

Abstract Algebra

Questions and Solutions on Permutation Group

P. Kalika* & K. Munesh†

August 13, 2015

Questions related to Permutation Group

1. Illustrate Cayley's Theorem by calculating the left regular representation for the group $V_4 = \{e, a, b, c\}$ where $a^2 = b^2 = c^2 = e, ab = ba = c, ac = ca = b, bc = cb = a$.
2. Show that A_5 has 24 elements of order 5, 20 elements of order 3, and 15 elements of order 2.
3. Show that if $n \geq m$ then the number of m -cycles in S_n is given by $n(n-1)(n-2)\dots(n-m+1)/m$.
4. Let σ be the m -cycle $(12\dots m)$. Show that σ^i is also an m -cycle if and only if i is relatively prime to m .
5. Let $n \geq 3$. Prove the following in S_n .
 - (a) Every permutation of S_n can be written as a product of at most $n-1$ transpositions.
 - (b) Every permutation of S_n that is not a cycle can be written as a product of at most $n-2$ transpositions.
6. Let σ be a permutation of a set A . We say that σ moves $a \in A$ if $\sigma(a) \neq a$. Let S_A denote the permutations on A .
 - (a) If A is a finite set then how many elements are moved by a n -cycle $\sigma \in S_A$?

*E-mail: klkaprsd@gmail.com, M.Sc Tech Mathematics, Central University of Rajasthan

†M.Sc Mathematics, Central University of Rajasthan

- (b) Let A be an infinite set and let H be the subset of S_A consisting of all $\sigma \in S_A$ such that σ only moves finitely many elements of A . Show that $H \leq S_A$.
- (c) Let A be an infinite set and let K be the subset of S_A consisting of all $\sigma \in S_A$ such that σ moves at most 50 elements of A . Is $K \leq S_A$? Why?
7. Show that if σ is a cycle of odd length then σ^2 is a cycle.
8. Let p be a prime. Show that an element has order p in S_n if and only if its cycle decomposition is a product of commuting p -cycles. Show by an explicit example that this need not be the case if p is not prime.
9. Show that if $n \geq 4$ then the number of permutations in S_n which are the product of two disjoint 2-cycles is $n(n-1)(n-2)(n-3)/8$.
10. Let $b \in S_7$ and suppose $b^4 = (2143567)$. Find b .
11. Let $b = (123)(145)$. Write b^{99} in disjoint cycle form.
12. Find three elements σ in S_9 with the property that $\sigma^3 = (157)(283)(469)$.
13. Show that if H is a subgroup of S_n , then either every member of H is an even permutation or exactly half of the members are even.
14. Suppose that H is a subgroup of S_n of odd order. Prove that H is a subgroup of A_n .
15. Prove that the smallest subgroup of S_n containing (12) and $(12\dots n)$ is S_n . In other words, these generate S_n .
16. Prove that for $n \geq 3$ the subgroup generated by the 3-cycles is A_n .
17. Prove that if a normal subgroup of A_n contains even a single 3-cycle it must be all of A_n .
18. Prove that A_5 has no non-trivial proper normal subgroups. In other words show that A_5 is a simple group.
19. Show that $Z(S_n)$ is trivial for $n \geq 3$.
20. Show that two permutations in S_n are conjugate if and only if they have the same cycle structure or decomposition. Given the permutation $x = (12)(34)$, $y = (56)(13)$, find a permutation a such that $a^{-1}xa = y$.

Solution of above problems

1. Illustrate Cayley's Theorem by calculating the left regular representation for the group $V_4 = \{e, a, b, c\}$ where $a^2 = b^2 = c^2 = e, ab = ba = c, ac = ca = b, bc = cb = a$.

Solution :

Let $V_4 = \{e, a, b, c\}$. Now computing the permutation σ_g induced by the action of left-multiplication by the group element a.

$$a.e = ae = a \text{ and so } \sigma_g(e) = a$$

$$a.a = aa = a^2 = e \text{ and so } \sigma_g(a) = e$$

$$a.b = ab = c \text{ and so } \sigma_g(b) = c$$

$$a.c = ac = b \text{ and so } \sigma_g(c) = b$$

Hence $\sigma_a = (ea)(bc)$.

Now computing σ_g induced by the action of left-multiplication by the group element b.

$$b.e = be = b \text{ and so } \sigma_g(e) = b$$

$$b.a = ba = c \text{ and so } \sigma_g(a) = c$$

$$b.b = bb = b^2 = e \text{ and so } \sigma_g(b) = e$$

$$b.c = bc = a \text{ and so } \sigma_g(c) = a$$

Hence $\sigma_b = (eb)(ac)$.

