = 0$ so $f(x)$ has so, it's an I.D (5)

Theorem : 5.12

$F[x]$ is an Euclidean ring

Proof :- [By theorem 5-11]

Given two polynomial $f(x)$ and $g(x) \neq 0$ in $F[x]$ then there exists two polynomial $t(x)$ and $r(x)$ in $f(x)$ such that

$f(x) = t(x)\, g(x) + r(x)$

Where $r(x) = 0$ (or) $\deg r(x) < \deg g(x)$

Hence $F[x]$ is an Euclidean ring (6)

Theorem: 5.13

$F[x]$ is an principle Ideal Ring.

Proof :- we know that, Every Euclidean ring is a principle ideal ring.

$F[x]$ is an Euclidean Ring [by thm 5-12]

$\therefore F[x]$ is an principle ideal Ring.

Corollary :- Theorem but no proof

Given two polynomial $f(x), g(x)$ in $F[x]$ they have a greatest common divisor $d(x)$ which can be realized as $d(x) = \lambda(x) f(x) + \mu(x) g(x)$

Definition :- Irreducible

A polynomial $p(x)$ in $F[x]$ is said to be irreducible over F if whenever $p(x) = a(x) b(x)$ with $a(x), b(x) \in F[x]$ then one of $a(x)$ or $b(x)$ has degree 0 [ie), is a constant]

Ex:- Irreducibility depends on the field for instance the polynomial x^2+1 is irreducible over the real field : but not over the complex

field, for there $(x^2+1) = (x+i)(x-i)$. where

Theorem: 5.14 Refer theorem 5.23

Any polynomial p_n $F[x]$ can be written in a u manner as a product of irreducible polynomials in $F[x]$ (1)

Theorem 5.15

The ideal $A = (p(x))$ in $F[x]$ is a maximal ideal iff $p(x)$ is irreducible over F

Proof: we know that $F = R$ (Unit-III) 28

$p(x) = x^2+1 \in R[x]$

If $p(x) = (x-r_1)(x-r_2)$

$\Rightarrow p(r_1)=0$ and $p(r_2)=0$

$\Rightarrow r^2+1=0$

$\Rightarrow r^2=-1$

$\Rightarrow$ no such $r \in R$ exist

$\Rightarrow p(x)$ contradicts to reducible

Then $p(x) = x^2+1$ is ideal

$\Rightarrow (x^2+1)$ is maximal

$\Rightarrow F[x]/(x^2+1)$ is a field

[By theorem, Let R be a commutative ring with identity, An ideal M of R is maximal iff R/M is a field]

$\therefore (x^2+1)$ is maximal

$(p(x))$ is maximal

Conversely, Assume $(p(x))$ is maximal

If I is an ideal of $F[x]$ and diff of maximal ideal

$(p(x)) \subseteq I \subseteq F[x]$

$M \subset U \subset R$

$U = M$ or $U = R$

$\Rightarrow I = (p(x))$ or $I = F[x]$

Suppose, $p(x) = q(x)r(x)$

then $(p(x)) \subseteq (q(x)) = I$

Thus $(q(x)) = (p(x)) \rightarrow (1)$

(or) $(q(x)) = F[x]$ → ②

② ⇒ $1 \in (q(x))$

$\Rightarrow 1 = q(x)\, g(x)$.

$\deg(1) = \deg(q(x)) + \deg(g(x))$

$0 = \deg(q(x)) + \deg(g(x))$

$\Rightarrow \deg(q(x)) = 0$ and $\deg(g(x)) = 0$

If $g(x)$ is unit then $p(x) = q(x)\, r(x)$ is not a reduction of $p(x)$

① ⇒ $(q(x)) = (p(x))$

$p(x) = p(x) \cdot 1 \in (p(x)) = (q(x))$

$\Rightarrow p(x) = q(x)\, \Delta(x)$

$\deg(p(x)) \leq \deg(q(x))$

there exist $\Delta(x)$ such that

$q(x) = p(x)\, \Delta(x)$

$\deg(q(x)) \leq \deg(p(x))$

then, $\deg(p(x)) = \deg(q(x))$

$\Rightarrow \deg(p(x)) = 0$

$p(x) = q(x)\, r(x)$ is not a reduction

Suppose $p(x)$ is irreducible

Let I be an ideal with $(p(x)) \subseteq I \subseteq F[x]$ (an ideal with unit element)

$F[x]$ is principle ideal domain.

