Department of Mathematics
Guru Nanak Dev University, Amritsar-143005
Notes on 'Symmetric Groups, Automorphims, Solvable groups' & assignment #5

If you dont learn from your mistakes, theres no sense making them.
–Herbert V. Prochnow

In these notes we study the Symmetric group S_n for $n = 3, 4, ...$ and the alternating group A_n.

0.1 Symmetric group

Recall that by a symmetric group of a nonempty set X is the group S_X of all bijections from X to X with the binary operation 'composition of maps'. If X is finite such that $|X| = n,\ n = 1, 2...$, then the Symmetric group S_X is called permutation group denoted S_n. Also recall that we defined alternating group A_n to be kernel of the homomorphism sign : $S_n \to \{-1, 1\}$. An element $\sigma \in S_n$ is called a $r-$**cycle** or **cycle of length** r if there exist r symbols $a_1, ..., a_r \in \{1, 2, ..., n\}$ such that

$$\sigma(a_1) = a_2,\ ..., \sigma(a_{r-1}) = a_r,\ \sigma(a_r) = a_1;\ \sigma(a_i) = a_i$$

for all $i \notin \{1, ..., r\}$. We represent the $r-$cycle σ by

$$\sigma = (a_1\ a_2 \cdots\ a_r).$$

It is easy to see that if $\sigma = (a_1 \cdots a_r)$ is an $r-$cycle in S_n then $|\sigma| = r$, since r is the lest positive integer such that $\sigma^r(a_i) = i\ \forall i = 1, ..., n$.

Definition: Two cycles in S_n are said to be disjoint if they are disjoint as sets.

Example: If we take $\sigma = (124)(38) \in S_8$ then this means

$$\sigma = (124)(38) = \begin{array}{l} 1 \mapsto 2 \\ 2 \mapsto 4 \\ 3 \mapsto 8 \\ 4 \mapsto 1 \\ 5 \mapsto 5 \\ 6 \mapsto 6 \\ 7 \mapsto 7 \\ 8 \mapsto 3 \end{array}$$

i.e. $1 \mapsto 2 \mapsto 4 \mapsto 1,\ 3 \mapsto 8 \mapsto 3,\ 5 \mapsto 5,\ 6 \mapsto 6,\ 7 \mapsto 7$ under σ.

Note that $\sigma = (124)(38)$ is product of $3-$cycle (124) and a $2-$cycle (38) which are disjoint therefore they commute i.e.

$$(124)(38) = (38)(124)$$

therefore the order of composition is immaterial and we do not insert the composition sign $\circ$ between disjoint cycles. We can also represent σ as a product of transpositions by

$$(124)(38) = (14) \circ (12) \circ (38).$$

This motivates the following definition.

Definition: A $2-$cycle in S_n is called a transposition.

Remark: Every $\sigma \in S_n$ can be written as a product of transpositions. To see this first note that if $\mu = (a_1 \cdots a_r)$ is an $r-$cycle then

$$(a_1 \cdots a_r) = (a_1\ a_r) \circ (a_1\ a_{r-1}) \circ \cdots \circ (a_1\ a_2)$$

which is product of transpositions. Since σ is product of such $r-$cycles each of which is product of transpositions, where each r is varying between 1 and n, it follows that σ is also a product of transpositions.

We now establish following important result concerning representation of permutations as product of disjoint cycles.

Theorem 0.1. *Every $\sigma \in S_n,\ n = 3, 4...$ can be expressed as a product of disjoint cycles.*

Proof. If σ itself is a single cycle, then $\sigma^m(1) \neq 1$ for all $m = 1, 2, ..., n-1$ and we are done. So now suppose that σ is not a cycle. Then there is a smallest positive integer $k < n$ such that $\sigma^k(1) = 1$. If σ fixes rest all the elements then $\sigma = (1\ \sigma(1)\ \cdots\ \sigma^{k-1}(1))$ and the result is proved otherwise there is a symbol $j \in \{1, 2, ..., n\} - \{1, \sigma(1), ..., \sigma^{k-1}(1)\}$ such that $\sigma(j) \neq j$ and we have another cycle $(j\ \sigma(j)\ \cdots\ \sigma^{r-1}(j))$. Here r is the least positive integer such that $\sigma^r(j) = j$. If σ fixes rest all the elements then

$$\sigma = (1\ \sigma(1)\ \cdots\ \sigma^{k-1}(1))(j\ \sigma(j)\ \cdots\ \sigma^{r-1}(j))$$

is the product of two disjoint cycles and we are done otherwise repeat the procedure to obtain σ as a product of disjoint cycles in finite number of steps (since σ can move at most n elements). □

[1]E-mail: sonumaths@gmail.com; Web page: https://sites.google.com/site/sonumaths2/

Proposition 0.2. *Disjoint cycles commute in S_n.*

Proof. Let σ and μ be disjoint cycles in S_n. If $\tau(i) = j$ then as $\sigma \cap \tau = \emptyset$ it follows that $\sigma(i) = i$ and $\sigma(j) = j$. Therefore

$$\sigma\tau(i) = \sigma(j) = j = \tau(i) = \tau(\sigma(i))$$

which shows that $\sigma\tau(i) = \tau\sigma(i)$ for all $i \in \tau$. Similarly we see that $\sigma\tau(k) = \tau\sigma(k)$ for all $k \in \sigma$. Now if an element $\ell \notin \sigma$ and $\ell \notin \tau$ then again $\sigma\tau(\ell) = \ell = \tau\sigma(\ell)$. We have proved that $\sigma\tau(i) = \tau\sigma(i)\ \forall\ i \in \{1, ..., n\}$. □

Proposition 0.3. *Let $\sigma \in S_n$ such that $\sigma = \sigma_{n_1} \cdots \sigma_{n_k}$ be product of k disjoint cycles σ_{n_i}, $i = 1, ..., k$, each of which is of length $n_1, ..., n_k$ respectively. Then*

$$|\sigma| = lcm(n_1, ..., n_k).$$

Proof. Let $\ell := \text{lcm}(n_1, ..., n_k)$. Then each of the n_i's divide ℓ and $(\sigma_{n_i})^\ell = (1)$. As a result of this and the fact that disjoint cycles commute, it follows that

$$(\sigma_{n_1} \cdots \sigma_{n_k})^\ell = \sigma_{n_1}^\ell \cdots \sigma_{n_k}^\ell = (1) \cdots (1) = (1).$$

This proves that $|\sigma| \leq \ell$. For the reverse inequality, not that

$$1 = (\sigma_{n_1} \cdots \sigma_{n_k})^{|\sigma|} = \sigma_{n_1}^{|\sigma|} \cdots \sigma_{n_k}^{|\sigma|}$$

which gives $\sigma_{n_1}^{|\sigma|} = (1), ..., \sigma_{n_k}^{|\sigma|} = (1)$ but then n_i divides $|\sigma|$ for each $i = 1, ..., k$, and $|\sigma|$ is a common multiple of $n_1, ..., n_k$ therefore $|\sigma| \geq \text{lcm}(n_1, ..., n_k) = \ell$. This establishes $|\sigma| = \ell$. □

Proposition 0.4. *Let $\sigma = (12 \cdots m)$ be an $m-$cycle in S_n. Then for any positive integer i, σ^i is also an $m-$cycle if and only if* $\gcd(i, m) = 1$.

Proof. Since σ is an $m-$cycle $|\sigma| = m$. Then as we know

$$|\sigma^i| = \frac{m}{\gcd(i, m)} = m \ \Leftrightarrow\ \gcd(i, m) = 1.$$

This proves the assertion. □

Remark: If $n \geq m$ then number of $m-$cycles in S_n is equal to the number $\dfrac{n(n-1)\cdots(n-m+1)}{m}$.

