SRIMAAN

TRB ASSISTANT PROFESSOR

Assistant Professor in Govt. Arts and Science Colleges and Govt. Colleges of Education in the Tamil Nadu Collegiate Educational Service

MATHEMATICS

UNIT-1- ALGEBRA

SRIMAAN COACHING CENTRE-TRICHY.

TO CONTACT:+91 8072230063.

TRB-ASSISTANT PROFESSOR

MATHEMATICS

ASSISTANT PROFESSORS IN TAMIL NADU COLLEGIATE EDUCATIONAL SERVICE FOR GOVERNMENT ARTS & SCIENCE COLLEGES

UNIT-1: ALGEBRA

Permutations, Combinations, Applications of classical number theoretic properties, Groups, Counting Principles, Cayley's theorem, Permutation groups, Sylow's theorems, Direct Products, Polynomial Rings, Vector spaces, Inner Product Spaces, Orthonormal bases, Modules, Fields, Roots of polynomials, Elements of Galois theory, Splitting fields, Degrees of Splitting fields of polynomials, Solvable groups, Linear transformations, Matrix representation, Canonical forms, Determinants, Cayley Hamilton theorem and Applications, Hermitian, Unitary and Normal Transformations, Quadratic Forms, Finite fields, Wedderburn's Theorem on Finite division rings, Frobenius Theorem, Integral Quaternions and Four Square Theorem.

Introduction. This chapter contains definitions and results related to groups, cyclic group, subgroups, normal subgroups, permutation group, centre of a group, homomorphism and isomorphism. All of these results will be helpful throughout the further study of the course.

Definitions.

Cartesian Product of Two Sets. Let A and B be two non-empty sets. Then, the set of all distinct ordered pairs whose first co-ordinate is an element of A and whose second co-ordinate is an element of B is called cartesian product of A and B and is denoted by $A \times B$. For example, let

$A = \{1,2\}$, $B = \{4,5\}$, then

$A \times B = \{(1,4),(1,5),(2,4),(2,5)\}$ and $B \times A = \{(4,1),(4,2),(5,1),(5,2)\}$.

Thus, in general, $A \times B \neq B \times A$ if $A \neq B$. Also, $A \times B = \phi$ if A or B or both of A and B are empty sets.

Function. Let A and B be two given non-empty sets. A correspondence denoted by f, which associates to each member of A a unique member of B is called a function. The function f from A to B is denoted by $f : A \to B$.

Binary Operation. A mapping $f : S \quad S \quad \times \quad S \to$ is called a binary operation on the set S.

Algebraic Structure. A non-empty set S equipped with one or more binary operations is called an algebraic structure. Suppose '*' is a binary operation on S. Then, (S,*) is called an algebraic structure.

Group. LetG be a non-empty set with a binary operation '*'. Then, G is called a group w.r.t. binary operation '*' if following postulates are satisfied:

(i) Associativity:

(ii) Existence of Identity

(iii) Existence of Inverse.

Abelian Group. A group G is called an Abelian group or commutative group if in addition to above postulates G also satisfies the commutative law.

Important Results.

(i) The identity element in a group is unique.

(ii) Every element in a group have a unique inverse.

(iii) If a,b,c be elements of G such that ab = ac, then b = c (Left cancellation law)

and ba = ac, then b = c (right cancellation law)

(iv) If $a \in G$, then $\left(a^{-1}\right)^{-1} = a.$

(v) If a,b $\in$ G, then $(ab)^{-1} = b^{-1}a^{-1}$

(vi) If G is an Abelian group, then for all a,b $\in$G and any integer n, we have $(\text{ab})^n = a^n b^n$.

(vii) If every element of the group is its own inverse, then the group is Abelian.

(viii) If a group has a finite number of elements, this number is called the order of the group and the group is called finite group. A group with an infinite number of elements is called an infinite group.

(ix) If G is a group such that $(\text{ab})^n = a^n b^n$ for three consecutive integers m and for all a,b $\in$G , then G is Abelian.

Subgroup. A non-empty subset H of a group G is said to be a subgroup of G if H itself is a group w.r.t. the same binary operation as in G.

Proper and Improper subgroups. The subgroups {e} and G itself are called improper subgroups of G. All other subgroups, other than {e} and G, are called proper subgroups of G.

Coset of a Subgroup. LetG be a group and H is any subgroup of G. Let 'a' be any element of G. Then, the set $\text{Ha} = \{\text{ha} : \text{h} \in \text{H}\}$ is called a right coset of H in G generated by 'a'. A left coset aH can be defined in a similar way. Also, a subset is called a coset of H in G generated by 'a' if Ha = aH.

Normal Subgroup. A subgroup N of a group G is said to be a normal subgroup of G iff Na = aN for all a G $\in$, that is, right and left cosets are same for every element of G. We denote a normal subgroup N of a group G by $N \underline{\Delta} G$.

Remark. (i) A subset H of a group G is a subgroup iff $ab^{-1} \in \text{H}$ for all $a, b \in \text{H}$.

(ii) A finite subset H of a group G is a subgroup iff $ab \in \text{H}$ for all $a, b \in \text{H}$.

(iii) Let H and K be two subgroups of a group G. Then, the set

$$\text{HK} = \{\text{x} : \text{x} = \text{hk where h} \in \text{H}, \text{k} \in \text{K}\}$$

is a subgroup of G iff HK = KH.

(iv) If H is a subgroup of G then Hg = H = gH iff $g \in \text{H}$.

(v) Any two right(left) cosets of a subgroup are either disjoint or identical.

(vi) If H is a finite subgroup of G. Then, $o(\text{H}) = \text{o}(\text{Ha})$ for all $a \in \text{G}$.

(vii) A group $G \neq \{e\}$ which does not have any non-trivial normal subgroup is called a **simple group**.

(viii) A subgroup H of a group G is normal iff $g^{-1}hg \in H$ for every $h \in H, g \in G$.

(ix) Every subgroup of an Abelian group is a normal subgroup.

(x) Let H be a subgroup of G. The number of distinct right cosets of H in G is called the index of H in G and written as [G : H].

(xi) If [G : H] = 2, then H is normal in G.

(xii) A subgroup H of a group G is a normal subgroup of G iff the product of two right cosets of H in G is again a right coset of H in G.

(xiii) Every subgroup of a cyclic group is cyclic.

(xiv) Order of a finite cyclic group is equal to the order of its generator.

(xv) If the order of a group is a prime number, then the group is cyclic and hence Abelian.

Cyclic group. A group G is said to be cyclic group generated by an element $a \quad G \quad \in$ if every $g \in G$ is such that $g = a^t$ for some integer t.

Order of an element. Let G be a group and $a \quad G \quad \in$ and the composition being denoted by multiplication. By the order of an element $a \in G$, we mean the least positive integer n, if exists, such that $a^n = e$, the identity in G.

Results. (i) Let G be a finite group and $a \quad G \quad \in$, then $\text{o}(\text{a})/\text{o}(\text{G})$.

(ii) Let G be a finite group and $a \in G$, then $\text{a}^{\text{o}(\text{G})} = e$.