Since, every ideal is principle ideal domain

∴ there exist $g(x) \in F[x]$ such that $I = (g(x))$

$\Rightarrow p(x) \in (g(x))$

$\Rightarrow p(x) = g(x)\, r(x)$

$\Rightarrow g(x)$ or $r(x)$ is a unit

$\Rightarrow I = F[x]$ (or) $(p(x)) = (g(x)) = I$ ①

∴ $p(x)$ is irreducible. Hence proved

Primitive polynomials

on:

The polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ where the $a_0, a_1, a_2 \ldots a_n$ are integers is said to be primiti the common divisors of $a_0, a_1, \ldots a_n$ is 1

Ex: $5x^3 + 2x^2 + 3x + 1$ not a primitive e

$(5, 2, 3, 1) = 1$

Theorem: 5.16

If $f(x)$ and $g(x)$ are primitive polynomials then $f(x)g(x)$ is primitive polynomials

[or]

The product of two primitive polynomials is again a primitive polynomial

Proof: Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$

$g(x) = b_0 + b_1 x + \cdots + b_m x^m$ be two Primitive polynomials

Let $f(x)\, g(x) = c_0 + c_1 x + \cdots + c_{m+n} x^{m+}$

where $c_i = a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0$

To prove, $f(x)\, g(x)$ is primitive polynomial

Suppose $f(x)g(x)$ is not a primitiv Polynomial

Hence all the coefficients of $f(x)\, g(x$ are divisible by some integer larger than 1.

$f(x)\, g(x)$ divisible some prime numbers

Since $f(x)$ is primitive p does not divide somecoefficient of $f(x)$

let a_r be the first coefficient of $f(x)$, divisible by p p/a_0, p/a_1, $\cdots$, p/a_{r-1} and $p \nmid a_r$

Since $g(x)$ is primitive p does not divides so coefficient of $g(x)$

Let b_s be the first coefficients of $g(x)$ not divisible by p

p/b_0, p/b_1, $\cdots$, p/b_{s-1} and $p \nmid b_s$ $\rightarrow (2)$

Now, the coefficient of x^{r+s} in $f(x)g(x)$

$$c_{r+s} = (a_0 b_{r+s} + a_1 b_{r+s-1} + \cdots + a_{r-1} b_{s+1}) + (a_r b_s) + (a_{r+1} b_{s-1} + \cdots + a_{r+s} b_0)$$

3) From ① & ② we get

$$P / a_0 b_{r+s} + a_1 b_{r-1+s-1} + \cdots + a_{r-1} b_{s+1}$$

$$P / a_{r+1} b_s + \cdots + a_{r+s} b_0$$

But $P \nmid a_r b_s$ then $P \nmid c_{r+s}$

Which is $\Rightarrow \Leftarrow$ to P / c_{r+s}

$f(x)g(x)$ is a primitive polynomial

Hence proved

Definition — **Content**

The content of the polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ where the a's are integers is the greatest common divisor of the integers $a_0, a_1, \cdots, a_n$

Clearly given any polynomial $p(x)$ with integer coefficient it can be written as $p(x) = dq(x)$ where $q(x)$ is a primitive polynomial

Ex: $5x^3 + 10x^2 + 15x + 5$

$5/10 \quad 5/15 \quad 5/5 \quad 5 = (5, 10, 15)$

Theorem : 5.1 — **Gauss Lemma.**

The Primitive polynomial $f(x)$ can be factored as a product of two polynomials having rational coefficients. It be factored as a product of two polynomial having integer coefficients

Proof: Suppose that $f(x) = u(x) \cdot v(x)$

Where $u(x)$ and $v(x)$ are having rational coefficients

Taking out the common factor are have,

$$f(x) = \frac{a}{b} [\lambda(x)\, \mu(x)] \rightarrow ①$$

Where a and b are integer and where both $\lambda(x)$ and $\mu(x)$ are polynomial having intege

coefficients and are primitive ④ implies

$$b f(x) = a(\lambda(x) \cdot \mu(x)) \quad \cdots$$

$\lambda(x)$ and $\mu(x)$ are primitive

The content of the LHS is b

The content of the RHS is a.

$$a = b$$

$$\Rightarrow \frac{a}{b} = 1$$

① becomes

$$f(x) = \lambda(x) \cdot \mu(x)$$

where $\mu(x)$, $\lambda(x)$ are two polynomial having integer coefficients

Definition (4) Integer Monic (5)

A polynomial is said to be an integer monic if all its coefficients are integers and its highest coefficient 1. Thus an integer monic polynomial is merely one of the form $x^n + a_1 x^{n-1} + \cdots + a_n$ where the a's are integers. clearly an integer monic polynomial is primitive

Ex: $2x^2 + 3x^3 + x^5$ [x^5 is coefficient

Theorem: 5.18 The Eisenstein theorem

Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ be a polynomial with integer co-efficients Suppose that for some prime number p. $p \nmid a_n$ $\cdot\cdot$ $p \mid a_1$, $p \mid a_2$, $\cdots$ $p \mid a_0$, $p^2 \nmid a_0$ then $f(x)$ is irreducible over the rationals.

