Subject : MATHEMATICS

Paper 1 : ABSTRACT ALGEBRA

Chapter 3 : Sylow Theorems

Module 4 : Applications of Sylow Theorems

Anjan Kumar Bhuniya
Department of Mathematics
Visva-Bharati; Santiniketan
West Bengal

Applications of Sylow Theorems

Learning Outcomes:	1. Characterization of simple groups of small order.
	2. A_5 is simple.
	3. Every simple group of order 60 is isomorphic to A_5.

The notion of simple group was introduced by Galois in his work on the insolvability of quintics. The simplicity of A_5 plays a crucial role in his proof that there are quintics which can not be solved by radicals. But simple groups are known as the El Dorado of finite group theory because of their role to study structure of finite groups. Their role in finite group theory is somewhat analogous to that of primes in number theory, that is, they are the basic building blocks for all groups. Theory of simple groups is vast and difficult. Here we consider only simple groups of small order.

The Cauchy's Theorem shows that no abelian group of composite order is simple. As a consequence of Cauchy's theorem we have no simple groups of order p^n, p is a prime and $n > 1$. Sylow theorems also help us to find possible orders of simple groups. Here we show that 60 is the smallest composite order of a noncommutative simple group and any noncommutative simple group of order 60 is isomorphic to A_5.

Recall the definition of simple group.

Definition 0.1. *A group $G \neq \{e\}$ is called simple if its only normal subgroups are the identity subgroup and the group itself.*

Example 0.2. *We show that no group of order 10 is simple.*

Let G be a group of order $10 = 5 \times 2$. Denote the number of Sylow 5-subgroups of G by n_5. Then $n_5 = 5k + 1$ for some integer $k \geq 0$ and $n_5|10$. It follows that $n_5 = 1$, that is, G has unique sylow 5-subgroup H of order 5. Hence H is normal in G, and so G is not simple.

Theorem 0.3. *No group of order pq, where p, q are prime integers, is simple.*

Proof. Let G be a group of order pq. If $p = q$, then $|G| = p^2$ implies that G is abelian. Also, by Cauchy's Theorem, G has an element a and hence a subgroup $H =< a >$ of order p. Since G is abelian, H is normal in G. Thus G is not simple.

Let $p > q$. Let n_p be the number of Sylolw p-subgroups of G. Then $n_p = kp + 1$ for some integer $k \geq 0$ and $n_p|pq$. Now gcd (n_p, p) = gcd $(kp + 1, p) = 1$ implies that $n_p|q$. Since $p > q$, so $n_p = kp + 1 \leq q$ holds only if $k = 0$, that is, $n_p = 1$. Thus G has unique Sylow p-subgroup H of order p, which is normal in G. Hence G is not simple. □

Example 0.4. *We show that no group of order* 30 *is simple.*

Let G *be a group of order* $30 = 5 \times 3 \times 2$. *Let* n_5 *denote the number of Sylow 5-subgroups of* G *and* n_3 *denote the number of Sylow 3-subgroups of* G. *If* $n_5 = 1$ *or* $n_3 = 1$ *then* G *has a normal subgroup of order* 5 *or* 3 *and* G *is not simple. If possible,* $n_5 \neq 1$ *and* $n_3 \neq 1$. *Now* $n_5 = 5k + 1$ *for some integer* $k \geq 0$ *and* $n_5|30$ *implies that* $n_5 = 6$*(since* $n_5 \neq 1$*). Similarly* $n_3 = 10$. *Let* $P_1, P_2, \cdots P_6$ *be the six Sylow 5-subgroups. Then* $|P_i| = 5$, *a prime implies that* $P_i \cap P_j = \{e\}$ *for all* $i \neq j$ *and their union contains* $6 \times 4 = 24$ *elements of order* 5. *Similarly the 10 Sylow 3-subgroups contain* $10 \times 2 = 20$ *elements of order* 3. *Thus* $|G| \geq 24 + 20 = 44$, *a contradiction. Thus* $n_5 = 1$ *or* $n_3 = 1$, *and* G *is not simple.*

In fact, every group of order 30 has normal subgroups of order 5 and 3.