Definition: Let $\sigma \in S_n$ be expressed as a product of disjoint cycles of lengths $n_1, ..., n_k$ such that $n_1 \leq \cdots \leq n_k$ including $1-$cycles, then the integers $n_1, ..., n_k$ are called **the cycle type** of σ.

For example cycle type of a $m-$cycle in S_n is $\underbrace{1, 1, ..., 1}_{(n-m)\text{times}}, m$.

Remark: If $\sigma \in S_n$ has a cycle type $n_1, ..., n_k$ then for each $i = 1, ..., k$, n_i-cycle is further a product of $n_i - 1$ transpositions. Therefore σ is a product of $\sum_{i=1}^k (n_i - 1)$ transpositions. Then

$$\text{sign}(\sigma) = (-1)^{\sum_{i=1}^k (n_i - 1)} = (-1)^{n_1 + \cdots + n_k - k}.$$

This gives us an algorithm to easily calculate the $\text{sign}(\sigma)$ for any $\sigma \in S_n$. For example if $\sigma = (12)(47)(6359) \in S_9$ then $\text{sign}(\sigma) = (-1)^{2+2+4-3} = -1$ which shows that σ is an odd permutation. In fact if a $\sigma \in S_n$ is a expressed as a product of $k-$transpositions then

$$\text{sign}(\sigma) = (-1)^k.$$

We can now directly construct the set of all even permutations of S_4 which is the subgroup A_4 and is given by

$$A_4 = \{(1), (123), (132), (124), (142), (134), (143),$$

$$(234), (243), (12)(34), (13)(24), (23)(14)\}$$

Note that the subgroup

$$H := \{(1), (12)(34), (13)(24), (23)(14)\} \cong D_4$$

of A_4 is normal in A_4. Therefore A_4 is not simple. Check that $A_4 \ncong D_{12}$.

Definition: If $n \in Z^+$, a partition of n is a non-decreasing sequence of positive integers whose sum is equal to n.

For example $1, 1, 2, 3$ is a partition of 7. Similarly $1, 1, 1, 1, 1, 1, 1$ and $2, 5$ are also partitions of 7.

Lemma 0.5. *Conjugate elements in S_n have same cycle type.*

Proof. Let $\sigma = (a_1 a_2 \cdots a_{n_1})(b_1 b_2 \cdots b_{n_2}) \cdots$, be cycle decomposition of σ. If $\tau \in S_n$ then

$$\sigma(i) = j \ \Leftrightarrow\ (\tau\sigma\tau^{-1})(\tau(i)) = \tau(\sigma(i)) = \tau(j)$$

which shows that

$$\tau\sigma\tau^{-1} = (\tau(a_1)\tau(a_2) \cdots \tau(a_{n_1}))(\tau(b_1)\tau(b_2) \cdots \tau(b_{n_2})) \cdots$$

which proves that σ and $\tau\sigma\tau^{-1}$ have same cycle type. □

Theorem 0.6. *Two elements in S_n are conjugates in S_n if and only if they have the same cycle type. The number of conjugacy classes of S_n is equal to the number of partitions of n.*

Proof. That conjugate elements in S_n have same cycle type follows from the preceding lemma 0.5.
Conversely, let σ and τ in S_n have the same cycle type say $n_1, ..., n_k$. Order the cycles in nondecreasing lengths including $1-$cycles. Then each cycle decomposition is a list in which all integers from 1 to n appear exactly once. Define μ to be the function that maps the integer at $i-$th place in the list for σ to the integers at $i-$th place in the list for τ. Then clearly $\mu \in S_n$ and $\mu\sigma\mu^{-1} = \tau$.
Since any cycle type in S_n is a partition of n and conversely, and that all elements in one conjugacy class have same cycle type (by lemma 0.5) it follows that total number of conjugacy classes of S_n is precisey equal to the total number of partitions of n. □

Theorem 0.7. *Let $\sigma \in S_n$ such that σ has k_i cycles of length m_i for each $i = 1, 2..., r, (r \in \mathbb{Z}^+)$ such that $\sum_{i=1}^{r} k_i m_i = n$. Then the number of conjugates of σ (i.e. orbit of σ under the action of S_n on itself via conjugation) is*

$$|\mathcal{O}_\sigma| = \frac{n!}{(k_1! m_1^{k_1}) \cdots (k_r! m_r^{k_r})}.$$

Proof. Identify an m_i-cycle as one object and any m_j-cycle s.t. $m_i \neq m_j$ is a different object. The total number of permutations of n objects in which k_1 objects are of same kind, k_2 objects of same kind,..., k_r objects are of same kind, is given by

$$\frac{n!}{k_1! \cdots k_r!}.$$

Note that in this counting each m_i-cycle is counted in exactly m_i ways (because its symbols can be cyclically permuted in m_i distinct ways to give the same permutation each time) therefore the k_i cycles are counted in exactly $m_i^{k_i}$ ways. Therefore the number of times the permutations have been counted repeatedly is $\prod_{i=1}^{r} m_i^{k_i}$. Hence the required number of conjugates of σ is

$$\frac{n!}{k_1! \cdots k_2! \prod_{i=1}^{r} {m_i}^{k_i}}$$

as required. □

Proposition 0.8. *If $H \leq S_n$, then H consists of even permutations or it has exactly $\frac{|H|}{2}$ even permutations.*

Proof. Since $\text{sign} : S_n \to \{-1, 1\}$ is a surjective homomorphism, if $H \leq S_n$ then $\text{sign}(H) \leq \{-1, 1\}$ Then the restriction $\varphi = \text{sign}|_H : H \to \{-1, 1\}$ is also a homomorphism. If $\varphi(H) = 1$ then H consists of even permutations. If $\varphi(H) \neq 1$ then φ is a surjective homomorphism. Therefore by first isomorphism theorem

$$H/\ker\varphi \cong \{-1, 1\}$$

where $[H : \ker\varphi] = 2$. This proves that the total number of even permutations in H is $|\ker\varphi| = \frac{|H|}{2}$. □

Theorem 0.9. (Cayley) *Every group is isomorphic to a subgroup of some symmetric group.*

Proof. Let G be a group and S_G be its symmetric group. Then the binary operation of G as an action of G on itself induces a homomorphism $\Psi : G \to S_G$ by

$$\Psi(g) := \sigma_g$$

such that $\sigma_g : G \to G$ is a bijection and for all $x \in G$, $\sigma_g(x) := g \bullet x := gx$. To verify that Ψ is a homomorphism, consider for $g_1, g_2 \in G$ the following

$$\Psi(g_1 g_2)(x) = \sigma_{g_1 g_2}(x) = (g_1 g_2)x = g_1(g_2 x) =$$

$$= g_1(\sigma_{g_2}(x)) = (\sigma_{g_1} \circ \sigma_{g_2})(x), \ \forall x \in G$$

which gives

$$\Psi(g_1 g_2) = (\sigma_{g_1} \circ \sigma_{g_2}) = \Psi(g_1)\Psi(g_2)$$

hence Ψ is a homomorphism. We now show that Ψ is injective. For this let $\Psi(g_1) = \Psi(g_2)$ then for all $x \in G$, $\sigma_{g_1}(x) = \sigma_{g_2}(x) \Rightarrow g_1 x = g_2 x$ which directly gives $g_1 = g_2$. Hence by first isomorphism theorem $G \cong \Psi(G) \leq S_G$. □

Corollary 0.10. *If G is a finite group of order n and p is the smallest prime dividing n. Then any subgroup of G of index p is normal in G.*