Proof: Without loss of generality, we may assume that $f(x)$ is primitive

Taking out the greatest common factor of its coefficient does not distrub the hypothes

33 since $P \nmid a_n$

If $f(x)$ factors as a product of two rational polynomials By Gauss Lemma

it $f(x)$ factories as the product of two polynomials having integer coefficients

Claim :

Suppose we assume that $f(x)$ is reducible

ie) $f(x) = (b_0 + b_1 x + \cdots + b_r x^r) \cdot (c_0 + c_1 x + \cdots + c_s x^s) \rightarrow (1)$

where the b's and c's are integers and where $r > 0$ and $s > 0$

$a_0 = b_0 c_0$

P must divide one of b_0 (or) c_0

since $P^2 \nmid a_0$

P cannot divide both b_0 and c_0

Suppose that $P \mid b_0$ and $P \nmid c_0$

Not all the co-efficients $b_0, \ldots, b_r$ can be divisible by P, otherwise all the coefficients of $f(x)$ would be divisible by P

which is $\Rightarrow \Leftarrow$

Let b_k be the first b not divisible by P

$k \leq r < n$

Thus $P \mid b_{k-1}$ $P \mid b_{k-1}$

Equating the k^{th} coefficients in (1) by the theorem 5.1b we get, $a_k = b_k c_0 + b_{k-1} c_1 + b_{k-2} c_2 + \cdots + b_0 c_k$

and $P \mid a_k$, $P \mid b_{k-1}, b_{k-2}, \ldots, b_0$

so that $p / b_k c_0 \rightarrow p / b_k$ (or) p / c_0

But $p \nmid c_0$ and $p \nmid b_k$

$\Rightarrow\Leftarrow$ Hence $f(x)$ is irreducible.

Hence proved

Prove that polynomial $f(x) = x^2 + 8x - 2$ is irreducible over $\mathbb{Q}$.

Solution Hence $a_0 = -2$, $a_1 = 8$, $a_2 = 1$

Let $p = 2$

Clearly, p / a_0, p / a_1 2/2, 2/8

$p \nmid a_2$, $p^2 \nmid a_0$. 4/2

$\therefore$ By Eisenstein Criterion $f(x)$ is irreducible over $\mathbb{Q}$.

Polynomial Ring over a commutative Ring

Let R be a commutative ring with unit element by the polynomial ring in x over R $[x]$. we shall mean the set of formal symbols $a_0 + a_1 x + \cdots + a_m x^m$ where $a_0, a_1, \ldots a_m$ are in R

The above polynomial ring $R[x]$ is a commutative ring with unit element

Let us define the ring of polynomial in 'n' variables $x_1, x_2, \ldots x_n$ over R namely. $R[x_1, x_2, \ldots x_n]$ is as follows

$R_n = R_{n-1}[x_n]$

Hence R_n is

Let $R_1 = R[x_1]$ $R_2 = R_1[x_2]$

The polynomial ring in x_2 over $R_1, R_2, \ldots R_n = R_{n-1}[x_n]$ R_n is called the ring of polynomial in $x_1, x_2 \cdots x_n$ over R.

Ill'y $R_n = R_{n-1}[x_n]$

Hence R_n is called the ring of polynomial is in n variables $x_1, x_2, \ldots x_n$ over R

35 $\therefore R[x_1, x_2 \ldots x_n]$ is the polynomial in n variables $x_1, x_2, \ldots, x_n$

Theorem: 5.19

If R is an Integral domain then so is $R[x]$

Proof: Let R be an Integral domain

we have to prove that

$R[x]$ is an Integral domain

we know that $R[x]$ is a commutative ring with unit element It is enough to prove that $R[x]$ has no zero divisor

Let $f(x) \neq 0$ and $g(x) \neq 0$ be any two element in $R[x]$.

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m$$

deg $f(x) = m$ $\quad a_m \neq 0$

$$g(x) = b_0 + b_1 x + \cdots + b_n x^n$$

deg $g(x) = n$ $\quad , b_n \neq 0$

R is an Integral domain

deg $[f(x)g(x)]$ = deg $f(x)$ + deg $g(x)$

$= m + n$

but for $f(x) \neq 0$ and $g(x) \neq 0$

It is impossible to have $f(x)g(x) = 0$. This implies that for $f(x) \neq 0$, $g(x) \neq 0$

we have $f(x) \cdot g(x) \neq 0$

$R[x]$ is an Integral domain

Corollary:

If R is an Integral domain $R[x_1, x_2, \ldots, x_n]$ is also an Integral domain

Proof: Let us assume that R is an integral domain. Let $R_1 = R[x_1]$

By theorem : If R is an integral domain $R[x]$ is an Integral domain.]