(iii) If $a \in G$ and $o(a) = n$, then $\text{a}^{\text{t}} = e$ iff n/t (n divides t).

(iv) If $o(a) = n$, then $o(a^k) = \dfrac{n}{g.c.d.(n,k)}$.

Homomorphisms. If $(G,.)$ and $(\overline{G},*)$ are two groups. A mapping $f : G \rightarrow \overline{G}$ is called a homomorphism, if $f(x.y) = f(x) * f(y)$ for all $x, y \in G$.

Results. If f is a homomorphism from the group G to the group G **,** then

(i) $f(e) = \bar{e}$, where e and $\bar{e}$ are identities of G and $\overline{G}$ respectively.

(ii) $f\left(g^{-1}\right)=\left(f\left(g\right)\right)^{-1}$ for all $g\in G$.

(iii) it is called epimorphism, if it is onto.

(iv) it is called monomorphism, if it is one – one.

(v) it is called isomorphism, if it is one – one and onto. We write as $G\cong\overline{G}$

(vi) it is called endomorphism, if $G=\overline{G}$.

Kernel of a Homomorphism. Let $:\quad f\ \ G\to\overline{G}$ be a homomorphism. Then, the kernel of f is the set $Kerf=\left\{g\in G:f\left(g\right)=\overline{e},\right.$ the identity element of $\left.\overline{G}\right\}$.

It should be noted that:

(i) $Kerf\ \underline{\Delta}\ G$.

(ii) f is monomorphism iff $Kerf=\{e\}$.

(iii) A homomorphism from a simple group is eithe trivial or one-to-one.

Quotient Group. Let G be a group and H be a normal subgroup of G, then the set G/H (G mod H) of all cosets of H in G is a subgroup w.r.t. multiplication of cosets. Itis called quotient group or factor group of G by H. If $,\quad a\ \ b\in G$, then HaHb = Hab. The identity element of G/H is H.

Canonical Homomorphism. The mapping $:\quad f\ \ G\to G/H\qquad f\ \ g)=Hg$ for all $g\in G$ is an onto homomorphism, where H be a normal subgroup of G. It is called natural or canonical homomorphism and $Kerf=H$.

Fundamental Theorem of Homomorphism. If G is homomorphic image of G under f (that is, f is onto), then $G/\ker_f\cong\overline{G}$.

First Theorem of Isomorphism. Let f be a homomorphism of a group G onto a group G. Let $\overline{K}$ is any normal subgroup of G and $K=\left\{x\in G:f\left(x\right)\in\overline{K}\right\}=f^{-1}\left(\overline{K}\right)$. Then, K is normal subgroup of G containing $\ker f$ and $G/K\cong\overline{G}/\overline{K}$.

Second Theorem of Isomorphism. Let H and K are subgroups of any group G, where $H\ \underline{\Delta}\ G$. Then, $K/H\cap K\cong HK/H$.

Third Theorem of Isomorphism. Let G be any group and $,\quad H\ \ K$ be two normal subgroups of G such that $H\subseteq K$. Then, $G/K\cong\dfrac{G/H}{K/H}$.

Permutations. SupposeS is a finite set having n distinct elements. Then, a one-one mapping of S onto itself is called a permutation of degree n.

Let $S=\{a_1,a_2,...,a_n\}$ be a finite set having n distinct elements. If $f:S\to S$ is a one-one onto mapping, then f is a permutation of degree n. Let $f(a_1)=b_1, f(a_2)=b_2,..., f(a_n)=b_n$, where $\{a_1,a_2,...,a_n\}=\{b_1,b_2,...,b_n\}$. Then, f is written as $f=\begin{pmatrix} a_1 & a_2 \ldots a_n \\ b_1 & b_2 \ldots b_n \end{pmatrix}$.

If S is a finite set of n distinct elements, then we have $|\underline{n}$ distinct arrangements of these n elements. So there will be $|\underline{n}$ distinct permutations of degree n. the set of all permutations of degree n is called **symmetric set of permutations** and is denoted by P_n or S_n.

Product of Permutations. Product of two permutations f and g of degree n is given by first carrying out the operation defined by g and then by f. It is denoted by fog. If $f=\begin{pmatrix} a_1 & a_2 \ldots a_n \\ b_1 & b_2 \ldots b_n \end{pmatrix}$ and $g=\begin{pmatrix} b_1 & b_2 \ldots \text{b}_n \\ c_1 & c_2 \ldots \text{c}_n \end{pmatrix}$. Then, $gof=\begin{pmatrix} a_1 & a_2 \ldots a_n \\ c_1 & c_2 \ldots \text{c}_n \end{pmatrix}$.

Results. (i) The set S$_n$of all permutations of n symbols is a finite group of order $\underline{n}$ w.r.t| product of permutations.

(ii) This group is Abelian for $n\le 2$ and non-abelian for $n\ge 3$.

Cyclic Permutation. Let $f=\begin{pmatrix} a_1 & a_2 \ldots a_k & a_{k+1} \ldots a_n \\ a_2 & a_3 \ldots a_1 & a_{k+1} \ldots a_n \end{pmatrix}$. It is cyclic of length k and can be written as $f=(a_1\ a_2\ \ldots\ a_k)$.

Transposition. A cyclic permutation of length 2 is called a transposition.

Inverse of a Cycle. Let $(\quad f = a_1\ a_2\ \ldots\ a_k)$ be a cycle of length k and degree n. Then, $f^{-1}=(a_1\ a_2\ \ldots\ a_k)^{-1}=(a_1\ a_k\ \ldots\ a_2)$.

Disjoint Cycles. Two cycles are said to be disjoint if they have no object in common in their onerowed representation.

Results. (i) Any two disjoint cycles commute with each other.

(ii) A permutation is said to be an "even permutation" if it can be expressed as a product of an even number of transpositions and is called "odd permutation" if it can be expressed as a product of odd number of transpositions.

For example, (1 2 3 4 5) = (1 2)(1 3)(1 4)(1 5) which is product of even number of permutations and so is even permutations.

(iii) Product of two even(odd) permutations is again an even permutation.

Centre of a group. Let G be a group then the centre of G is given by

$$Z\;G\; = C(G) = \{x \in G : xy = yx \text{ for all } y \in G\}$$

Normalizer of a subgroup. Let G be any group and H be its subgroup. Then, normalizer of H in G is given by

$$N(H) = \{x \in G : xH = Hx\}.$$

N(H) is the largest subgroup of G in which H is normal. In particular, $H \,\Delta\, G$ iff $N(H$

Result. (i) If $o(G) = p^n$ for some prime p, then centre of G is non-trivial.

(ii) If $o(G) = p^2$, where p is a prime, then G is abelian.

THE SYLOW THEOREMS

Introduction. This chapter contains many important results related to the p-groups, Sylow psubgroups, equivalent classes of the Sylow subgroups, number of sylow p-subgroups.

Objective. The objective of these contents is to provide some important results to the reader like:

(i) Conjugate of an element.

(ii) Sylow First Theorem.

(iii) Sylow Second Theorem.

