~~permutate~~

unit II M.Sc. 1st year mathematics
paul madam
abstract algebra

~~* permutation group:~~
~~Let x be a nonempty set. The group of all permutation of x under composition of mapping is called the symmetric group on x and is~~

* permutation group:
Let S be a non-empty set. permutation on S means a bijective (1-1 & onto) function $F: S \to S$. Let $A(S)$ = The set of all permutation on S.

: Show that $A(S)$ is a group under composition
→ ① closure property:
$\forall F, g \in A(S)$
i.e $F: S \to S$ & $g: S \to S$ are bijective function.
$\Rightarrow f \circ g : S \to S$ is also bijective function.
$\Rightarrow f \circ g \in A(S)$

② Associative property:
$\forall F, g, h \in A(S)$
i.e $F: S \to S$, $g: S \to S$, $h: S \to S$ are bijective function. we have
$f \circ (g \circ h) : S \to S$ is a bijective function
& $(f \circ g) \circ h : S \to S$ is a bijective function.
$\Rightarrow f \circ (g \circ h) = (f \circ g) \circ h$.

③ Existance of Identity:
$I: S \to S$ given by $I(x) = x$ $\forall x \in S$ is a permutation on S & ~~FoI~~
$F \circ I = I \circ F = F$ $\forall F \in A(S)$
i.e $I \in A(S)$ is the identity elements

④ Existance of Inverse:
$\forall F \in A(S)$ i.e $F: S \to S$ is a bijective functions we also have $F^{-1}: S \to S$ is also bijective i.e $f^{-1} \in A(S)$

Scanned by CamScanner

$$(f \circ f^{-1})(x) = f(f^{-1}(x)) = f \cdot f^{-1}(x) = x$$

$$(f \circ f^{-1})(x) = I(x)$$

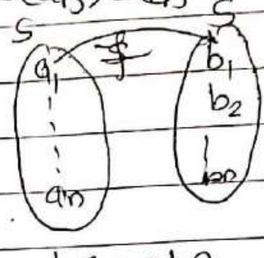
$$\Rightarrow f \circ f^{-1} = I = f^{-1} \circ f.$$

$\therefore$ $(A(S), \circ)$ is a group.

Note-

Let $S = \{a_1, a_2 --- a_n\}$ be a finite set having n elements permutation on S is of degree n.

Let $f : S \to S$ be a permutation on S i.e a bijection. Let $f(a_1) = b_1$, $f(a_2) = b_2$ --- $f(a_n) = b_n$



f is 1-1 given $a_i \neq a_j$

$$\Rightarrow f(a_i) \neq f(a_j) \Rightarrow b_i \neq b_j$$

f is onto gives $S = f(S)$

i.e $\{a_1, a_2 -- a_n\} = \{b_1, b_2 -- b_n\}$.

$b_1, b_2 --- b_n$ ~~are~~ is a arrangment of objects $a_1, a_2 --- a_n$

There are $n!$ arrangments of n objects. $a_1, a_2 --- a_n$ & each arrangents gives a permutation

$\therefore$ $A(S)$ is a group of order $n!$

for $|S| = n$ $A(S)$ is denoted by S_n

S_n = The set of all permution on g.on n symbols.

Def^n ~~Transposition~~ :-

Let $\sigma \in S_n$ If there exists a list of distinct integers $x_1, x_2 --- x_r \in n$ such that $\sigma(x_i) = x_{i+1}$ $i = 1, 2 --- r-1$

$\sigma(x_r) = x_1$ $\sigma(x) = x$ if $x \notin \{x_1, x_2 -- x_r\}$

then σ is called cycle of length r & denoted by $(x_1, x_2 -- x_r)$. A cycle of length 2 is called a permutation / transposition

Theorem :- Cayley

Every group is isomorphic to a permutation group.

Let G be a group

For any given $a \in G$ the mapping

$f_a : G \to G$ given by

$f_a(x) = ax \quad \forall \; x \in G$

i) f_a is ~~one-one~~ well defined & one-one :-

Since $ax_1 = ax_2$

$\Leftrightarrow \; ax_1 = ax_2 \qquad a \in G.$

$\Leftrightarrow \; f_a(x_1) = f_a(x_2) \qquad \forall \; x_1, x_2 \in G$

2) f_a is onto :-

$\forall \; y \in G =$ codomain of f_a

$a \in G \Rightarrow a^{-1}y \in G =$ domain of f_a

Then

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

$= y$

$\therefore$ f_a is onto.

$\therefore$ f_a is bijection function

Consider the mapping

$\phi : G \longrightarrow S_G$ given by,

$\Rightarrow \; \phi(a) = f_a \qquad \forall \; a \in G$

Where S_G is the symmetric group on the set G $\forall \; a, b, x \in G$

$\phi(ab) = f_{ab}$

But $f_{ab}(x) = abx = a(bx) = f_a(bx)$

$= \cancel{a(bx) =} \qquad = f_a(f_b(x))$

Hence $\qquad = (f_a \circ f_b)(x)$

$\phi(ab) = (f_a \circ f_b).$

$= \phi(a) \circ \phi(b)$

Therefore ϕ is a homomorphism and $\mathrm{Im}\,\phi$ is a subgroup of S_G. Moreover

$\phi(a) = \phi(b)$

$f_a = f_b$

$\Rightarrow f_a(x) = f_b(x)$

$\Rightarrow ax = bx \qquad \forall \; x \in G$

$\Rightarrow a = b \qquad \forall \; x \in G$

$\therefore$ ϕ is an injective homomorphism

$\therefore$ G is isomorphic to a subgroup of S_G.

* Cycle :- Let set containing $\{a_1, a_2, \ldots a_k\} \subseteq S$

Decomposition.

then $\sigma = (a_1 a_2 a_3 \ldots a_{k-1} a_k)$ is called a cycle of length k which is a permutation on S such that every element in the cycle followed by it's σ-image image of last element is first elements & elements of S are invarient under F if they are not in the cycle

i.e $f_\sigma(a_1) = a_2$, $f_\sigma(a_2) = a_3$ ---- $f_\sigma(a_{k-1}) = a_k$, $f_\sigma(a_k) = a$

& $\sigma(x) = x$ for every other x in n.

*

Two cycles $(a_1, a_2 \ldots a_r), (b_1 b_2 \ldots b_s)$ in S_n are disjoint permutations iff the sets $\{a_1, a_2 \ldots a_r\}$ and $\{b_1, b_2 \ldots b_s\}$ are disjoint.

Note - a cycle of length r canbe written in r ways namely as $(a_1, a_2 \ldots a_r)$ & $(a_i a_{i+1} \ldots a_r a_1 \ldots a_{i-1})$ $i = 2, 3, \ldots r$.

A cycle of length r is also called an r-cycle.

Theorem - Any permutation $\sigma \in S_n$ is a product of pairwise disjoint cycles. This cyclic factorization is unique except for the order in which the cycles are written & the inclusion or omission of cycles of length 1.

→ We prove the theorem by induction on n.

If n = 1 the theorem is obvious. Let $i_1 \in \{1, 2 \ldots n\}$ then $\exists$ a smallest positive integer r such that

$\sigma^r(i_1) = i_1$ Let $i_2 = \sigma(i_1)$, $i_3 = \sigma(i_2)$

~~$\Rightarrow i_2 =$~~

$i_3 = \sigma(\sigma(i_1))$

$\Rightarrow i_3 = \sigma^2(i_1)$

$i_r = \sigma(i_{r-1}) = \sigma^{r-1}(i_1)$

Next

Let $X = \{1, 2 \ldots n\} - \{i_1, i_2 \ldots i_r\}$

If $x = \phi$ then σ is a cycle and we are done. So let $x \neq \phi$.

Let $\sigma^* = \sigma|x$ then σ^* is a permutation of set consisting of $n-r$ elements.

By Induction

$$\sigma^* = C_2 C_3 \cdots C_m \text{ where } C_i \text{ are}$$

pairwise disjoint cycles.

But since $\sigma = \sigma^* C_1$ where $C_1 = (i_1 i_2 \cdots i_r)$ it follows that σ is a ~~product of~~ product of disjoint cycles.

To prove uniqueness,

Suppose σ has two decompositions into disjoint cycles of length > 1

Say

$$\sigma = \gamma_1 \cdots \gamma_k = \beta_1 \beta_2 \cdots \beta_l$$

Let $x \in n$. If x does not appear in any γ_i then $\sigma(x) = x$

Hence x does not apper in any β_j.

then $\sigma(x) \neq x$. Hence x must be in some β. But then $\sigma^r(x)$ occurs in both γ_i & β_j for every $r \in \mathbb{Z}$ i.e.

Hence γ_i & β_j are identical cycles. This proves that the two decompositions written earlier are identical except for the ordering of factors.