Proof. Suppose $H \leq G$ such that $[G : H] = p$. Define a map $\varphi : G \to S_{G/H}$ by $\varphi(g) = \sigma_g$ such that $\sigma_g(xH) = (gx)H$. Clearly φ is a homomorphism with $\ker\varphi = \{g \in G \mid (gx)H = xH \Leftrightarrow x^{-1}gx \in H \Leftrightarrow g \in xHx^{-1} \ \forall x \in G\} = \cap_{x \in G} xHx^{-1} \subseteq H$ so let $|H|/|\ker\varphi| = k$ for some positive integer k. By first isomorphism theorem it follows that

$$G/\ker\varphi \cong \varphi(G) \leq S_{G/H}.$$

Since $|S_{G/H}| = |G/H|! = p!$ it follows by Lagrange's theorem that $|G|/|\ker\varphi|$ divides $p!$. Now observe that

$$\frac{|G|}{|\ker\varphi|} = \frac{|G|}{|H|}\frac{|H|}{|\ker\varphi|} = pk$$

which shows that pk divides $p!$ or k divides $(p-1)!$. If $k > 1$ then there is a prime q dividing k but then q divides $(p-1)!$ since p does not divide $(p-1)!$, it follows that $q < p$ but then q divides $|G|$ which contradicts minimality of prime p. Hence there is no prime dividing k and therefore $k = 1$. This means $H = \ker\varphi$ or $H \trianglelefteq G$. □

Example: (Groups of order 12) Let $|G| = 12$. We show that either G has a normal Sylow$-3-$subgroup or $G \cong A_4$.
Suppose that $n_3 \neq 1$ then let H =Sylow$-3-$subgroup of G. As n_3 divides 4 and $n_3 \equiv 1 \mod 3$ it follows that $n_3 = 4$. Since each of these subgroups is of order three therefore they intersect in identity. Hence G has 8 elements of order 3. Also $|N_G(H)| = 3 = |H|$ thus $N_G(H) = H$ and G acts on these four subgroups via conjugation and by Cayley's theorem $G \cong$a subgroup $\varphi(G)$ of $S_{G/H} \cong S_4$. Since $\varphi(G)$ contains 8 elements of order 3 and S_4 has exactly 8 elements of order 3 all contained in A_4 therefore $|\varphi(G) \cap A_4|$ is at least 9. Since $|\varphi(G)|$ divides $|S_4| = 24$ the only possibility is $|\varphi(G)| = 12 = |A_4|$ such that $|\varphi(G) \cap A_4| \geq 9$. From this we see that $\varphi(G) = A_4$ i.e. $G \cong A_4$. Since A_4 is not simple, it follows that G is not simple.

Theorem 0.11. (Odd test) $|G| = 2n$, *where n is an odd integer > 1, then G is not simple*

Proof. From the proof of Cayley's theorem 0.9 observe that $\varphi : G \to S_G$ defined by $\varphi(g) = \sigma_g$ s.t. $\sigma_g(x) = gx \ \forall \ x \in G$ is an injective homomorphism. Therefore $G \cong \varphi(G) \leq S_G$. By Cauchy's theorem G has an element g of order 2. Then $\varphi(g) = \sigma_g \in \varphi(G)$ is of order 2. Hence σ_g =product of disjoint cycles of lengths ≤ 2. If $\sigma_g(x) = x$ for some $x \in G$ then $gx = x$ or $g = 1$, which contradicts the fact that $|g| = 2$. Hence σ_g =product of all $2-$cycles in $\varphi(G)$. Since there are exactly n distinct-disjoint $2-$cycles in $\varphi(G)$ and n is odd, it follows that $\text{sign}(\sigma_g) = (-1)^n = -1$. So $\varphi(G)$ contains an odd permutation. By proposition 0.8 $\varphi(G)$ has exactly n even permutations which in turn proves that $\varphi(G)$ has a subgroup of index 2. Thus $\varphi(G)$ is not simple hence G is not simple. □

Example: From the Odd test we see that groups of order

$$30 = 2 \times 15, \ 90 = 2 \times 45, \ 150 = 2 \times 125, \ 1450 = 2 \times 725$$

are not simple.

We present a generalization of Cayley's theorem

Theorem 0.12. (Generalized Cayley's theorem) *Let $H \leq G$. Then there is a homomorphism*

$$\Psi : G \to S_{G/H}$$

such that $\ker \Psi \leq H$ *and for all $K \trianglelefteq G$, such that $K \leq H$ then $K \leq \ker \Psi$.*

Proof. Proof follows from the proof of the corollary 0.10 to the Cayley's theorem. Define $\Psi : G \to S_{G/H}$ by $\Psi(g) = \sigma_g$ s.t. $\sigma_g(xH) = (gx)H$. Then clearly Ψ is a homomorphism with

$$\ker \Psi := \cap_{x \in G} xHx^{-1} \subseteq H.$$

Finally if $K \trianglelefteq G$ such that $K \leq H$ then $K = xKx^{-1} \subseteq xHx^{-1}, \ \forall x \in G$ hence $K \leq \cap_{x \in G} xHx^{-1} = \ker \Psi$. □

The generalized Cayley's theorem enables us the following very important corollary regrading testing non-simplicity of a finite group from its order.

Corollary 0.13. (Index theorem) *If G is a finite group and $H \leq G$ such that $|G|$ does not divide $|G/H|!$, then H contains a nontrivial normal subgroup of G. Thus G is not simple.*

Proof. From the proof of the theorem0.12 we have $G/\ker \Psi \cong \Psi(G) \leq S_{G/H}$ and that $\ker \Psi \leq H$. Then $\dfrac{|G|}{|\ker \Psi|}$ divides $|G/H|!$. Since $|G|$ does not divide $|G/H|!$ it follows that $|\ker \Psi| > 1$. □

Theorem 0.14. (Embedding theorem) *Let G be a finite non-abelian simple group and $H \leq G$ such that $[G : H] = n$ for some positive integer n. Then G is isomorphic to a subgroup of A_n.*

Proof. Let $H \leq G$ such that $[G : H] = n$. Then from the generalized Cayley's theorem there is a nontrivial homomorphism $\Psi : G \to S_{G/H} \cong S_n$. Since G is simple and Ψ is nontrivial it follows that $\ker \Psi = 1$. Hence $G \cong \Psi(G) \leq S_{G/H}$. If there is an odd permutation in $\Psi(G)$ then by proposition 0.8 $\Psi(G)$ has a normal subgroup of index 2 and so does G has. This contradicts the fact that G is simple. So $\Psi(G)$ consists of even permutations of $S_{G/H}$ hence $G \cong \Psi(G) \leq A_{G/H} \cong A_n$. □

Thus from the embedding theorem we see that every non-abelian finite simple group having a subgroup of index n is embedded in A_n.

Example: (Groups of order 80) As an application of embedding theorem. Consider a group G s.t.

$$|G| = 80 = 16 \times 5.$$

By Sylow's 3rd theorem, G has a Sylow$-2-$subgroup of order 16 of index 5; by embedding theorem $G \cong \Psi(G) \leq A_5$ then $|G| = 80$ must divide $|A_5| = 60$ which is a contradiction. Hence there does not exist any simple group of order 80.

Embedding theorem can be used to conclude that groups of orders $12, 24, 36, 48, 96, 108, 112, 160, 192$ can not be simple.

0.2 Simplicity of A_n for $n = 5, 6, ...$

Theorem 0.15. (Simplicity of A_5) *The alternating group A_5 is simple.*

Proof. Elements of A_5 are of the form $(1), (12)(34), (123)$ or (12345) i.e. cycle types

$$(1,1,1,1,1), (1,2,2), (1,1,3), (5).$$

Consider the action of S_5 on itself via conjugation. Then

Number of elements of order $2 = \dfrac{5!}{2!2^2} = 15.$

Number of elements of order $3 = \dfrac{5!}{(1!3)(2!1)} = 20.$

Number of elements of order $5 = \dfrac{5!}{1!5} = 24.$

We have

$C_{S_5}((12)(34)) := \{(1), (12)(34), (13)(24), (23)(14);$
$(12), (34), (1423), (1324)\}$

therefore $C_{A_5}((12)(34)) = C_{S_5}((12)(34)) \cap A_4$ whose order is 4 and under the action of A_5 on itself via conjugation $|\mathcal{O}_{(12)(34)}| = 60/|C_{A_5}((12)(34))| = 15$. We have established that all the 15 elements of order 2 each of which is a products of two disjoint transpositions, are in one orbit in A_5.

