15 Izreki Sylowa

1. Če je $|G| = p^2$, kjer je p praštevilo, potem je G abelska.

Izrek (prvi izrek Sylowa)
Naj bo G končna grupa reda $p^k q$, kjer je p praštevilo, $k, q \in \mathbb{N}$ in $\gcd(p, q) = 1$. Potem za vsak i $(1 \leq i \leq k)$ velja, da ima G najmanj edno podgrupo reda p^i.

2. Dokaži izrek zgoraj.

3. Če praštevilo p deli red končne grupe G, potem G vsebuje najmanj en element reda p.

Pripomba. Posledica tega primera je Cauchy-ev izrek za končne grupe.

Definicija (p-podgrupa, p-grupa)
Naj bo p praštevilo. Podgrupa H grupe G se imenuje p-podgrupa, če je red vsakega elementa iz H enak potenci števila p. Podobno, če je red vsakega elementa iz grupe G enak potenci števila p, potem se G imenuje p-grupa.

Izrek Končna grupa G je p-grupa če in samo če je $o(G)$ enak potenci števila p.

4. Dokaži izrek zgoraj.

5. Katera od naslednjih grup je p-grupa:
(i) grupa G reda 21?
(ii) grupa G reda 25?
(iii) grupa G reda 128?

Definicija (Sylowa p-podgrupa)
Naj bo G končna grupa in naj bo p praštevilo. Podgrupa grupe G reda p^k $(k \in \mathbb{N})$ se imenuje Sylowa p-podgrupa grupe G, če p^k deli $o(G)$ in p^{k+1} ne deli $o(G)$.

Pripomba. Po definiciji Sylowe p-podgrupe, so vse Sylove p-podgrupe končne grupe istega reda.

6. Če je P Sylowa p-podgrupa končne grupe G, potem je za vsak $x \in G$, $x^{-1}Px$ tudi Sylowa p-podgrupa grupe G.

Opomba. Če je P edina Sylowa p-podgrupa, potem je $x^{-1}Px = P \ \forall x \in G$. Naj bosta $g \in G$, $h \in P$. Potem $ghg^{-1} = (g^{-1})^{-1}hg^{-1} = x^{-1}hx \in x^{-1}Px$ (vzemo $x = g^{-1}$), $ghg^{-1} \in P \ \forall g \in G$, $h \in P$, P je edinka v grupi G.

7. Naj bo $o(G) = p^k q$ kje je p praštevilo, $k, q \in \mathbb{N}$ in $\gcd(p, q) = 1$ in naj bo P Sylowa p-podgrupa grupe G. Če je H p-podgrupa grupe G t.d. $P \subseteq H \subseteq G$, potem pokaži, da je $H = P$.

Opomba. Iz primera zgoraj opazimo, da p-podgrupa grupe G ne more strogo vsebovati Sylowe p-podgrupe grupe G.

Definicija (S konjugirana množici T, relacija konjigiranosti na množici)
Naj bo G grupa in naj bosta S, T neprazni podmnožici grupe G. Pravimo, da je množica S konjugirana množici T, če obstaja element $x \in G$ t. d.

$$S = x^{-1}Tx = \{x^{-1}tx : t \in T\}.$$

Če je S konjugiran množici T, pišemo $S \sim T$ in to relacijo '$\sim$' imenujemo relacijo konjigiranosti na množici vseh nepraznih podmnožic grupe G.

Izrek. Relacija konjugiranosti na množici vseh nepraznih podmnožic grupe G je ekvivalenčna relacija.

8. Dokaži izrek zgoraj.

Definicija (dvojni odsek)
Naj bo G grupa, x njen element in H ter K njeni podgrupi (ne nujno različni). Množici

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

rečemo dvojni odsek podgrup H in K v grupi G in označujemo s HxK.

Izrek. Naj bosta H in K dve (ne nujno različni) podgrupi končne grupe G. Za $x, y \in G$, sta dvojna odseka HxK in HyK bodisi enaka, bodisi disjunktna.

Izrek. Naj bosta H in K dve (ne nujno različni) podgrupi končne grupe G. Za $x \in G$

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

Izrek. (Frobenius). Če sta H in K dve (ne nujno različni) podgrupi končne grupe G, potem

$$o(G) = \sum \frac{o(H)o(K)}{o((x^{-1}Hx) \cap K)},$$

kjer vsota (na desni strani) teče po elementih x, ki so predstavniki dvojnih odsekov HyK.

9. Dokaži izreke zgoraj.

Izrek (drugi izrek Sylowa)
Naj bo G končna grupa reda $p^k q$, kjer je p praštevilo, $k, q \in \mathbb{N}$ in $\gcd(p, q) = 1$. Potem sta vsaki dve podgrupi reda p^k konjugirani.

10. Če je S Sylowa p-podgrupa končne grupe G, pokaži da je potem število Sylowih p-podgrup grupe G enako $\frac{o(G)}{o(N(S))}$.

Izrek (tretji izrek Sylowa)
Naj bo G končna grupa reda $p^k q$, kjer je p praštevilo, $k, q \in \mathbb{N}$ in $\gcd(p, q) = 1$. Potem je število podgrup reda p^k oblike $1 + mp$, kjer je m neko ne-negativno celo število. Velja tudi, da $1 + mp$ deli $o(G)$.

Definicija (enostavna grupa)
Grupa G je enostavna, če sta njeni edini edinki trivijalna grupa in grupa G.

11. Poišči mogoče število Sylowih 11-podgrup, Sylovih 7-podgrup in Sylowih 5-podgrup v grupi reda $5^2 \cdot 7 \cdot 11$.

12. (a.) Pokaži, da grupa reda 28 ni enostavna.
(b.) Pokaži, da grupa reda 40 ni enostavna.

13. Pokaži, da v grupi reda 20449 obstaja Sylowa 11-podgrupa, ter da grupa ni enostavna.

14. Pokaži, da grupa reda 56 ni enostavna.

15. Če ima grupa G reda 28 edinko reda 4, potem pokaži, da je grupa G abelska.

16. Pokaži, da ne obstaja enostavna grupa reda 48.

17. (a.) Do izomorfizma natančno določi vse grupe reda 99.
(b.) Do izomorfizma natančno določi vse grupe reda 66.

18. Pokaži, da je edina grupa reda 255 grupa $\mathbb{Z}_{255}$.

4

Sylow's Theorems

1. INTRODUCTION

In this chapter, we shall prove Sylow's theorems which would guarantee the existence of subgroups of prime power order. As a prerequisite to Sylow's theorems, we shall prove Cauchy's theorems.

2. CAUCHY'S THEOREMS

Theorem 1. (Cauchy's theorem for abelian groups) *Let G be a finite abelian group and $p/o(G)$, where p is a prime number. Then there exists an element $a(\neq e) \in G$ such that $a^p = e$.*

Proof. $p/o(G)$ implies $o(G) = n_1 p$, where $n_1 \geq 1$. We shall prove the result by using induction on n_1.

$n_1 = 1 \Rightarrow o(G) = p$. Since $o(G)$ is prime, G must be cyclic. Therefore, there exists $a \in G$ such that $G = (a)$ and $o(a) = p$. Thus, $a (\neq e) \in G$ and $a^p = e$.

$\therefore$ The result is true for $n_1 = 1$.

Now let the result be true for every abelian group G' for which $o(G') = n_2 p$ and $n_2 < n_1$. Since $o(G) = n_1 p$, a composite number and every group of composite order must have a proper subgroup, the group G has proper subgroups.

Let there be a proper subgroup H of G such that $p/o(H)$. Let $o(H) = mp$. $\therefore$ $m < n_1$.

$\therefore$ H is an abelian group such that $o(H) = mp$ and $m < n_1$.

$\therefore$ By induction hypothesis, $\exists\, a \in H$ such that $a \neq e$ and $a^p = e$.

Since $H \subset G$, we have $a \in G$. $\therefore$ $\exists\, a(\neq e) \in G$ such that $a^p = e$.

Now let no proper subgroup of G be there whose order is divisible by p.

Let H be any proper subgroup of G. $\therefore$ $p \nmid o(H)$.

Since G is abelian, H is a normal subgroup of G.

$\therefore$ The quotient group G/H is defined and is also abelian.

Now $$o(G/H) = \frac{o(G)}{o(H)} < o(G) \qquad (\because\ o(H) > 1)$$

Also $p/o(G/H)$, because $p/o(G)$ and $p \nmid o(H)$. Let $o(G/H) = m'p$, where $m' < n_1$.

$\therefore$ G/H is an abelian group for which $o(G/H) = m'p$ and $m' < n_1$.

$\therefore$ By induction hypothesis $\exists\ Hb \in G/H$ such that $Hb \neq H$ (the identity of G/H) and $(Hb)^p = H$.

$\Rightarrow$ $Hb^p = H \Rightarrow b^p \in H \Rightarrow (b^p)^{o(H)} = e \Rightarrow (b^{o(H)})^p = e \Rightarrow a^p = e$, where $a = b^{o(H)}$

Now $b \in G$ implies $b^{o(H)} \in G$ *i.e.*, $a \in G$.

If possible, let $a = e$.

$\Rightarrow\ b^{o(H)} = e \quad \Rightarrow\ Hb^{o(H)} = H \ \Rightarrow\ (Hb)^{o(H)} = H \ \Rightarrow\ o(Hb)/o(H) \ \Rightarrow\ p/o(H)$

$(\because\ (Hb)^p = H$ and p is prime $\Rightarrow\ o(Hb) = p)$

This is impossible, because $p \nmid o(H)$. $\therefore\ a \neq e$.

$\therefore$ There exists $a(\neq e) \in G$ such that $a^p = e$. This completes the proof.

Remark. $o(a) = n \ \Rightarrow\ n/p \ \Rightarrow\ n = 1$ or $p \ \Rightarrow\ n = p \quad (\because\ a \neq e)$

$\therefore\ o(a) = p$.

Theorem 2. (Cauchy's theorem) *Let G be a finite group and $p/o(G)$, where p is a prime number. Then there exists an element $a(\neq e) \in G$ such that $a^p = e$.*

Proof. $p/o(G)$ implies $o(G) = n_1 p$, where $n_1 \geq 1$. We shall prove the result by using induction on n_1.

$$n_1 = 1 \ \Rightarrow\ o(G) = p.$$

Since $o(G)$ is prime, G must be cyclic. Therefore, there exists $a \in G$ such that $G = (a)$ and $o(a) = p$. Thus $a(\neq e) \in G$ and $a^p = e$.

$\therefore$ The result is true for $n_1 = 1$.

Now let the result be true for every group G′ for which $o(G') = n_2 p$ and $n_2 < n_1$. Since $o(G) = n_1 p$, a composite number and every group of composite order must have a proper subgroup, the group G has proper subgroups.

Let there be a proper subgroup H of G such that $p/o(H)$. Let $o(H) = mp$. $\therefore\ m < n_1$.

$\therefore$ H is a group such that $o(H) = mp$ and $m < n_1$.

$\therefore$ By induction hypothesis, $\exists\ a \in H$ such that $a \neq e$ and $a^p = e$.

Since $H \subset G$, we have $a \in G$. $\therefore\ \exists\ a(\neq e) \in G$ such that $a^p = e$.

Now let no proper subgroup of G be there whose order is divisible by p.

Let Z be the centre of the group G. The *class equation* of the group G is

$$o(G) = o(Z) + \sum_{a \in Z} \frac{o(G)}{o(N(a))},$$

where the sum runs over elements a taken one each from each conjugate class containing more than one element.

For $a \notin Z$, $N(a)$ is a proper subgroup of G.

$$\Rightarrow \qquad p \nmid o(N(a)) \ \Rightarrow\ p \Big/ \frac{o(G)}{o(N(a))} \ \Rightarrow\ p \Big/ \sum_{a \in z} \frac{o(G)}{o(N(a))}$$

$$\Rightarrow \qquad p \Big/ \left(o(G) - \sum_{a \in Z} \frac{o(G)}{o(N(a))} \right) \ \Rightarrow\ p/o(Z).$$

Since Z is a subgroup of G and $p/o(Z)$, so by our assumption it cannot be a proper subgroup of G. $\therefore$ $Z = G$. Since Z is abelian, the group G is also abelian.