Corollary 1.2 Every permutation can be expressed as a product of transformation

→ Consider

Identity permutation

$(1) = (12)(12)$ = product of two permutation

2-cycle

$(123) = (13)(12)$

3-cycle $(1234) = (14)(13)(12)$ &

$\vdots$

n-cycle $(1234 \cdots n) = (1n)(1\ n-1) \cdots (12)$

σ = product of two transpositions

$\therefore$ Every permutation can be expressed as product of two transposition.

Theorem -

If $\alpha, \sigma \in S_n$ then $\tau = \alpha\sigma\alpha^{-1}$ is the permutation obtained by applying α to the symbols in σ. Hence any two conjugate permutations in S_n have the same cycle. Structure. Conversely any two permutations in S_n with the same cycle structure are conjugate.

$\rightarrow$ If $\sigma(i) = j$ then

$$\tau\,\alpha(i) = \cancel{\sigma\alpha\sigma}(\alpha\sigma\alpha^{-1})(\alpha(i))$$
$$= \alpha\sigma(\alpha^{-1}\alpha(i))$$
$$= \alpha\sigma(i)$$
$$= \alpha(j)$$

$\therefore$ If $(a_1, a_2 \ldots a_m)$ is a cycle in the decomposition of σ then

$(\alpha(a_1)\,\alpha(a_2) \ldots \alpha(a_m))$ is a cycle in the decomposition of τ

Hence the cycle decomposition of τ is obtained by substituting $\alpha(x)$ for x everywhere in the decomposition of σ.

Thus, σ & τ have the same cycle structure.

Conversely, Suppose that σ & τ have the same cycle structure $(pq \ldots r)$ Then σ & τ have cycle decompositions.

$$\sigma = (a_1 a_2 \ldots a_p)(a_{p+1} \ldots a_{p+q}) \ldots (a_{n-r+1} \ldots a_n)$$
$$\tau = (b_1 b_2 \ldots b_q)(b_{p+1} \ldots b_{p+q}) \ldots (b_{n-r+1} \ldots b_n)$$

Define

$\alpha \in S_n$ by $\alpha(a_i) = b_i \quad i = 1, 2 \ldots n.$

Then

$$(\alpha\sigma\alpha^{-1})(b_i) = \alpha\sigma(\alpha^{-1}(b_i)) = \alpha\sigma(a_i)$$
$$= \alpha(a_j)$$
$$= b_j = \tau(b_i)$$

Hence $\alpha 6 \alpha^{-1} = \tau$.

$\therefore$ 6 & τ are conjugate.

Corollary :-

There is a one-one correspondence between the set of conjugate classes of S_n & the set of partitions of n.

* Alternating group :- A_n.

The set $A_n = \{ f \in S_n \mid f$ is an even permutation$\}$ ~~Show that~~ is called Alternating group. and it is denoted by A_n. Order of alternating group is $\frac{n!}{2}$

* Show that Alternating group is subgroup of Symmetric group S_n.

→ Consider the

$S_n = \{ 6 \in S_n \mid 6 : S \to S$ is bijective permutation$\}$

and $A_n = \{ f \in S_n \mid f$ is an even permutation in $S_n \}$

Consider

$(1) \in S_n$ But we know that Identity permutation is an even permutation.

$\therefore (1) \in A_n \subseteq S_n$ $\therefore A_n$ is non empty

$\forall$ $f, g \in A_n$ i.e f & g both are even permutation

fg is an even permutation

i.e $f \cdot g \in A_n$

$\forall$ $f \in A_n$ i.e f is an even permutation

$\Rightarrow f^{-1} \in A_n$ i.e f^{-1} is an even permutation

$\therefore$ A_n is subgroup of S_n.

Theorem - If a permutation $\sigma \in S_n$ is a product of r transpositions & also a product of s transpositions are either both even or odd.

proof - Let $\sigma = \eta_1 \eta_2 \cdots \eta_r = \eta_1' \cdots \eta_s'$

where η_i & η_i' are transpositions.

Let $p = \prod_{i<j} (x_i - x_j)$ be a polynomial in the variables $x_1, x_2 \cdots x_n$ Define

$$\eta(p) = \prod_{i<j} (x_{\eta(i)} - x_{\eta(j)}) \qquad \eta \in S_n$$

We show that if η is a transposition then $\eta(p) = -p$

Let $\eta = (k\ l) \qquad k < l$

Now one of the factors in the polynomial p is $x_k - x_l$ & in $\eta(p)$ the corresponding factor becomes $x_l - x_k$.

Any factor of p of the form $x_i - x_j$ where neither i or j is equal to k or l is unaltered under the mapping η. All other factors can be paired to form products of the form $\pm(x_i - x_k)(x_i - x_l)$ with the sign determined by the relative magnitude of i, k & l But since the effect of η is just to interchange x_k & x_l any such product of pairs is unaltered.

Therefore, the above argument gives that the only effect of η is to change the sign of p

This proves our Assertion

finally,

$$\sigma(p) = (\eta_1 \cdots \eta_r)\, p = (-1)^r p$$

Also,

$$\sigma(p) = (\eta_1' \cdots \eta_s')\, p = (-1)^s p$$

Thus $(-1)^r = (-1)^s$ proving that r & s are both even or both odd.

Def^n –

A permutation in S_n is called an even (odd) permutation if it is a product of an even (odd) number of transposition.

The Sign of a permutation σ written $sgn(\sigma)$ or $\epsilon(\sigma)$

Def^n – Let $\phi : n \to n$ then.

$$\epsilon(\phi) = \begin{cases} +1 & \text{If } \phi \text{ is an even permutation} \\ -1 & \text{If } \phi \text{ is an odd permutation.} \\ 0 & \text{If } \phi \text{ is not a permutation} \end{cases}$$

Lemma :- Let ϕ, ψ be mapping from n to n then $\epsilon(\phi\psi) = \epsilon(\phi)\epsilon(\psi)$

Hence for any $\sigma \in S_n$ $\epsilon(\sigma^{-1}) = \epsilon(\sigma)$

→ If ϕ & ψ are both permutations the result follows.

If ϕ or ψ are not a permutation then $\phi\psi$ are not a permutation.

Hence $\epsilon(\phi\psi) = 0$

$\Rightarrow \epsilon(\phi).\epsilon(\psi) = 0$

If σ is a permutation

$\epsilon(\sigma)\epsilon(\sigma^{-1}) = \epsilon(\sigma\sigma^{-1}) = 1$

Hence $\epsilon(\sigma^{-1}) = \epsilon(\sigma)$

Theorem :- A_n is a normal subgroup of S_n

If $n > 1$, A_n is of index 2 in S_n and hence $|A_n| = \frac{1}{2} n!$.

→ If $n = 1$ $S_1 = \{e\} = A_1$

Hence A_1 is trivially a normal subgroup

Let $n > 1$ Let $G = \{1, -1\}$ be the multiplicative group of integers $1, -1$

Consider the mapping $\phi : S_n \longrightarrow G$ given by $\phi(\sigma) = \epsilon(\sigma)$

① ϕ is homomorphism :-

$\forall\ \sigma, \tau \in S_n$

$$\phi(\sigma\tau) = \epsilon(\sigma\tau)$$
$$= \epsilon(\sigma)\epsilon(\tau)$$
$$= \phi(\sigma) \cdot \phi(\tau)$$

$\therefore$ ϕ is homomorphism

Because $n > 1$ the transposition $\tau = (12)$ is in S_n and $\phi(\tau) = -1$ Hence ϕ is surjective

there fore

$$\ker\phi = \{\sigma \in S_n \mid \phi(\sigma) = 1\}$$
$$= \{\sigma \mid \phi(\sigma) = 1\}$$
$$= A_n = \{\text{set of all even permutations}\}$$

$\therefore$ By the fundamental theorem of homomorphism.

$$\frac{S_n}{\ker\phi} \cong G$$

$$\Rightarrow \frac{S_n}{A_n} \cong G$$

$$\Rightarrow [S_n : A_n] = \left|\frac{S_n}{A_n}\right| = |G|$$

$$\Rightarrow \frac{|S_n|}{|A_n|} = 2$$

$$\Rightarrow \frac{n!}{|A_n|} = 2 \quad \Rightarrow |A_n| = \frac{n!}{2}.$$

Lemma - The Alternating group A_n is generated by the set of all 3-cycles in S_n

proof - The result holds trivially for $n = 1, 2$ for then $A_n = \{e\}$ & S_n does not have any 3-cycle. So let $n > 2$ Now every 3-cycle is an even permutation & hence an element of A_n

Conversely,

Every element in A_n is a product of an even number of transpositions.

ii Consider the product of any two transpositions σ & τ. If σ & τ are disjoint

Say $\sigma = (ab)$, $\tau = (cd)$

then

$$(abc)(bcd) = (ab)(cd) = \sigma\tau$$

Otherwise $\sigma = (ab)$, $\tau = (bc)$ gives

$$\sigma\tau = (ab)(bc) = (abc)$$

Thus every even permutation is a product of 3-cycles Hence A_n is generated by the set of all 3-cycles in S_n.