$R[x_1]$ is an integral domain

ie) R_1 is an integral domain

Again Let $R_2 = R_1[x_2]$

$\Rightarrow R_2$ is an integral domain

since R is an integral domain

$\Rightarrow R_1[x_2]$ is an integral domain

$R_2 = R[x_1, x_2]$ is an integral domain

Proceeding like this we get

$R[x_1, x_2, \ldots, x_n]$ is an integral domain

If R is an integral domain

Hence proved.

Definition Unique Factorization

An Integral domain R with unit element is a unique factorization domain

a) Any non-zero element in R is either a unit o can be written as the product of a finite number irreducible element of R

b) The decomposition in part (a) is unique upt the order and associates of the irreducible eleme

Theorem : 5.20

If R is a unique factorization domain and if a, b are in R. then a and b have a greatest common divisor (a, b) in R Moreover, if a and b are relatively prime (ie) (a, b) = 1 whenever a/c

Proof.

Since (a, b) = 1

There exist $x, y \in R$ such that $ax + by = 1$

$\therefore acx + bcy = 1$

Now, a/acx

Also $a/bc \Rightarrow a/bcy$.

$\therefore a/acx + bcy$

Hence a/c

Corollary :-

If $a \in R$ is an irreducible element and a/bc then a/b or a/c

Proof :- suppose a does not divide b

then $(a, b) = 1$ [since a is prime]

By theorem 5.20 $\therefore a/c$

Theorem : 5.21

If R is a unique Factorization domain then the product of two primitive polynomials in $R[x]$ again a primitive polynomial in $R[x]$

Proof :-

Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$

$g(x) = b_0 + b_1 x + \cdots + b_m x^m$ be two Primitive polynomials in $R[x]$

Let P be any irreducible element in R

since $f(x)$ and $g(x)$ are primitive polynomials

P does not divide a_i's and p does not divide all b_j's

Let a_r be the first coefficient of $f(x)$ not divisible by P.

$P/a_1, P/a_2, \cdots P/a_{r-1} \rightarrow ①$ and $P \nmid a_r$

Let b_s be the first coefficient of $g(x)$ not divisible by P

$P/b_1, P/b_2, \cdots, P/b_{s-1} \rightarrow ②$ and $P \nmid b_s$

Now, the coefficient of x^{r+s} in $f(x)\,g(x)$ is given by

$$c_{r+s} = (a_0 b_{r+s} + a_1 b_{r+s} + \cdots + a_{r-1} b_{s+1}) + a_r b_s + (a_{r+1} b_{s-1} + \cdots + a_{r+s} b_0)$$

From ① & ② we get

$P/(a_0 b_{r+s} + \cdots + a_{r-1} b_{s+1})$

$P/(a_{r+1} b_{s-1} + \cdots + a_{r+s} b_0)$

and $P \nmid a_r b_s$

p does not divide c_r ts

Thus for any irreducible element p in R there exists some coefficient of $f(x)g(x)$ not di by p. Hence $f(x)g(x)$ primitive

Corollary:

If R is unique factorization domain and if $f(x)$, $g(x)$ are in $R[x]$ then $C(fg) = c(f)\,c(g)$

Solu: Given $f(x), g(x)$ in $R[x]$

we can write $f(x) = a\, f_1(x)$

$g(x) = b\, g_1(x)$

Where $f_1(x)$ and $g_1(x)$ are primitive

Thus $f(x)\,g(x) = ab\, f_1(x)\, g_1(x)$

By theorem 5.21 $f(x)\,g(x)$ is primitive

Hence the content of $f(x)\,g(x)$ is ab

(ie) $c(f)\,c(g)$

Theorem: 5.22 $c(fg) = c(f)\,c(g)$.