(iv) Sylow Third Theorem.

(v) Survey of groups.

Conjugate of an element. Let G be any group and $a, b \in G$, then a is called conjugate of b if there exists an element $x \in G$ such that $a = x$

Equivalence Class. Let $a \in G$, then equivalence class or conjugate class of 'a' is given by:
$Cl(a) = \{x \in G : a \sim x\}$ = Set of all conjugates of 'a' = $\{g^{-1}ag : g \in G\}$

Remark. Since the conjugacy relation '~' is an equivalence relation on G, so G is union of all conjugate classes and any two conjugate class are either disjoint or identical. Keeping this in mind, we can say that $o(G) = \sum_a o(Cl(a))$, where the sum runs over element a which is taken one each from each conjugate class.

Clearly, $Cl(e) = \{e\}$ and $Cl(a) = Cl(b)$ iff $a \sim b$.

Result. If G is a finite group and $a \in G$, then $o(Cl(a)) = \dfrac{o(G)}{o(N(a))}$

Class Equation. Let G be a finite group and $Z(G)$ denote the centre of G. Then, the equation

$$o(G) = \left(o\ \ Z(G)\right) + \sum_{a} \frac{o(G)}{o\left(N(a)\right)}$$

where 'a' ranges over each conjugate class containing more than one element, is called class-equation.

Another forms of class equation.

(i) $o(G) = \sum_{a} \frac{o(G)}{o\left(N(a)\right)}$, where the sum runs over 'a' taken one from each conjugate class.

(ii) $o(G) = o(Z(G)) + \sum_{a \notin Z(G)} \frac{o(G)}{o\left(N(a)\right)}$, where the sum runs over 'a' taken one from each conjugate class.

(iii) $o(G) = o(Z(G)) + \sum_{N(a) \neq G} \frac{o(G)}{o\left(N(a)\right)}$, where the sum runs over 'a' taken one from each conjugate class.

(iv) $o(G) = o(Z(G)) + \sum_{a \notin Z(G)} [G : N(a)]$, where the sum runs over 'a' taken one from each conjugate class.

Results.

1. If $o(G) = p^n$ for some prime p then $Z(G) \neq \{e\}$ that is, $Z(G)$ is non-trivial, that is, $o\left(Z(G)\right) > 1$.
2. If $o(G) = p^2$ for some prime p, then G is abelian.
3. A group of order p^3 may not be abelian e.g. Q_8 whose order is 2^3.
4. If G is a non-abelian group of order p^3 for some prime p, then $o\left(Z(G)\right) = p$.
5. If Z is the centre of a group G such that G/Z is cyclic, then show that G is abelian.

Commutator. Let G be any multiplicative group. The commutator of two elements x and y of G is the element $x^{-1}y^{-1}xy \in G$. We denote it by $[x, y]$.

Proposition. G is abelian iff $[x, y] = e \ \forall \ x, y \in G$.

Proof. If G is abelian then

$$[x, y] = x^{-1}y^{-1}xy = x^{-1}xy^{-1}y = e.e = e.$$

Conversely, let $[x, y] = e \ \forall \ x, y \in G$.

$$\Rightarrow \quad x^{-1}y^{-1}xy = e$$

$$\Rightarrow \quad (yx)^{-1}.(xy) = e$$

$$\Rightarrow \quad xy = yx \ \forall \ x, y \in G. \qquad \Rightarrow \quad G \text{ is abelian.}$$

Proposition. $a \in Z(G)$ iff $[a, x] = e \ \forall \ x \in G$.

Proof. Let $a \in Z(G)$ = centre of G

Then $[a, x] = a^{-1}x^{-1}ax = a^{-1}x^{-1}xa = a^{-1}a = e$ [Since $a \in Z(G)$]

Conversely. $[a, x] = e \ \forall \ x \in G$

$$\Rightarrow \quad a^{-1}x^{-1}ax = e \quad \Rightarrow \quad ax = xa \ \forall \ \in G \quad \Rightarrow \quad a \in Z(G).$$

p[;'\/Commutator Element. The element y of G is said to be a commutator element of G if $\exists \ a, b \in G$ such that $[a, b] = y$ that is, $a^{-1} b^{-1}ab = y$. e.g. Identity element is always a commutator element. Let us find the commutator elements of S_3. We know that

$$S_3 = \{I \ , \ (12) \ , \ (13) \ , \ (23) \ , \ (123) \ , \ (132)\}$$

Now, $[I, (12)] = I$, Similarly $[I, x] = I \ \forall \ x \in S_3$.

Now, $[(12), I] = I$, $[(12), (12)] = I$

$[(12),(13)] = (123)$, $[(12), (23)] = (132)$

$[(12), (123) = (132)$, $[(12), (132)] = (123)$

So, (123) and (132) are also commutator elements of S_3. We can show that I, (123), and (132) are the only commutator elements of S_3.

Derived Subgroup. The subgroup of G generated by all the commutators of G is called the derived subgroup of G. We denote it by $\delta(G)$ and G'

that is, $$\delta(G) = G' = < [x, y] : x, y \in G >$$

For example, let $G = S_3$, then

$$\delta(S_3) = < [x, y] : x, y \in S_3 > = < I, (123), (132)> = \{I, (123), (132)\}.$$

$\delta(G)$ is also known as first derived subgroup.

***n*th Derived Subgroup.** Let G be a group, for every non-negative integer n, define $G^{(n)}$ inductively as follows:

$$G^0 = G, \ G^{(n+1)} = \left(G^{(n)}\right)',$$

the commutator subgroup of $G^{(n)}$. The $G^{(n)}$ is called n^{th} commutator subgroup or n^{th} derived subgroup of G.

$$G^{(n+1)} = \left(G^{(n)}\right)' = [G^{(n)}, \ G^{(n)}] = < [x, y] : x, y \in G^{(n)} >.$$

Sylow Theorems

Sylow's First Theorem. Let p be a prime number such that $(p)^m / o\ G$, where m is a positive integer. Then G has a subgroup of order p^m.

Proof. We shall prove the Theorem by induction on $o(G)$.

If $o(G) = 1$, then Theorem is trivially true.

As our induction hypothesis, we assume that Theorem is true for all groups of order less than order of *G*. In other words, we have assumed that if *G*′ is a group such that $o(G') < o(G)$ and

$p^k / o(G')$, for some integer *k*, then *G*′ has a subgroup of order p^k.

We shall prove the result for *G*. For this we consider two cases separately.

Case I. If p^m divides the order of a proper subgroup, say *H*, of *G* that is, $p^m / o(H)$ and $o(H) < o(G)$. Then by induction hypothesis on *H*, we obtain that *H* (and hence *G*) has a subgroup of order p^m.

Case II. Let p^m does not divide the order of any proper subgroup of *G* that is, $p^m \nmid o(H)$, for all proper subgroup *H* of *G*.