Lemma - The derived group of S_n is A_n

proof - For $n = 1, 2$ $S_n' = \{e\} = A_n$

Consider $n > 2$ & Let $\alpha = (12)$, and $\beta = (123)$ then

$$\alpha\beta\alpha^{-1}\beta^{-1} = (12)(123)(21)(321) = (123)$$

Hence $(123) \in S_n'$ Because $S_n' \triangle S_n$

S_n' must contain every conjugate of (123).

Hence S_n' contains every 3-cycle therefore $A_n \subset S_n'$

on the other hand every commutator $aba^{-1}b^{-1}$ in S_n' is an even permutation.

Hence $S_n' \subset A_n$. this proves that $S_n' = A_n$

$\therefore$ The derived group of S_n is A_n

Theorem -

The alternating group A_n is simple if $n > 4$

Consequetly S_n is not solvable if $n > 4$

proof - Suppose H is a nontrivial normal subgroup of A_n. we first prove that H must contain a 3-cycle Let $\sigma \neq e$ be a permutation in H that moves the least number of integers in n, Being an even permutation σ cannot be a cycle of even length Hence σ must be a 3-cycle or have a decomposition of the form

$$\sigma = (abc \text{ ---- }) \quad \text{——— (1)}$$

or $$\sigma = (ab)(cd) \text{ ---- } \quad \text{——— (2)}$$

Scanned by CamScanner

Where a, b, c, d are distinct. consider first case (1) 12 PET.SRT@gmail.com

Because σ Cannot be a 4-cycle, it must move at least two more elements, say d & e

Let $\alpha = (cde)$ Then

$$\alpha\sigma\alpha^{-1} = (cde)(abc\cdots)(edc)$$
$$= (abd\cdots)$$

Now let $\tau = \sigma^{-1}(\alpha\sigma\alpha^{-1})$ then $\tau(a) = a$ & $\tau(x) = x$ Whenever $\sigma(x) = x$ Thus, τ moves fewer elements than σ. But $\tau \in H$ a contradiction.

Consider now Case (2) with $\alpha = (cde)$ as before

$$\alpha\sigma\alpha^{-1} = (cde)(ab)(cd)\cdots(edc)$$
$$= (ab)(de)\cdots$$

Let $\beta = \sigma^{-1}(\alpha\sigma\alpha^{-1})$ then $\beta(a) = a$, $\beta(b) = b$ and for every x other than e, $\beta(x) = x$ if $\sigma(x) = x$ Thus, $\beta \in H$ and moves fewer integers than σ. a contradiction. Hence, we conclude that σ must be a 3-cycle.

Let τ be any 3-cycle in S_n. Because any two cycles of the same length are conjugate in S_n, $\tau = \alpha\sigma\alpha^{-1}$ for some $\alpha \in S_n$. If α is odd, choose a transposition β in S_n such that σ & β are disjoint. (This is possible because $n > 4$) Then $\alpha\beta \in A_n$ &

$$(\alpha\beta)(\sigma)(\alpha\beta)^{-1} = \alpha(\beta\sigma\beta^{-1})\alpha^{-1} = \alpha\sigma\alpha^{-1} = \tau.$$

Hence, σ & τ are conjugate in A_n. Therefore $\tau \in H$ Thus H Contains every 3-cycle in S_n. Therefore $H = A_n$ Hence A_n has no proper normal subgroup which proves that A_n is simple if $n > 4$

Consider now the derived group of A_n Because A_n' is a normal subgroup of A_n & A_n is simple either A_n' is trivial or $A_n' = A_n$ But A_n is nonabelian if $n > 3$ Hence A_n' is not trivial therefore $A_n' = A_n$ for every $n > 4$. Consequetly $S_n^{(2)} = A_n' = A_n$. Hence $S_n^{(k)} = A_n$ for all $k \geq 1$. This proves that S_n is not solvable.

Scanned by CamScanner

Page : Date : / /

* Structure theorems of groups :

*** Theorem :**

Let $H_1, H_2 \cdots H_n$ be a family of subgroup of a group G and Let $H = H_1 \cdots H_n$ Then the following are equivalent.

(i) $H_1 \times H_2 \times \cdots \times H_n \cong H$ under the canonical mapping that sends $(x_1, x_2, \cdots x_n)$ to $x_1 \cdots x_n$

(ii) $H_i \triangle H$ and every element $x \in H$ can be uniquely expressed as $x = x_1 \cdots x_n$, $x_i \in H_i$

(iii) $H_i \triangle H$ & if $x_1 \cdots x_n = e$ then each $x_i = e$.

iv) $H_i \triangle H$ & $H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_n) = \{e\}$ $1 \le i \le n$

proof - ~~(i) ⇒ (ii)~~

~~Let $H_1' = \{(e, \cdots h_i, \cdots e)$~~

Let H be a group with identity e & $H_1, H_2 \cdots H_n$ are subgroups of H s.t

$H = H_1 \cdot H_2 \cdots H_n = \{x_1 x_2 \cdots x_n \mid x_i \in H_i, 1 \le i \le n\}$

Let $\phi : H_1 \times H_2 \times \cdots \times H_n \longrightarrow H$ be given by

$\phi(x_1, x_2 \cdots x_n) = (x_1 x_2 \cdots x_m)$, $x_i \in H_i$ $\forall i$

clearly ϕ is onto.

(i) ⇒ (ii) Assume (i) i.e $H_1 \times H_2 \times \cdots \times H_n \cong H$

under onto isomorphism $\phi : H_1 \times H_2 \times \cdots \times H_n \longrightarrow H$

for each $i \in \{1, 2, \cdots n\}$ consider

$H_i' = \{(e, e \cdots h_i, e \cdots e) \in H_1 \times H_2 \times \cdots \times H_n \mid h_i \in H_i\}$

H_i' is a nonempty subset of $H_1 \times H_2 \times \cdots \times H_n$

<u>To prove</u> - $H_i' < H_1 \times H_2 \times \cdots \times H_n$

Consider any $a = (e, e \cdots e, h_i, e \cdots e)$
& $b = (e, e \cdots k_i, e \cdots e) \in H_i'$ any $h_i, k_i \in H_i$

Then

$ab^{-1} = (e \cdots h_i, e \cdots e)(e, e \cdots k_i, e \cdots e)^{-1}$

$= (e, \cdots h_i e \cdots e)(e, e \cdots k_i^{-1} e, \cdots e)$

$= (e, \cdots h_i k_i^{-1}, e \cdots e)$ $\because h_i, k_i \in H_i < H$

$\Rightarrow h_i k_i^{-1} \in H_i$

Hence $H_i' < H_1 \times H_2 \times \cdots \times H_n$

<u>To prove</u> - $H_i' \triangle H_1 \times H_2 \times \cdots \times H_n$

Consider any $a = (e, e \dots e\, h_i, e \dots e) \in H_i'$ &
$x = (x_1, x_2 \dots x_n) \in H_1 \times H_2 \times \dots \times H_n$

Then

$x a x^{-1} = (x_1, x_2 \dots x_n)(e, e \dots h_i, e \dots e)(x_1^{-1}, x_2^{-1} \dots x_n^{-1})$

$= (x_1 x_1^{-1}, x_2 x_2^{-1} \dots x_i h_i x_i^{-1} \dots x_n x_n^{-1})$

$= (e, e, \dots x_i h_i x_i^{-1} \dots e) \in H_i'$
$(\because h_i, x_i \in H_i < G$
$\Rightarrow x_i h_i x_i^{-1} \in H_i)$

$\therefore H_i' \triangle H_1 \times H_2 \times H_3 \times \dots \times H_n$

Now

$\phi(H_i') = \{\phi(e, e \dots h_i, \dots e) \mid h_i \in H_i\}$

$= \{(e, e \dots h_i, \dots, e) \mid h_i \in H_i\}$
$= \{h_i \mid h_i \in H_i\} = H_i$

$\therefore \phi : H_1 \times H_2 \times \dots \times H_n \longrightarrow H$ is onto isomorphism
& $H_i' \triangle H_1 \times H_2 \times \dots \times H_n$ so $\phi(H_i) \triangle H$
i.e $H_i \triangle H \quad \forall\ i = 1, 2, 3 \dots n$

Let $x \in H$ with $x = x_1 x_2 \dots x_n$ where $x_i \in H_i$ for $i = 1, 2 \dots n$. Let $x = y_1 y_2 \dots y_n$ with $y_i \in H_i$ for $i = 1, 2 \dots n$.