Similarly

$$C_{S_5}((123)) = \{(1), (123), (132), (45), (123)(45), (132)(45)\}$$

out of which only three elements are in A_5 therefore $C_{A_5}((123)) = \{(1), (123), (123)^2\}$ and $|\mathcal{O}_{123}| = 60/|C_{A_5}((123))| = 20$. Thus all 20 elements of order 3 of S_5 are in one orbit in A_5.

Now consider $C_{S_5}((12345)) = \langle(12345)\rangle \subset A_5$ therefore $C_{A_5}((12345)) = \langle(12345)\rangle$ and thus $|\mathcal{O}_{(12345)}| = 60/5 = 12$. Since there are 24 elements of order 5 in A_5, it follows that rest of the 12 elements are in other orbit which is precisely $\mathcal{O}_{13245}$ and $|\mathcal{O}_{13245}| = 12$. Hence A_5 decomposes into disjoint union of its orbits i.e.

$$A_5 = \mathcal{O}_{(1)} \cup \mathcal{O}_{(12)(34)} \cup \mathcal{O}_{(123)} \cup \mathcal{O}_{(12345)} \cup \mathcal{O}_{(13245)}$$

with $1, 15, 20, 12, 12$ elements in these orbits respectively. Now we are ready to prove the theorem. If possible let $H \trianglelefteq A_5$ be a nontrivial proper. Then $|H|$ divides 60 and $xHx^{-1} \subseteq H$ for all $x \in A_5$. Therefore if H intersects any orbit $\mathcal{O}_g$ for any $g \in A_5$ then it follows that $\mathcal{O}_g \subseteq H$. This means $|H|$ =sum of elements of orbits in A_5. The possibilities are $|H| = 13, 16, 21, 25, 28, 33, 36, 40, 45, 48$; none of these integers divide 60 which leads to a contradiction to the hypothesis that H was assumed to be a proper nontrivial normal subgroup of A_5. Hence A_5 is simple. □

Theorem 0.16. (Simplicity of A_n, $n \geq 5$) *The alternating group A_n for $n = 5, 6, ...$ is simple.*

Proof. We prove the theorem by induction on n. If $n = 5$ then from theorem 0.1, A_5 is simple. Let us assume that A_n is simple for all $n = 5, 6, ..., k-1$ for sum positive integer $k > 5$. Let $G = A_k$. To the contrary, let us assume that $H \trianglelefteq G$ such that $H \neq 1, G$. For each $i = 1, ..., k$ define

$$G_i := \{\sigma \in G \mid \sigma(i) = i\}.$$

Then clearly G_i consists of all even permutations on $k-1$ symbols therefore $G_i \cong A_{k-1}$. By induction hypothesis G_i is simple for all $i = 1, ..., k$.

Claim 1: Any non identity element of H does not fixes any element of the set $\{1, ..., k.\}$ If possible let $1 \neq \tau \in H$ s.t. $\tau(i) = i$ for some $i \in \{1, ..., k\}$. Then $\tau \in G_i \cap H \trianglelefteq G_i$. Since G_i is simple this gives $G_i \cap H = G_i$ or $G_i \subseteq H$. Since for all $\sigma \in G$, $\sigma G_i \sigma^{-1} = G_{\sigma(i)}$ $\forall$ i which means $\sigma G \sigma^{-1} \subseteq \sigma H \sigma^{-1} \subseteq H$ $\forall$ i. It follows that $G_j \leq H$ for all $j = 1, ..., k$. Let $\lambda \in G$ then λ can be written as a product of even number of transpositions i.e.

$$\lambda = \lambda_1 \cdots \lambda_t$$

for some positive integer t where each of $\lambda_1, ..., \lambda_t$ is a product of 2-transpositions in G and since each λ_ℓ fixes $k-4$ symbols ($\because$ $k > 5$), it follows that each $\lambda_\ell \in G_j$, $\ell = 1, ..., t$ for some j. Thus

$$G = \langle G_1, ..., G_k \rangle \leq H$$

which is a contradiction to the assumption that H is proper subgroup of G. This proves the claim. Thus for any $\tau_1, \tau_2 \in H$ if $\tau_1(i) = \tau_2(i)$ for some i then $(\tau_1^{-1} \circ \tau_2)(i) = i$ where $\tau_1^{-1} \circ \tau_2 \in H$ by above claim $\tau_1^{-1}\tau_2 = (1)$ or $\tau_1 = \tau_2$.

Claim 2: For all $\sigma \in H$ the cycle decomposition of σ does not contain any cycle of length ≥ 3. Suppose there is a $\sigma \in H$ such that cycle decomposition of τ contains a cycle of length ≥ 3 say

$$\sigma := (a_1 a_2 a_3 \cdots)(b_1 b_2 \cdots) \cdots .$$

Choose $\tau \in G$ such that

$$\tau(a_1) = a_1,\ \tau_(a_2) = a_2,\ \tau(a_3) \neq a_3$$

then clearly $\tau \neq \sigma$. Consider

$$\tau\sigma\tau^{-1} = (\tau(a_1)\tau(a_2)\tau(a_3)\cdots)(\tau(b_1)\tau(b_2)\cdots)\cdots$$

$$= (\tau(a_3)\cdots)(\tau(b_1)\tau(b_2)\cdots)\cdots$$

which shows that σ and $\tau\sigma\tau^{-1}$ are two distinct elements ($\because$ $\sigma(a_2) = a_3 \neq a_2 = \tau\sigma\tau^{-1}(a_2)$)of H such that $\sigma(a_1) = a_2 = \tau\sigma\tau^{-1}(a_1)$ this contradicts claim 1. Thus no permutation in H contain any cycle of length ≥ 3.

Claim 3: No permutation of H contains any $2-$cycle. If possible let $\sigma \in H$ such that

$$\sigma = (a_1a_2)(a_3a_4)(a_5a_6)\cdots, \ (\because n \geq 6)$$

and choose $\tau \in H$ such that

$$\tau = (a_1a_2)(a_3a_5) \in G$$

then $\tau\sigma\tau^{-1} = (a_1a_2)(a_5a_4)(a_3a_6)\cdots$ and σ and $\tau\sigma\tau^{-1}$ are two distinct permutations ($\because \sigma(a_6) = a_5 \neq a_3 = \tau\sigma\tau^{-1}(a_6)$)of H such that $\sigma(a_1) = a_2 = (\tau\sigma\tau^{-1})(a_1)$ which again contradicts claim 1.
From claim 2 and 3 together we see that for all $\sigma \in H$ σ does not contain a cycle of length ≥ 2, but then $\sigma = (1)$ or $H = 1$ a contradiction. Hence $G = A_k$ is simple. This completes the last step of induction. □

0.3 Solvable groups

Definition: A group G is said to be solvable if it has a finite chain of subgroups

$$1 = G_0 \leq G_1 \leq \cdots \leq G_s = G$$

such that $G_i \trianglelefteq G_{i+1}, \ \forall \ i = 1, ..., s-1$ and each factor group G_{i+1}/G_i is **abelian**.

Definition: The finite sequence of subgroups of G, $1 = G_0 \leq G_1 \leq \cdots \leq G_s = G$ is called a normal series or subnormal series if $G_i \trianglelefteq G_{i+1}, \ \forall \ i = 1, ..., s-1$

Definition: A normal series $1 = G_0 \leq G_1 \leq \cdots \leq G_s = G$ is called a solvable series if each factor group $G_{i+1}/G_i, \ i = 1, ..., s-1$, is abelian.