Let R be a unique factorization domain. Let F be the field of quotients of R. Let $f(x) \in R[x]$ and deg $f(x) > 0$. If $f(x)$ is irreducible in $R[x]$ then $f(x)$ is also irreducible in $F[x]$. Also if $f(x)$ is primitive in $R[x]$ and irreducible in $F[x]$ then $f(x)$ is irreducible in $R[x]$

Proof:

let $f(x) \in R[x]$ and deg $f(x) > 0$

Suppose $f(x)$ is irreducible in $R[x]$ but reducible in $F[x]$

then $f(x) = g(x)\,h(x)$ where $g(x), h(x) \in F[x]$ and are of positive integer

Since F is the field of quotients of R each coefficients of $g(x)$ and $h(x)$ is of the form a/b where $a, b \in R$

By clearing denominators we get

39 $d f(x) = e\, r(x)\, s(x)$ where $r(x), s(x) \in R[x]$

Now By theorem (a)

[Let R be a unique factorization domain. Let $f(x) \in R[x]$ be a non-constant polynomial then $f(x)$ can be written as $f(x) = c\, f_1(x)$ where $c = c(f)$ and $f_1(x) \in R[x]$ is primitive. This decomposition of $f(x)$ as an element of R and a primitive polynomial in $R[x]$ is unique except for multiplication by unit sine].

$f(x) = c\, f_1(x)$, $r(x) = c_1 r_1(x)$ and $s(x) = c_2 s_1(x)$ where $f_1(x), r_1(x), s_1(x)$ are primitive polynomials in $R[x]$.

$\therefore d\, c\, f_1(x) = e\, c_1 c_2 r_1(x) s_1(x)$

[Now by theorem (b).

Let R be a unique factorization Domain the product of two primitive polynomials in $R[x]$ is again a primitive polynomials in $R[x]$]

$r_1(x)\, s_1(x)$ is primitive

Also $f_1(x)$ is primitive

Hence by the uniqueness part of theorem (a)

$e c_1 c_2 = d c u$ where u is a unit in R

$\therefore d\, c\, f_1(x) = d\, c\, u\, r_1(x)\, s_1(x)$

$\therefore c\, f_1(x) = c\, u\, r_1(x)\, s_1(x)$

$\therefore f(x) = c\, u\, r_1(x)\, s_1(x)$ and this is a non-trivial factorization of $f(x)$ in $R[x]$

$\therefore f(x)$ is reducible in $R[x]$ which is a contradiction

$\therefore f(x)$ is irreducible in $F[x]$

Conversely, Suppose $f(x)$ is primitive in $R[x]$ and Irreducible in $F[x]$

We claim that $f(x)$ is irreducible in $R[x]$

Suppose $f(x) = g(x)h(x)$ where $g(x)\ h(x) \in$

Since $R[x] \subseteq F[x]$, we have $g(x)\ h(x)$ $F[$

But $f(x)$ is irreducible in $F[x]$

$\therefore g(x) = k$ and $k \in R$

40 $\therefore f(x) = k \cdot h(x)$ But $f(x)$ is primiti

$\therefore k$ must be unit in R

$\therefore f(x)$ is irreducible in $R[x]$

Hence the theorem.

Theorem 5.23

Let R be a unique factorization domain then any primitiv polynomial $p(x) \in R[x]$ can be factored in a unique way as the product of irreducible elements in $R[x]$.

Proof:- Let F be a quotient field of R

Since $F[x]$ is a unique factorization domain

we can write $p(x) = p_1(x)\, p_2(x) \cdots p_n(x)$ where each $p_i(x)$ is irreducible in $F[x]$

Now, each coefficient in $p_i(x)$ of the form a/b where $a, b \in R$. Hence clearing all denominators we get, $d\, p(x) = e\, q_1(x)\, q_2(x) \cdots q_n(x)$

where $d, e \in R$ and $q_i(x) \in R[x]$

Now, Let $q_i(x) = c_i \cdot r_i(x)$ where $r_i(x)$ is primitive in $F[x]$

Hence $d\, p(x) = e\, c_1 c_2 \cdots c_n\, r_1(x) \cdots r_n(x)$

[Now by theorem.

Let R be a unique factorization domain the product of two primitive polynomial in $R[x]$ is again a primitive polynomial in $R[x]$]

The product $r_1(x)\, r_2(x) \cdots r_n(x)$ is primiti

and by hypothesis it is $p(x)$ is primitive

Hence $d = e c_1 c_2 \cdots c_n$ [by the uniqueness contents]

$\therefore d\, p(x) = d\, u r_1(x) r_2(x) \cdots r_n(x)$

$p(x) = u r_1(x) r_2(x) \cdots r_n(x)$

Now, since each $p_i(x)$ is irreducible in $F[x]$

$r_i(x)$ is also irreducible in $F[x]$

Further each $r_i(x)$ is primitive

[Hence By theorem, Let R be unique factorization domain. Let F be the field of quotient of R. Let $f(x) \in R[x]$ and deg. $f(x) > 0$. If $f(x)$ is irreducible in $F[x]$. Also if $f(x)$ is primitive in $R[x]$ and irreducible in $F[x]$ then $f(x)$ is irreducible in $R[x]$].