$\therefore$ By the *Cauchy's theorem for abelian groups*, there exists an element $a(\neq e) \in G$ such that $a^p = e$. This completes the proof.

Remark 1. $o(a) = n \ \Rightarrow\ n/p \ \Rightarrow\ n = 1$ or $p \ \Rightarrow\ n = p \quad (\because\ a \neq e)$

$\therefore\ o(a) = p$.

Remark 2. If G is a finite group and p is a prime number such that $p/o(G)$, then by **Cauchy's theorem**, there exists an element $a(\neq e) \in G$ such that $a^p = e$.

$\therefore\ o(a) = p$ and the set $\{e, a, a^2, \ldots\ldots, a^{p-1}\}$ is a subgroup of G of order p.

3. Prove that every subgroup of index 2 is a normal subgroup. Find an example of a subgroup of index 3 that is not normal.

Solution Let N be a subgroup of index two in G. Since the left cosets of N form a partition of G consisting of exactly two elements, the coset of N distinct from N consists of all the elements of G that are not in N. The same is true for the right cosets, that, again, are N and N^c.

We want to show that for any element $g \in G$, $gNg^{-1} = N$. We distinguish two cases. Let us assume first that g belongs to N. In that case for any element $n \in N$ the element gng^{-1} is still an element of N since N is a group, hence $gNg^{-1} = N$.

Let us now assume that g doesn't belong to N, then the left coset gN is not N since it contains the element g that, by assumption, doesn't belong to N and hence consists of all the element of G that are not in N. The same is true for the right coset, in particular we get that $gN = Ng$. This implies that for any n in N there is $n' \in N$ such that $gn = n'g$ multiplying on the right g^{-1} we get $gng^{-1} = n'$ and this implies that $gNg^{-1} = N$.

In order to give an example of a subgroup of index 3 that is not normal, let us consider the symmetric group S_3 and the subgroup H generated by the permutation $h = (12)$. The group S_3 has order 6, and the group H has order 2, since the transposition (12) has order 2. In order to show that H is not normal let us consider the permutation $g = (13)$:

$$ghg^{-1} = (13)(12)(13) = (132).$$

Since ghg^{-1} do not belong to H, the subgroup H is not normal.

It is interesting to compute the left and the right cosets of the group H and see that they give two different partitions of G:

Left cosets	Right cosets
$eH = \{e, (12)\}$	$He = \{e, (12)\}$
$(13)H = \{(13), (123)\}$	$H(13) = \{(13), (132)\}$
$(23)H = \{(23), (132)\}$	$H(23) = \{(23), (123)\}$.

Question:

10. a) Prove that every subgroup of index 2 is normal.

b) Give an example of a subgroup of index 3 which is not normal.

Answer:

a) Let G be a group and H be a subgroup of index 2. H partitions G into 2 left cosets H and aH, and similarly H partitions G into 2 right cosets, H, Ha.

If $a \in H$ then $aH = H = Ha$ since H is a subgroup of G.

If $a \in G - H$ then $aH = G - H = Ha$.

Thus, $aH = Ha$ for all $a \in G$, and H is normal in G.

b) Let $G = S_3$ and $H = \{1, (12)\}$ a subgroup of index 3. Then $(123)H = \{(123), (13)\}$ and $H(123) = \{(123), (12)\}$, thus $(123)H \neq H(123)$ and H is not normal.

 # 9.7 Prove that every subgroup of index 2 is normal.

- *# 9.7*: Suppose that H has index 2 in G. Then, for any a not in H, we have that $aH \cap H = \emptyset$ and $aH \cup H = G$. Therefore, the complement of H in G is simply aH. The exact same argument where Ha is considered instead of aH shows that the complement of H also equals Ha. Thus $aH = Ha$ for all a not in H. For any $b \in H$, $bH = H = Hb$. Thus, for all $g \in G$, we have $gH = Hg$, so that H is normal.

$\therefore$ If $p/o(G)$, then G has a subgroup of order p.

$\therefore$ The converse of **Lagrange's theorm** holds for prime factors of $o(G)$.

Example 1. *If G is a group of order 2p, where p is prime then it has a normal subgroup of order p.*

Sol. We have $o(G) = 2p$. $\therefore$ $p/o(G)$

$\therefore$ By *Cauchy's theorem,* there exists an element $a(\neq e) \in G$ such that $a^p = e$.

$\therefore$ $H = \{e, a, a^2, \ldots\ldots, a^{p-1}\}$ is a subgroup of G and its order is p.

$\therefore$ Index of H in $G = \dfrac{o(G)}{o(H)} = \dfrac{2p}{p} = 2$

Since every subgroup of G having index 2 is always normal, the subgroup H is a normal subgroup of G.

Example 2. *Show that an abelian group of order pq, where p and q are distinct primes, is cyclic.* (M.D.U. 2005)

Sol. Let G be an abelian group of order pq. Since p and q are both prime numbers and are divisors of pq, by **Cauchy's theorem,** there exists $a(\neq e)$, $b(\neq e)$ in G such that

$a^p = e$, $b^q = e$.

Let $o(a) = n$, $1 \leq n \leq p$

$\Rightarrow$ n/p $\Rightarrow$ $n = 1$ or p $\Rightarrow$ $n = p$ $(\because\ a \neq e \Rightarrow o(a) \neq 1)$

$\therefore$ $o(a) = p$. Similarly, $o(b) = q$.

We claim that $ab \neq e$. If possible, let $ab = e$.

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

$\Rightarrow$ $q = p$, which is impossible.

$\therefore$ $ab \neq e$.

Since $ab \in G$, we have $o(ab)/pq$

$\therefore$ $o(ab) = 1$ or p or q or pq. We assume that $p < q$.

$o(ab) = 1 \Rightarrow ab = e$, which is impossible.

$o(ab) = p \Rightarrow (ab)^p = e \Rightarrow a^p b^p = e \Rightarrow eb^p = e$ $(\because$ G is abelian)

$\Rightarrow b^p = e$, which is impossible.

$(\because\ o(b) = q$ and $p < q \Rightarrow b^p \neq e)$

$o(ab) = q \Rightarrow (ab)^q = e \Rightarrow a^q b^q = e \Rightarrow a^q e = e \Rightarrow a^q = e$

$\Rightarrow a^{pk+r} = e \Rightarrow (a^p)^k a^r = e \Rightarrow e^k a^r = e$ (Taking $q = pk + r$)

$\Rightarrow a^r = e$, which is impossible. $(\because\ 0 \leq r < p \Rightarrow a^r \neq e)$

$\therefore$ We are left with only one choice *i.e.*, $o(ab) = pq$.

$\therefore$ The group G of order pq contains an element of order pq.

$\therefore$ The group G must be cyclic.

Remark. Abelian groups of order 6, 10, 14, 21, 22, ... are all cyclic because $6 = 2 \times 3$, $10 = 2 \times 5$, $14 = 2 \times 7$, $21 = 3 \times 7$, $22 = 2 \times 11$, ...

Example 3. *Show that every abelian group of order 6 is cyclic.*

Sol. Let G be an abelian group of order 6. Since 2 and 3 are both prime numbers and are divisors of 6, by *Cauchy's theorem*, there exists elements $a(\neq e)$, $b(\neq e)$ in G such that $a^2 = e$, $b^3 = e$.

$\therefore$ $o(a) = 2, o(b) = 3$ $(\because$ 2, 3 are prime)

We claim that $ab \neq e$. If possible, let $ab = e$.

$\Rightarrow \quad a^{-1}(ab) = a^{-1}e \quad \Rightarrow \quad b = a^{-1} \quad \Rightarrow \quad o(b) = o(a^{-1}) \quad \Rightarrow \quad 3 = 2$, which is impossible.

$(\because \quad o(a^{-1}) = o(a) = 2)$

$\therefore \qquad ab \neq e.$

Now $\quad (ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = a^2b^2 = eb^2 = b^2 \neq e \qquad (\because \quad o(b) = 3)$

Also $\quad (ab)^3 = (ab)^2(ab) = (a^2b^2)(ab) = (a^2a)(b^2b) = (ea)e = a \neq e$

$\therefore$ $o(ab) > 3$. Since $o(ab)$ must divide $o(G)$, the value of $o(ab)$ must be 6.

$\therefore$ The group G of order 6 contains an element of order 6.

$\therefore$ The group G must be cyclic.

Example 4. *Find all non-abelian groups of order 6.*

Sol. Let G be a non-abelian group of order 6. Since 2 and 3 are both prime numbers and are divisors of 6, by **Cauchy's theorem**, there exist elements $a(\neq e)$, $b(\neq e)$ in G such that $a^2 = e$, $b^3 = e$.

$\therefore \qquad o(a) = 2, \quad o(b) = 3 \qquad (\because \quad 2, 3 \text{ are prime})$

Let $\qquad H = (b). \quad \therefore \quad o(H) = o(b) = 3$

$$\therefore \qquad [G : H] = \frac{o(G)}{o(H)} = \frac{6}{3} = 2$$

Since every subgroup of G having index 2 is always normal, the subgroup H is a normal subgroup of G.

$a \in H \quad \Rightarrow \quad o(a) / o(H)$ *i.e.* 2/3, which is impossible.

$\therefore \qquad a \notin H$

$\therefore$ H and Ha are disjoint right cosets of H in G.

$\therefore \qquad G = H \cup Ha = \{e, b, b^2, ea, ba, b^2a\}$

$= \{e, b, b^2, a, ba, b^2a\}$

Since H is normal in G, we have $aba^{-1} \in H$.

$\therefore \qquad aba^{-1} = e$ or b or b^2

$aba^{-1} = e \quad \Rightarrow \quad a^{-1}(aba^{-1})a = a^{-1}ea \quad \Rightarrow \quad b = e$, which is not true.

$aba^{-1} = b \quad \Rightarrow \quad ab = ba$

Using $ab = ba$, we can show that $xy = yx \; \forall \; x, y \in G$.

$\therefore$ G is abelian, which is not true.

$\therefore \qquad aba^{-1} = b^2$ or $aba^{-1} = b^{-1} \qquad (\because \quad b^3 = e)$

$\therefore \qquad G = \{e, b, b^2, a, ba, b^2a\}$, where $a^2 = e = b^3$ and $aba^{-1} = b^{-1}$.

This is the only non-abelian group of order 6.

Theorem 3. *Prove the converse of the Lagrange's theorem for finite abelian groups.*

Proof. Let G be a finite abelian group of order n. We shall prove the result by using P.M.I. on n.

The result is trivially true for $n = 1$.

Let the result be true for all finite abelian groups of order less than n.

Let m/n we shall show that there exists a subgroup of G of order m. If $m = 1$, then the subgroup $\{e\}$ serve our purpose. So let $m > 1$. Let p be a prime number such that p/m.

$\therefore$ p/n, because m/n.

$\therefore$ By **Cauchy's theorem** for abelian groups there exists an element $a(\neq e) \in G$ such that $a^p = e$.

Let $o(a) = \lambda$.

$\Rightarrow \lambda/p \Rightarrow \lambda = 1 \text{ or } p \Rightarrow \lambda = p$ $(\because a \neq e)$

$\therefore o(a) = p$

Let $N = \{e, a, a^2, \ldots\ldots, a^{p-1}\}$

$\therefore$ N is a subgroup of G. Since G is abelian, N is normal in G.

$\therefore$ G/N is a finite abelian group.

Now $o(G/N) = \dfrac{o(G)}{o(N)} = \dfrac{n}{p} < nZ$ $(\because p > 1)$

Also $o(G) = o(G/N)\, o(N)$ ...(1)

We have p/m and m/n.

Let $m = \lambda_1 p$ and $n = m\lambda_2$ for some positive integers λ_1 and λ_2.