Examples: Following examples can be verified as an easy consequence of the above definitions:

1. Any abelian group G is solvable since $1 \trianglelefteq G$ is the solvable series.
2. Any group of order pq, p, q primes, is solvable. Here solvable series is $1 \trianglelefteq H(\cong Z_{\max\{p,q\}}) \trianglelefteq G$.
3. S_3 and S_4 are solvable.(obtain the solvable series for S_4)
4. $A_n, \ n = 5, 6...$ is not solvable since A_n is simple non-abelian. The only normal series for A_n is $1 \trianglelefteq A_n$ where the factor $A_n/1 \cong A_n$ is not abelian.
5. Every $p-$group is solvable. (we will prove it later)

We now establish a necessary and sufficient condition for solvability of a finite group.

Theorem 0.17. *A finite group is solvable if and only if there is a normal series for G whose factors are cyclic of prime orders.*

Proof. If there is a normal series for G whose factors are cyclic of prime order then all such factors are abelian and by definition, G is solvable.
Conversely let G be solvable. Let $1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_s = G$ be a solvable series for G. Since each factor $\frac{G_{i+1}}{G_i}$ is finite abelian. consider any composition series for $\frac{G_{i+1}}{G_i}$ which is of the form

$$1 = \frac{G_i}{G_i} \trianglelefteq \frac{{H_1}^i}{G_i} \trianglelefteq \cdots \trianglelefteq \frac{H^i_{k_i}}{G_i} = \frac{G_{i+1}}{G_i}$$

where each of the factor group

$$(H^i_{j+1}/G_i)/(H^i_j/G_i) \cong H^i_{j+1}/H^i_j, \ j = 1, ..., k_i - 1$$

is simple-abelian therefore cyclic of prime order. Hence the sequence of subgroups given by

$$1 = G_0 \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq \cdots G_i \trianglelefteq H^i_1 \trianglelefteq \cdots$$

$$\trianglelefteq H^i_{k_i-1} \trianglelefteq G_{i+1} \trianglelefteq \cdots \trianglelefteq G$$

is a normal series for G where each of the factors is cyclic of prime order. This completes the proof. □

0.3.1 Automorphisms

Definition: (Group of Automorphisms of G) Let G be a group. Then any isomorphism $\sigma : G \to G$ is called an automorphism of G. The set of all automorphisms of G denoted $\mathrm{Aut}(G)$ is a group under the composition of mappings and it is called the group of automorphims of G.

Definition: Let G be a group and $g \in G$. Then the isomorphism $\sigma_g : G \to G$ defined by

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

is an automorphism of G and it is called an inner-automorphism of G. The set of all inner automorphisms of G denoted $\mathrm{Inn}(G)$ is called as group of inner automorphims of G. It is easy to see that

$$\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G).$$

Proposition 0.18. *Let $H \trianglelefteq G$. Under the action of G on H via conjugation induces a homomorphism $\psi : G \to Aut(H)$ by $\psi(g)(h) = \sigma_g(h) = ghg^{-1} \in H$ such that $G/C_G(H) \cong \psi(G) \leq Aut(H)$.*

Proof. Since $\psi(g)(h) = \sigma_g(h) = ghg^{-1}, \forall\ h \in H$ clearly $\sigma_g \in \mathrm{Aut}(H)$ and we have

$$\psi(g_1g_2) = \sigma_{g_1g_2}(h) = \sigma_{g_1}(g_2hg_2^{-1}) = (\sigma_{g_1} \circ \sigma_{g_2})(h)$$

which shows that $\psi(g_1g_2) = \psi(g_1) \circ \psi(g_2)$ therefore ψ is a homomorphism. By 1st isomorphism theorem

$$G/\ker\psi \cong \psi(G) \leq \mathrm{Aut}(H)$$

where

$$\ker\psi := \{g \in G \mid \sigma_g(h) = ghg^{-1} = h,\ \forall\, h \in H\} = C_G(H).$$

Hence $G/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$. □

Note that if $K \leq G$ then for all $g \in G$ $\sigma_g(x) = gxg^{-1},\ \forall\ x \in G$ is an automorphism of G. Then $K \cong \sigma(K) = gKg^{-1}$. Also if we replace the role of G by $N_G(H)$ in the proposition 0.18, we see that $N_G(H)/C_{N_G(H)}(H) = N_G(H)/C_G(H) \cong$ to a subgroup of $\mathrm{Aut}(H)$.

Corollary 0.19. *Let G be a group then $G/Z(G) \cong Inn(G)$.*

Proof. Taking $G = H$ in the proposition 0.18 we have $G/Z(G) \cong$ to a subgroup of $\mathrm{Aut}(G)$. Since for each $g \in G,\ \psi(g)(x) = gxg^{-1},\ \forall x \in G$ is an inner automorphism of G it follows that $\psi(G) = \mathrm{Inn}(G)$ and hence $G/Z(G) \cong \mathrm{Inn}(G)$. □

0.3.2 Automorphisms of $S_n,\ n \neq 6$

Lemma 0.20. *For all $\Gamma \in Aut(S_n),\ n = 3, 4, \ldots$ under the action of S_n on itself via conjugation, the orbit (conjugacy class of $\Gamma((12))$)*

$$\mathcal{O}_{\Gamma((1\ 2))} = \begin{cases} \mathcal{O}_{((1\ 2))} & \text{if } n \neq 6 \\ \mathcal{O}_{((1\ 2))} \text{ or } \mathcal{O}_{((12)(34)(56))} & \text{if } n = 6 \end{cases}$$

Proof. First we observe that If G is a group and $\mathcal{O}_x$ is a conjugacy class of $x \in G$ then for all $g \in G,\ gxg^{-1} \in \mathcal{O}_x$, therefore for any $\Gamma \in \mathrm{Aut}(G)$ $\Gamma(gxg^{-1}) = \Gamma(g)\Gamma(x)\Gamma(g)^{-1} \in \mathcal{O}_{\Gamma(x)}$. Thus

$$\Gamma(\mathcal{O}_x) = \mathcal{O}_{\Gamma(x)}$$

is the conjugacy class of $\Gamma(x)$.
Now if $\mathcal{O}_{(12)}$ is a conjugacy class of all transpositions in S_n then for $\Gamma \in \mathrm{Aut}(S_n)$ the conjugacy class of $\Gamma((12))$ is $\Gamma(\mathcal{O}_{(12)}) = \mathcal{O}_{\Gamma((12))}$. Since Γ is a bijection, it follows that $|\Gamma(\mathcal{O}_{(12)})| = |\mathcal{O}_{\Gamma((12))}|$. As $2 = |(12)| = |\Gamma((12))|$ we see that $\Gamma((12))$ =either a transposition or a product of disjoint transpositions. Let $\Gamma((12))$ be a product of $k, (1 \leq k \leq \frac{n}{2})$ disjoint transpositions then using theorem 0.7 we have

$$|\mathcal{O}_{\Gamma((12))}| = \frac{n!}{k!2^k(n-2k)!1^{n-2k}} = \frac{n!}{1!2^1(n-2)!1^{n-2}} = |\mathcal{O}_{(12)}|$$

which gives

$$2^{k-1}(n-2k)!k! = (n-2)! \tag{0.1}$$

Clearly $k = 1$ is a solution of Eq.(0.1) and $k = 2$ is not a solution. For the other values of k, we have for $k > 2$

$$\begin{aligned} 2^{k-1}k! &= (n-2)\cdots(n-2k+1) \geq (2k-2)!,\ n \geq 2k, \\ &\Rightarrow\ 2^{k-1}k! \geq (2k-2)! \\ &\Rightarrow\ k \geq 1 \cdot 3 \cdot 5 \cdots (2k-3), \end{aligned}$$

where equality holds only for $k = 3 = 2k - 3$ for $n = 2k = 6$ and for all $k > 3$, $k < 1 \cdot 3 \cdots (2k-3)$, therefore there is no other solution satisfying Eq.(0.1). This proves the result. □

Lemma 0.21. *For all $\Gamma \in Aut(S_n),\ n \neq 6$*

$$\Gamma((1k)) = (ab_k)$$

for distinct $a, b_2, ..., b_n \in \{1, ..., n\}$.