Theorem 0.5. *Let* p *be a prime integer and* $n > 1$ *be an integer. Then no group of order* p^n *is simple.*

Proof. Let G be a group of order p^n. Then $|Z(G)| > 1$. If $G = Z(G)$ then G is abelian and so G can not be simple, since $n > 1$. Let $G \neq Z(G)$. Then $Z(G)$ becomes a nontrivial proper normal subgroup of G. Hence G is not simple. □

Example 0.6. *We show that no group of order* 40 *is simple.*

Let G *be a group of order* $40 = 5 \times 2^3$. *Denote the number of Sylow 5-subgroups of* G *by* n_5. *Then* $n_5 = 5k + 1$ *for some integer* $k \geq 0$ *and* $n_5|40$. *It follows that* $n_5 = 1$. *Thus* G *has unique Sylow 5-subgroup* H *of order* 5, *which is normal in* G. *Hence* G *is not simple.*

Example 0.7. *We show that no group of order* 96 *is simple.*

Let G *be a group of order* $96 = 2^5 \times 3$. *Denote the number of Sylow 2-subgroups by* n_2. *Then* $n_2 = 2k + 1$ *for some integer* $k \geq 0$ *and* $n_2|96$. *It follows that* $n_2 = 1$ *or* 3. *If* $n_2 = 1$, *then* G *has unique Sylow 2-subgroup* H *which is normal in* G. *Now, let* $n_2 = 3$ *and* A, B, C *be the three Sylow 2-subgroups of* G. *Then* $|AB| = \frac{|A||B|}{|A \cap B|}$ *implies that* $\frac{32 \times 32}{|A \cap B|} \leq 96$ *and hence* $|A \cap B| \geq 10$. *Also, by the Lagrange's theorem,* $|A \cap B|$ *divides* $|A| = 32$. *Thus* $|A \cap B| = 16$. *Since* $[A : A \cap B] = 2$ *and* $[B : A \cap B] = 2$, *so* $A \cap B$ *is normal in both* A *and* B, *which implies that* $A, B \subseteq N(A \cap B)$. *Thus* $AB \subseteq N(A \cap B)$. *Now* $|AB| = \frac{|A||B|}{|A \cap B|} = 64$ *implies that* $|N(A \cap B)| \geq 64$. *By the Lagrange's theorem,* $|N(A \cap B)|$ *divides 96. Therefore* $|N(A \cap B)| = 96$ *and* $N(A \cap B) = G$. *Hence* $A \cap B$ *is a normal subgroup of* G *of order* 16.

Example 0.8. *We show that no group of order* 56 *is simple.*

Let G *be a group of order* $56 = 7 \times 2^3$. *Let* n_7 *be the number of Sylow 7-subgroups of* G. *Then* $n_7 = 7k + 1$ *for some integer* $k \geq 0$ *and* $n_7|56$. *Hence* $n_7 = 1$ *or* 8. *If* $n_7 = 1$, *then* G *has unique Sylow 7-subgroup of order* 7, *which is normal in* G. *Thus* G *is not simple. Let* $n_7 = 8$ *and* $P_1, P_2, \cdots, P_8$ *be the* 8 *Sylow 7-subgroups in* G. *Since* P_i *are distinct and* $|P_i| = 7$, $P_i \cap P_j = \{e\}$ *for*

$i \neq j$. Every nonidentity element of P_i is of order 7 and so G has $8 \times 6 = 48$ elements of order 7. If we denote the number Sylow 2-subgroups of G by n_2, then similarly, it follows that $n_2 = 1$ or 7. If $n_2 = 1$ then G has unique Sylow 2-subgroup of order 8, which is normal in G. Thus G is not simple. Let $n_2 = 7$ and $Q_1, Q_2, \cdots, Q_7$ be the 7 Sylow 2-subgroups. Since $Q_1 \neq Q_2$, $|Q_1 \cap Q_2| \leq 4$ and hence $Q_1 \cup Q_2$ contains at least $8+8-4 = 12$ elements of order $2, 4$ or 8. Thus we get $|G| \geq 48+12 = 60$, a contradiction. Hence either $n_7 = 1$ or $n_2 = 1$, ensuring that G has a nontrivial proper normal subgroup. Therefore G is not simple.