$r_i(x)$ is irreducible in $R[x]$

Thus $p(x)$ is a product of irreducible factor in $R[x]$. Now, we prove that the uniqueness of Factorization. Let $p(x) = s_1(x)\, s_2(x) \cdots s_n(x)$ be another factorization of $p(x)$ where each $s_i(x)$ is irreducible in $R[x]$.

Since $p(x)$ is primitive each $s_i(x)$ is primitive. Hence $s_i(x)$ is irreducible in $F[x]$

Now, since $F[x]$ is a union Factorization Domain we see that $r_i(x)$ and $s_i(x)$ are equal upto associative in some order

Hence $p(x)$ has a unique factorization as a product of irreducible element in $R(x)$

rem: 5.24 (4) V.U.

R is a unique factorization Domain so in R[x]

Proof: Given R is a unique factorization Domain

Claim:- R[x] is a unique factorization D

Let f(x) be an arbitrary element in R[x]

$f(x) = c f_1(x)$ where $c = c(f)$

$f_1(x) \in R[x]$ is primitive

By theorem 5.23

we can decompose $f_1(x)$ in a unique way as the product of irreducible elements of R[x].

suppose that $c = a_1(x) \cdot a_2(x) \cdots a_m(x)$ in R[x] then $0 = \deg a_1(x) + \deg a_2(x) + \cdots + \deg a_m$

Each $a_i(x)$ must be degree 0.

ie) the only factorization of c as an element of R[x] also its an element of R.

In particular,

An irreducible element in R is irreducible in R[x]

Since R is a unique factorization Domain and c has a unique factorization as a product of irreducible element of R[x]

Repeated

c has a unique factorization as a product of irreducible element of R[x]

Also $f(x) = c \cdot f_1(x)$ where $c = c(f)$

Hence f(x) has a unique factorization as the product of irreducible element in R[x]

Hence Proved.

Corollary: 1

If R is a unique factorization Domain then so is $R[x_1, \cdots x_n]$ a special case of corollary

but of independent interest and importance.

Corollary - 2

If F is a field then $F[x_1, \ldots, x_n]$ is a unique factorization.

Relatively prime :

In the Euclidean ring R. a and b in R are said to be the relatively prime if their greatest common divisor is a unit of R.

Theorem 5.25

Let R be a Euclidean ring suppose that for $a, b, c \in R$ a/bc but the $(a, b) = 1$ then a/c

Proof ..... [: By theorem 5:20]

Theorem : 5-26

If π is a prime element in Euclidean ring R. and π/ab where $a, b \in R$ then π divides atleast one of a (or) b

proof Corollary 5.20

Corollary :

If π is a prime element in the euclidean ring R and $\pi/a_1, a_2, \ldots, a_n$ then π divides atleast one $a_1, a_2, \ldots a_n$

Theorem 5.27 unique factorization theorem

Let R be a Euclidean Ring and $a \neq 0$ a non-unit in R. suppose that $a = \pi_1, \pi_2, \ldots \pi_n = \pi_1', \pi_2', \ldots \pi'_n$ where the π_i and π_j are prime elements of R. Then $n = m$ and each π_j $(1 \leq i \leq n)$ is associative of some π_j' $(i \leq j \leq m)$ and conversely. each π'_k is an associative of some π_q

Proof :- Let R be a Euclidean Ring. and $a \neq 0$ be a non-unit element of R.

Let $a = \pi_1 \pi_2 \ldots \pi_n = \pi_1' \pi_2' \ldots \pi_m'$

clearly $\pi_1 / \ldots$ for some i

$\Rightarrow \pi_1 / \pi_1 \pi_2 \cdots \pi_n \Rightarrow \pi_1 / \pi_1' \pi_2' \cdots$

theorem 5.7

If π is a prime element in the Euclidean ring R and π / ab where $a, b \in R$ then π divide least one of a (or) b].

π_1 divides atleast of $\pi_1' \pi_2' \cdots \pi_n'$ without loss of generality.

Let us assume that π_1 / π_1' since π_i and are both prime elements of R

π_1 and π_1' must be associatives

By definition

$\pi_1' = u_1 \pi_1$ where u_1 is unit in R

Now, $\pi_1 \pi_2 \cdots \pi_n = \pi_1' \pi_2' \cdots \pi_{i-1}' \pi_i' \pi_{i+1}' \cdots$

$\pi_1 \pi_2 \cdots \pi_n = \pi_1' \pi_2' \cdots \pi_{i-1}' \pi_1 u_1 \pi_{i+1}' \cdots$

$\pi_2 \cdots \pi_n = \pi_1' \pi_2' \cdots \pi_{i-1}' u_1 \pi_{i+1}' \cdots \pi_m'$

Repeat the arrangement on this oclation with π_2 we ge

$\pi_3 \pi_4 \cdots \pi_n = u_1 u_2 \pi_1' \pi_2' \cdots \pi_{i-1}' \pi_{i+1}' \cdots \pi_{j-1}' \pi_j \cdots \pi_m'$

Now, If $n < m$

After n-steps the left side becomes 1 and the right side becomes certain units

which is impossible.

since π' are not units

Hence we get $n \geq m$

$n \leq m$

Hence $n = m$

In this process we can also proove that every π_i has π_1 as associates and conversely.