$x_1, x_2 \dots x_n = y_1, y_2 \dots y_n$
$\Rightarrow \phi(x_1, x_2 \dots x_n) = \phi(y_1, y_2 \dots y_n)$
$\Rightarrow x_1, x_2 \dots x_n = y_1, y_2 \dots y_n$
$\Rightarrow x_i = y_i \quad \forall\ i = 1, 2 \dots n.$

i.e each $x \in H$, with $x = x_1, x_2 \dots x_n$ $x_i \in H_i$ is uniquely expressed i.e (ii)

Hence (i) $\Rightarrow$ (ii) follows.

(ii) $\Rightarrow$ (iii) Assume (ii) i.e $H_i \triangle H$ $\forall i$ & every $x \in H$ is uniquely expressed as $x = x_1 x_2 \dots x_n$, $x_i \in H_i \forall i$
Let $e = x_1, x_2 \dots x_n$ be the identity of H ($x_i \in H_i \forall i$) we also have $e = e \dots e$ $e \in H_i \forall i$
By uniqueness of the representation of $e \in H$

we have
$x_1 = e,\ x_2 = e, \ldots\ x_n = e$ i.e $x_i = e\ \forall i$

(iii) $\Rightarrow$ (iv) Assume (iii) i.e $H_i \Delta H\ \forall i$ &
$e = x_1 x_2 \ldots x_n\quad x_i \in H_i\ \forall i \Rightarrow x_i = e\ \forall i$
For any $i \neq j$ consider $H_i \cap H_j < H\ \forall x \in H_i \cap H_j$
we have
$x^{-1} \in H_i \cap H_j$ (i.e $x^{-1} \in H_i,\ x x^{-1} \in H_j$)
& $e = x x^{-1} = x^{-1} \cdot x$
$= e \ldots e x e \ldots e x^{-1} e \in H_1 H_2 \ldots H_n$
$\Rightarrow x = e = x^{-1}$ by (iii)
$\therefore H_i \cap H_j = \{e\}\ \forall i \neq j$
Also
$H_i \Delta H,\ H_j \Delta H$
$\Rightarrow xy = yx\quad \forall x \in H_i\ \forall y \in H_j$
Let
$x_i \in H_i \cap (H_1, \ldots H_{i-1} H_{i+1} \ldots H_n)$
$x_i = x_1 x_2 \ldots x_{i-1} x_{i+1} \ldots x_n$
Where each $x_k \in H_k\ \forall k = 1, 2 \ldots n$.

$\Rightarrow e = x_i^{-1} x_1 x_2 \ldots x_{i-1} x_{i+1} \ldots x_n$
i.e $e = x_1, x_2 \ldots x_{i-1} x_i^{-1} x_{i+1} \ldots x_n$
where $x_j \in H_j\ \forall j \neq i$ & $x_i^{-1} \in H_i$
By (iii) $x_j = e\ \forall j \neq i$ & $x_i^{-1} = e$ i.e $x_i = e$

$\therefore H_i \cap (H_1 H_2 \ldots H_{i-1} H_{i+1} \ldots H_n) = \{e\}$
$\forall i = 1, 2 \ldots n$

(iv) $\Longrightarrow$ (i) Assume (iv)
i.e $H_i \Delta G\ \forall i$ & $H_i \cap (H_1 \ldots H_{i-1} H_{i+1} \ldots H_n) = \{e\}$
$\forall i = 1, 2 \ldots n$

for $j \neq i$ $H_j \subset H_1 \ldots H_{i-1} H_{i+1} \ldots H_n$
So we have $H_i \cap H_j = \{e\}$
Also we have $xy = yx\ \forall x \in H_i$ & $\forall y \in H_j$ — (*)
$\phi : H_1 \times H_2 \times \ldots \times H_n \longrightarrow H = H_1 \cdot H_2 \ldots H_n$
given by
$\phi(x_1, x_2 \ldots x_n) = x_1 \cdot x_2 \ldots x_n\ \forall x_i \in H_i$
is onto.
for any $X = (x_1, x_2 \ldots x_n), Y = (y_1, y_2 \ldots y_n) \in$
$H_1 \times H_2 \times \ldots \times H_n$ i.e $\forall x_i, y_i \in H_i\ \forall i$

we have

$\phi(xy) = \phi(x_1y_1, x_2y_2 - - - x_ny_n)$

$= x_1y_1 . x_2y_2 - - - - . x_ny_n$

$= (x_1 x_2 - - - x_n)(y_1 , y_2 - - - . y_n)$

$= \phi(X)\,\phi(Y)$

$\therefore$ ϕ is an onto group homomorphism

$\ker\phi = \{ X = (x_1, x_2 - - x_n) \in H_1 \times H_2 - - - \times H_n$
$/ \phi(X) = e$ identity of $H \}$

$= \{ (x_1, - - - x_n) \,/\, x_1 x_2 - - - x_n = e \}$

In these case $x_1^{-1} = x_2 x_3 - - - x_n \in H_1 \cap H_2 - - - H_n = \{e\}$

i.e $x_1^{-1} = e$ & so $x_1 = e$

similarly $x_2 = e$, $x_3 = e$ - - - $x_n = e$

$\ker\phi = \{(e, e - - - e)\}$ trivial subgroup of $H_1 \times H_2 \times - - - \times H_n$

$\therefore$ ϕ is one-one

Thus $\phi : H_1 \times H_2 \times - - - \times H_n \rightarrow H$ is an onto group isomorphism

$\therefore$ under the canonical map ϕ,

$H_1 \times H_2 \times - - - \times H_n \cong H = H_1 H_2 - - - H_n$

Def^n –

Let $H_1\ H_2 - - H_n$ be subgroups of a group H & $H_i \triangle H$ $\forall i$ if any condition of theorem 1-1 is satisfied then $H_1 H_2 - - - H_n$ is called an internal direct product of the group H

i.e

$H_i \cap H_1 - - - - H_{i-1} H_{i+1} - - - H_n = \{e\}$

$\forall i = 1, 2, - - - n$

If H is an additive group then we write

$H = H_1 + H_2 + - - - + H_n = \{ x_1 + x_2 + - - + x_n /\ x_i \in H_i$
$1 \le i \le n \}$

$H \cong H_1 \times H_2 \times - - - - \times H_n$

Page: Date: / /

Theorem (Fundamental theorem of finitely generated abelian group)

Let A be a finitely generated abelian group then A can be decomposed as a direct sum of a finite number of cyclic groups C_i precisely

$$A = C_1 \oplus C_2 \oplus C_3 \oplus \cdots \oplus C_k$$

Such that either $C_1, C_2, \ldots C_k$ are all infinite or for some $j \le k$, $C_1, C_2 \ldots C_j$ are of order $m_1, m_2, \ldots m_j$ respectively, with $m_1 | m_2 | m_3 \ldots | m_j$ and $C_{j+1}, C_{j+2}, \ldots C_k$ are infinite cyclic group. $(C_i \cong \mathbb{Z})$

→ Let A be a finitely generated additive abelian group. Let k be the smallest positive integer s.t A is generated by a set k elements of A.

We prove the theorem using induction on k.

[I] If k = 1 then A is a cyclic group i.e

$$A = \cancel{[\{a_1\}]} = \cancel{C}.C_1 = [a_1]$$

Hence theorem is trivially true.

Let k > 1 Assme that theorem is hold for every abelian group generated by a set of k−1 elements.

First we consider $\{a_1, a_2 \ldots a_k\}$ as a generating set of A with the property that for all $x_1, x_2 \ldots x_k \in \mathbb{Z}$

$$x_1 a_1 + x_2 a_2 + \cdots + x_k a_k = 0$$

$$\Rightarrow x_1 = x_2 = \cdots = x_k = 0 \quad \text{--- (1)}$$

This implies that each $a \in A$ has a unique representation

$$a = a_1 x_1 + a_2 x_2 + \cdots + a_k x_k \quad (x_i \in \mathbb{Z})$$

Consider $a = a_1 y_1 + a_2 y_2 + \cdots + a_k y_k \quad (y_i \in \mathbb{Z})$

Then substraction

$$(x_1 - y_1) a_1 + (x_2 - y_2) a_2 + \cdots + (x_k - y_k) a_k = 0$$

$$\Rightarrow x_1 - y_1 = 0, \; x_2 - y_2 = 0 \; \cdots \; (x_k - y_k) = 0$$

$$\Rightarrow x_1 = y_1, \; x_2 = y_2 \; \cdots \; x_k = y_k$$

i.e $x_i = y_i \quad \forall i$ by (1)

Hence uniqueness of a as a linear combination of $a_1, a_2, a_3 \cdots a_k$ follows.