$\therefore$ (1) $\Rightarrow n = o(G/N) \cdot p \Rightarrow m\lambda_2 = o(G/N) \cdot p \Rightarrow \lambda_1 p \lambda_2 = o(G/N) \cdot p$

$\Rightarrow o(G/N) = \lambda_1\lambda_2 \quad \therefore \lambda_1/o(G/N)$

$\therefore \lambda_1/o(G/N)$ and G/N is a finite abelian group of order less than n.

$\therefore$ By induction hypothesis, G/N has a subgroup H/N of order λ_1.

$\therefore o(H/N) = \lambda_1$, where H is a subgroup of G containing N.

$\Rightarrow \dfrac{o(H)}{o(N)} = \lambda_1 \Rightarrow o(H) = \lambda_1\, o(N) = \lambda_1 p = m$

$\therefore$ H is a subgroup of G of order m. This completes the proof.

Example 5. *Let G be a finite group of order p^n, where p is a prime number. Show that G has subgroups of orders 1, p, p^2, ..., p^n.*

Sol. We have $o(G) = p^n$.

We shall prove the result by using induction on n.

Let $n = 1$. $\therefore o(G) = p^1 = p$

Here $\{e\}$ and G are subgroups of G of orders 1 and p respectively.

$\therefore$ The results holds for $n = 1$.

Now let the result be true for every group G', where $o(G') = p^{n_1}$ and $n_1 < n$.

Since $o(G) = p^n$, we have $o(Z) > 1$.

By **Lagrange's theorem**, $o(Z)/o(G)$ *i.e.*, $o(Z)/p^n$.

Let $o(Z) = p^m$ for some $0 < m \leq n$.

$\therefore$ $p/o(Z)$ and thus by **Cauchy's theorem**, there exists $a(\neq e) \in Z$ such that $a^p = e$.

$\therefore$ $H = \{e, a, a^2, \ldots\ldots, a^{p-1}\}$ is a subgroup of Z of order p.

Since p is prime, the subgroup H is cyclic.

$\therefore$ H is normal subgroup of G $(\because a \in Z \text{ and } H = (a))$

$\therefore$ G/H is a group and $o(G/H) = \dfrac{o(G)}{o(H)} = \dfrac{p^n}{p} = p^{n-1} < p^n$.

$\therefore$ By induction hypothesis, G/H has subgroups H/H, H_1/H, H_2/H, ..., H_{n-1}/H of orders $1, p, p^2, \ldots\ldots, p^{n-1}$ respectively.

$\therefore$ H, H_1, H_2, ..., H_{n-1} are subgroups of G of orders $p, p^2, p^3, \ldots\ldots, p^n$ respectively.

$\therefore$ $\{e\}$, H, H_1, H_2, ..., H_{n-1} are subgroups of G of orders $1, p, p^2, \ldots\ldots, p^n$ respectively. This completes the proof.

3. SYLOW'S FIRST THEOREM

Statement. *Let G be a finite group of order $p^k q$, where p is prime, $k, q \in \mathbf{N}$ and $(p, q) = 1$. Then for each $i (1 \le i \le k)$, G has at least one subgroup of order p^i.*

Proof. We have $o(G) = p^k q$, where $k, q \in \mathbf{N}$ and $(p, q) = 1$.

We shall prove the result by using induction on $o(G)$.

Let $p = 2, k = 1, q = 1. \quad \therefore \quad o(G) = (2)^1.1 = 2$

$\therefore$ G, being its subgroup, is the required subgroup of order $(2)^1$ *i.e.*, 2.

Now let the result be true for all groups with order less than $o(G)$.

Let Z be the centre of the group G. $\therefore$ Z is an abelian normal subgroup of G.

Now either $p/o(Z)$ or $p \nmid o(Z)$.

Case I. $p/o(Z)$. Since Z is a finite abelian group and $p/o(Z)$, by *Cauchy's theorem for abelian groups*, there exists an element $a (\ne e) \in Z$ such that $a^p = e$. Since p is prime, we have $o(a) = p$.

If $k = 1$, then $o(G) = pq$ and (a) is the required subgroup of G of order p.

Let $k > 1$.

$$a \in Z \Rightarrow ax = xa \quad \forall\, x \in G$$

Let $a^i x = x a^i \ \forall\, x \in G$

Now, for $x \in G$, $a^{i+1}x = a(a^i x) = a(xa^i) = (ax)a^i = (xa)a^i = xa^{i+1}$.

$\therefore$ By induction, $a^m x = x a^m \quad \forall\, m \in \mathbf{N}$ and $x \in G$.

$\therefore$ (a), the subgroup generated by a, is a normal subgroup of G.

$$\therefore \quad o(G/(a)) = \frac{o(G)}{o((a))} = \frac{p^k q}{p} = p^{k-1} q < p^k q.$$

$\therefore$ By induction hypothesis, $G/(a)$ contains subgroups $H_1, H_2, \ldots, H_{k-1}$ of orders $p, p^2, \ldots, p^{k-1}$ respectively.

Let $H_i = K_i/(a)$ for some subgroup K_i of G containing (a), $1 \le i \le k-1$.

$$\therefore \quad o(K_i) = o(H_i).\, o((a)) = p^i p = p^{i+1}, \ 1 \le i \le k-1.$$

$\therefore$ $(a), K_1, K_2, \ldots\ldots, K_{k-1}$ are subgroups of G of orders $p, p^2, p^3, \ldots\ldots, p^k$ respectively.

Case II. $p \nmid o(Z)$. The class equation of the group G is

$$o(G) = o(Z) + \sum_{a \in Z} \frac{o(G)}{o(N(a))},$$

where the sum runs over elements a taken one from each conjugate class containing more than one element.

If possible, let $p \Big/ \dfrac{o(G)}{o(N(a))} \quad \forall\, a \notin Z.$

$$\Rightarrow \quad p \Big/ \sum_{a \in Z} \frac{o(G)}{o(N(a))} \quad \Rightarrow \quad p \Big/ \left(o(G) - \sum_{a \in Z} \frac{o(G)}{o(N(a))} \right) \qquad (\because \ p/o(G))$$

$\Rightarrow$ $p/o(Z)$, which is impossible.

$\therefore$ There exists at least one $a \in G$ such that $p \nmid \dfrac{o(G)}{o(N(a))}$ and $a \notin Z$.

Now $o(G) = \dfrac{o(G)}{o(N(a))} \times o(N(a))$ and $p^k/o(G), p \nmid \dfrac{o(G)}{o(N(a))}$, so we must have $p^k/o(N(a))$.

Also $a \notin Z \Rightarrow N(a) \neq G \Rightarrow o(N(a)) < o(G)$.

$\therefore$ By induction hypothesis, $N(a)$ has at least one subgroup of order p^i, where $i = 1, 2, 3, \ldots\ldots, k$. Since $N(a)$ is a subgroup of G, these subgroups of $N(a)$ are also subgroups of G.

This completes the proof.

Example 6. *If a prime number p divides the order of a finite group G, then G contains at least one element of order p.*

Proof. We have $p/o(G)$.

Let $o(G) = p^k q$, where $k, q \in N$ and $(p, q) = 1$.

$\therefore$ By *Sylow's first theorem*, G has subgroups of orders $p, p^2, \ldots\ldots, p^k$.

Let H be a subgroup of G of order p.

Since p is prime, H is cyclic. Let $H = (a)$, where $a \in G$. $\therefore$ $o(a) = p$.

$\therefore$ The result holds.

Remark. The result of this example is the *Cauchy's theorem for finite group.*

4. p-SUBGROUP

Let p be a prime number. A subgroup H of a group G is called a **p-subgroup** if the order of each element of H is a power of p.

In particular, if the order of each element of G is a power of p, then G is called a **p-group.**

Theorem 1. *A finite group G is a p-group if and only if o(G)is a power of p.*

Proof. Let $o(G) = p^k$.

As a consequence of *Lagrange's theorem*, $o(a)/o(G)$ *i.e.*, $o(a)/p^k \ \forall \ a \in G$.

$\therefore$ The order of a is a power of p.

$\therefore$ The order of each element of G is a power of p.

$\therefore$ G is a p-group.

Conversely, let G be a p-group.

$\therefore$ No prime $q(\neq p)$ can divide $o(G)$, otherwise by *Cauchy's theorem*, G will contain an element of order q.

$\therefore$ $o(G) = p^k$ for some k.

Example 7. *Which of the following is a p-group :*

(i) group G of order 21 ? *(ii) group G of order 25 ?*

(iii) group G of order 128 ?

Sol. (*i*) We have $o(G) = 21$

21 cannot be written in the form p^n, where p is a prime.

$\therefore$ G is not a p-group.

(*ii*) We have $o(G) = 25$

$\therefore$ $o(G) = p^2$, where $p = 5$

$\therefore$ G is a p-group, where $p = 5$

(*iii*) We have $o(G) = 128$

$\therefore$ $o(G) = p^7$, where $p = 2$

$\therefore$ G is a p-group, where $p = 2$.

5. SYLOW p-SUBGROUP

Let G be a finite group and p, a prime number. A subgroup of G of order $p^k, k \in N$ called a **Sylow p-subgroup** of G if $p^k/o(G)$ and $p^{k+1} \nmid o(G)$.

Remark. According to the definition of Sylow p-subgroup, all Sylow p-subgroups of a finite group are of same order.

Example 8. *If P is a Sylow p-subgroup of a finite group G, then for each $x \in G$, $x^{-1}Px$ is also a Sylow p-subgroup of G.*

Sol. Let $o(P) = p^\alpha$, where p is a prime.

$\therefore$ $p^\alpha / o(G)$ and $p^{\alpha+1} \nmid o(G)$.

Let $x \in G$ be arbitrary.

$x^{-1}Px$ is a subgroup of G.

$$e \in P \Rightarrow x^{-1}ex\,(= x^{-1}x = e) \in x^{-1}Px \quad \therefore \quad x^{-1}Px \neq \phi$$

Let $x^{-1}h_1x, x^{-1}h_2x \in x^{-1}Px$

Now $(x^{-1}h_1x)(x^{-1}h_2x)^{-1} = (x^{-1}h_1x)(x^{-1}h_2^{-1}(x^{-1})^{-1}) = x^{-1}h_1(xx^{-1})\,h_2^{-1}x$

$= x^{-1}h_1h_2^{-1}x \in x^{-1}Px$ $\quad (\because\ h_1, h_2 \in P \Rightarrow h_1h_2^{-1} \in P)$

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

$o(x^{-1}Px) = p^\alpha$. Define $\phi : P \to x^{-1}Px$ by $P(h) = x^{-1}hx\ \forall\ h \in P$.

ϕ is a well defined mapping.

Let $h_1, h_2 \in P$ and $\phi(h_1) = \phi(h_2)$.

$\Rightarrow$ $x^{-1}h_1x = x^{-1}h_2x \Rightarrow x(x^{-1}h_1x)\,x^{-1} = x(x^{-1}h_2x)\,x^{-1}$

$\Rightarrow$ $(xx^{-1})\,h_1(xx^{-1}) = (xx^{-1})\,h_2(xx^{-1}) \Rightarrow h_1 = h_2$.

$\therefore$ ϕ is one-one.

Let $x^{-1}hx \in x^{-1}Px$. $\therefore$ $h \in P$ and $\phi(h) = x^{-1}hx$.

$\therefore$ ϕ is onto.

$\therefore$ There one-to-one correspondence between the elements of P and $x^{-1}Px$.

$\therefore$ $o(P) = o(x^{-1}Px) \quad \therefore \quad o(x^{-1}Px) = p^\alpha$

$\therefore$ $x^{-1}Px$ is a subgroup of G of order p^α. Also $p^\alpha / o(G)$ and $p^{\alpha+1} \nmid o(G)$.

$\therefore$ $x^{-1}Px$ is a Sylow p-subgroup of G.

Remark. If P is the only sylow p-subgroup then $x^{-1}Px = P\ \forall\ x \in G$.