Now we recall the generalized Cayley theorem.

Theorem 0.9. *Let G be a group and H be a subgroup of G. If $S = \{aH | a \in G\}$, then there is a homomorphism $\varphi : G \longrightarrow A(S)$, the group of all permutations on S such that $ker\varphi \subseteq H$.*

Also recall that $\varphi : G \longrightarrow A(G)$ is defined by $\varphi(g) = \tau_g$ for all $g \in G$, where $\tau_g : S \longrightarrow S$ is given by $\tau_g(aH) = (ga)H$ for all $aH \in S$.

Now we have following two important consequences of the generalized Cayley Theorem.

Theorem 0.10. *(Index Theorem) Let G be a finite group. If G has a proper subgroup H such that $[G : H] = m$ and $|G| \nmid m!$, then G is not simple.*

Proof. Let $S = \{aH | a \in G\}$. Defined $\tau_g : S \longrightarrow S$ by $\tau_g(aH) = (ga)H$ for all $aH \in S$. Then $\tau_g \in A(S)$ and the mapping $\varphi : G \longrightarrow A(S)$ defined by $\varphi(g) = \tau_g$ for all $g \in G$, is a homomorphism such that $ker\varphi \subseteq H$, by the generalized Cayley theorem. From the first isomorphism theorem, $\frac{G}{ker\varphi} \cong \varphi(G)$, a subgroup of $A(S)$. Since $|A(S)| = m!$, so $|\frac{G}{ker\varphi}|$ divides $m!$. But $|G| \nmid m!$ implies that $|ker\varphi| > 1$. Thus $ker\varphi$ becomes a nontrivial proper normal subgroup of G, and G is not simple. □

Example 0.11. *We show that no group of order 12 is simple.*

Let G be a group of order $12 = 3 \times 2^2$. Let H be a Sylow 2-subgroup of G. Then $|G| = 2^2 = 4$ implies that $[G : H] = 3$. Since $12 \nmid 3!$, so G is not simple, by the index theorem.

Similarly we can show that no group of order 15, 21, 24, 28, 33 etc. is simple.

Theorem 0.12. *Every finite simple group having a subgroup of index n, is isomorphic to a subgroup of A_n.*

Proof. Let G be a finite simple group and H be a subgroup of G such that $[G : H] = n$. Denote $S = \{aH : a \in G\}$. Then $|S| = n$ which implies that $A(S) \cong S_n$. By the generalized Cayley theorem, there is a non-trivial homomorphism $\varphi : G \longrightarrow S_n$. Then $ker\varphi \neq G$. Since G is simple and $Ker\varphi$ is a normal subgroup of G so $ker\varphi = \{e\}$ and φ is one-to-one. Thus $G \cong \varphi(G)$, a subgroup of S_n. Then $\varphi(G)$ consists of only even permutations or half even and half odd. If $\varphi(G)$ is of later type then the set of all even permutations in $\varphi(G)$ becomes a subgroup of index 2 and so a normal subgroup of $\varphi(G)$. This contradicts that G is simple. Thus $\varphi(G) \subseteq A_n$ and G is isomorphic to a subgroup of A_n. □

If in the generalized Cayley theorem, we take $H = \{e\}$, then $S = \{\{a\} \mid a \in G\}$ and τ_g is actually a left translation of G. Thus we can take $\tau_g : G \longrightarrow G$ as:

$$\tau_g(a) = ga \text{ for all } a \in G,$$

and $\psi : G \longrightarrow A(G)$ is a monomorphism. Therefore, G is isomorphic to a subgroup of the permutation group on G. This is the Cayley Theorem.

Now we apply the Cayley Theorem to check simplicity of groups.