Now $A = [\{a_1, a_2 \cdots a_k\}]$

$$= \{x_1 a_1 + x_2 a_2 + \cdots + x_k a_k \mid x_i \in \mathbb{Z},\ 1 \le i \le k\}$$

$A = [a_1] \oplus [a_2] \oplus \cdots \oplus [a_k]$ is the internal direct sum of $[a_1], [a_2] \cdots [a_k]$

i.e $A = C_1 \oplus C_2 \oplus \cdots \oplus C_k$

Where $C_i = [a_i]$ is a cyclic subgroup generated by a_i of A, $i = 1, 2 \cdots n$

Moreover since $x_i a_i = 0 \Rightarrow x_i = 0 \ \forall i = 1, \cdots k$

$\Rightarrow C_i = [a_i]$ is an infinite cyclic subgroup of A generated by a_i

Then $A = C_1 \oplus C_2 \oplus \cdots \oplus C_k$ is the direct sum of infinite cyclic subgroup $C_1, C_2 \cdots C_k$

Now consider that any generating set $\{a_1, a_2 \cdots a_k\}$ of A does not satisfies condition (1)

i.e $\exists\ x_i (\neq 0) \in \mathbb{Z}$ such that

$x_1 a_1 + x_2 a_2 + \cdots + x_k a_k = 0 \quad (x_j \in \mathbb{Z}, j = 1, \cdots k)$

i.e
$$\sum_{j=1}^{k} x_j a_j = 0 = \sum_{j=1}^{k} (-x_j) a_j$$ gives at least one

$x_j > 0$ or $-x_j > 0$

Let us consider $x_j > 0$ for some j.

Consider now all possible generating sets $\{a_1, a_2 \cdots a_k\}$ of A with k-elements and let X denotes the set of all k-tuples of image $(x_1, x_2, \cdots x_n)$ such that

$$\sum_{i=1}^{k} x_i a_i = 0$$ where $\{a_1, a_2 \cdots a_n\}$ is any generating set of A.

Let m_1 be the least positive integer that occurs in any component of k-tuples in X without loss of generality we take m_1 to be the first component so that for some generating set $\{a_1, a_2 \cdots a_k\}$

Scanned by CamScanner

$\cdot m_1 a_1 + x_2 a_2 + \cdots + x_k a_k = 0$ — ② By D.A

where $x_i = m_1 q_i + r_i$ where $0 \le r_i < m_1$, $i = 1, 2, \ldots k$

then ② becomes

$$m_1 a_1 + (m_1 q_2 + r_2) a_2 + \cdots + (m_1 q_k + r_k) a_k = 0$$

i.e $m_1 b_1 + r_2 a_2 + \cdots + r_k a_k = 0$.

Where

$$b_1 = a_1 + q_2 a_2 + q_3 a_3 + \cdots + q_k a_k \in A \quad — ③$$

Now $b_1 \ne 0$ otherwise $a_1 + q_2 a_2 + \cdots + q_k a_k = 0$

i.e $a_1 = -q_2 a_2 - \cdots - q_k a_k$.

which implies that A is generated by $\{a_2, a_3, \ldots a_k\}$ by $k-1$ element which is contradiction

$\therefore b_1 \ne 0 \Rightarrow a_1 = b_1 - q_2 a_2 + \cdots + q_k a_k$

Hence $\{b_1, a_2, a_3, \ldots a_k\}$ is also generating set of A

$\therefore$ by minimal positive property of m_1 gives by ③ $r_2 = r_3 = \cdots = r_k = 0$.

$\Rightarrow m_1 b_1 = 0$

Let $G_1 = [b_1]$ because m_1 is the least positive integer such that $m_1 b_1 = m_1 b_1 + 0 \cdot a_2 + \cdots + 0 \cdot a_k$

G_1 is a cyclic subgroup of order m_1

$$|G_1| = o(b_1) = m_1$$

Let A_1 be the subgroup generated by $\{a_2, a_3 \ldots a_k\}$ then $A = \{b_1, a_2, \ldots a_k\}$

$$= [b_1] + [\{a_2 \ldots a_k\}]$$

$$= G_1 + A_1$$

Where $A_1 = [\{a_2 \ldots a_k\}]$

$G_1 \cap A_1$ is a subgroup of A.

$\forall x \in G_1 \cap A_1 \Rightarrow x \in G_1$ & $x \in A_1$

$\Rightarrow x = x_1 b_1$ & $x = x_2 a_2 + \cdots + x_k a_k$

$\Rightarrow x_1 b_1 = x_2 a_2 + \cdots + x_k a_k$

$\Rightarrow x_1 b_1 - x_2 a_2 - \cdots - x_k a_k = 0$

Where $0 \le x_1 \le m_1 - 1 < m_1$

$\Rightarrow x_1 = 0$ by minimality of m_1

$\therefore G_1 \cap A_1 = \{0\}$ $G_1 \triangle A$, $A_1 \triangle A$.

$\Rightarrow A = G_1 + A_1 = G_1 \oplus A_1$

Now A_1 is generated by a set $k-1$ elements namely $\{a_2, a_3 \cdots a_k\}$

Moreover A cannot be generated by a set which is less than k-1 element for otherwise A is generated by a set of elements less than k a contradiction

By Induction hypothesis theorem is true for abelian group A_1 generated by k-1 elements. So

$$A = C_1 \oplus C_2 \oplus \cdots \oplus C_k$$

Where $C_2 = [b_2]$, $C_3 = [b_3] \cdots C_k = [b_k]$ are cyclic groups.

Either all are infinite cyclic groups. or $\exists$ $j \leq k$ such that $C_2, C_3 \cdots C_j$ are finite cyclic groups of orders $m_2, m_3 \cdots m_j$ respectively, with $m_2 | m_3 | m_4 | \cdots | m_j$ and $C_{j+1}, C_{j+2}, \cdots C_k$ are infinite cyclic group.

Let us consider $|C_2| = m_2$ etc

Here $\{b_1, b_2 \cdots b_k\}$ is a generating set of A & $C_i = [a_i]$ $\forall i$

we have

$$o(a_1) = m_1, \quad o(a_2) = m_2$$

i.e $m_1 a_1 = 0$, $m_2 a_2 = 0$ $(m_1, m_2 \in \mathbb{N})$

$\Rightarrow m_1 a_1 + m_2 a_2 + 0 \cdot a_3 + \cdots + 0 a_k = 0$ — (4)

By definition of $m_1 \leq m_2$ & by division algorithm

$$m_2 = m_1 q + r \quad \text{for } q, r \in \mathbb{Z} \quad 0 \leq r < m_1$$

Then (4) $\Rightarrow$

$$m_1 a_1 + (m_1 q + r) a_2 + 0 \cdot a_3 + \cdots + 0 \cdot a_k = 0$$

& $\{a_1 + q a_2, a_3, \cdots a_k\}$ is a generating set for A

$\Rightarrow$ $r = 0$ by minimal property of m_1

$m_2 = m_1 q + r$ i.e $m_1 | m_2$

$\cancel{= mq}$

Thus $A = C_1 \oplus C_2 \oplus \cdots \oplus C_k$

Where either all $C_1, C_2 \cdots C_k$ are infinite cyclic groups or $\exists$ $j \leq k$ s.t $C_1, C_2 \cdots C_j$ are finite cyclic subgroups $m_1 m_2 \cdots m_j$ are all infinite cyclic groups

~~Hence by~~

* Invarients of a finite abelian group:-

Th^m - Let A be a finite abelian group. then there exists a unique list of integers $m_1 . m_2 ---- m_k$ (all > 1) such that.

$$|A| = m_1 . m_2 ---- m_k ; \; m_1 | m_2 | m_3 --- | m_k$$

and

$A = C_1 \oplus C_2 \oplus ---- \oplus C_k$ Where $C_1, ---- C_k$ are cyclic subgroups of A of orders $m_1, m_2, ----, m_k$ respectively consequently

$$A \cong \mathbb{Z}_{m_1} \oplus ---- \oplus \mathbb{Z}_{m_k}$$

→ Let A be a finite additive abelian group. then by fundamental theorem of finitely generated abelian group

$$A = C_1 \oplus C_2 \oplus --- \oplus C_k \cong C_1 \times C_2 \times ---- \times C_k$$

Where $C_1, C_2, --- C_k$ are cyclic subgroup of A of order $m_1, m_2 --- m_k$ respectively Such that $m_1 | m_2 | --- | m_k$ As

$$|S \times T| = |S| \cdot |T| \text{ any finite sets of } S \& T$$

it follows that $|A| = |C_1||C_2| --- |C_k|$
$= m_1 . m_2 --- m_k$

Moreover any cyclic group of order m is isomorphic to $\mathbb{Z}_m$.