We know that the class-equation for *G* is $o(G) = o(Z(G)) + \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}$ (1)

If $N(a) \neq G$, then *N*(*a*) is a proper subgroup of *G*, and so by hypothesis of this case,

/ $p^m \nmid (o (N))a$

Now, $o(G) = \frac{o(G)}{o(N(a))}.o(N(a))$

Given that $p^m / o(G)$, and if $p^m \nmid o(N(a))$ then by above expression, we obtain

$$p \Big/ \frac{o(G)}{o(N(a))}, \text{ whenever } N(a) \neq G.$$

Now, we know that every subgroup of G/K is of the form L/K where *L* is a subgroup of *G* containing *K*. So, we must have

$T = L/K$, where *L* is a subgroup of *G* containing *K*.

$$\Rightarrow \quad o(T) = o(L/K) = \frac{o(L)}{o(K)}$$

$$\Rightarrow \quad o(L) = o(T).o(K) = p^{m-1}.p = p^m$$

Thus G has a subgroup L of order p^m.

Remark. Sylow′s first Theorem can also be stated in following ways:

(i) If any power of prime divides the order of a group G, then G has a subgroup of order equal to that power of prime.

(ii) If $o(G)=p^k q$, where p is a prime number and q is a positive integer such that gcd(p,q)=1, then G has subgroups of orders $p, p^2,..., p^k$.

Example of Sylow's first Theorem.

Example. Let G be a group such that $(o)G = 9000$. By Sylow first Theorem, find the order of subgroups which G certainly contains.

Solution. First we do the prime factorization of 9000 and obtain

$$o(G) = 2^3 \,.\, 3^2 \,.\, 5^2$$

Here, 2, 3 and 5 are prime numbers so by Sylow's first Theorem, G contains the subgroups of order 2^1, 2^2, 2^3, 3^1, 3^2, 5^1, 5^2 that is, 2, 4, 8, 3, 9, 5, 25.

However, by Sylow's first Theorem, nothing can be said about the existence of subgroups of order 6, 15, 10 etc. as they are not powers of a prime.

Sylow *p*-subgroup. Let p be a prime number such that p^k divides $o(G)$ and p^{k+1} does not divide $o(G)$. Then a subgroup of order p^k is called a Sylow p-subgroup of G.

-OR-

If $o(G) = p^k q$ where p is a prime number and gcd(p, q) = 1, then a subgroup of order p^k is called a Sylow p-subgroup of G.

-OR-

Sylow p -subgroup of a group G is a subgroup whose order is p^k where k is the largest power of p such that p^k divides $o(G)$.

-OR-

A subgroup of G is called a Sylow p-subgroup if its order is equal to the maximum power of p occurring in the order of the group.

Example. Find the order of different Sylow p–subgroups for G where

(i) $o(G) = 45$ **(ii)** $o(G) = 1125$.

Solution. (i) $o(G) = 45 = 3^2 5^1$.

Then, G has Sylow 3–subgroups and Sylow 5–subgroups. A sylow 3−subgroup is that whose order is 3^2, that is, 9 and a sylow 5-subgroup is that whose order is $5^1 = 5$.

(ii) $o(G) = 1125 = 3^2 5^3$.

In this case, a sylow 3-subgroup is that whose order is 9 and a sylow 5-subgroup is that whose order is 125.

Note. By above example, it is clear that in different groups Sylow p-subgroup may have different orders for some fixed prime p.

Example. If H is a Sylow p-subgroup of G, then prove that $x^{-1}Hx$ is also a sylow p-subgroup of G for any $x \in G$.

Solution. Let $p^n / o(G)$ and $p^{n+1} \nmid o(G)$.

As H is a Sylow p -subgroup of G, we have $o(H) = p^n$.

Let $H = \{h_1, h_2, h_3, \ldots, h_{p^n}\}$, then for any $x \in G$, we have

$$x^{-1}Hx = \{x^{-1}h_1x \ , \ x^{-1}h_2x \ , \ldots, \ x^{-1}h_{p^n}x\} \qquad (1)$$

First we prove that $x^{-1}Hx$ is a subgroup of G. For this let $x^{-1}h_1x$ and $x^{-1}h_2x$ be any two arbitrary element.

Then $(x^{-1}\, h_1\, x)\, (x^{-1}\, h_2\, x)^{-1} = x^{-1}\, h_1\, x\, x^{-1} h_2^{-1} (x^{-1})^{-1}$

$$= x^{-1}h_1h_2^{-1}x \in x^{-1}Hx \ \left[\text{Since } h_1h_2^{-1} \in H \text{ as } H \text{ is a subgroup}\right]$$

Thus, $x^{-1}Hx$ is a subgroup.

Secondly, we prove that $o(x^{-1}Hx) = o(H)$.

For this it is sufficient to prove that all elements in (1) are distinct.

Let if, possible $x^{-1}h_1x = x^{-1}h_2x$, where $h_1 \neq h_2$

$$\Rightarrow \qquad xx^{-1}h_1xx^{-1} = xx^{-1}h_2xx^{-1}$$

$$\Rightarrow \qquad h_1 = h_2 \text{, which is a contradiction.}$$

Hence, $o(x^{-1}Hx) = o(H)$, that is, $o(x^{-1}Hx) = p^n$.

Thus, $x^{-1}Hx$ is a Sylow p-subgroup of G.

***p* group.** Let p be a prime number. A group G is said to be a p – group if order of every element of G is some power of p. For example,

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

The group of quaternions is a 2–group because

$$o(1) = 2^0,\ o(-1) = 2^1,\ o(i, -i, j, -j, k, -k) = 2^2,$$

that is, order of every element of Q_8 is a some power of 2.

Theorem. A finite group G is a p-group iff $(\ o)G\ = p^n$ for some integer n.

Proof. Suppose G is a p-group. We shall prove that $(\ o)\ G\ = p^n$ for some integer $n \geq 1$.

For this, it is sufficient to prove that p is the only prime dividing $o(G)$.

Let, if possible, $q(\neq p)$ be any other prime such that $q/o(G)$. By Cauchy Theorem, there exists an element $a(\neq e) \in G$ such that $o(a) = q$

Since $a \in G$ and G is a p-group, so $o(a) = p^r$ for some $r \geq 1$. Thus $p^r = q$

$\Rightarrow$ p/q, which is a contradiction since a prime can never divide other prime.

Hence p is the only prime dividing $o(G)$, so $o(G)\ = p^n$ for some n.

Conversely, Suppose $o(G)\ = p^n$. Let $a \in G$ be any element, then $o(a)/o(G)$

$$\Rightarrow \quad o(a)/p^n \ \Rightarrow\ o(a) = p^r \text{ for some } r.$$

Thus order of every element of G is some power of p. Hence G is a p-group.

Remark. Now we introduce the concept of Double Cosets which will be very useful in proving the Sylow's second and third Theorem.

Double Coset. Let H and K be two subgroups of a group G and $x \quad G \quad \in$ be any element. Then the set $H \text{ x } K = \{\ hxk:\ \ h \in H\ \ k \in\} K$ is called a double coset.

Double Coset Decomposition. If H and K are two subgroups of a group G then prove that

(i) any two double cosets are either disjoint or identical

(ii) G is the union of all distinct double cosets that is, $G = \bigcup\limits_{x \in G} H\ x\ K$ where union runs over x taken one from each double coset.