Let $g \in G, h \in P$.

$\therefore$ $ghg^{-1} = (g^{-1})^{-1}\,h\,g^{-1} = x^{-1}hx \in x^{-1}Px$ (Taking $x = g^{-1}$)

$\therefore$ $ghg^{-1} \in P\ \forall\ g \in G, h \in P$

$\therefore$ P is normal in G.

Example 9. *Let $o(G) = p^kq$, where p is prime, $k, q \in \mathbf{N}$ and $(p, q) = 1$ and P be a Sylow p-subgroup of G. If H is a p-subgroup of G such that $P \subseteq H \subseteq G$, then show that $H = P$.*

Sol. We have p^k / p^kq and $p^{k+1} \nmid p^kq$, because $(p, q) = 1$.

$\therefore$ $p^k / o(G)$ and $p^{k+1} \nmid o(G)$

$\therefore$ The order of the Sylow p-subgroup P of G is p^k.

Since H is a p-subgroup of G, the order of each element of H is a power of p.

$\therefore$ No prime $r (\neq p)$ can divide $o(H)$, otherwise by *Cauchy's theorem*, H will contain an element of order r.

$\therefore$ $o(H) = p^t$ for some t. By *Lagrange's theorem* p^t / p^kq. Since $(p, q) = 1$, we have $t \leq k$.

Also, $P \subseteq H \Rightarrow o(P) \leq o(H) \Rightarrow p^k \leq p^t \Rightarrow k \leq t$.

$\therefore$ $t = k$ or $p^t = p^k$ or $o(H) = o(P)$. $\therefore$ $H = P$.

Remark. From the above example, we note that a p-subgroup of G cannot properly contain a Sylow p-subgroup of G.

6. CONJUGACY RELATION ON SETS

Let G be a group and S, T be non-empty subsets of G. The set S is said to be **conjugate** of T if there exists an element $x \in G$ such that

$$S = x^{-1}Tx = \{x^{-1}tx : t \in T\}.$$

If S is conjugate of T then we write $S \sim T$ and this relation '~' is called the **conjugacy relation** on the set of non-empty subsets of G.

Remark 1. If S and T are conjugate subsets of a finite group G then $o(S) = o(T)$, because we can write $T = x^{-1}Sx$ for some $x \in G$ and define a one-one onto mapping

$$\phi : S \to T \quad \text{by} \quad \phi(s) = x^{-1}sx \quad \forall s \in S.$$

Remark 2. Every conjugate of a sylow p-subgroup of a finite group is also a sylow p-subgroup.

Theorem 1. *The conjugacy relation on the set of non-empty subsets of a group is an equivalence relation.*

Proof. Let G be a group and the conjugacy relation on the set of non-empty subsets of G be denoted by ~. We shall show that ~ is an equivalence relation.

1. **Reflexivity.** Let $S(\neq \phi) \subseteq G$.

We have $e^{-1}Se = eSe = S$

$\therefore$ $S = e^{-1}Se$ *i.e.*, $S \sim S$

$\therefore$ $S \sim S$ for $S(\neq \phi) \subseteq G$. $\therefore$ ~ is reflexive.

2. **Symmetry.** Let $S(\neq \phi), T(\neq \phi) \subseteq G$ and $S \sim T$.

$\therefore$ $\exists\, x \in G$ $\therefore$ $S = x^{-1}Tx$

$\Rightarrow$ $xSx^{-1} = x(x^{-1}Tx)x^{-1} = (xx^{-1})T(xx^{-1}) = eTe = T$

$\Rightarrow$ $T = xSx^{-1}$ *i.e.*, $T = (x^{-1})^{-1}\, S(x^{-1})$

$\therefore$ $T \sim S$, because $x^{-1} \in G$.

$\therefore$ $S \sim T \Rightarrow T \sim S$. $\therefore$ ~ is symmetric.

3. **Transitivity.** Let S, T, U be non-empty subsets of G and $S \sim T$ and $T \sim U$.

$\therefore$ $\exists\, x, y \in G : S = x^{-1}Tx$ and $T = y^{-1}Uy$.

$\therefore$ $S = x^{-1}(y^{-1}Uy)\, x = (x^{-1}y^{-1})\, U(yx) = (yx)^{-1}\, U(yx)$

$\therefore$ $S \sim U$, because $yx \in G$

$\therefore$ $S \sim T$ and $T \sim U \Rightarrow S \sim U$. $\therefore$ ~ is transitive.

$\therefore$ The conjugacy relation on the set of non-empty subsets of a group is an equivalence relation.

Remark. In particular, the relation of conjugacy on the set of subgroups of a group is also an equivalence relation.

7. CONJUGATE CLASS

We know that an equivalence relation on a set partitions it into mutually disjoint equivalence classes.

Let C(S) denote the equivalence class of a non-empty subset S of G with respect to the conjugacy relation ~ on the set of non-empty subsets of the group G. The set C(S) is called the **conjugate class** of S in G.

$\therefore$
$$\begin{aligned} C(S) &= \{T : T(\neq \phi) \subseteq G \text{ and } T \sim S\} \\ &= \{T : T(\neq \phi) \subseteq G \text{ and } T = x^{-1}Sx \text{ for some } x \in G\} \\ &= \{x^{-1}Sx : x \in G\} \\ &= \text{set of all conjugates of S.} \end{aligned}$$

Since the relation '~' is reflexive, $S \in C(S)\ \forall\ S(\neq \phi) \subseteq G$

Also, $C(S) \subseteq P(G)\ \forall\ S(\neq \phi) \subseteq G$,

where P(G) is the set of all non-empty subsets of G.

$$\therefore \quad P(G) = \bigcup_{S(\neq\phi)\subseteq G} \{S\} \subseteq \bigcup_{S(\neq\phi)\subseteq G} C(S) \subseteq P(G)$$

$$\therefore \quad P(G) = \bigcup_{S(\neq\phi)\subseteq G} C(S).$$

In particular, let G be a finite group and

$$P(G) = \bigcup_{i=1}^{t} C(S_i), \qquad \text{(P(G) is the set of all non-empty subsets of G)}$$

where the equivalence classes $C(S_1), C(S_2), \ldots\ldots, C(S_t)$ are mutually disjoint.

$$\therefore \quad o(P(G)) = \sum_{i=1}^{t} o(C(S_i)).$$

8. NORMALIZER OF A SET *(K.U. 2005)*

Let G be a group and K, a subgroup of G. For $S(\neq \phi) \subseteq G$, the set $\{x \in K : x^{-1}Sx = S\}$ is called the **normalizer** of the set S in K and it is denoted by $N_K(S)$.

In particular, G is a subgroup of G and we have

$$N_G(S) = \{x \in G : x^{-1}Sx = S\}.$$

For simplicity, we write $N_G(S)$ as N(S) and call it as the normalizer of S.

Thus, $N(S) = \{x \in G : x^{-1}Sx = S\}$.

Remark. If G is an abelian group and $S(\neq \phi) \subseteq G$, then $x^{-1}Sx = S \quad \forall\ x \in G$.

$\therefore \quad N(S) = G \quad \forall\ S(\neq \phi) \subseteq G.$

Theorem 1. *Let G be a group. For any non-empty subset S of G, the normalizer N(S) of S is a subgroup of G.* (K.U. 2005)

Proof. We have $N(S) = \{x \in G : x^{-1}Sx = S\}$.

$e \in N(S)$, because $e^{-1}Se = eSe = S$. $\therefore$ N(S) is non-empty.

Let $x, y \in N(S)$. $\therefore\ x^{-1}Sx = S, y^{-1}Sy = S$

Now $(xy)^{-1}\ S(xy) = (y^{-1}x^{-1})\ S(xy) = y^{-1}(x^{-1}Sx)\ y = y^{-1}Sy = S$

$\therefore \quad (xy)^{-1}\ S(xy) = S \qquad \therefore\ xy \in N(S)$

Let $x \in N(S)$. $\therefore\ x^{-1}Sx = S$

$\Rightarrow \quad x(x^{-1}Sx)\ x^{-1} = xSx^{-1} \quad \Rightarrow \quad (xx^{-1})\ S(xx^{-1}) = xSx^{-1} \quad \Rightarrow \quad eSe = xSx^{-1}$

$\Rightarrow \quad xSx^{-1} = S \quad \Rightarrow \quad (x^{-1})^{-1}\ S(x^{-1}) = S$

$\therefore \quad x^{-1} \in N(S)$

$\therefore$ N(S) is a subgroup of G.

Remark. The normalizer N(S) may not be a normal subgroup of G.

Example 10. *Let G be a group and K, a subgroup of G. If $S(\neq \phi) \subseteq G$, then show that $N_K(S)$ is a subgroup of G.*

Sol. We claim that $N_K(S) = N(S) \cap K$.

$$x \in N_K(S) \Leftrightarrow x^{-1}Sx = S \text{ and } x \in K \Leftrightarrow x \in N(S) \text{ and } x \in K$$

$\Leftrightarrow\ x \in N(S) \cap K. \quad \therefore\ N_K(S) = N(S) \cap K.$

Since N(S) is a subgroup of G and the intersection of two subgroups is again a subgroup, the set $N_K(S)$ is also a subgroup of G.

Example 11. *Let H be a subgroup of a group G. Show that H is normal iff N(H) = G.* (M.D.U. 2005)

Sol. Let H be a normal subgroup of the group G.

$\Rightarrow \quad ghg^{-1} \in H \quad \forall\, h \in H, g \in G$

Let $x \in G, \quad h \in H.$

$\therefore \quad x^{-1}hx = x^{-1}h(x^{-1})^{-1} \in H \qquad (\because \quad x^{-1} \in G)$

$\Rightarrow \quad x^{-1}Hx \subseteq H$

Also $\quad h = x^{-1}(xhx^{-1})x \in x^{-1}Hx \qquad (\because \quad xhx^{-1} \in H)$

$\Rightarrow \quad H \subseteq x^{-1}Hx$

$\Rightarrow \quad x^{-1}Hx = H \quad \Rightarrow \quad x \in N(H)$

$\therefore \quad N(H) = G$

Conversely, let $N(H) = G.$

Let $x \in G, h \in H.$

$\Rightarrow \quad x \in N(H) \quad \Rightarrow \quad x^{-1}Hx = H \quad \Rightarrow \quad xx^{-1}Hxx^{-1} = xHx^{-1}$

$\Rightarrow \quad xHx^{-1} = H \quad \Rightarrow \quad xhx^{-1} \in H$

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

Theorem 2. *If G is a finite group and $S(\neq \phi) \subseteq G$ then $o(C(S)) = \dfrac{o(G)}{o(N(S))}$.*

Proof. We have $\quad C(S) = \{x^{-1}Sx : x \in G\}.$

Let A be the set of all right cosets of the subgroup N(S) in G.

Define $\phi : A \to C(S)$ by $\phi(N(S)x) = x^{-1}Sx \quad \forall\, x \in G$

ϕ is well defined. Let $x, y \in G.$

$N(S)x = N(S)y \quad \Rightarrow \quad xy^{-1} \in N(S) \qquad (\because \quad Ha = Hb \quad \Leftrightarrow \quad ab^{-1} \in H)$

$\Rightarrow \quad (xy^{-1})^{-1}\, Sxy^{-1} = S \quad \Rightarrow \quad yx^{-1}\, Sxy^{-1} = S \quad \Rightarrow \quad y^{-1}(yx^{-1}Sxy^{-1})y = y^{-1}Sy$

$\Rightarrow \quad (y^{-1}y)(x^{-1}Sx)y^{-1}y = y^{-1}Sy \quad \Rightarrow \quad x^{-1}Sx = y^{-1}Sy$

$\Rightarrow \quad \phi(N(S)x) = \phi(N(S)y).$

$\therefore \quad \phi$ is well defined.