Hence $A \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times --- \times \mathbb{Z}_{m_k}$

i.e

$$A \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus --- \oplus \mathbb{Z}_{m_k}$$

To prove uniqueness of the list $m_1, m_2 --- m_k$ of A:-

Assume $A = C_1 \oplus C_2 \oplus ---- \oplus C_k =$
$D_1 \oplus D_2 \oplus --- \oplus D_l$ —— (1)

Where C_i, D_j are cyclic subgroups of A with $|C_i| = m_i$ $|D_j| = n_j$ & $m_1 | m_2 | --- | m_k$ & $n_1 | n_2 --- | n_l$

Now D_l has an element of order n_l

But order of every elements in A is m_k

So $n_l \le m_k$

Similarly we have $m_k \le n_l$ Hence $m_k = n_l$

Now consider

$$m_{k-1} A = \{ m_{k-1} a \mid a \in A \}$$

From ①

$$m_{k-1} A = (m_{k-1} C_1) \oplus (m_{k-1} C_2) \oplus \cdots \oplus (m_{k-1} C_k) = (m_{k-1} D_1) \oplus \cdots (m_{k-1} D_l)$$

Because $m_i \mid m_{k-1}$ for $i = 1, 2 \cdots k-1$ it follows

$$m_{k-1} C_i = \{0\}$$

So

$m_{k-1} A = m_{k-1} C_k$ is a cyclic subgroup of A &

$$|m_{k-1} A| = |m_{k-1} C_k| = |m_{k-1} D_l| = \frac{m_k}{m_{k-1}}$$

$$\therefore m_{k-1} A = m_{k-1} C_k = m_{k-1} D_l$$

& hence $m_{k-1} D_j = \{0\} \ \forall j$

$m_{k-1} D_{l-1} = \{0\}$ & D_{l-1} is cyclic

$\Rightarrow |D_{l-1}|$ divides m_{k-1}

i.e $n_{l-1} \mid m_{k-1}$

By symmetry argument $m_{k-1} \mid n_{l-1}$

$\therefore m_{k-1} = n_{l-1}$ proceding in this manner we can show that $m_{k-r} = n_{l-r}$ $r = 0, 1, \cdots$

But by ①

$$|C_1||C_2| \cdots |C_k| = |A| = |D_1||D_2| \cdots |D_l|$$

i.e $m_1 m_2 \cdots m_k = |A| = n_1 n_2 \cdots n_l$

Hence $k = l$ & $m_i = n_i$ for $i = 1, 2 \cdots k$

This proves uniqueness of the list $m_1 m_2 \cdots m_k$ with $m_1 | m_2 | m_3 \cdots | m_k$ etc

*Def^n :- Let A be a finite abelian group if

$$A \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_k} \text{ where } 1 < m_1 | m_2 \cdots | m_k$$

then A is said to be of type $(m_1, m_2 \cdots m_k)$ and the integers $m_1, m_2 \cdots m_k$ are called the invariants of A.

Lemma - There is a 1-1 correspondance between the family F of nonisomorphic abelian groups of order p^e, p prime and the set p(e) of partitions of e.

→ Let p be prime, $e \in \mathbb{N}$ & F be the family of all nonisomorphic abelian groups of order p^e. Let $A \in F$ then A determines a unique tuple $(p^{e_1}, p^{e_2} \cdots p^{e_k})$ where $1 \le e_1 \le e_2 \cdots \le e_k$

$$e_1 + e_2 + \cdots + e_k = e$$

Define a map $\sigma : F \longrightarrow p(e)$

$$\sigma(A) = (e_1, e_2 \cdots e_k)$$

$\therefore$ σ is clearly one-one.

Consider any $(e_1, e_2 \cdots e_s) \in p(e)$ i.e $e_1 \le e_2 \cdots \le e_s$ & $e_1 + e_2 + \cdots + e_s = e$

then $\exists$ an abelian group B of order $p^{e_1} p^{e_2} \cdots p^{e_s} = p^{e_1 + e_2 + \cdots + e_s} = p^e$

Such that

$$B \cong \mathbb{Z}_{p^{e_1}} \times \mathbb{Z}_{p^{e_2}} \times \cdots \times \mathbb{Z}_{p^{e_s}}$$

&

$$\sigma(B) = (e_1, e_2 \cdots e_s)$$

($\because$ B has invariants $p^{e_1}, p^{e_2} \cdots p^{e_s}$)

$\therefore$ σ is onto.

Thus $\sigma : F \longrightarrow p(e)$ is a one-one correspondence and lemma follows.

Example :- Find the nonisomorphic abelian group of order 360.

$\rightarrow$ $n = 360$

$= 2^3 \times 3^2 \times 5$

$P_1 = 2$, $P_2 = 2$, $P_3 = 5$

$f_1 = 3$ $f_2 = 2$ $f_3 = 1$

$p(3) = 3$ $p(2) = 2$ $p(1) = 1$

$$\prod_{j=1}^{3} |P(f_j)| = |P(f_1)|\,|P(f_2)|\,|P(f_3)|$$

$$= |P(3)|\,|P(2)|\,|P(1)|$$

$$= 3 \times 2 \times 1$$

$$= 6$$

$\therefore$ 6 nonisomorphic abelian groups of order 360 they are

① $\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$,

② $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

③ $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

④ $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

⑤ $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

⑥ $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

25

& $A = S(P_1) \oplus S(P_2) \oplus \cdots \oplus S(P_k)$ — (1)

$P_1^{e_1} P_2^{e_2} \cdots P_k^{e_k} = P_1^{s_1} P_2^{s_2} \cdots P_k^{s_k}$ it follows that

$s_i = e_i \ \forall i$ &

$|S(P_1)| = P_1^{e_1}, \ |S(P_2)| = P_2^{e_2} \cdots |S(P_k)| = P_k^{e_k}$

To prove — Decomposition of A gives by (1) is unique

Assume $A = H_1 \oplus H_2 \oplus \cdots \oplus H_k$

where $H_i \triangle A$ & $|H_i| = P_i^{\alpha_i} \ \forall i = 1, 2 \cdots K$

$P_1^{e_1} P_2^{e_2} \cdots P_K^{e_K} = P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_K^{\alpha_K}$

$\Rightarrow \alpha_i = e_i \ \forall i$

Hence

$|H_i| = P_i^{e_i} = |S(P_i)|$.

Theorem — Let $n = \prod_{j=1}^{k} P_j^{f_j}$, P_j distinct primes

Then the number of nonisomorphic groups n is

$$\prod_{j=1}^{k} |P(f_j)|$$

→

Let $n = \prod_{j=1}^{k} P_j^{f_j}$ where $P_1, P_2 \cdots P_K$ are

are distinct primes & $f_j \in \mathbb{N} \ \forall j$

Let Ab_n be the family of nonisomorphic abelian group of order n.

Let $A \in Ab_n$ then $A = S(P_1) \oplus S(P_2) \oplus \cdots \oplus S(P_K)$

where $S(P_i)$ is a subgroup of A of order $P_j^{f_j}$ $i = 1, 2 \cdots k$

Number of nonisomorphic abelian group of order $P_i^{f_i}$ is $|P(f_j)|$ i.e there are

$|P(f_i)|$ choise for $S(P_i)$

Hence $|Ab_n| = |P(f_1)| \, |P(f_2)| \cdots |P(f_K)|$

$$= \prod_{j=1}^{k} |P(f_j)|$$

<u>Example</u> :- Find the nonisomorphic abelian group of order 360.

$\rightarrow$ $n = 360$

$= 2^3 \times 3^2 \times 5$

$p_1 = 2$, $p_2 = 2$, $p_3 = 5$

$f_1 = 3$ $f_2 = 2$ $f_3 = 1$

$p(3) = 3$ $p(2) = 2$ $p(1) = 1$

$$\prod_{j=1}^{3} |p(f_j)| = |p(f_1)|\,|p(f_2)|\,|p(f_3)|$$

$$= |p(3)|\,|p(2)|\,|p(1)|$$

$$= 3 \times 2 \times 1$$

$$= 6$$

$\therefore$ 6 nonisomorphic abelian groups of order 360 they are

① $\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$,

② $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

③ $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

④ $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

⑤ $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

⑥ $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

* Sylow theorem :- 27

* Definition :-

Let G be a finite group and let p be a prime. Let $p^m \mid |G|$, $p^{m+1} \nmid |G|$, $m>0$ then any subgroup of G of order p^m is called a Sylow p-subgroup of G

* Definition :-

Let p be prime. A group G is called a p-group if the order of every element in G is some power of p. Likewise a subgroup H of any group G is called a p-subgroup of G if the order of every element in H is some power of p

<u>Lemma</u> :- (Cauchy's theorem for abelian group)

Let A be a finite abelian group and let p be a prime. If p divides $|A|$ then A has an element of order p.

<u>proof</u> - Let A be a finite abelian group i.e $|A| = n \in \mathbb{N}$ & p is a prime with $p \mid |A|$ i.e $p \mid n$

We prove the theorem by using induction on n

If $p = n$. or A is a cyclic group then A has exactly one subgroup H of order p

Every element of H except identity is of order p.