Proof. From the preceding lemma 0.20 it follows that automorphisms of $S_n,\ n \neq 6$ preserve the conjugacy class of transpositions i.e. for all $\Gamma \in \mathrm{Aut}(S)_n,\ n \neq 6$, $\Gamma(\mathcal{O}_{ab}) = \mathcal{O}_{\Gamma(ab)} = \mathcal{O}_{ab}$. Thus Γ maps a transposition to a transposition i.e.

$$\Gamma((1k)) = (ab_k)$$

for distinct $a, b_2, ..., b_n \in \{1, ..., n\}$. □

Lemma 0.22. *For any distinct $a, b_2, ..., b_n \in \{1, ..., n\}$*

$$S_n = \langle (12), ..., (1n) \rangle = \langle (ab_2), ..., (ab_n) \rangle .$$

Thus each automorphism of $S_n,\ n \neq 6$ is uniquely determined by $(1k) \mapsto (ab_k),\ k = 2, ..., n$ and there are at most $n!$ of such maps determine by different choices for $a, b_2, ..., b_n$.

Proof. Since every $\sigma \in S_n$ is product of transpositions where each transposition $(xy) \in S_n$ can be written as

$$(xy) = (1x)(1y)(1x) = (ax)(ay)(ax)$$

for all distinct $1 \neq x, 1 \neq y, a \in \{1, ..., n\}$, we see that σ is generated by the set of transpositions $(1, 2), ..., (1, n)$ i.e.

$$S_n = \langle (12), ..., (1, n) \rangle = \langle (ab_2), ..., (a, b_n) \rangle .$$

where $a, b_2, ..., b_n$ are distinct symbols from the set $\{1, ..., n\}$.

From the last lemma 0.21 we see that every $\Gamma \in \mathrm{Aut}(S_n)$ is such that $\Gamma((1k)) = (ab_k),\ k = 2, ..., n$ which is uniquely determined as it maps bijectively a set of generators of S_n to a set of generators of S_n. The total number of possibilities of choosing the correspondence $(1k) \mapsto (ab_k)$ depends upon number of ways in which a and b_k can be chosen. Clearly number of ways in which a can be chosen is n, once a has been picked up b_2 can be chosen from the list $\{1, ..., n\} - \{a\}$ i.e. in at most $n-1$ ways and so on. This way the total number of ways in which under an automorphism the generators $(12), ..., (1n)$ can be mapped bijectively to the set of generators $(ab_2), ..., (ab_n)$ is $|\mathrm{Aut}(S_n)| \leq n(n-1)\cdots 21 = n!$. □

Theorem 0.23. (Automorphisms of $S_n,\ n \neq 6$) *For all $n \geq 3$ and $n \neq 6$, $Aut(S_n) \cong S_n$.*

Proof. From the preceding lemma 0.22 we see that for $n \neq 6$, $|\mathrm{Aut}(S_n)| \leq n!$ but since $n! = |\mathrm{Inn}(S_n)| \leq |\mathrm{Aut}(S_n)|$ it follows that

$$\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n) \cong S_n \ \forall n \neq 6$$

where the isomorphism of $\mathrm{Inn}(S_n)$ and S_n follows from the fact that $Z(S_n) = \{1\}\ \forall\ n \geq 3$ together with the corollary 0.3.1 which gives $S_n \cong S_n/Z(S_n) \cong \mathrm{Inn}(S_n)$ and this proves the theorem. □

Remark: For $n = 6$, we can show that

$$\mathrm{Aut}(S_6)/\mathrm{Inn}(S_6) \cong Z_2$$

as follows. First note that $\mathrm{Inn}(S_6) \cong S_6$ therefore $|\mathrm{Inn}(S_6)| = 6!$. From lemma 0.20 we see that under any automorphism $\Gamma \in \mathrm{Aut}(S_6)$ a conjugacy class of $(12) \in S_6$ can be mapped either to itself or to a conjugacy class of $(12)(34)(56)$. If this is the case then there are at least 6! more automorphisms in addition to the inner automorphims. We explicitly obtain an automorphims of S_6 which is not inner namely the following

$$\begin{array}{c} \underline{\Gamma \in \mathrm{Aut}(S_6)} \\ (12) \mapsto (12)(34)(56) = \sigma_1 \\ (23) \mapsto (14)(25)(36) = \sigma_2 \\ (34) \mapsto (13)(24)(56) = \sigma_3 \\ (45) \mapsto (12)(36)(45) = \sigma_4 \\ (56) \mapsto (14)(23)(56) = \sigma_5 \end{array}.$$

where

$$\sigma_i^2 = 1\ \forall i, (\sigma_i\sigma_j)^2 = 1 \forall |i-j| \geq 2,$$
$$(\sigma_i\sigma_{i+1})^3 = 1\ \forall\ i = 1, ..., 4.$$

It can be shown that the sets $\{(12), (23), (34), (45), (56)\}$ and $\{\sigma_1, ..., \sigma_5\}$ are two sets of generators for S_6 which establishes the assertion.

0.3.3 Commutator subgroup

Definition: The commutator $[x, y]$ of two elements x and y of a group G is defined as

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

Note that $xy = [x, y]yx$ which means $xy = yx \Leftrightarrow [x, y] = 1$.

Definition: For any nonempty subsets $A, B \subseteq G$ define the subgroup

$$[A, B] := \langle [a, b] \mid a \in A,\ b \in B \rangle .$$

Definition: (Commutator subgroup) The subgroup

$$[G, G] = \langle [x, y] \mid x, y \in G \rangle$$

is called **commutator subgroup** of G. We denote the commutator subgroup of G by G' or $G^{(1)}$. Note that G is abelian if and only if $G' = 1$.

Lemma 0.24. *$G' \trianglelefteq G$ and G/G' is abelian.*

Proof. Let $x, y, g \in G$ then $[x, y] \in G'$ and

$$\begin{aligned} g[x, y]g^{-1} =& gxyx^{-1}y^{-1} \\ =& (gxg^{-1})(gyg^{-1})(gx^{-1}g^{-1})(gy^{-1}g^{-1}) \\ =& XYX^{-1}Y^{-1} \in G' \end{aligned}$$

where $X = gxg^{-1},\ Y = gyg^{-1} \in G$. We have shown that conjugate of any commutator (generator of G') is again a commutator. Therefore conjugate of any element of G' which is just a conjugate of product of commutators is in G' hence $G' \trianglelefteq G$.
Now consider $xG', yG' \in G/G'$ since $xyx^{-1}y^{-1} \in G' \Leftrightarrow xyG' = yxG'$ i.e.

$$xG' * yG' = yG' * xG'$$

hence G/G' is abelian. □

Remark: If $\sigma \in \mathrm{Aut}(G)$ then $\sigma([x, y]) = [\sigma(x), \sigma(y)] \in G'$. Therefore $\sigma(G') \subseteq G'$. Since σ is a bijection it follows that $\sigma(G') = G'$. Thus the commutator subgroup is an invariant of all automorphims of G.

0.3.4 Characteristic subgroup

A subgroup of a group which is invariant under the automorphisms of the group is called characteristic subgroup. More precisely,

Definition: (Characteristic subgroup) A subgroup H of G is called characteristic subgroup of G denoted $H \text{char} G$ if $\sigma(H) = H$ for all $\sigma \in \text{Aut}(G)$.