ϕ is one-one. Let $x, y \in G.$

$\phi(N(S)x) = \phi(N(S)y) \quad \Rightarrow \quad x^{-1}Sx = y^{-1}Sy \quad \Rightarrow \quad y(x^{-1}Sx)\,y^{-1} = y(y^{-1}Sy)\,y^{-1}$

$\Rightarrow \quad (yx^{-1})\, S(xy^{-1}) = (yy^{-1})\, S(yy^{-1}) \quad \Rightarrow \quad (xy^{-1})^{-1}\, S(xy^{-1}) = S \quad \Rightarrow \quad xy^{-1} \in N(S)$

$\Rightarrow \quad N(S)x = N(S)y.$

$\therefore \quad \phi$ is one-one.

ϕ is onto. Let $T \in C(S)$

$\therefore \quad \exists\, x \in G : T = x^{-1}Sx.$

Now $N(S)x \in A$ and $\phi(N(S)x) = x^{-1}Sx = T.$

$\therefore \quad \phi$ is onto.

$\therefore$ There is one-to-one correspondence between the right cosets of N(S) in G and the conjugates of S.

Since the group G is finite, we have

$o(C(S))$ = number of elements of C(S)

= number of conjugates of S.

$$= \text{number of right cosets of } N(S) \text{ in } G \qquad (\because \ \phi \text{ is 1–1 and onto})$$

$$= \frac{o(G)}{o(N(S))}$$

$$\therefore \qquad o(C(S)) = \frac{o(G)}{o(N(S))}.$$

In other words, the number of conjugates of S is equal to the index of N(S) in G *i.e.*, $o(C(S)) = [G : N(S)]$.

Example 12. *Let G be a group and S, a subgroup of G. Show that S is a normal subgroup of N(S). Also, N(S) is the largest subgroup of G, in which S is normal.*

Sol. We know that N(S) is a subgroup of the group G.

Let $x \in S$. We claim that $x^{-1}Sx = S$.

$$s \in S \ \Rightarrow \ s = ese = (x^{-1}x)\, s(x^{-1}x) = x^{-1}(xsx^{-1})\, x \in x^{-1}Sx$$

$$(\because \ x, s \in S \ \Rightarrow \ xsx^{-1} \in S)$$

$$\therefore \qquad S \subseteq x^{-1}Sx$$

$$x^{-1}sx \in x^{-1}Sx \ \Rightarrow \ s \in S \ \Rightarrow \ x^{-1}sx \in S \qquad (\because \ x, s \in S \ \Rightarrow \ x^{-1}sx \in S)$$

$$\therefore \qquad x^{-1}Sx \subseteq S$$

Combining, we get $x^{-1}Sx = S$. $\therefore \ x \in N(S)$

$\therefore \qquad S \subseteq N(S)$. $\therefore$ S is a subgroup of N(S).

Let $x \in N(S)$ and $s \in S$. $\therefore \ x^{-1}Sx = S$

$$\Rightarrow \qquad x(x^{-1}Sx)x^{-1} = xSx^{-1} \ \Rightarrow \ (xx^{-1})S(xx^{-1}) = xSx^{-1} \ \Rightarrow \ eSe = xSx^{-1} \ \Rightarrow \ xSx^{-1} = S$$

$$\therefore \qquad xsx^{-1} \in S \quad \therefore \ S \text{ is a normal subgroup of } N(S).$$

Now let H be any subgroup of G in which S is normal.

We shall show that $H \subseteq N(S)$.

Let $h \in H$.

$\therefore \ hsh^{-1} \in S \quad \forall \quad s \in S$

In order to show that $h \in N(S)$, it is sufficient to show that $h^{-1}Sh = S$.

Let $s \in S$. $h \in H$ implies $h^{-1} \in H$.

$\therefore \ h^{-1}s(h^{-1})^{-1} \in S$ *i.e.*, $h^{-1}sh \in S$

$$\therefore \qquad h^{-1}Sh \subseteq S$$

Also, $\qquad s = ese = (h^{-1}h)\, s(h^{-1}h) = h^{-1}(hsh^{-1})\, h \qquad \ldots(1)$

Now $h \in H$, $s \in S$ implies $hsh^{-1} \in S$.

$$\therefore \qquad h^{-1}(hsh^{-1})h \in h^{-1}Sh$$

$$\therefore \ (1) \ \Rightarrow \qquad s \in h^{-1}Sh$$

$$\therefore \qquad S \subseteq h^{-1}Sh$$

Combining, we get $h^{-1}Sh = S$.

$$\therefore \qquad h \in N(S). \quad \therefore \ H \subseteq N(S)$$

$\therefore$ N(S) is the largest subgroup of G in which S is normal.

9. DOUBLE COSET

Let H and K be two (not necessarily distinct) subgroups of a group G and let $x \in G$. The set $\{hxk : h \in H, k \in K\}$ is called a **double coset** of the group G and is denoted by HxK.

Theorem 1. *Let H and K be two (not necessarily distinct) subgroups of a group G. For $x, y \in G$, the double cosets HxK and HyK are either disjoint, or identical.*

Proof. If $HxK \cap HyK = \phi$, we have nothing to prove.

Let $HxK \cap HyK \neq \phi$. Let $z \in HxK \cap HyK$.

$\therefore$ $\exists\ h, h' \in H$ and $k, k' \in K$ such that $z = hxk = h'yk'$.

$\therefore$ $HzK = H(hxk)K = (Hh)\,x(kK) = HxK$

and $HzK = H(h'yk')K = (Hh')\,y(k'K) = HyK$

$\therefore$ $HxK = HyK$.

$\therefore$ The results holds.

Theorem 2. *Let H and K be two (not necessarily distinct) subgroups of a finite group G. For $x \in G$,*

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

Proof. Define $\phi : HxK \to x^{-1}HxK$ by

$$\phi(hxk) = x^{-1}hxk \quad \forall\ h \in H, k \in K.$$

ϕ is well defined. Let $hxk, h'xk' \in HxK$.

$$hxk = h'xk' \quad \Rightarrow \quad x^{-1}hxk = x^{-1}h'xk' \quad \Rightarrow \quad \phi(hxk) = \phi(h'xk')$$

$\therefore$ ϕ is well defined.

ϕ is one-one. Let $hxk, h'xk' \in HxK$.

$$\phi(hxk) = \phi(h'xk') \Rightarrow x^{-1}hxk = x^{-1}h'xk' \Rightarrow x(x^{-1}hxk) = x(x^{-1}h'xk') \Rightarrow hxk = h'xk'$$

$\therefore$ ϕ is one-one.

ϕ is onto. Let $x^{-1}hxk \in x^{-1}HxK$.

$\therefore$ $hxk \in HxK$ and $\phi(hxk) = x^{-1}hxk$. $\therefore$ ϕ is onto.

$\therefore$ There is one-to-one correspondence between the elements of finite sets HxK and $x^{-1}HxK$.

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

$\Rightarrow$ $o(HxK) = o((x^{-1}Hx)K) = \dfrac{o(x^{-1}Hx)\,o(K)}{o((x^{-1}Hx) \cap K)}$ ($\because$ $x^{-1}Hx$ is a subgroup of G)

$\therefore$ $\mathbf{o(HxK) = \dfrac{o(H)o(K)}{o((x^{-1}Hx) \cap K)}}$. ($\because$ $o(x^{-1}Hx) = o(H)$)

This completes the proof.

Theorem 3. (Frobenius). *If H and K be two (not necessarily distinct) subgroups of a finite group G then*

$$o(G) = \sum \frac{o(H)\,o(K)}{o((x^{-1}Hx) \cap K)},$$

where the summation on the right side is taken over elements x chosen one from each disjoint double coset HxK.

Proof. $x \in G \Rightarrow x\ (= exe) \in HxK \Rightarrow x \in \bigcup_{x \in G} HxK \Rightarrow G \subseteq \bigcup_{x \in G} HxK$

---

*If H and K are subgroups of a finite group G, then

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

Also, for $x \in G$, $HxK \subseteq G$. $\therefore \bigcup_{x \in G} HxK \subseteq G$

$$\therefore \quad G = \bigcup_{x \in G} HxK$$

Writing disjoint union, we have $o(G) = \sum o(HxK)$.

$$\Rightarrow \quad o(G) = \sum \frac{o(H)\, o(K)}{o((x^{-1}Hx) \cap K)},$$

where the summation on the right side is taken over elements x chosen one from each disjoint double coset HxK.

10. SYLOW'S SECOND THEOREM

Statement. *Let G be a finite group of order $p^k q$, where p is prime, $k, q \in N$ and $(p, q) = 1$. Then any two subgroups of order p^k are conjugate.* (K.U. 2005)

Proof. We have $o(G) = p^k q$, where $k, q \in N$ and $(p, q) = 1$.

By *Sylow's first theorem*, there exists subgroups of orders $p, p^2, \ldots\ldots, p^k$. Let A and B be any two subgroups of G of order p^k each. Since $p^k / o(G)$ and $p^{k+1} \nmid o(G)$, A and B are Sylow p-subgroups of G. We shall prove that the subgroups A and B are conjugate. If possible let the subgroups A and B be not conjugate *i.e.*, $B \neq x^{-1}Ax \ \forall\, x \in G$. We decompose G into double cosets of A and B.

$$\therefore \quad G = \cup (AxB)$$

where double cosets on the right are all mutually disjoint.

$$\therefore \quad o(G) = \sum o(AxB) \qquad \ldots(1)$$

where double cosets on the right are all mutually disjoint.

Now $$o(AxB) = \frac{o(A)\, o(B)}{o((x^{-1}Ax) \cap B)} \qquad \ldots(2)$$

Since $x^{-1}Ax \neq B \quad \forall\, x \in G$, we have $(x^{-1}Ax) \cap B \subset B \quad \forall\, x \in G$.

$\therefore$ $o((x^{-1}Ax) \cap B) < o(B)$, which is p^k.

Also, $(x^{-1}Ax) \cap B$ is a subgroup of B, so by *Lagrange's theorem* let $o((x^{-1}Ax) \cap B) = p^i$ for some $i < k$.

$$\therefore \quad (2) \quad \Rightarrow \quad o(AxB) = \frac{p^k \cdot p^k}{p^i} = p^{2k-i} = p^{k+1} p^{k-i-1}$$

$$\Rightarrow \quad p^{k+1} / o(AxB) \quad \forall\, x \in G \qquad (i < k \ \Rightarrow \ k - i > 0 \ \Rightarrow \ k - i - 1 \geq 0)$$

$\therefore$ Using (1), we have $p^{k+1} / o(G)$.

This is impossible, because $p^{k+1} \nmid o(G)$.

$\therefore$ Our supposition is wrong.

$\therefore$ There exists at least one $x \in G$ such that $B = x^{-1} Ax$.

$\therefore$ The Sylow p-subgroups A and B are conjugate. This completes the proof.

Example 13. *If S is a Sylow p-subgroup of a finite group G then the number of Sylow p-subgroups of G is equal to* $\dfrac{o(G)}{o(N(S))}$.

Sol. Let C(S) denote the equivalence class of S with respect to the conjugacy relation '~' defined on the set of subgroups of G.

$\therefore$ $C(S) = \{T : T \text{ is subgroup of } G \text{ and } T \sim S\}$

$= \{T : T \text{ is subgroup of } G \text{ and } T = x^{-1}Sx \text{ for some } x \in G\}$

$= \{x^{-1} Sx : x \in G\}$

= set of all conjugate subgroups of S

Since order of conjugate subgroups of a finite group are equal, each conjugate subgroup of S is a Sylow p-subgroup of G. Also, by **Sylow's second theorem,** the Sylow p-subgroups of a finite group are conjugate.

$\therefore$ C(S) contains all Sylow p-subgroups of G and nothing else.

$\therefore$ No. of Sylow p-subgroups of $G = o(C(S))$

$$= \frac{o(G)}{o(N(S))}. \qquad \left(\because o(C(S)) = \frac{o(G)}{o(N(S))}\right)$$

11. SYLOW'S THIRD THEOREM

Statement. *Let G be a finite group of order $p^k q$, where p is prime, $k, q \in N$ and $(p, q) = 1$. Then the number of subgroups of order p^k is of the form $1 + mp$, where m is some non-negative integer and also $(1 + mp)/o(G)$.* (M.D.U. 2005)

Proof. We have $o(G) = p^k q$, where $k, q \in N$ and $(p, q) = 1$.