In this case theorem is true

Next consider $n > p$ & A is a noncyclic but abelian group.

Assume that theorem is true for any abelian group of order $m < n$ & $p \mid m$

Consider $b \in A$, $b \neq e$ then $[b] \Delta A$,

$A \neq [b] \neq \{e\}$

If $p \mid |[b]|$ then the cyclic group $[b]$ has a subgroup of order p and hence an element $a \in [b]$ with $o(a) = p$

If $p \nmid |[b]|$ then $p \mid \left|\frac{A}{[b]}\right|$ & $\left|\frac{A}{[b]}\right| = \frac{|A|}{o[b]} = \frac{|A|}{o(b)} = \frac{n}{o(b)} < n$

Hence by induction hypothesis's in $\frac{A}{[b]}$ has an element $a[b]$ of order p

i.e $o(a[b]) = p$

Let $o(a) = k$ i.e $a^k = e$

$\therefore (a[b])^k = a^k[b] = e[b] = [b]$ identity of group $\frac{A}{[b]}$

$\Rightarrow o(a[b]) \mid k$ i.e $p \mid k$ i.e $p \mid |[a]|$ ($\because k = o(a) = |[a]|$)

$\Rightarrow$ cyclic subgroup $[a]$ has a subgroup of order p

$\therefore \exists\ c \in [a]$ s.t $o(c) = p$ & also $c \in A$

Thus if p is prime & $p \mid |A|$ then $\exists\ x \in A$ such that $o(x) = p$.

* **Theorem** :- (First Sylow theorem)

Let G be a finite group and let p be a prime If p^m divides $|G|$ then G has a subgroup of order p^m.

Proof - Let G be finite group of order n i.e $|G| = n \in \mathbb{N}$. Let p be a prime such that $p^m \mid |G|$ i.e $p^m \mid n$ ($m \in \mathbb{N} \cup \{0\}$)

We prove the theorem using induction on n.

If $n = 1$ then $p^0 \mid n$ (i.e $1 \mid 1$) & G has a subgroup $G = \{e\}$ of order p^0.

Theorem is true for $n = 1$ Also true for $m = 0$

Consider $n > 1$ & $m \in \mathbb{N}$

Assume theorem is true for any group whose order is less than n.

Now $Z(G) \trianglelefteq G$ we have either

$p \mid |Z(G)|$ or $p \nmid |Z(G)|$

I) Let $p \mid |Z(G)|$. $Z(G)$ ~~be~~ is an ~~eleme~~ abelian normal subgroup of G & $p \mid |Z(G)|$

By Cauchy's theorem for finite abelian group $\exists\ a \in Z(G)$ such that $o(a) = p$

$\therefore C = [a] < Z(G)$ & hence $[a] < Z(G) \trianglelefteq G \Rightarrow [a] \trianglelefteq G$

& $|[a]| = o(a) = p$

then $\frac{G}{C}$ is a group & $\left|\frac{G}{C}\right| = \frac{|G|}{|C|} = \frac{|G|}{|[a]|} = \frac{|G|}{p}$ &

$p^{m-1} \mid \left|\frac{G}{C}\right|$ $\because p^m \mid G$, $\left|\frac{G}{C}\right| = \frac{|G|}{|C|} = \frac{n}{|[a]|} = \frac{n}{p} < n$ &

$p^{m-1} \mid \left|\frac{G}{C}\right|$

By induction hypothesis $\frac{G}{C}$ has a subgroup $\overline{H}$ of order p^{m-1} Now

$$\overline{H} < \frac{G}{C} \Rightarrow \overline{H} = \frac{H}{C}.$$

Where H is a subgroup of G containing C

Now $p^{m-1} = |\overline{H}| = \left|\frac{H}{C}\right| = \frac{|H|}{|C|} = \frac{|H|}{p} \Rightarrow |H| = p^{m-1}p$

$\Rightarrow |H| = p^m$

Hence H is a subgroup of G of order p^m.

II) Let $p \nmid Z(G)$

class equation of the group G is

$$n = |G| = |Z(G)| + \sum_a [G : N(a)] \quad \text{—— (1)}$$

Where summation runs over one element from each conjugate class having more than one element.

[$a \in Z(G)$ iff $cl(a) = \{a\}$ iff $N(a) = G$

iff $[G : N(a)] = 1$ &

$a \in G - Z(G)$ i.e $a \notin Z(G)$

iff $|cl(a)| = |\{xax^{-1} \mid x \in G\}| > 1$

iff $N(a) < G$ i.e $[G : N(a)] > 1$]

As $p \mid n$ i.e $p \mid |G|$ & $p \nmid Z(G)$

So by (1) $p \nmid [G : N(a)]$ for some $a \in G - Z(G)$

Here $p^m \mid |G|$ i.e $p^m \mid |N(a)| \cdot [G : N(a)]$ &

$\gcd(p^m, [G : N(a)]) = 1$

$\Rightarrow p^m \mid |N(a)|$ & $N(a)$ is a proper subgroup of G

i.e $|N(a)| < |G| \Rightarrow |N(a)| < n$

By induction hypothesis $N(a)$ has a subgroup say H of order p^m

$H < N(a) < G \Rightarrow H$ is a subgroup of G

& $|H| = p^m$. thus G has a subgroup of order p^m

Hence proved.

Corollary - (Cauchy's theorem)

If the order of a finite group G is divisible by a prime number p then G has an element of order p.

proof - Let G is a finite group & p is a prime with $p \mid |G|$ By first Sylow theorem, G has a subgroup H of order p i.e $\exists\, a \in G$ such that $H = [a]$ &

$o(G) = |H| = p$ Thus $\exists\, a \in G$ with $o(a) = p$

Note -

In H there are $\phi(p) = p-1$ element each of order p.

Corollary - A finite group G is a p-group iff it's order is a power of p.

→ Let G be a finite group & p be a prime.

I) Let order of G be a power of p.

i.e $|G| = p^n$ for some $n \in \mathbb{N}$

By a corollary, $o(a) \mid |G|$ i.e $o(a) \mid p^n \; \forall a \in G$

$\Rightarrow o(a) = p^k$ where $k = \{0, 1, 2 \dots n\} \; \forall a \in G$

i.e Every element in G has order as integral power of p.

$\therefore G$ is a p-group

II) Let G be a p-group

$\therefore$ Each element of G has an integral power of p i.e $p \mid |G|$ then $|G| = p^n . m$ for some $n, m \in I$

& $\gcd(p, m) = 1$ i.e $p \nmid m$

Suppose $m \neq 1$ then $m > 1$ & m has a prime factor say q & $q \neq p$ As $q \mid m$, $m \mid |G|$

So $q \mid |G|$ & q is prime So, by cauchy theorem of finite group G has an element of order q. a contradiction to hypothesis $(q \neq p)$

$\therefore$ Supposition $m \neq 1$ is wrong

Hence $m = 1$ & so $|G| = p^n m = p^n$.

* **Theorem** (second and third Sylow theorem)

Let G be a finite group and let p be a prime then all Sylow p-subgroup of G are conjugate and their number n_p divides $o(G)$ and satisfies $n_p \equiv 1 (\mod p)$.

→ Let G be a finite group $|G| = p^m q$ where p is a prime & $m, q \in \mathbb{N}$ such that $p \nmid q$ i.e $\gcd(p, q) = 1$. Any subgroup of G of order p^m is a Sylow p-subgroup of G

Let S be a Sylow p-subgroup of G of order p^m i.e $S < G$ & $|S| = p^m$

Let $m = C(S)$ be the collection of conjugate of S.

<u>To prove</u> :- Every Sylow p-subgroup is conjugate to S i.e in m.

Suppose $\exists$ a Sylow p-subgroup H is not conjugate to S i.e $H \notin m$.

Let K be any Sylow p-subgroup of G different from H

Since $|H| = |K| = p^m$ & $H \neq K$ so $H \nsubseteq K$ & $K \nsubseteq K$

Then $\exists$ $x \in H$ & $x \notin K$ then $xKx^{-1} \neq K$

otherwise $xKx^{-1} = K \Rightarrow x \in N(K)$ & as $x \in H$

i.e $o(x) \mid o(H) = p^m$

i.e x has order as a power of p

$x \in K$ a contradiction ($\because x \notin K$)

Thus $xKx^{-1} \neq K$ $\forall$ $x \in H - K$

$\therefore$ The number of conjugate of K determined by elements of H is more than one.

Since these number is equal to

$$|C_H(K)| = [H : N_H(K)]$$ which is generated than so $N_H(K)$ is a proper subgroup of H

$$\text{i.e } [H : N_H(K)] = \frac{|H|}{|N_H(K)|} > 1 \quad \text{i.e } N_H(K) \neq H$$

$$p^m = |H| = [H : N_H(K)]\,|N_H(K)|$$

$\Rightarrow [H : N_H(k)] / p^m$

i.e no. of conjugate of k by elements H.
is $|C_H(k)| = [H : N_H(k)]$ & $1 < |C_H(k)| \mid p^m$.