Example: The commutator subgroup G' is a characteristic subgroup of G since $\sigma(G') = G'$ for all $\sigma \in \text{Aut}(G)$.

Remark: Following are some properties of characteristic subgroups.

- $H \text{char} G \Rightarrow H \trianglelefteq G$. To prove this consider for all $g \in G$, $\sigma_g \in \text{Inn}(G)$ s.t. $\sigma_g(x) = gxg^{-1}$. As $H \text{char} G$ by definition $\sigma_g(H) = H$ i.e. $gHg^{-1} = H \ \forall \ g \in G$. Hence $H \trianglelefteq G$.
- If H is unique subgroup of G of a given order then for all $\sigma \in \text{Aut}(G)$, $\sigma(H) \leq G$, since $|\sigma(H)| = |H|$ and H is the only subgroup of its order, it follows that $\sigma(H) = H$. Thus $H \text{char} G$.
- If $H \text{char} K$ and $K \trianglelefteq G$ then $H \trianglelefteq G$. To see this consider $\sigma_g \in \text{Inn}(G)$ s.t. $\sigma_g(x) = gxg^{-1}$. Then for all $k \in K$ $gkg^{-1} \in K$ and thus the restriction of σ_g onto K is an automorphism of K. Since $H \text{char} K$, it follows that $\sigma_g(H) = H$ or $gHg^{-1} = H$ i.e. $H \trianglelefteq G$.

Lemma 0.25. *G/G' is the largest abelian quotient of G in the sense that if $H \trianglelefteq G$ such that G/H is abelian then $G' \leq H$.*

Proof. Let $H \trianglelefteq G$ and G/H be abelian. Then for all $x, y \in G$, $xH * yH = yH * xH$ or $xyH = yxH$ or $xyx^{-1}y^{-1} = [x, y] \in H$. Thus $G' = \langle [x, y] \mid x, y \in G \rangle \leq H$. □

Definition: (Derived series) Define $G^{(0)} := G$, $G^{(1)} = [G, G]$, $G^{(2)} = [G^{(1)}, G^{(1)}], \cdots G^{(i+1)} = [G^{(i)}, G^{(i)}]$, $\forall\, i = 1, 2...$ Then clearly $G^{(i+1)} \text{char} G^{(i)}$ and $G^{(i+1)} \trianglelefteq G^{(i)}$, $\forall i = 1, 2...$ Then inductively, it follows that

$$G^{(2)} \text{char} G^{(1)},\ G^{(1)} \trianglelefteq G \Rightarrow G^{(2)} \trianglelefteq G^{(1)}$$

i.e.

$$G^{(i)} \trianglelefteq G \ \forall\ i = 1, 2, ...$$

Then the series of commutator subgroups

$$\cdots G^{(2)} \trianglelefteq G^{(1)} \trianglelefteq G^{(0)} = G$$

is called a derived series for G.

Note that if $A \subseteq B \subset G$ then $[A, A] \subseteq [B, B]$. We will use this simple fact in proving the next theorem.

Theorem 0.26. *A group G is solvable if and only if $G^{(n)} = 1$ for some positive integer n.*

Proof. If $G^{(n)} = 1$ for some positive integer n then

$$1 = G^{(n)} \trianglelefteq G^{(n-1)} \trianglelefteq \cdots \trianglelefteq G^{(1)} \trianglelefteq G$$

is a solvable series since each factor $G^{(i)}/G^{(i+1)}$, $i = 0, ..., n-1$, is abelian.
Conversely, let G be solvable. Let

$$1 = H_n \trianglelefteq H_{n-1} \trianglelefteq \cdots \trianglelefteq H_1 \trianglelefteq H_0 = G$$

be a solvable series for G. Since G/H_1 is abelian and $G/G^{(1)}$ is the largest abelian quotient of G, it follows by lemma 0.25 that $G^{(1)} \leq H_1$. Since each derived group $G^{(i)} \trianglelefteq G$, $i = 1, 2...$ and $G^{(1)} \leq H_1$, it follows that

$$G^{(i)} \trianglelefteq H_1,\ \forall\ i = 1, 2...$$

Then $G^{(2)} = [G^{(1)}, G^{(1)}] \trianglelefteq [H_1, H_1] \trianglelefteq H_2$ since H_1/H_2 is abelian. Therefore

$$G^{(2)} \trianglelefteq H_2.$$

Inductively, it follows that Inductively it follows that

$$G^{(k)} = [G^{(k)}, G^{(k)}] \leq [H_{k-1}, H_{k-1}] \trianglelefteq H_k \ \forall\ k = 2, 3...$$

which gives

$$G^{(k)} \trianglelefteq H_{(k)},\ \forall\ k = 1, 2, ...$$

In particular for $k = n$

$$G^{(n)} \trianglelefteq H_n = 1$$

i.e. $G^{(n)} = 1$ which proves the assertion. □

Corollary 0.27. *A subgroup of a solvable group is solvable.*

Proof. Let G be solvable and $H \leq G$. Let $\varphi : G \to K$ be a surjective homomorphism. Then since $\varphi([x, y]) = [\varphi(x), \varphi(y)]\ \forall\ x, y \in G$, it follows that $\varphi(G') = \varphi(G)' = K'$. Inductively $\varphi(G^{(i)}) = K^{(i)}\ \forall\ i = 0, 1, ...$ Then $\varphi(G^{(n)} = 1) = 1 = K^{(n)}$ for some positive integer n. Hence $K$is solvable. □

Proposition 0.28. *If $N \trianglelefteq G$ such that N and G/N are solvable then G is solvable.*

Proof. Let N and G/N are solvable and let

$$1 = N_0 \trianglelefteq \cdots \trianglelefteq N_s = N,\ 1 = \frac{G_0}{N} \trianglelefteq \cdots \trianglelefteq \frac{G_k}{N} = \frac{G}{N}$$

be solvable series for N and G/N respectively. Then the factors N_{i+1}/N_i, $i = 0, ..., s-1$ and $\frac{G_{j+1}}{G_j} \cong (G_{j+1}/N)/(G_j/N)$, $j = 0, ..., k-1$ are abelian. Therefore

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq N_k \trianglelefteq G_1 \trianglelefteq G_k = G$$

is a solvable series for G. Hence G is solvable. □

0.4 Solvability of $p-$groups

Recall that a group of order equal to a prime power is called a $p-$group and if G is a $p-$group then $Z(G) \neq 1$. We have the following lemma.

Lemma 0.29. *If $1 \neq H \trianglelefteq G$ and G is a $p-$group then $H \cap Z(G) \neq 1$. In particular if $|H| = p$ then $H \leq Z(G)$.*

Proof. First note that under the action of G on itself via conjugation, if $\mathcal{O}_x$ is a conjugacy class of x in G then either $\mathcal{O}_x \subseteq H$ (here $x \in H$)or $\mathcal{O}_x \cap H = \emptyset$(here $x \notin H$). Since $H = G \cap H = (H \cap Z(G)) \cup_{x \notin Z(G)} \mathcal{O}_x$ and therefore

$$|H| = |H \cap Z(G)| + \sum_{x \notin Z(G)} \frac{|G|}{|C_G(x)|}$$

where summation is carried over only those orbits which H intersects. Since p divides $[G : C_G(x)], \forall x \notin Z(G)$, it follows that p divides $\sum_{x \notin Z(G)} \frac{|G|}{|C_G(x)|}$, and as p divides H, we see that p divides $|H| - \sum_{x \notin Z(G)} \frac{|G|}{|C_G(x)|} = |H \cap Z(G)|$. Thus $H \cap Z(G) \neq 1$. In particular if $|H| = p$ then $|H \cap Z(G)| = p \leq |Z(G)|$ therefore $H = H \cap Z(G) \leq Z(G)$. □