By *Sylow's first theorem,* there exists subgroups of orders $p, p^2, \ldots\ldots, p^k$.

$\therefore$ There is at least one subgroup of order p^k.

Let P be a subgroup of G of order p^k.

Since $p^k / o(G)$ and $p^{k+1} \nmid o(G)$, P is a Sylow p-subgroup of G.

We decompose G into double cosets of P and P.

$\therefore$ $$G = \bigcup PxP,$$

where double cosets on the right are all mutually disjoint.

$\Rightarrow$ $$o(G) = \Sigma\, o(PxP) \qquad \ldots(1)$$

The element x involved in a double coset PxP in (1) may or may not be in N(P).

$\therefore$ (1) $\Rightarrow$ $$o(G) = \sum_{x \in N(P)} o(PxP) + \sum_{x \in N(P)} o(PxP) \qquad \ldots(2)$$

Case I. $x \in N(P)$. In this case, $x^{-1}Px = P$.

$\Rightarrow$ $x(x^{-1}Px) = xP \Rightarrow Px = xP \Rightarrow P(Px) = PxP \Rightarrow Px = PxP$ *i.e.,* $PxP = Px$

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

Now we shall show that $\sum_{x \in N(P)} o(Px) = o(N(P))$.

Let $$y \in \bigcup_{x \in N(P)} Px.$$

$\therefore$ There exists $p \in P$ and $z \in N(P)$ such that $y = pz$.

Now $$y^{-1}Py = (pz)^{-1} P(pz) = z^{-1}(p^{-1}Pp)z = z^{-1}Pz = P$$

$(\because \quad z \in N(P) \quad \Rightarrow \quad z^{-1}Pz = P)$

$\therefore$ $y \in N(P)$ $\therefore$ $$\bigcup_{x \in N(P)} Px \subseteq N(P)$$

Also, $$y \in N(P) \Rightarrow y(= ey) \in Py \Rightarrow y \in \bigcup_{x \in N(P)} Px$$

$$\therefore \quad N(P) \subseteq \bigcup_{x \in N(P)} Px$$

Combining, we get $\bigcup_{x \in N(P)} Px = N(P)$.

$$\therefore \quad \sum_{x \in N(P)} o(Px) = o(N(P))$$

Using (3), we have $\sum_{x \in N(P)} o(PxP) = o(N(P))$.

Case II. $x \notin N(P)$.

We have $$o(PxP) = \frac{o(P)o(P)}{o\left((x^{-1}Px) \cap P\right)} \qquad ...(4)$$

$x \notin N(P) \Rightarrow x^{-1}Px \neq P \Rightarrow (x^{-1}Px) \cap P \subset P \Rightarrow o((x^{-1}Px) \cap P) < o(P)$, which is p^k

Also, $(x^{-1}Px) \cap P$ is a subgroup of P, so by **Lagrange's theorem**, let $o((x^{-1}Px) \cap P) = p^i$ for some $i < k$.

$$\therefore \quad (4) \Rightarrow \quad o(PxP) = \frac{p^k \cdot p^k}{p^i} = p^{2k-i} = p^{k+1}p^{k-i-1}$$

$$\Rightarrow \quad p^{k+1} / o(PxP) \quad \forall \quad x \notin N(P) \qquad (\because \quad i < k \Rightarrow k - i > 0 \Rightarrow k - i - 1 \geq 0)$$

$$\Rightarrow \quad p^{k+1} \Big/ \sum_{x \in N(P)} o(PxP)$$

Let $\sum_{x \in N(P)} o(PxP) = \lambda p^{k+1}$, where λ is some non-negative integer.

$$\therefore \quad (2) \Rightarrow \quad o(G) = o(N(P)) + \lambda p^{k+1} \qquad ...(5)$$

Dividing by $o(N(P))$, we get

$$\frac{o(G)}{o(N(P))} = 1 + \frac{\lambda p^{k+1}}{o(N(P))} \qquad ...(6)$$

Since N(P) is a subgroup of G, we have $o(N(P)) / o(G)$.

$\therefore$ $\dfrac{o(G)}{o(N(P))}$ is a positive integer.

$\therefore$ By (6), $1 + \dfrac{\lambda p^{k+1}}{o(N(P))}$ is a positive integer.

$\Rightarrow$ $\dfrac{\lambda p^{k+1}}{o(N(P))}$ is a non-negative integer.

Since N(P) is a subgroup of G and $p^{k+1} \nmid o(G)$, we have $p^{k+1} \nmid o(N(P))$

$\therefore$ $\dfrac{\lambda p^{k+1}}{o(N(P))}$ is a multiple of p, say mp, where m is some non-negative integer.

$$\therefore \quad (6) \Rightarrow \quad \frac{o(G)}{o(N(P))} = 1 + mp \qquad ...(7)$$

$$\Rightarrow \quad o(C(P)) = 1 + mp$$

$\therefore$ Number of conjugates of P in G = $1 + mp$

Since P is a Sylow p-subgroup and each conjugate of P is a Sylow p-subgroup of G, the number of Sylow p-subgroups of G is $1 + mp$.

Also, (7) $\Rightarrow$ $\dfrac{o(G)}{1+mp} = o(N(P))$, a positive integer.

$\therefore$ $(1 + mp) / o(G)$. This completes the proof.

Illustration : Let $G = S_3$. Here $o(G) = 6 = 2.3$. The number 2 is prime and $2 / o(G)$ and $(2)^2 \nmid o(G)$. Also $1 + 2m$ divides 6 for $m = 0, 1$.

$$m = 0 \Rightarrow 1 + 2m = 1 \quad \text{and} \quad m = 1 \Rightarrow 1 + 2m = 3.$$

$\therefore$ There are either one or three Sylow 2-subgroups.

S_3 has three Sylow 2-subgroups, namely {I, (12)}, {I, (13)}, {I, (23)}.

Also, 3 is a prime number and $3 / o(G)$ and $(3)^2 \nmid o(G)$ and $1 + 3m$ divides 6 for $m = 0$

$$m = 0 \Rightarrow 1 + 3m = 1$$

$\therefore$ There is only one Sylow 3-subgroup of G, namely {I, (123), (132)}.

Example 14. *Find the possible number of Sylow 11-subgroups, Sylow 7-subgroups, and Sylow 5-subgroups in a group of order $5^2 . 7 . 11$.*

Sol. Let G be a group of order $5^2 . 7 . 11$.

Sylow 11-subgroups. We have $o(G) = 5^2 . 7 . 11 = 11^1 . 175$.

Here 11 is prime and $(11, 175) = 1$.

By *Sylow's first theorem,* G has a subgroup of order 11. Since $11 / o(G)$ and $11^2 \nmid o(G)$, this subgroup is a sylow 11-subgroup of G.

By *Sylow's third theorem,* the number of Sylow 11-subgroups is of the form $1 + 11\,m$, where $(1 + 11\,m) / o(G)$. Since $1 + 11\,m$ being prime to 11, $1 + 11\,m$ must divide 175.

This is true only for $m = 0$.

$$m = 0 \Rightarrow 1 + 11\,m = 1 + 11(0) = 1$$

$\therefore$ There is only one Sylow 11-subgroup of G.

Sylow 7-subgroups. We have $o(G) = 5^2 . 7 . 11 = 7 . 275$.

Here 7 is prime and $(7, 275) = 1$.

By *Sylow's first theorem,* G has a subgroup of order 7. Since $7 / o(G)$ and $7^2 \nmid o(G)$, this subgroup is a Sylow 7-subgroup of G.

By *Sylow's third theorem,* the number of Sylow 7-subgroups is of the form $1 + 7m$, where $(1 + 7m) / o(G)$. Since $1 + 7m$ being prime to 7, $1 + 7m$ must divide 275.

This is true only for $m = 0$.

$$m = 0 \Rightarrow 1 + 7m = 1 + 7(0) = 1$$

$\therefore$ There is only one Sylow 7-subgroup of G.

Sylow 5-subgroups. We have $o(G) = 5^2 . 7 . 11 = 5^2 . 77$.

Here 5 is prime and $(5, 77) = 1$.

By *Sylow's first theorem,* G has a subgroup of order 5^2 *i.e.,* 25.

Since $5^2 / o(G)$ and $5^3 \nmid o(G)$, this subgroup is a Sylow 5-subgroup of G.

By *Sylow's third theorem,* the number of Sylow 5-subgroups is of the form $1 + 5\,m$, where $(1 + 5\,m) / o(G)$. Since $1 + 5\,m$ being prime to 5 and hence to 5^2, $1 + 5\,m$ must divide 77.

This is true only for $m = 0, 2$.

$$m = 0 \Rightarrow 1 + 5\,m = 1 + 5(0) = 1$$

$$m = 2 \Rightarrow 1 + 5\,m = 1 + 5(2) = 11$$

$\therefore$ The group has either one or eleven Sylow 5-subgroups of G.

Example 15. *Show that a group of order 28 is not simple.*

Sol. Let G be a group of order 28.

$\therefore \quad o(G) = 28 = 7^1 \cdot 4$

Here 7 is prime and (7, 4) = 1.

By *Sylow's first theorem,* G has a subgroup H of order 7. Since $7 / o(G)$ and $7^2 \nmid o(G)$, the subgroup H is a Sylow 7-subgroup of G.

By *Sylow's third theorem,* the number of Sylow 7-subgroups is of the form $1 + 7m$, where $(1 + 7m) / o(G)$. Since $1 + 7m$ being prime to 7, $1 + 7m$ must divide 4.

This is true only for $m = 0$.

$\therefore$ There is only one Sylow 7-subgroup of G. Since there is only one Sylow 7-subgroup of G, it must be normal. ($\because \quad 1 + 7(0) = 1$)

$\therefore$ G has a proper normal subgroup. ($\because \quad o(H) = 7$)

$\therefore$ G is not simple.

Example 16. *Show that a group of order 40 is not simple.* (K.U. 2005)

Sol. Let G be a group of order 40.

$\therefore \quad o(G) = 40 = 5^1 \cdot 8$

Here 5 is prime and (5, 8) = 1.

By *Sylow's first theorem,* G has a subgroup of order 5. Since $5 / o(G)$ and $5^2 \nmid o(G)$, this subgroup is a Sylow 5-subgroup of G.

By *Sylow's third theorem,* the number of Sylow 5-subgroups is of the form $1 + 5m$, where $(1 + 5m) / o(G)$. Since $1 + 5m$ being prime to 5, $1 + 5m$ must divide 8.

This is true only for $m = 0$. ($\because \quad 1 + 5(0) = 1$)

$\therefore$ There is only one Sylow 5-subgroup. Since there is only one Sylow 5-subgroup of G, it must be normal.

$\therefore$ G has a proper normal subgroup.

$\therefore$ G is not simple.

Example 17. *Show that a group of order 20449 has a normal Sylow 11-subgroup and hence not simple.*

Sol. Let G be a group of order 20449.

$\therefore \quad o(G) = 20449 = 11 \times 1859 = 11 \times 11 \times 169 = 11^2 \cdot 169$

Here 11 is prime and (11, 169) = 1.

By *Sylow's first theorem,* G has a subgroup H of order 11^2 *i.e.,* 121.

Since $11^2 / o(G)$ and $11^3 \nmid o(G)$, the subgroup H is a Sylow 11-subgroup of G.

By *Sylow's third theorem,* the number of Sylow 11-subgroups is of the form $1 + 11m$, where $(1 + 11m) / o(G)$. Since $1 + 11m$ being prime to 11 and hence to 11^2, $1 + 11m$ must divide 169.

This is true only for $m = 0$.