Theorem : 5.28 Ng.

The ideal $A = (a_0)$ is a maximal ideal of the Euclidean ring R iff a_0 is a prime element of R

Proof :-

Proof: Let us assume that a_0 is prime element

To prove that $A = (a_0)$ is a maximal ideal

Suppose a_0 is not a prime element.

If $a_0 = bc$ where $b, c \in R$ and neither b nor c is a unit

Let $B = (b)$

Clearly $a_0 \in B$

so that $A \subset B$

We claim that $A \neq B$ and $B \neq R$

Now we to prove that $A = (a_0)$ is not maximal ideal

If $B = R$ then $1 \in R$

so that $1 = x \cdot b$ for some $x \in R$.

$\Rightarrow \Leftarrow$ to b is not a unit in R

Now if $A = B$ then $b \in B = A$

$\therefore b = x a_0$ for some $x \in R$

We know that

$$a_0 = bc$$

$$\therefore a_0 = x a_0 c$$

$$1 = xc$$

$\Rightarrow \Leftarrow$ to c is not a unit in R

$$A \neq B$$

Hence $A \subset B \subset R$ where $B \neq A$ and $B \neq R$

$\therefore A$ is not a maximal ideal of R

Conversely,

Suppose a_0 is a prime element of R.

and U is an ideal of R such that

$$A = (a_0) \subset U \subset R \rightarrow (1)$$

By theorem 5.1

$$U = (u_0)$$

Since $a_0 \in A \subset U = u_0$.

$$a_0 = x u_0 \rightarrow (2) \text{ for some } x \in R$$

But a_0 is a prime element of R

then $u = R$

on the other hand

If x is a unit R then $x^{-1} \in R$

(5) $\Rightarrow$ $a_0 = x u_0$

$\Rightarrow u_0 = x^{-1} a_0 \in A$

Since A is an ideal of R

$\Rightarrow U \subset A$

Illy $A \subset U$

we have $A \subset U$ and $U \subset A$

$\Rightarrow U = A$ (or) $U = R$

Hence A is a maximal ideal.

Theorem : 5.29 Cauchy theorem for abelian group

Suppose G is a finite abelian group and $P / o(G)$ where p a prime number then there is an element $a \neq e \in G$ such that $a^p = e$.

Proof :-

We proceed by Induction over $o(G)$.

This theorem is trivally true for all group having single element

Assume this theorem is true for all abelian groups having fewer element then G

To prove.

This result is true for G

Then G has no subgroup $H \neq (e)$ we have G ust be cyclic of prime order.

This prime must be p and G has $p-1$ element $a \neq e$ satisfying $a^p = a^{o(G)} = e$

Suppose G has a subgroup $N \neq e$ if $P / o(N)$

By Induction hypothesis

since $o(N) < o(G)$, N is abelian

there is an element $b \in N$, $b \neq e$ satisfying $b^p = e$: since $b \in N \subset G$

So we have there is an element $b \neq e \in G$ such that $b^p = e$

since $b \in N \subset G$

$\therefore b \neq e \in G$

So we may assume that $P \nmid o(N)$

Since G_1 is an abelian

N is a normal subgroup of G_1

so G_1/N is abelian

Moreover, $O(G_1/N) = \frac{O(G_1)}{O(N)} < O(G_1)$

G_1 is abelian

By induction hypothesis

There is an element $X \in G_1/N$ satisfying $X^P = e$

the unit element G_1/N, $X \neq e$

Let $X = Nb$, $b \in G_1$

$$X^P = (Nb)^P = Nb^P$$

Since $e_1 = Ne$

$$X^P = e_1, \quad X \neq e_1$$

we have $Nb^P = Ne = N$

$$Nb^P = N$$

$$Nb \neq N$$

Thus $b^P \in N$ but $b \notin N$

By the corollary of lagrange's theorem

$$(b^P)^{O(N)} = e$$

i.e) $b^{O(N)\cdot P} = e$

Let $c = b^{O(N)}$

$$c^P = e$$

Inorder to such that c is an element that satisfies the conclusion of theorem

we have to such that $c \neq e$

if suppose $c = e$

$$b^{O(N)} = e$$

$$(Nb)^{O(N)} = N$$

combining with $(Nb^P) = N$

But $P \nmid O(N)$, P is prime number

we find $Nb = N$ so $b \in N$

which is contradiction

$$c \neq e, \quad c^P = e$$

Theorem: 5.30 (4) U.O.