$\Rightarrow [C_H(k)] = p^l$ for some $l \in \mathbb{N}$
= a multiple of p

Thus, if H & k are sylow p-subgroup of G & $H \neq k$ then number of conjugate of k by elements of H is a multiple of p

on m defined a relation $\sim$ by for $S_1, S_2 \in M$ $S_1 \sim S_2$ means $S_1 = x S_2 x^{-1}$ for some $x \in H$ Then $\sim$ is an equivalence relation. on m & it devides m into disjoint equivalence classes

For any $k \in M$, $k \neq m$ the number of conjugate of k determined by element of H is a multiple of p

$\therefore |M| = |C(S)|$ = a multiple of p

i.e $t = |C(S)|$ is divisible by p

i.e $p \mid t$

But $|C(S)| = [G : N(S)]$

$p^m q = |G| = |S| [G : S] = p^m$

$[G : S] = q$, $p \nmid q$

Now. $q = [G : S] = [G : N(S)] [N(S) : S] = t$

$[N(S) : S] \Rightarrow t \mid q$ But $p \nmid q$

so $p \nmid t \rightarrow \leftarrow$ to $p \mid t$

$\therefore$ Supposition $\exists$ sylow p-subgroup H with $H \notin m$ is wrong.

Hence for any sylow p-subgroup H of G we have $H \in m$.

Let H, k be any sylow p-subgroup of G

$\Rightarrow H \in m$, $k \in m$ i.e $H \sim S$, $k \sim S$. i.e $S \sim k$

$\Rightarrow H \sim S$

$\because \sim$ is an equivalence classes

Thus, any two sylow p-subgroups are Conjugate to each other.

$M = C(S) = \{xSx^{-1} \mid x \in G\}$

For $S_1, S_2 \in M$

Let $S_1 \sim S_2$ means $S_1 = xS_2x^{-1}$ for some $x \in H$ Where H is a sylow p-subgroup of G then $\sim$ is an equivalence relation on M & hence M is divided into equivalence classes for $K \in M$ equivalence classes $C_H(k)$ & $|C_H(k)| =$ a multiple of p for $k \neq H$

Now

$H \in M$ also $C_H(H) = \{xHx^{-1} \mid x \in H\} = \{H\}$

i.e $|C_H(H)| = 1$

Thus M is divided into equivalence classes where one class is of cardinality 1 & remaining equivalence class have number of element as multiple p Thus if n_p is the number of Sylow p-subgroup in the group G then

$$n_p = |M| = |C(S)|$$
$$= 1 + \text{sum multiple of } p$$
$$= 1 + rp \quad \text{for some } r \geq 0$$

we have $|G| = |N(S)|\,|G : N(S)|$

$$= |N(S)|\,|C(S)|$$
$$= |N(S)|\, n_p$$

$\Rightarrow n_p \mid |G|$ where $n_p = 1 + rp$

$n_p - 1 = rp$

$\Rightarrow p \mid n_p - 1$

$\Rightarrow n_p \equiv 1 \bmod p$

Corollary: A sylow p-subgroup of a finite group G is unique iff it is normal.

$\Rightarrow$ Let G be a finite group p be a prime

$n_p =$ No. of sylow p-subgroup of $G = |C(k)|$

$= [G : N(k)]$

G has unique sylow p-subgroup k iff $n_p = 1$

iff $[G : N(k)] = 1$ i.e $\frac{|G|}{|N(k)|} = 1$ iff $|G| = |N(k)|$ iff $G = \{x \in G \mid xkx^{-1} = k\}$

prove that there are no simple group of orders 63, 56 & 36

→ First consider any group of order 56

① $|G| = \cancel{56}\,63 = 3 \times 21$
$= 3^2 \times 7$

By sylow's first theorem
G has a Sylow-7 subgroup containg 7 elemen & Sylow-3 subgroup containg 9 element

n_7 = Number of sylow-7 subgroup of G
$n_7 \mid \cancel{o(G)}\,63$ & $n_7 = 1 + 7r \equiv 1 \bmod p$

i.e $1+7r \mid \cancel{o(G)}\,63$ & $\gcd(1+7\cancel{x}, 7) = 1$.

$1+7r \mid 9 \times 7$ & $\gcd(1+7r, 7) = 1$

$\Rightarrow 1+7r \mid 9 \Rightarrow 1+7r \mid 3^2$ & $n_7 \equiv 1 \pmod 7$

~~& $r \geq 0 \Rightarrow 1 \mid 3^2$, 8/9, 9 & $n_7 \equiv 1 \bmod 7$)~~
~~$1 + n_7 \equiv 1 \bmod 7$~~

This is true for $r = 0$.
$1 \mid 3^2$, & $n_7 \equiv 1 \pmod 7$)
$n_7 = 1 + 7r = 1 + 70 = 1$.

∴ G has a unique sylow 7 subgroup that must be normal subgroup.
∴ G ~~has~~ is not a simple group.

② $|G| = 56 = 2^3 \times 7$

~~Con~~ By sylow's ~~first~~ Theorem,
G has sylow's 7-subgroup (containg 7 element) & a sylow's 2-subgroup (containg 8-elements)

n_7 = Number of sylow 7-subgroup of G
& $n_7 = (1+7r) \mid |G|$.

i.e $(1+7r) \mid 8\times 7^{3r}$ & $\gcd(1+7r, 7)=1$

$\Rightarrow$ $(1+7r) \mid 8$ & $n_7 = 1+7r \equiv 1 \pmod 7$

$\therefore$ This is true for $r=0$ or $r=1$ only

If $r=0$ then $n_7 = 1+7r = 1$,

i.e G has unique sylow 7-subgroup

$\therefore$ it has a normal subgroup H.

$\therefore$ G ~~has~~

i.e H is a nontrivial normal subgroup of G.

So the group G is not simple.

If $r=1$ then $n_7 = 1+7r = 8$

i.e G has a 8-different sylow 7-subgroup each of order 7

Each of these 8 sylow-7 subgroup has 6 generators (each of order 7)

There are $6\times 8 = 48$ element in G each of order 7.

Then $56-48=8$ remaining elements of G forms a unique sylow 2-subgroup.

i.e $K \trianglelefteq G$, $|K|=8$ i.e K is a nontrivial normal subgroup of G

$\therefore$ Group G is not simple.

(3) Let G be any group of order 36

$|G| = 36 = 2^2\times 3^2$

$\therefore$ G has a sylow 3-subgroup (containg 9 element) say H of order 9

$$[G:H] = \left|\frac{G}{H}\right| = \frac{|G|}{|H|} = \frac{36}{9} = 4$$

Then $\exists$ a group homomorphism $\phi : G \to S_4$

As $|G| = 36$, $|S_4| = 4! = 24$

the homomorphism ϕ is not 1-1 &

So $\ker\phi \neq \{e\}$ i.e $|\ker\phi| > 1$

Also $\ker\phi \trianglelefteq G$ & $\ker\phi = \bigcap_{x\in G} xHx^{-1} \le eHe^{-1} = H$

$$|\ker\phi| \le |H| = 9$$

Thus $\ker\phi \trianglelefteq G$ & $\{e\} \neq \ker\phi \neq G$

$\therefore$ G has a nontrivial normal subgroup

Kerϕ

$\therefore$ group G is not simple.

Note -

Let G be a finite group with $|G| = pq$ where p & q are distinct primes $p<q$ then

1) G contains a normal subgroup of order q
2) G is not simple
3) If $p \nmid q-1$ then G is cyclic (& hence abelian) group

Example ① ~~Any~~ Show that any group of order 15 is cyclic

$\rightarrow$ Let G be any group of order 15

$\therefore |G| = 15 = 3 \times 5 \quad p = 3 \ \& \ q = 5 \quad p<q$

If $p \nmid q-1 \Rightarrow 3 \nmid 5-1$

$\Rightarrow$ G is cyclic

② Show that Any group of order 21 is not simple.

$\rightarrow |G| = 21 = 7 \times 3$ where 3 & 7 are primes & $3<7$

then G contain a normal subgroup of order 7

$\therefore$ G has proper normal subgroup

$\therefore$ G is not simple

Or

$|G| = 21 = 7 \times 3$

$n_7 \mid 7 \times 3 \quad n_7 \equiv 1 \pmod p$

$\Rightarrow 1+7r \mid 7 \times 3, \ \gcd(1+7r, 7) = 1 \Rightarrow n_7 = 1+7r \equiv 1 \bmod 7$

$1+7r \mid 3, \quad r = 0 \quad n_p = 1+7r = 1$

$(n_7 = 1)$

$\therefore$ it has unique normal subgroup of order 7.

$\therefore$ G is not simple.