Proof. We define a relation ~ for any two elements x and y of G as $x \sim y$ iff $x = hyk$ for some $h \in H$ and $k \in K$

First we prove that this relation is an equivalence relation.

(i) Reflexivity: Clearly $x \sim x$ as $x = e\,x\,e$, where $e \in H$, $e \in K$.

(ii) Symmetry: Let $x \sim y \Rightarrow x = h\,y\,k$ for some $h \in H$, $k \in K$

$$\Rightarrow \quad h^{-1}\,x\,k^{-1} = h^{-1}\,h\,y\,k\,k^{-1} \ \Rightarrow\ y = h^{-1}\,x\,k^{-1} \text{ where } h^{-1} \in H\ ,\ k^{-1} \in K \Rightarrow\ y \sim x.$$

(iii) Transitivity: Let $x \sim y$ and $y \sim z$

$$\Rightarrow \quad x = hyk \text{ and } y = h'zk' \text{ for some } h, h' \in H \text{ and } k, k' \in K$$

$$\Rightarrow \quad x = hh'zk'k$$

where union runs over x taken one from each conjugate class. $G = \bigcup_{x \in G} cl(x)$ (1)

Then,

$$cl_{(x)} = \{y \in G \ : \ y \sim x\}$$

$$= \{y \in G \ : \ y = hxk \text{ for some } h \in H \ , k \in K\}$$

$$= \{hxk \ : \ h \in H \ , \ k \in K\} = H\,x\,K$$

$$\Rightarrow \quad cl(x) = H\,x\,K \qquad (2)$$

Thus equivalence class of any element comes out to be a double coset. Also we know that any two equivalence classes are either disjoint or identical. Thus we obtain that any two double cosets are either disjoint or identical, which proves (i).

Using (2) in (1), we obtain

$$G = \bigcup_{x \in G} H\ x\ K$$

where union runs over x taken one from each double coset which proves (ii).

This is called double coset decomposition of G by H and K.

Lemma. Let H and K be finite subgroups of a group G and $x \in G$ then

$$o(H\ x\ K) = \frac{o(H)\ o(K)}{o(H \cap x\ K\ x^{-1})}.$$

Proof. We define a mapping $\phi \ : \ H\ x\ K \to H\ x\ K\ x^{-1}$ by setting

$$\phi(hxk) = hxkx^{-1} \text{ for } h \in H \text{ and } k \in K.$$

We prove that ϕ is well-defined, one-one and onto.
(i) ϕ is well-defined: Let $h_1xk_1 = h_2xk_2$

$$\Rightarrow \quad h_1xk_1x^{-1} = h_2xk_2x^{-1}$$

$$\Rightarrow \quad \phi(h_1xk_1) = \phi(h_2xk_2)$$

So, ϕ is well-defined.

(ii) ϕ is one-one. Let $\phi(h_1xk_1) = \phi(h_2xk_2)$

$$\Rightarrow \quad h_1xk_1x^{-1} = h_2xk_2x^{-1}$$

$$\Rightarrow \quad h_1xk_1 = h_2xk_2$$

So, ϕ is one-one.

(iii) ϕ is onto. Let $hxkx^{-1} \in HxKx^{-1}$ be any element then clearly $hxk \in HxK$ and

$$\phi(hxk) = hxkx^{-1} \quad \Rightarrow \quad hxk \text{ is pre-image of } hxkx^{-1} \text{ under } \phi.$$

So, ϕ is onto.

Hence, there exists a one-to-one correspondence between $H\ x\ K$ and $HxK\ x^{-1}$ and so their orders must be same that is,

$$o(HxK) = o(HxKx^{-1}) \qquad (1)$$

Now we know that if K is a subgroup of G then xKx^{-1} is also a subgroup of G of the same order, that is, $o(K) = o(xKx^{-1})$.

Also, we know a result that if A and B are two finite subgroups of G, then

$$o(AB) = \frac{o(A)\ o(B)}{o(A \cap B)}$$

Putting $A = H$ and $B = xKx^{-1}$ in above, we obtain

$$o(HxKx^{-1}) = \frac{o(H)\ o(xKx^{-1})}{o(H \cap xKx^{-1})}$$

$$\Rightarrow \qquad o(HxKx^{-1}) = \frac{o(H)\ o(K)}{o(H \cap xKx^{-1})} \quad [\text{Since } o(K) = o(xKx^{-1})] \ (2)$$

By (1) and (2), we obtain

$$o(HxK) = \frac{o(H)\ o(K)}{o(H \cap xKx^{-1})}$$

Sylow's Second Theorem. Any two Sylow p-subgroups of a finite group G are conjugates in G.

Proof. Let H and K be two Sylow p-subgroups of G. Let n be the highest power of p such that $p^n / o(G)$ that is,

$$p^{n+1} \nmid o(G) \qquad (1)$$

Then, $o(H) = o(K) = p^n$

We have to show that H and K are conjugate in G that is, $H = xKx^{-1}$ for some $x \in G$

Let, if possible this is false that is, $H \neq xKx^{-1}$ for all $x \in G$.

$\Rightarrow$ $H \cap xKx^{-1}$ is a subgroup of H which is properly contained in H

that is, $$H \cap xKx^{-1} \subsetneqq H \qquad (2)$$

Now, by Lagrange's Theorem,

$$o(H \cap xKx^{-1}) / o(H) = p^n$$

$$\Rightarrow \qquad o(H \cap xKx^{-1}) = p^m \text{ for some } m \leq n .$$

But in view of (2) clearly $m \neq n$, so $o(H \cap xKx^{-1}) = p^m$, where $m < n$.

By above Lemma, we have

$$o(HxK) = \frac{o(H)\, o(K)}{o(H \cap xKx^{-1})} = \frac{p^n . p^n}{p^m} = p^{2n-m}$$

$$= p^{n+1+n-m-1} = p^{n+1} . p^{n-m-1}$$

$$\Rightarrow \qquad p^{n+1} \text{ divides } o(HxK)$$

$$\Rightarrow \qquad p^{n+1} \text{ divides} \sum_{x \in G} o(HxK) \qquad (3)$$

Now, by double coset decomposition, we know that

$$G = \bigcup_{x \in G} H\ x\ K \text{, where } H\, x\, K \text{ are mutually disjoint.}$$

$$\Rightarrow \qquad o(G) = \sum_{x \in G} o(HxK) \qquad (4)$$

By (3) and (4), we have p^{n+1} divides $o(G)$, which is a contradiction to (1).

Hence $H = xKx^{-1}$ for some $x \in G$ that is, H and K are conjugates in G.

Lemma. Let P be a Sylow p -subgroup of a group G, then the number n_p of Sylow p-subgroups of G is equal to $\dfrac{o(G)}{o(N(P))}$.

Proof. We know that $o(cl(P)) = \dfrac{o(G)}{o(N(P))}$ (1)

Now, $cl(P)$ contains all subgroups which are conjugate to P.