$\therefore$ There is only one Sylow 11-subgroup of G. Since there is only one Sylow 11-subgroup of G, it must be normal . ($\because \quad 1 + 11(0) = 1$)

$\therefore$ G has a proper normal subgroup. ($\because \quad o(H) = 121$)

$\therefore$ G is not simple.

Example 18. *Show that a group of order 56 is not simple.*

Sol. Let G be a group of order 56.

$\therefore \quad o(G) = 2^3 \cdot 7$

Here 2 is prime and (2, 7) = 1.

By *Sylow's first theorem,* G has a subgroup of order 2^3. Since $2^3 / o(G)$ and $2^4 \nmid o(G)$, this subgroup is a Sylow 2-subgroup of G.

By *Sylow's third theorem,* the number of Sylow 2-subgroups is of the form $1 + 2m$, where $(1 + 2m) / o(G)$. Since $1 + 2m$ being prime to 2 and hence to 2^3, it must divide 7. This is true only for $m = 0, 3$.

$$m = 0 \Rightarrow 1 + 2m = 1, \; m = 3 \Rightarrow 1 + 2m = 7.$$

$\therefore$ There are either 1 or 7 Sylow 2-subgroups of G.

Also, $o(G) = 7^1 \cdot 8$

Here 7 is prime and (7, 8) = 1.

By *Sylow's first theorem,* G has a subgroup of order 7. Since $7 / o(G)$ and $7^2 \nmid o(G)$, this subgroup is a Sylow 7-subgroup of G.

By *Sylow's third theorem,* the number of Sylow 7-subgroup is of the form $1 + 7m$ where $(1 + 7m) / o(G)$. Since $1 + 7m$ being prime to 7, it must divide 8.

This is true only for $m = 0, 1$.

$$m = 0 \Rightarrow 1 + 7m = 1, \; m = 1 \Rightarrow 1 + 7m = 8$$

$\therefore$ There are either 1 or 8 Sylow 7-subgroups of G.

Let n_p denote the number of Sylow p-subgroups. We have four possibilities.

Case I. $n_2 = 1, n_7 = 1$

In this case, we have normal subgroups of order 8 and 7.

$\therefore$ G is not simple.

Case II. $n_2 = 1, n_7 = 8$

In this case, we have a normal subgroup of order 8.

$\therefore$ G is not simple.

Case III. $n_2 = 7, n_7 = 1$

In this case, we have a normal subgroup of order 7.

$\therefore$ G is not simple.

Case IV. $n_2 = 7, n_7 = 8$

$n_7 = 8$ implies that there are 8 distinct Sylow 7-subgroups of G, say, $H_1, H_2, \ldots\ldots, H_8$.

Now $\quad H_i \cap H_j \subseteq H_i, \; 1 \le i, j \le 8$

$\therefore$ $H_i \cap H_j$ is a subgroup of H_i.

$\therefore \quad o(H_i \cap H_j) / o(H_i)$ *i.e.*, $7 \quad \therefore \quad o(H_i \cap H_j) = 1$ or 7

$H_i \neq H_j \Rightarrow H_i \cap H_j \neq H_i$

$\therefore \quad o(H_i \cap H_j) = 1$ *i.e.*, $H_i \cap H_j = \{e\}$.

Also $\quad a(\neq e) \in H_i \Rightarrow a^7 = e$

$\therefore \quad o(a) = 7 \quad \forall \, a(\neq e) \in H_i \qquad (\because \; 7$ is prime)

$\therefore$ There are $8 \times (7 - 1) = 48$ non-identity elements of order 7. Since $56 - 48 = 8$, the remaining 8 elements can form at most one Sylow 2-subgroup of order 8. $\therefore \quad n_2 \neq 7$.

$\therefore$ This case is impossible.

$\therefore$ The group G is not simple.

Example 19. *If a group G is of order 28 has a normal subgroup of order 4, show that it is abelian.*

Sol. We have $o(G) = 28$.

$\therefore \quad o(G) = 7 \cdot 4$

Here 7 is prime and $(7, 4) = 1$.

By *Sylow's first theorem*, G has a subgroup H of order 7. Since $7 / o(G)$ and $7^2 \nmid o(G)$, H is a Sylow 7-subgroup of G.

By *Sylow's third theorem*, the number of Sylow 7-subgroups is of the form $1 + 7m$, where $(1 + 7m) / o(G)$. Since $1 + 7m$ being prime to 7, $1 + 7m$ must divide 4. This is true only for $m = 0$.

$$m = 0 \Rightarrow 1 + 7m = 1$$

$\therefore$ There is only one Sylow 7-subgroup of G. Since there is only one Sylow 7-subgroup of G, it must be normal.

Let K be a normal subgroup of G of order 4. Now $H \cap K \subset H$ and $o(H) = 7$.

$\therefore \quad o(H \cap K) / 7 \quad \therefore \quad o(H \cap K) = 1 \text{ or } 7$

$\therefore \quad o(H \cap K) = 1 \qquad (\because \quad (H \cap K) < o(H))$

Now $o(HK) = \dfrac{o(H) \cdot o(K)}{o(H \cap K)} = \dfrac{7 \times 4}{1} = 28.$

$\therefore \quad HK = G$

Since H, K are normal subgroups of G and $H \cap K = \{e\}$, we have $hk = kh \ \forall \ h \in H, k \in K$.

Let $g_1, g_2 \in G$.

$\therefore \ g_1 = h_1k_1, g_2 = h_2k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$.

$\therefore \quad g_1g_2 = (h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = h_1(h_2k_1)k_2 = (h_1h_2)(k_1k_2)$

H is abelian, because a group of prime order is cyclic and so abelian.

K is abelian, because $o(K) = p^2$, where $p = 2$.

$\therefore \quad g_1g_2 = (h_2h_1)(k_2k_1) = h_2(h_1k_2)k_1 = h_2(k_2h_1)k_1 = (h_2k_2)(h_1k_1) = g_1g_2.$

$\therefore$ G is abelian.

Example 20. *Show that there is no simple group of order 48.*

Sol. Let G be a group of order 48.

$\therefore \quad o(G) = 2^4 \cdot 3$

Here 2 is prime and $(2, 3) = 1$.

By *Sylow's first theorem*, G has a subgroup of order 2^4. Since $2^4 / o(G)$ and $2^5 \nmid o(G)$, this subgroup is a Sylow 2-subgroup of G.

By *Sylow's third theorem*, the number of Sylow 2-subgroups is of the form $1 + 2m$, where $(1 + 2m) / o(G)$. Since $1 + 2m$ being prime to 2 and hence to 2^4 *i.e.*, 16, it must divide 3.

This is true only for $m = 0, 1$.

$$m = 0 \Rightarrow 1 + 2m = 1, \ m = 1 \Rightarrow 1 + 2m = 3$$

$\therefore$ There are either 1 or 3 Sylow 2-subgroups of G.

Case I. $\mathbf{n_2 = 1}$

In this case, G has a normal subgroups of order 16.

$\therefore$ G is not simple.

Case II. $\mathbf{n_2 = 3}$

Let H and K be any two Sylow 2-subgroups of G.

$\therefore \quad o(H) = 16, o(K) = 16$

Now $\quad o(HK) = \dfrac{o(H) \cdot o(K)}{o(H \cap K)} = \dfrac{16 \times 16}{o(H \cap K)} = \dfrac{256}{o(H \cap K)}$

$$o(HK) \le 48 \quad \Rightarrow \quad \frac{256}{o(H \cap K)} \le 48 \quad \Rightarrow \quad o(H \cap K) \ge \frac{256}{48} \quad \Rightarrow \quad o(H \cap K) \ge 5\frac{1}{3}$$

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

$\therefore$ $o(H \cap K)/o(H)$ *i.e.*, 16

$\therefore$ $o(H \cap K) = 8$ or 16

$H \neq K \Rightarrow H \cap K \subset H$

$\Rightarrow$ $o(H \cap K) < o(H) \Rightarrow o(H \cap K) = 8$

Now index of $H \cap K$ in $H = \frac{o(H)}{o(H \cap K)} = \frac{16}{8} = 2$.

$\therefore$ $H \cap K$ is a normal in H. Similarly, $H \cap K$ is normal in K. Since $N(H \cap K)$ is the largest subgroup of G in which $H \cap K$ is normal, we have

$$H \subseteq N(H \cap K) \text{ and } K \subseteq N(H \cap K)$$

$\therefore$ $16/o(N(H \cap K))$, $o(N(H \cap K)) \subseteq 48$ and $o(N(H \cap K)/48$.

$\therefore$ $o(N(H \cap K)) = 16$

$\therefore$ $H \cap K = N(H \cap K)$ $(\because H \cap K \subseteq N(H \cap K))$

$\therefore$ $H \cap K$ is a normal subgroup of G because $N(H \cap K)$ is so. Since $H \cap K$ is a proper normal subgroup of G, the group G is not simple.

IMPORTANT RESULTS

1. **(Cauchy's theorem for abelian groups).** *Let G be a finite abelian group and $p/o(G)$, where p is a prime number. Then there exists an element $a (\neq e) \in G$ such that $a^p = e$.*
2. **(Cauchy's theorem).** *Let G be a finite group and $p/o(G)$, where p is a prime number. Then there exists an element $a(\neq e) \in G$ such that $a^p = e$.*
3. **(Sylow's first theorem).** *Let G be a finite group of order $p^k q$, where p is a prime, $k, q \in \mathbf{N}$ and $(p, q) = 1$. Then for each $i(1 \le i \le k)$, G has at least one subgroup of order p^i.*
4. *A finite group G is a p-group if and only if $o(G)$ is a power of p.*
5. *The conjugacy relation on the set of non-empty subsets of a group is an equivalence relation.*
6. *The conjugacy relation on the set of subgroups of a group is also an equivalence relation.*
7. *Let G be a group. For any non-empty subset S of G, the normalizer $N(S)$ of S is a subgroup of G.*
8. *If G is a finite group and $S(\neq \phi) \subseteq G$ then $o(C(S)) = \frac{o(G)}{o(N(S))}$.*
9. *Let H and K be two (not necessarily distinct) subgroups of a group G. For $x, y \in G$, the double cosets HxK and HyK are either disjoint or identical.*
10. *Let H and K be two (not necessarily distinct) subgroups of a finite group G.*

    For $x \in G$, $o(HxK) = \frac{o(H)\,o(K)}{o((x^{-1}Hx) \cap K)}$.
11. **(Frobenius).** *If H and K be two (not necessarily distinct) subgroups of a finite group G, then $o(G) = \sum \frac{o(H)\,o(K)}{o((x^{-1}Hx) \cap K)}$,*

    where the summation on the right side is taken over elements x chosen one from each disjoint double coset HxK.

12. **(Sylow's second theorem).** *Let G be a finite group of order $p^k q$, where p is a prime, $k, q \in \mathbf{N}$ and $(p, q) = 1$. Then any two subgroups of order p^k are conjugate.*

13. **(Sylow's third theorem).** *Let G be a finite group of order $p^k q$, where p is a prime, $k, q \in \mathbf{N}$ and $(p, q) = 1$. Then the number of subgroups of order p^k is of the form $1 + mp$, where m is some non-negative integer and also $(1 + mp) / o(G)$.*

EXERCISE 1

1. Show that a group of order 10 has a normal subgroup of order 5.
2. (*i*) Show that every abelian group of order 10 is cyclic.
   (*ii*) Show that every abelian group of order 15 is cyclic.
3. Let G be a finite group and K, a subgroup of G. If $S(\neq \phi) \subseteq G$, then show that the number of conjugates of S determined by the elements of K is equal to the index of $N_K(S)$ in K.
4. If a finite group has exactly one Sylow p-subgroup, then show that this subgroup is normal in G.
5. Let G be a finite group of order 45 and A and B be two subgroups of G of order 9 each. Show that there must exist an element $x \in G$ such that $A = x^{-1}Bx$.
6. (*i*) Show that the Sylow 13-subgroup in a group of order 130 is normal.
   (*ii*) Show that the Sylow 17-subgroup in a group of order 255 is normal.
7. Let $G = \{\pm 1, \pm i\}$. G is a group with usual multiplication as the binary operation. By using Sylow's theorems, show that there is only one subgroup of G of order 2 and this subgroup is also normal.
8. Show that a Sylow p-subgroup of a finite group is unique if and only if it is normal.
9. If $o(G) = 36$, show that G has either 1 or 4 Sylow 3-subgroups of G.
10. If $o(G) = 56$, show that G has either 1 or 8 Sylow 7-subgroups of G.
11. Discuss the number and nature of the Sylow 3-subgroups and Sylow 5-subgroups of a group of order 225.
12. Show that a group of order 30 is not simple.