Theorem 0.13. *Let G be a group of order $2m$, where m is an odd integer. Then G has a subgroup of order m and hence G is not simple.*

Proof. We have, by the Cayley's theorem, that there is a monomorphism $\psi : G \longrightarrow A(G)$ given by:

$$\psi(g) = \tau_g \text{ for all } g \in G,$$

where $\tau_g : G \longrightarrow G$ is defined by: $\tau_g(x) = gx$ for all $x \in G$. Since G is of even order, it contains an element of order 2, say a. Now $\tau_a(x) = ax$ and $\tau_a(ax) = a^2x = x$ implies that the permutation τ_a is a product of the transpositions of the form $(x\ ax)$. It follows from the cancelation property of G that $x \neq ax$ for all $x \in G$. Since $|G| = 2m$, so τ_a is a product of such m transpositions; and hence τ_g is an odd permutation. Now define

$$f : \psi(G) \longrightarrow \{1, -1\}$$

by

$$f(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is an permutaion} \\ -1 & \text{if } \sigma \text{ is a odd permutation} \end{cases}$$

for all $\sigma \in \psi(G)$. Then f is a homomorphism. Since $\psi(G)$ contains both odd permutation (viz. τ_a) and even permutation (viz. the identity permutation), so f is an epimorphism. Hence, by the first isomorphism theorem,

$$\psi(G)/\ker f \simeq \{-1, 1\}.$$

Then $|\psi(G)/\ker f| = 2$ implies that $|G|/|\ker f| = 2$, that is, $2m/|\ker f| = 2$ and it follows that $|\ker f| = m$. Thus $\psi(G)$ contains a normal subgroup $\ker f$ of order m, and hence G contains a normal subgroup of order m. □

From this result it follows that no group of order 14, 18, 22 etc is simple.

Now recall that if G is a group of order pn where p is a prime and $p \geq n$, then G has a normal subgroup of order p. Thus no group of such order is simple. Hence no group of order 6, 10, 14, 15, 20, 21 etc. is simple.

From all the above results we have:

Theorem 0.14. *Let $1 \leq n < 60$ be an integer which is not prime. Then no group of order n is simple.*

Now we show that the alternating group A_5 is a simple group of order 60. We conclude this section with the characterization of all simple groups of order 60.

Theorem 0.15. *Let G be a group of order 60. If G has more that one Sylow 5-subgroup, then it is simple.*

Proof. Let $|G| = 60$ and G has more than one Sylow 5-subgroup. Now the number n_5 of Sylow 5-subgroups is of the form $5k+1$ for some integer $k \geq 0$ and $n_5 \mid 60$ implies that $n_5 = 6$, since $n_5 \neq 1$.

If possible, assume that G is not simple and H is a non-trivial proper normal subgroup of G.

If $5 \mid |G|$, then H contains a Sylow 5-subgroup P of G. Since H is normal in G, and every Sylow 5-subgroup of G is a conjugate of P, so H contains all 6 Sylow 5-subgroups of G. Total number of elements in these 6 Sylow 5-subgroups is $1 + 6 \times 4 = 25$ which implies that $|H| \geq 25$. Since $|H| \mid 60$ and H is proper, so $|H| = 30$, this contradicts that every group of order 30 has unique Sylow 5-subgroup. Thus $5 \nmid |H|$.

If $|H| = 6$ or 12, then H has a normal Sylow subgroup which is also normal in G. Thus, we may assume, by replacing H by its normal subgroup if necessary, that $|H| = 2, 3, 4$. Then $|G/H| = 30, 20$ ore 15 which implies that G/H has a normal subgroup K/H of order 5, where K is a normal subgroup of G. Now $|K| = |K/H| \cdot |H| = 5 \cdot |H|$ implies that $5 \mid |K|$ which contradicts the preceding paragraph. Thus G is simple. □

Corollary 0.16. *A_5 is simple.*

Proof. The subgroups $< (12345) >$ an $< (13245) >$ are distinct Sylow 5-subgroups of A_5 and so A_5 is simple. □

Lemma 0.17. *Every simple group of order 60 contains a subgroup of order 12.*

Proof. Let G be a group of order $60 = 5 \times 3 \times 2^2$. Since G is simple, it has more than one Sylow 5-subgroup. In fact G has exactly six Sylow 5-subgroups which contain $6 \times 4 = 24$ elements of order 5.