But by Sylow second Theorem, all sylow p-subgroups are conjugate to each other and hence $cl(P)$ contains all Sylow p-subgroups of G.

Hence, number of Sylow p-subgroups = $n_p = o(cl(P))$ (2)

By (1) and (2), $n_p = \dfrac{o(G)}{o(N(P))}$.

Sylow's Third Theorem. The number n_p of Sylow p-subgroups of a finite group G is given by $n_p = 1 + kp$ such that $1 + kp / o(G)$, and k is a non-negative integer.

Proof. Let *P* be a Sylow *p*-subgroup of *G*.

Let *n* be the highest power of *p* such that $p^n / o(G)$ that is, $p^{n+1} \nmid o(G)$.

By double coset decomposition of *G*, we know that

$$G = \bigcup_{x \in G} H\ x\ K \text{, where union runs over } x \text{ taken one from each double coset.}$$

$$\Rightarrow \qquad o(G) = \sum_{x \in G} o(HxK) \text{ where sum runs over } x \text{ taken one from each double coset.}$$

Taking $H = K = P$ in above, we get

$$o(G) = \sum_{x \in G} o(PxP)$$

$$\Rightarrow \qquad o(G) = \sum_{x \in N(P)} o(PxP) + \sum_{x \notin N(P)} o(PxP) \qquad (1)$$

We take up two sums in (1) one by one.

If $x \in N(P)$ then $xPx^{-1} = P \Rightarrow \quad xP = Px$

$$\Rightarrow PxP = PPx$$

$$\Rightarrow PxP = Px \qquad [\text{Since } P \text{ is a subgroup , so } PP = P\ ]$$

$$\Rightarrow \bigcup_{x \in N(P)} P\ x\ P = \bigcup_{x \in N(P)} P\ x \qquad (2)$$

Now *P* is a subgroup of *N*(*P*) and so *Px* is a right coset of *P* in *N*(*P*). Further we know that union of all distinct right cosets of a subgroup is equal to the group, so we get

$$\bigcup_{x \in N(P)} P\ x = N(P)$$

Using this in (2), we get

$$\bigcup_{x \in N(P)} P\ x\ P = N(P)$$

$$\Rightarrow \qquad \sum_{x \in N(P)} o(PxP) = o(N(P)) \qquad (3)$$

Again, if $x \notin N(P)$ then $xPx^{-1} \neq P$

$\Rightarrow \qquad P \cap xPx^{-1}$ is a subgroup of *P* properly contained in *P*,

that is, $\qquad o(P \cap xPx^{-1}) < o(P) = p^n$

Also by Lagrange's Theorem

$$o(P \cap xPx^{-1}) / o(P) = p^n$$

$\Rightarrow$ $$o(P \cap xPx^{-1}) = p^m \text{ with } m < n.$$

Now we know that,

$$o(PxP) = \frac{o(P)\, o(P)}{o(P \cap xPx^{-1})} = \frac{p^n.p^n}{p^m} = p^{2n-m}$$

$$= p^{n+1+n-m-1} = p^{n+1}.p^{n-m-1}$$

$\Rightarrow$ p^{n+1} divides $o(P\,x\,P)$ whenever $x \notin N(P)$

that is, $p^{n+1} \Big/ \sum_{x \notin N(P)} o(PxP)$

$\Rightarrow$ $\sum_{x \notin N(P)} o(PxP) = p^{n+1}\ t$ for some integer t (4)

Using (3) and (4) in (1), we obtain

$$o(G) = o(N(P)) + p^{n+1}\ t$$

$\Rightarrow$ $$\frac{o(G)}{o(N(P))} = 1 + \frac{p^{n+1}t}{o(N(P))} \qquad (5)$$

As $N(P)$ is a subgroup of G, by Lagrange's Theorem, $o(N(P))$ divides $o(G)$ and so $\frac{o(G)}{o(N(P))}$ is an integer.

So, by (5), we obtain that $\frac{p^{n+1}t}{o(N(P))}$ is an integer.

Now, P is a subgroup of $N(P)$, so by Lagrange's Theorem

$$o(P)/o(N(P)) \quad \Rightarrow \quad p^n/o(N(P))$$

$\Rightarrow$ $o(N(P)) = p^n\ r$ for some integer r.

Thus, we obtain that $\frac{p^{n+1}t}{o(N(P))} = \frac{p^{n+1}t}{p^n r} = p\frac{t}{r}$ is an integer.

$\Rightarrow$ $\frac{t}{r}$ is an integer, say k $\Rightarrow$ $\frac{p^{n+1}t}{o(N(P))} = kp$

Using this in (5), we have

$$\frac{o(G)}{o(N(P))} = 1 + kp$$

By above Lemma, the number n_p of Sylow p-subgroups is given by $n_p = \frac{o(G)}{o(N(P))}$.

Hence, $n_p = \dfrac{o(G)}{o(N(P))} = 1 + kp$

Finally, $o(G) = o(N(P)).(1 + kp)$ implies that $1 + kp / o(G)$

Thus number of Sylow p-subgroups is $1 + kp$ such that $1 + kp / o(G)$.

Corollary. Show that a Sylow p-subgroup of a finite group G is unique iff it is normal.

Proof. *Condition is necessary*: Suppose H be a unique Sylow p-subgroup of G. Let $p^n / o(G)$ and $p^{n+1} \nmid o(G)$, then

Clearly, $o(H) = p^n$

Let $x \in G$ be any arbitrary element, then we know that $x^{-1}Hx$ is also a Sylow p-subgroup.

Since H is the only Sylow p-subgroup of G, therefore

$$x^{-1}Hx = H \quad \text{for all } x \in G$$

$$\Rightarrow \qquad Hx = xH \quad \text{for all } x \in G$$

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

Condition is sufficient :

Let H be a Sylow p-subgroup of G such that $H \,\underline{\Delta}\, G$. We shall prove that H is unique. Suppose K be any other Sylow p -subgroup of G. Then, by Sylow second Theorem, H and K must be conjugate in G that is,

$$K = x^{-1}Hx \text{ for some } x \in G$$

$$\Rightarrow \qquad K = x^{-1}xH \qquad [\text{Since } H \,\underline{\Delta}\, G]$$

$$\Rightarrow \qquad K = H$$

Hence H is unique Sylow p-subgroup of G.

Simple Group. A simple group is one having no proper normal subgroup.

Remark. To show that a finite group G of certain order is not simple, obtain a unique Sylow p -subgroup G for some prime p. Then, it becomes normal and obviously H is proper, which shows that G is not simple.

Example. Show that a group of order 28 is not simple.

-OR-

Let $o(G)$ = 28, then show that group G has a normal subgroup of order 7.

Solution. We have $o(G)$ = 28 = $2^2 7^1$. By Sylow first Theorem, G has Sylow 2 – subgroups each of order 4 and Sylow 7 – subgroups each of order 7.