S_{p^k} has p-sylow subgroups

Proof:- We prove this theorem an induction method.

If $k=1$, then the element $(1, 2, \ldots p)$ is S_p of order p, generated a subgroup of order, since $n(1)=1$

The result is true for $k=1$

Suppose that theorem is true for $k-1$

We want to prove that on induction k Divide the Integer $1, 2, \ldots p^k$ into p

The Clump each with p^{k-1} elements as follow.

$$\{1, 2, \ldots p^{k-1}\} \{p^{k-1}+1, p^{k-1}+2, \ldots, 2p^{k-1}\}$$
$$\ldots \{(p-1)p^{k-1}+1, \ldots p^k\}.$$

The Permutation σ defined by

$$\sigma = (1, p^{k-1}+1, 2p^{k-1}+1, \ldots, (p-1)p^{k-1}+1) \ldots$$
$$(j, p^{k-1}+j, 2p^{k-1}+j, \ldots, (p-1)p^{k-1}+j \ldots$$
$$(p-1)p^{k-1}+1+j) \ldots (p^{k-1}, 2p^{k-1}, \ldots (p-1)p^{k-1}, p^k)$$

has the following properities

1) $\sigma^p = e$

2) If τ is permutation that leaves all i, Fixed for $i > p^{k-1}$. then $\sigma^{-1}\tau\sigma$ moves only elements in $\{p^{k-1}+1, p^{k-2}+2, \ldots 2p^{k-1}\}$ are generally $\sigma^{-j}\tau\sigma^j$ moves only elements in $\{jp^{k-1}+1, jp^{k-1}+2, \ldots, (j+1)p^{k-1}\}$

Consider $A = \{\tau \in S_{p^k} / \tau(i) = i \text{ if } i > p^{k-1}\}$

A is a subgroup of S_{p^k} and elements in A can carry out any permutation on $1, 2, \ldots, p^{k-1}$

$\therefore A \cong S_{p^{k-1}}$

By induction A has a subgroup P_1 of order $p^{n(k-1)}$

Let $T = P_1 (\sigma^{-1} P_1 \sigma)(\sigma^{-2} P_1 \sigma^2) \cdots (\sigma^{-(p-1)} P_1 \sigma^{p-1})$

$T = P_1 P_2 \cdots P_{n-1}$

where $P_i = \sigma^{-i} P_1 \sigma^i$ each P_i is isomorphic to P_i

so has order $p^{n(k-1)}$

Thus T is a subgroup of Sp^k

Since $P_i \cap P_j = (e)$ if $0 \le i \ne j \le p-1$

$$O(T) = (O(P_1)^P) = p^{Pn(k-1)}$$

T is not a p-sylow subgroup

since $\sigma^p = e$ and $\sigma^{-i} P_1 \sigma^i = P_i$

we have, $\sigma^{-1} T \sigma^1 = T$

Let $P = \{\sigma^j t / t \in T, 0 \le j \le p-1\}$

since $\sigma \notin T$ and $\sigma^{-1} T \sigma = T$

Further, T is a subgroup of Sp^k

$$O(P) = O(T)$$

$$p \cdot p^{n(k-1)P} = p^{n(k-1)P+1}$$

P is the sylow subgroup of Sp^k

It is $p^{n(k-1)P+1}$

But $n(k-1) = 1 + p + \cdots + p^{k-2}$

Hence $p^{n(k-1)+1} = 1 + p + \cdots + p^{k-1}$

$= n(k)$

since $O(P) = p^{n(k)}$

$\therefore$ P is the p-sylow subgroup of Sp^k

Problem : 1

) Find the greatest common divisor in $J[i]$ of

a) $3+4i$

proof. $\frac{a}{b} = \frac{3+4i}{4-3i} \times \frac{4+3i}{4+3i} = \frac{12+9i+16i-12}{16+9}$

$= \frac{25i}{25} = i$ [$\because a = 0b + 3 + 4i$]

$a = 0b + i\,(4-3i)$ $\quad r_1 = 4i+3$

Now, $q_1 = 0$, $\sigma_1 = 3+4i$

$b/r_1 = \frac{4-3i}{3+4i} \times \frac{3-4i}{3-4i}$