Denote the number of Sylow 2-subgroups of G by n_2. Then $n_2 = 2k+1$ for some integer $k \geq 0$ and $n_2 \mid 60$ implies that $n_2 = 1, 3, 5$ or 15.

Since G is simple $n_2 \neq 1$. Let $n_2 = 15$ and $B_1, B_2, \cdots, B_{15}$ be the 15 Sylow 2-subgroups of G. If $B_i \cap B_j = \{e\}$ for every $i \neq j$, then these 15 Sylow 2-subgroups contain $15 \times 3 = 45$ elements of order 2 or 4. Thus $|G| \geq 24 + 45$ which is a contradiction. Hence there are l, k such that $|B_l \cap B_k| = 2$. Then $B_l \cap B_k$ is normal in B_l as well as in B_k and so $B_l B_k \subseteq N(B_l \cap B_K)$. Since $|B_l B_k| = \frac{4 \times 4}{2} = 8$, it follows that $8 \leq |N(B_l \cap B_k)|$ which also divides 60. Also $|B_l| \mid |N(B_l \cap B_k)|$.

Thus $|N(B_l \cap B_k)| = 12, 20$ or 60. Since G is simple, $N(B_l \cap B_k)| \neq 60$ and by the index theorem, $N(B_l \cap B_k)| \neq 20$. Thus $N(B_l \cap B_k)$ is a subgroup of order 12.

Let $n_2 = 3$ or 5, and P be a Sylow 2-subgroup of G. Then $n_2 = [G : N(P)]$ implies that $|N(P)| \neq 4$. Since P is a subgroup of $N(P)$, so $4 \mid |N(P)|$. Also $|N(P)| \mid 60$. Thus $|N(P)| = 12, 20$ or 60. Similarly as above, we get $|N(P)| = 12$.

Thus G must have a subgroup of order 12. □

Theorem 0.18. *If G is a simple group of order 60, then $G \simeq A_5$.*

Proof. Let G be a simple group of order 60. Then G has a subgroup H of order 12. Hence, by the generalized Cayley theorem, there is a non-trivial homomorphism.

$$\psi : G \longrightarrow S_5.$$

Since G is simple, $ker\psi = \{e\}$ and ψ is one-to-one. Thus $G \simeq \psi(G)$. Then $\psi(G) \subseteq A_5$ or half of the elements of $\psi(G)$ even and half odd. In the later case the even permutation of $\psi(G)$ is a normal subgroup of $\psi(G)$ which contradicts that G is simple. Thus $\psi(G) \subseteq A_5$. Now $|\psi(G)| = |G| = 60 = |A_5|$ implies that $\psi(G) = A_5$. Hence $G \simeq A_5$. □

We also have the following generalization of the above result which we will not prove here. For a proof, we refer the readers to *Abstract Algebra* by Dummit and Foote.

Theorem 0.19. *For every $n \geq 5$, the group A_n is simple.*

1 Summary

- A group $G \neq \{e\}$ is called simple if its only normal subgroups are the identity subgroup and the group itself.
- No group of order pq, where p, q are prime integers, is simple.
- (Generalized Cayley theorem) Let G be a group and H be a subgroup of G. If $S = \{aH | a \in G\}$, then there is a homomorphism $\varphi : G \longrightarrow A(S)$, the group of all permutations on S such that $ker\varphi \subseteq H$.
- (Index Theorem) Let G be a finite group. If G has a proper subgroup H such that $[G : H] = m$ and $|G| \nmid m!$, then G is not simple.
- Every finite non-abelian simple group having a subgroup of index n, is isomorphic to a subgroup of A_n.
- Let G be a group of order $2m$, where m is an odd integer. Then G has a subgroup of order m and hence G is not simple.

- Let $1 \leq n < 60$ be an integer which is not prime. Then no group of order n is simple.
- A_5 is simple.
- If G is a simple group of order 60, then $G \simeq A_5$.
- For every $n \geq 5$, the group A_n is simple.