By Sylow third Theorem, the number n_7 of Sylow 7 – subgroups is given by $1 + 7k$ such that

$$+ \ k/o \ G \quad \Rightarrow \quad 1+7k/28$$

$$\Rightarrow \quad 1+7k/2^2.7$$

$$\Rightarrow \quad 1+7k/4 \qquad \text{[Since } (1 + 7k, 7) = 1]$$

$$\Rightarrow \quad k=0$$

Thus, $n_7 = 1$ that is, there is unique Sylow 7 -subgroup say H and $o(H) = 7$

But we know that "a Sylow p -subgroup is unique iff it is normal".

Thus H is a normal subgroup of order 7. Obviously H is proper. Hence G is not simple.

Proposition. Let G be a finite group such that $(\ o)G = p^n$, where p is a prime. Prove that any subgroup of order p^{n-1} is a normal subgroup of G.

Proof. We shall prove the result by induction on n.

For $n = 1$, G is a group of order p and the only subgroup of order p^{n-1} that is, of order $p^{1-1} = p^0 = 1$ is $\{e\}$. The identity subgroup $\{e\}$ is obviously a normal subgroup of G. Thus the result is true for $n = 1$.

As our induction hypothesis, we assume that result is true for all groups of order p^m, where $m < n$.

Let H be a subgroup of G of order p^{n-1}. We shall prove that H is normal in G.

Now, $H \subseteq N(H) \subseteq G$ and so by Lagrange's Theorem,

$$o \ H \ /o(N(H)) \quad \text{and} \quad o(N(H))/o(G)$$

that is, $$p^{n-1}/o(N(H)) \quad \text{and} \quad o(N(H))/p^n$$

$$\Rightarrow \quad o(N(H)) = p^{n-1} \ \text{ or } \ p^n$$

If $o(N(H)) = p^n$, then $o(N(H)) = o(G) \Rightarrow N(H) = G$

$\Rightarrow$ H is normal in G, which is what we want to prove.

Now, we finish our proof by showing that $o(N(H)) = p^{n-1}$ is impossible.

Let, if possible, $o(N(H)) = p^{n-1}$, then as $o(H) = p^{n-1}$ and $H \subseteq N(H)$, we get

$$H = N(H) \qquad (1)$$

Now, $o(G) = p^n$, we know by class equation, that $o(Z(G)) > 1$ (2)

By Lagrange's Theorem, $o(Z(G))/o(G) = p^n \quad \Rightarrow \quad o(Z(G)) = p^s, \ 0 \le s \le n$

But if $s = 0$, then $o(Z(G)) = 1$, which is a contradiction by (1).

Hence, $o(Z(G)) = p^s, s > 0 \quad \Rightarrow \quad p/o(Z(G))$

So, by Cauchy Theorem for finite groups, there exists an element $a(\neq e) \in Z(G)$ such that $o(a) =$

Let K be the cyclic subgroup of G generated by 'a' that is,

$$K = <a> = \{a, a^2, a^3, ..., \} a^p = e$$

As 'a' belongs to centre, every element $x \in G$ commutes with a and all its powers, so

$$Kx = xK \quad \text{for all } x \in G$$

$$\Rightarrow \quad K \text{ is a normal subgroup of } G.$$

Hence G/K is well-defined and

$$o(G/K) = \frac{o(G)}{o(K)} = \frac{p^n}{p} = p^{n-1}, \text{ where } n-1 < n$$

Also, $o(H/K) = \dfrac{o(H)}{o(K)} = \dfrac{p^{n-1}}{p} = p^{n-2}$

So, by induction hypothesis, H/K must be a normal subgroup of G/K .

$p \quad \Rightarrow \quad H$ is a normal subgroup of $G \;\Rightarrow + \; kN(H) = G$ (3)

By (1) and (3) we obtain, $H = G$, which is absurd.

Hence $o(H) = p^{n-1}$ is not possible.

Example. Show that no group of order 108 is simple.

Let G be a group of order 108. Show that G has a normal subgroup of order 27 or 9.

Solution. We have $o(G) = 108 = 2^2.3^3$. By Sylow third Theorem, the number n_3 of Sylow 3–subgroups is given by $1 + 3k$ such that

$$1 + 3k/o(G) = 2^2.3^3 \quad \Rightarrow \quad 1 + 3k/4 \;\; [\text{Since } (1 \quad 3 \;\;, 3 \;\;) \quad 1]$$

$$\Rightarrow \quad k = 0 \text{ or } 1$$

$$\Rightarrow \quad n_3 = 1 + 3.0 \text{ or } 1 + 3.1$$

$$\Rightarrow \quad n_3 = 1 \text{ or } 4$$

We consider the two cases separately.

Case (i). $n_3 = 1$, that is, G has a unique Sylow 3 -subgroup, say H. Since H is unique, it must be normal and $o(H) = 3^3 = 27$. Thus G has a normal subgroup of order 27 in this case and hence G is not simple.

Case (ii). $n_3 = 4$, that is, G has four Sylow 3 – subgroups each of order 27. Let H and K be any two distinct sylow 3 – subgroups. We claim that $o(H \cap K) = 9$ and $H \cap K$ is a normal subgroup of G.

Clearly, $H\cap K\subseteq H$, and so by Lagrange's Theorem.

$$o(H\cap K)/o(H)=27$$

$$\Rightarrow \qquad o(H\cap K)=1 \text{ or } 3 \text{ or } 9 \text{ or } 27.$$

If $o(H\cap K)$ = 27 then since $o(H)$ = $o(K)$ = 27, we obtain H = K, which is a contradiction. Hence $o(H\cap K)\neq 27$.

If $o(H\cap K)$ = 1 or 3 then $o(H\,K)$ = $\dfrac{o(H)\,o(K)}{o(H\cap K)}=\dfrac{27.27}{1\,or\,3}>108=o(G)$, which is not possible.

Hence $o(H\cap K)$ ≠ 1, 3 and so $o(H\cap K)$ = 9.

We now show that $H\cap K$ is normal in G. For this we shall prove that $N(H\cap K)$ = G.

Now, we know a that, if $o(H)$ = p^{n-1} and $o(G)$ = p^{n} then H is a normal subgroup of G.

Using this, we conclude that $H\cap K$ is a normal subgroup of both H and K as $o(H\cap K)$ = 3^2 and $o(H)$ = $o(K)$ = 3^3.

Let $x\in H$ be any element, then

$$(H\cap K)x=x(H\cap K) \qquad \text{[Since } (H\cap K)\ \underline{\Delta}\ H]$$

$$\Rightarrow \qquad x\in N(H\cap K), \text{ normalizer of } H\cap K.$$

$$\Rightarrow \qquad H\subseteq N(H\cap K)$$

Similarly, $K\subseteq N(H\cap K) \quad \Rightarrow \quad HK\subseteq N(H\cap K)$

$$\Rightarrow \qquad o\big(N(H\cap K)\big)\geq o(HK)=\frac{o(H).o(K)}{o(H\cap K)}=\frac{27.27}{9}=81$$

$$\Rightarrow \qquad o\big(N(H\cap K)\big)\ \geq\ 81 \qquad (1)$$

On the other hand, $N(H\cap K)$ is a subgroup of G so by Lagrange's Theorem

$$o\big(N(H\cap K)\big)/o(G),$$

that is, $\qquad o\big(N(H\cap K)\big)/108 \qquad (2)$

Both (1) and (2) are possible only when

$$o\big(N(H\cap K)\big)=108=o(G)$$

$$\Rightarrow \qquad o\big(N(H\cap K)\big)=o(G)$$

$$\Rightarrow \qquad N(H\cap K)=G$$

$$\Rightarrow \qquad H\cap K \text{ is normal in } G. \qquad [\text{Since } N(H)=G \text{ iff } H\ \underline{\Delta}\ G]$$

Hence G is not simple.