Theorem 0.30. *If $H \trianglelefteq G$ G is a $p-$group then H contains a subgroup K of G s.t. $K \trianglelefteq G$ and $|K| = p^b$ for every divisor p^b of $|H|$. In particular G has a normal subgroup of all orders as divisors of $|G|$.*

Proof. Let $|G| = p^n$. We use induction on n. If $n = 1$ or $H = 1$ then the result is trivial. So let $n > 1$ and $H \neq 1$. Then by preceding lemma0.29, $H \cap Z(G) \neq 1$. By Cauchy's theorem $H \cap Z(G)$ has an element z of order p. Then $\langle z \rangle \leq Z(G)$ therefore $\langle z \rangle \trianglelefteq G$. Consider $G/\langle z \rangle$ whose order is p^{n-1} and $H/\langle z \rangle \trianglelefteq G/\langle z \rangle$ apply induction hypothesis that the result is true for all $p-$groups of order $\leq p^{n-1}$. Then $H/\langle z \rangle$ has a subgroup $K/\langle z \rangle$ of order p^b such that p^b divides p^{n-1} and $|K/\langle z \rangle| = p^b$, $b = 0, ..., n-1$ and $K/\langle z \rangle \trianglelefteq G/\langle z \rangle$. But then $K \trianglelefteq G$ and $K \leq H$. Also $|K| = p^{b+1}$ such that $1 \leq b+1 \leq n$ or $0 \leq b \leq n-1$. This completes the proof. □

Corollary 0.31. *Every $p-$group is solvable.*

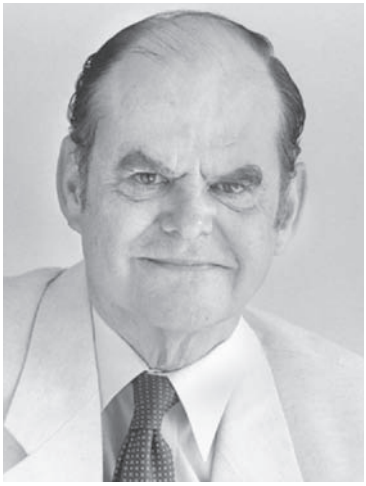
Proof. Let $|G| = p^n$ for some prime p. By theorem 0.30 G has a normal subgroup of order p^α for all $0 \leq \alpha \leq n-1$. Let these subgroups be $1 = H_0, H_1, ..., H_n = G$ with orders $1, p, ..., p^n$ respectively. Then the sequence of subgroups

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G$$

is a normal series whose factors are cyclic of prime orders, hence it is a solvable series. Therefore G is solvable. □

We now list some **difficult to prove** results on solvable groups as the following theorem

Theorem 0.32.
1. **Burnside.** *If $|G| = p^a q^a$, p, q primes, then G is solvable.*
2. **Hall.** *If $|G| = p^\alpha m$, $\gcd(p, m) = 1$, and G has subgroup of order m then G is solvable.*
3. **Feit-Thompson.** *All finite groups of odd order are solvable.*



John G. Thompson was born on October 13, 1932, in Ottawa, Kansas. In 1951, he joined divinity in the Yale University but switched his career to to study mathematics. In 1955, he earned his Ph.D. from University of Chicago. In his dissertation, he verified a 50-year-old conjecture about finite groups possessing a certain kind of automorphism. The proof of the Feit-Thompson Theorem (1963) filled an entire issue of the Pacific Journal of Mathematics, 255 pages in all. This result provided the machinery to classify the finite simple groupsthat is, a program to discover all finite simple groups and prove that there are no more to be found.
The assimilation and extension of Thompsons methods by others throughout the 1960s and 1970s ultimately led to the classification of finite simple groups.
Among Thompsons many honors are the Cole Prize in algebra and the **Fields Medal** **which is amongst the highest awards for mathematical achievements and is given at the opening session of the International Congress of Mathematicians held once every four years.** Unfortunately, no Indian could win a Fields medal till date. The Ramanujan could have won one for us if the award could have started during his time!
He was elected to the National Academy of Sciences in 1967, the Royal Society of London in 1979, and the American Academy of Arts and Sciences in 1998. In 2000, President Clinton presented Thompson the National Medal of

Science. In 2008 he was a co-winner of the $\$1,000,000$ **Abel Prize** given by the Norwegian Academy of Science and Letters.
For more about Thompson, visit:
`http://www-groups.dcs.st-and.ac.uk/~history/`

References:

[1] D.S. Dummit and R.M. Foote. *Abstract Algebra*, John Wiley (2007).

[2] Surjeet Singh and Q. Zameeruddin, *Modern Algebra*, Vikas Pub. Eighth Ed. (2009).

[3]* Joseph A. Gallian. *Contemporary Abstract Algebra.* Brooks/Cole Pub. 7th Ed. (2010).

[4] Book by Gallian is an excellent text in abstract algebra which is full of motivation, applications, and historical development of the subject. Therefore this book is strongly recommended.

[5] W. Feit and J. G. Thompson, Solvability of Groups of Odd Order, *Pacific Journal of Mathematics* **13** (1963), 775-1029.

Exercises

1. Let P be a group and d_P :=minimum number of generators of P. Also define $m_P = \max_{A \leq P}(d_P)$ where A is abelian subgroup of P. Define the **Thompson subgroup** J_P of P by

   $$J_P := \langle A \mid d_A = m_P \rangle .$$

   Determine Thompson subgroup of D_8.

2. Let $n \geq 3,\ n \neq 6$ be a positive integer.

   (a) Prove that for each $\sigma \in \mathrm{Aut}(G)$ and each conjugacy class $\mathcal{O}_x$ of G, $\sigma(\mathcal{O}_x)$ is also a conjugacy class of G.

   (b) Let $\mathcal{O}_x$ be a conjugacy class of transpositions in S_n and $\mathcal{O}'_x$ be the conjugacy class of any element of S_n which is not a transposition. Prove that $|\mathcal{O}_x| \neq |\mathcal{O}'_x|$.

   (c) Prove that for each $\sigma \in \mathrm{Aut}(S_n)$, $\sigma((1\ i))) = (a\ \ b_i)$ for some distinct $a, b_2, b_3, ..., b_n \in \{1, 2, ..., n\},\ i = 2, ..., n$.

   (d) Show that $S_n = \langle (1,2), (1,3), ..., (1,n) \rangle$ and deduce that any automorphism of S_n is uniquely determined by its action on these elements.

   (e) Use (2c) to show that S_n has at most $n!$ automorphisms and conclude that $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n),\ n \neq 6$.

3. Prove that $\mathrm{Aut}(Q_8) \cong S_4$. (Note that $Q_8 = \langle i, j \rangle$)

4. Prove that $\mathrm{Aut}(D_8) \cong D_8$.

5. Show that every group of order 112 contains a proper nontrivial normal subgroup.

6. Show that a group of order 120 is not simple.

7. Prove that if G is a finite group and H is a proper normal subgroup of G of largest order, then G/H is simple.

8. Prove that the only nontrivial normal subgroup of S_5 is A_5.

9. Show that A_5 is the only simple group of order 60. (See for proof Dummit and Foote [1])

10. Prove that a simple group can not have a subgroup of index 4.

11. Prove that the alternating group A_4 does not have a subgroup of index 6.

12. Let $H = \{(1), (12)\}$ and $K = \{(1), (123), (132)\}$ are two subgroups of S_4. Check that neither of these is normal in S_4. However establish that $HK = KH$ i.e. $HK \leq S_4$.

13. For $n = 3, 4, ...$ prove that every element of the alternating group A_n can be written as a product of $3-$cycles.

14. If any normal subgroup H of $A_n,\ n \geq 5$ contains a $3-$cycle then prove that $H = A_n$.

15. If any normal subgroup H of $A_n,\ n \geq 5$ contains a $2-$cycle then prove that $H = A_n$.