12. CENTRALIZER OF A SET *(K.U. 2005)*

Let G be a group. For $S(\neq \phi) \subseteq G$, the set $\{x \in G : x^{-1}sx = s, \forall\, s \in S\}$ is called the **centralizer** of the non-empty subset S of G.

Theorem. *Let G be a group. For any non-empty subset S of G, the centralizer of S is a subgroup of G.* (K.U. 2005)

Proof. Let C be the centralizer of S in G.

$\therefore \quad C = \{x \in G : x^{-1}sx = s, \forall\, s \in S\}$

$e \in C$, because $e^{-1}se = ese = s \quad \forall\, s \in S$. $\therefore$ C is non-empty.

Let $x, y \in C$. $\therefore \quad x^{-1}sx = s, y^{-1}sy = s \quad \forall\, s \in S$

Now $\quad (xy)^{-1}s(xy) = (y^{-1}x^{-1})\, s(xy) = y^{-1}(x^{-1}sx)y = y^{-1}sy = s$

$\therefore \quad (xy)^{-1}s(xy) = s \quad \forall\, s \in S \quad \therefore \quad xy \in C$

Let $\quad x \in C. \quad \therefore \quad x^{-1}sx = s \quad \forall\, s \in S$

$\Rightarrow \quad x(x^{-1}sx)x^{-1} = xsx^{-1} \quad \Rightarrow \quad (xx^{-1})s(xx^{-1}) = xsx^{-1}$

$\Rightarrow \quad ese = xsx^{-1} \quad \Rightarrow \quad xsx^{-1} = s \quad \Rightarrow \quad (x^{-1})^{-1}s(x^{-1}) = s$

$\therefore \quad (x^{-1})^{-1}s(x^{-1}) = s \quad \forall\, s \in S \quad \therefore \quad x^{-1} \in C$

$\therefore$ C is a subgroup of G.

■ **EXAMPLE 1** Consider the Sylow 2-subgroups of S_3. They are $\{(1), (12)\}$, $\{(1), (23)\}$, and $\{(1), (13)\}$. According to Sylow's Third Theorem, we should be able to obtain the latter two of these from the first by conjugation. Indeed,

$$(13)\{(1), (12)\}(13)^{-1} = \{(1), (23)\},$$
$$(23)\{(1), (12)\}(23)^{-1} = \{(1), (13)\}.$$ ■

■ **EXAMPLE 2** Consider the Sylow 3-subgroups of A_4. They are $\{\alpha_1, \alpha_5, \alpha_9\}$, $\{\alpha_1, \alpha_6, \alpha_{11}\}$, $\{\alpha_1, \alpha_7, \alpha_{12}\}$, and $\{\alpha_1, \alpha_8, \alpha_{10}\}$. (See Table 5.1.) Then,

$$\alpha_2\{\alpha_1, \alpha_5, \alpha_9\}\alpha_2^{-1} = \{\alpha_1, \alpha_7, \alpha_{12}\},$$
$$\alpha_3\{\alpha_1, \alpha_5, \alpha_9\}\alpha_3^{-1} = \{\alpha_1, \alpha_8, \alpha_{10}\},$$
$$\alpha_4\{\alpha_1, \alpha_5, \alpha_9\}\alpha_4^{-1} = \{\alpha_1, \alpha_6, \alpha_{11}\}.$$

Thus, the number of Sylow 3-subgroups is 1 modulo 3, and the four Sylow 3-subgroups are conjugate. ■

■ **EXAMPLE 3** Say G is a group of order 40. What do the Sylow theorems tell us about G? A great deal! Since 1 is the only divisor of 40 that is congruent to 1 modulo 5, we know that G has exactly one subgroup of order 5, and therefore it is normal. Similarly, G has either one or five subgroups of order 8. If there is only one subgroup of order 8, it is normal. If there are five subgroups of order 8, none is normal and all five can be obtained by starting with any particular one, say H, and computing xHx^{-1} for various x's. Finally, if we let K denote the normal subgroup of order 5 and let H denote any subgroup of order 8, then $G = HK$. (See Example 5 in Chapter 9.) If H happens to be normal, we can say even more: $G = H \times K$. ■

■ **EXAMPLE 4** Consider a group of order 30. By Sylow's Third Theorem, it must have either one or six subgroups of order 5 and one or 10 subgroups of order 3. However, G cannot have both six subgroups of order 5 *and* 10 subgroups of order 3 (for then G would have more than 30 elements). Thus, the subgroup of order 3 is unique or the subgroup of order 5 is unique (or both are unique) and therefore is normal in G. It follows, then, that the product of a subgroup of order 3 and one of order 5 is a group of order 15 that is both cyclic (Exercise 33) and normal (Exercise 9 in Chapter 9) in G. [This, in turn, implies that *both* the subgroup of order 3 and the subgroup of order 5 are normal in G (Exercise 59 in Chapter 9).] So, if we let y be a generator of the cyclic subgroup of order 15 and let x be an element of order 2 (the existence of which is guaranteed by Cauchy's Theorem), we see that

$$G = \{x^i y^j \mid 0 \leq i \leq 1, 0 \leq j \leq 14\}.$$ ■

■ **EXAMPLE 5** We show that any group G of order 72 must have a proper, nontrivial normal subgroup. Our arguments are a preview of those in Chapter 25. By Sylow's Third Theorem, the number of Sylow 3-subgroups of G is equal to 1 mod 3 and divides 8. Thus, the number is 1 or 4. If there is only one, then it is normal by the corollary of Sylow's Third Theorem. Otherwise, let H and H' be two distinct Sylow 3-subgroups. By Theorem 7.2, we have that $|HH'| = |H||H'|/|H \cap H'| = 81/|H \cap H'|$. Since $|G| = 72$ and $|H \cap H'|$ is a subgroup of H and H', we know that $|H \cap H'| = 3$. By the corollary to Theorem 24.2, $N(H \cap H')$ contains both H and H'. Thus, $|N(H \cap H')|$ divides 72, is divisible by 9, and has at least $|HH'|' = 27$ elements. This leaves only 36 or 72 for $|N(H \cap H')|$. In the first case, we have from Exercise 9 of Chapter 9 that $N(H \cap H')$ is normal in G. In the second case, we have by definition that $H \cap H'$ is normal in G. ■

If G is a group of order pq, where p and q are primes, $p < q$, and p does not divide $q - 1$, then G is cyclic. In particular, G is isomorphic to Z_{pq}.

Let H be a Sylow p-subgroup of G and let K be a Sylow q-subgroup of G. Sylow's Third Theorem states that the number of Sylow p-subgroups of G is of the form $1 + kp$ and divides pq. So $1 + kp = 1$, p, q, or pq. From this and the fact that $p \nmid q - 1$, it follows that $k = 0$, and therefore H is the only Sylow p-subgroup of G.

Similarly, there is only one Sylow q-subgroup of G. Thus, by the corollary to Theorem 24.5, H and K are normal subgroups of G. Let $H = \langle x \rangle$ and $K = \langle y \rangle$. To show that G is cyclic, it suffices to show that x and y commute, for then $|xy| = |x||y| = pq$. But observe that, since H and K are normal, we have

$$xyx^{-1}y^{-1} = (xyx^{-1})y^{-1} \in Ky^{-1} = K$$

and

$$xyx^{-1}y^{-1} = x(yx^{-1}y^{-1}) \in xH = H.$$

Thus, $xyx^{-1}y^{-1} \in K \cap H = \{e\}$, and hence $xy = yx$.

■ EXAMPLE 6 Determination of the Groups of Order 99

Suppose that G is a group of order 99. Let H be a Sylow 3-subgroup of G and let K be a Sylow 11-subgroup of G. Since 1 is the only positive divisor of 99 that is equal to 1 modulo 11, we know from Sylow's Third Theorem and its corollary that K is normal in G. Similarly, H is normal in G. It follows, by the argument used in the proof of Theorem 24.6, that elements from H and K commute, and therefore $G = H \times K$. Since both H and K are Abelian, G is also Abelian. Thus, G is isomorphic to Z_{99} or $Z_3 \oplus Z_{33}$. ■

▮ EXAMPLE 7 Determination of the Groups of Order 66

Suppose that G is a group of order 66. Let H be a Sylow 3-subgroup of G and let K be a Sylow 11-subgroup of G. Since 1 is the only positive divisor of 66 that is equal to 1 modulo 11, we know that K is normal in G. Thus, HK is a subgroup of G of order 33 (see Example 5 in Chapter 9 and Theorem 7.2). Since any group of order 33 is cyclic (Theorem 24.6), we may write $HK = \langle x \rangle$. Next, let $y \in G$ and $|y| = 2$. Since $\langle x \rangle$ has index 2 in G, we know it is normal. So $yxy^{-1} = x^i$ for some i from 1 to 32. Then, $yx = x^i y$ and, since every member of G is of the form $x^s y^t$, the structure of G is completely determined by the value of i. We claim that there are only four possibilities for i. To prove this, observe that $|x^i| = |x|$ (Exercise 5, Supplementary Exercises for Chapters 1–4). Thus, i and 33 are relatively prime. But also, since y has order 2,

$$x = y^{-1}(yxy^{-1})y = y^{-1}x^i y = yx^i y^{-1} = (yxy^{-1})^i = (x^i)^i = x^{i^2}.$$

So $x^{i^2-1} = e$ and therefore 33 divides $i^2 - 1$. From this it follows that 11 divides $i \pm 1$, and therefore $i = 0 \pm 1$, $i = 11 \pm 1$, $i = 22 \pm 1$, or $i = 33 \pm 1$. Putting this together with the other information we have about i, we see that $i = 1$, 10, 23, or 32. This proves that there are at most four groups of order 66.

To prove that there are exactly four such groups, we simply observe that Z_{66}, D_{33}, $D_{11} \oplus Z_3$, and $D_3 \oplus Z_{11}$ each has order 66 and that no two are isomorphic. For example, $D_{11} \oplus Z_3$ has 11 elements of order 2, whereas $D_3 \oplus Z_{11}$ has only three elements of order 2. (See Exercises 27–30 of the Supplementary Exercises for Chapters 5–8.) ▮

▮ EXAMPLE 8 The Only Group of Order 255 is Z_{255}

Let G be a group of order $255 = 3 \cdot 5 \cdot 17$, and let H be a Sylow 17-subgroup of G. By Sylow's Third Theorem, H is the only Sylow 17-subgroup of G, so $N(H) = G$. By Example 15 in Chapter 10, $|N(H)/C(H)|$ divides $|\text{Aut}(H)| = |\text{Aut}(Z_{17})|$. By Theorem 6.5, $|\text{Aut}(Z_{17})| = |U(17)| = 16$. Since $|N(H)/C(H)|$ must divide 255 and 16, we have $|N(H)/C(H)| = 1$. Thus, $C(H) = G$. This means that every element of G commutes with every element of H, and, therefore, $H \subseteq Z(G)$. Thus, 17 divides $|Z(G)|$, which in turn divides 255. So $|Z(G)|$ is equal to 17, 51, 85, or 255 and $|G/Z(G)|$ is equal to 15, 5, 3, or 1. But the only groups of order 15, 5, 3, or 1 are the cyclic ones, so we know that $G/Z(G)$ is cyclic. Now the G/Z Theorem (Theorem 9.3) shows that G is Abelian, and the Fundamental Theorem of Finite Abelian Groups tells us that G is cyclic. ▮