Theorem. Let $o(G) = pq$, where p and q are distinct primes, $p < q$ and $p \nmid q-1$, then show that G is cyclic.

Proof. By Sylow third Theorem, the number n_p of Sylow p-subgroups is given by 1 + kp such that $1+kp/o(G) = pq$

$\Rightarrow \quad 1+kp/q \quad$ [Since $(1+kp, p) = 1$]

$\Rightarrow \quad 1+kp = 1$ or $1 + kp = q$ [Since q is a prime]

If $1 + kp = q$, then $kp = q-1$

$\Rightarrow \quad p/q-1$, which is a contradiction.

Hence $n_p = 1+kp = 1$. Thus G has a unique Sylow p-subgroup, say, H of order p. Also since H is unique, it must be normal. Thus we obtained

$o(H) = p$ and $H \underline{\Delta} G$ (1)

Again, by Sylow third Theorem, the number n_q of Sylow q-subgroups is given by $1+k'q$ such that $1+k'q/o(G) = pq \quad \Rightarrow \quad 1+k'q/p$ [Since $(1+k'q\ , q) = 1$]

$\Rightarrow \quad 1+k'q = 1$ or $1+k'q = p$

If $1+k'q = p$ then we get $q < p$, which is a contradiction.

Hence $n_q = 1+k'q = 1$. Thus G has a unique Sylow q-subgroup, say, K of order q. Also since K is unique it must be normal. Thus we obtained

$o(K) = q$ and $K \underline{\Delta} G$ (2)

Now, we know that a group of prime order is always cyclic and here H and K both are of prime orders, so they must be cyclic.

Let $H = < a >$ and $K = < b >$ then $o(H) = o(a)$ and $o(K) = o(b)$ (3)

Using (1) and (2) in (3), we get

$o(a) = p$ and $o(b) = q$ (4)

Now, we prove that $H \cap K = \{e\}$. Let $x \in H \cap K$ be any element.

Then $x \in H$ and $x \in K \quad \Rightarrow \quad o(x)/o(H)$ and $o(x)/o(K)$

$\Rightarrow \quad o(x)/p$ and $o(x)/q$

$\Rightarrow \quad o(x)/\gcd(p,q)$

$\Rightarrow \quad o(x) = 1$

$\Rightarrow \quad x = e$ for all $x \in H \cap K \quad \Rightarrow \quad H \cap K = \{e\}$ (5)

Now, we prove that $ab = ba$.

For this consider the element $a^{-1}b^{-1}ab$. We see that

$$a^{-1}b^{-1}ab \;=\; a^{-1}(b^{-1}ab) \in H\,,$$

because $H \;\underline{\Delta}\; G$, so that $b^{-1}ab \in H$ and also $a^{-1} \in H$.

Again, $a^{-1}b^{-1}ab \;=\; (a^{-1}b^{-1}a)b \in K$, because $K \;\underline{\Delta}\; G$, so that $a^{-1}b^{-1}a \in K$ and also $b \in K$

Hence, we get $\qquad a^{-1}b^{-1}ab \;\in\; H \cap K$

$\Rightarrow \qquad a^{-1}b^{-1}ab = e \qquad\qquad$ [By (5)]

$\Rightarrow \qquad baa^{-1}b^{-1}ab = ba.e$

$\Rightarrow \qquad ab = ba$

Lastly, by (3), we see that $\gcd(o(a), o(b)) = \gcd(p, q) = 1$

We know that, if $a, b \in G$ such that $ab = ba$ and $\big(o(a), o(b)\big) = 1$ then $o(ab) = o(a).o(b)$

Therefore, $\qquad o(ab) = o(a)\; o(b) = pq = o(\mathrm{G})$

$\Rightarrow \qquad G$ contains an element ab of order pq

$\Rightarrow \qquad G = < ab >$

$\Rightarrow \qquad G$ is cyclic.

Remark. Due to the above result, we can say that groups of order 15, 33, 35, 65, 51 etc. are cyclic.

Theorem. Let P be a Sylow p-subgroup of G and let $x \in N(P)$ be an element such that $o(x) = p^r$. Then show that $x \in P$.

Proof. Since P is given to be a Sylow p-subgroup of G and let

$$p^n / o(G) \text{ but } p^{n+1} \nmid o(G) \qquad\qquad (1)$$

Then, clearly $\qquad o(P) = p^n$.

We know that $P \;\underline{\Delta}\; N(P)$, so $N(P)/P$ is well-defined.

As $x \in N(P)$, $Px \in N(P)/P$ and $(Px)^{p^r} = P.x^{p^r} = P.e \qquad$ [Since $o(x) = p^r$]

$\Rightarrow \qquad (Px)^{p^r} = P =$ Identity of $N(P)/P$

$\Rightarrow \qquad o(Px)/p^r \;\Rightarrow\; o(Px) = p^s$ for some $s \geq 0$

If $s = 0$, then $o(Px) = p^s = p^0 = 1 \;\Rightarrow\; Px \;=\; P$

$\overline{H} \;=\; < Px >$ then $o(\overline{H}) = o(Px) \;=\; p^s \qquad\qquad (2)$

Since $\overline{H}$ is a subgroup of $N(P)/P$, it must be of the form $\overline{H} \;=\; H/P$ where H is a subgroup of $N(P)$ containing P. Now, $\qquad o(H) = p^s \qquad\qquad$ [By (2)]

$\Rightarrow \qquad o(H/P) = p^s$

$$\Rightarrow \quad \frac{o(H)}{o(P)} = p^s \quad \Rightarrow \quad o(H) = p^{n+s} \ , \ s > 0$$

$\Rightarrow$ $p^{n+s} / o(G)$, which is a contradiction by (1), as $s > 0$.

Hence $s > 0$ is not possible and in case $s = 0$, we have already shown that $x \in P$.

Structure of Finite Abelian Groups.

If a group is direct product of some of its subgroups, then the structure of the group can be determined by determining the structures of subgroups appearing in the direct product. This simplifies our work as determination of structure of a big group is broken into determination of structures of comparatively smaller groups.

Let us call the subgroups appearing in the direct product as "building blocks". Now the procedure will be more simple if these building blocks are taken to be cyclic subgroups since cyclic groups are always easy to deal with.

Now a natural question arise "Is it always possible to write a group as the direct product of its cyclic subgroups".

The answer is no, in general. However, luckily, it is possible for finite abelian groups, due to Fundamental Structure Theorem for finite abelian groups.

Before the formal statement of this Theorem, let us study another Theorem in this regard.

.....To be continued.....