Similarly Computing σ_g induced by the action of left-multiplication by the group element c.

$$c.e = ce = c \text{ and so } \sigma_g(e) = c$$

$$c.a = ca = b \text{ and so } \sigma_g(a) = b$$

$$c.b = cb = a \text{ and so } \sigma_g(b) = a$$

$$c.c = cc = c^2 = e \text{ and so } \sigma_g(c) = e$$

Hence $\sigma_c = (ec)(ab)$.

Which explicitly gives the permutation representation $V_4 \rightarrow V_4$ associated to this action.

2. Show that A_5 has 24 elements of order 5, 20 elements of order 3, and 15 elements of order 2.

Solution :

Since we can decompose any permutation into a product of disjoint cycle. In S_5 , since disjoint cycle commutes. Let $V_5 = \{e, a, b, c, d\}$ Here an element of S_5 must have one the following forms:

(i) $(abcde)$ - even

(ii) $(abc)(de)$ - odd (even P * odd P)

(iii) (abc) - even

(iv) $(ab)(cd)$ - even (odd P * odd P)

(v) (ab) - odd

(vi) (e) -even

So element of A_5 is of the form (i), (iii), (iv) and (vi). As we know that, when a permutation is written as disjoint cycles, it's order is the lcm (least common multiple) of the lengths of the cycles.

(i) $(abcde)$ has order 5

(iii) (abc) has order 3

(iv) $(ab)(cd)$ has order 2

(vi) (e) has order 1

Now since elements of order 5 in A_5 are of the form (i). There are $5!$ distinct expression for cycle of the form $(abcde)$ where all a, b, c, d, e are distinct. since expression representation of the element of type

$(abcde) = (bcdea) = (cdeab) = (deabc) = (eabcd)$ are equivalent. So total elements of order 5 are $\frac{5 \times 4 \times 3 \times 2 \times 1}{5} = 24$.

Now for elements of order 3. Since elements of order 3 in A_5 is of the form (abc) . Here there are 5 choices for a, 4 choices for b and 3 choices for c. so there are $5 \times 4 \times 3 = 60$ possible ways to write such a cycle. Since expression representation of the element of type $(abc) = (bca) = (cab)$ are equivalent. So total no. of elements of order 3 in A_5 are $\frac{60}{3} = 20$.

Here since even permutation of order 2 are of the form $(ab)(cd)$. so there are $5 \times 4 \times 3 \times 2$ ways to write such permutation. Since disjoint cycles commute there, so there are 8 different ways that differently represent the same permutations :-

$(ab)(cd) = (ab)(dc) = (ba)(dc) = (ba)(cd) = (cd)(ab) = (dc)(ab) = (dc)(ba) = (cd)(ba)$.

So there are $\frac{5 \times 4 \times 3 \times 2}{8} = 15$ elements of order 2.

{No. of ways of selecting r different things out of n is nPr }

3. Show that if $n \geq m$ then the number of m -cycles in S_n is given by $\frac{n(n-1)(n-2)\dots(n-m+1)}{m}$.

Proof :

For any given S_n , there are n elements in $S_n = \{1, 2, 3, \dots, m, \dots, n\}$. so we must have n-choices for 1st element, then n-1 choices for 2nd element, n-2 choices for 3rd element and so on... and we have n-m+1 choices for m^{th} element etc. So there are total no. of $n(n-1)(n-2)\dots(n-m+1)$ for a m-cycles.

Now we want to count m-cycles in S_n , since for 2-cycles $(ab) = (ba)$

{two equivalent notation , i.e same permutation}

For 3-cycles $(a, b, c) = (b, c, a) = (c, a, b)$ {i.e 3-equivalent notation}

For 4-cycles $(a, b, c, d) = (b, c, d, a) = (c, d, a, b) = (d, a, b, c)$ {four equivalent notation}

Similarly for m-cycles there are m-equivalent notation for any permutations.

Now, Since we have, $n(n-1)(n-2)\dots(n-m+1)$ choices to form a m-cycle in which there are m-equivalent notations for any permutation of length m.

So the no. of m-cycles in S_n is

$$\frac{n(n-1)(n-2)\dots(n-m+1)}{m}$$

4. Let σ be the m -cycle $(12\dots m)$. Show that σ^i is also an m -cycle if and only if i is relatively prime to m .

Proof :

First we note that if τ is k cycle then $|\tau| = k$
since $\sigma^i(x) \equiv x+i \pmod m$ for any x , $1 \leq x \leq m$

Claim : $\sigma^i = (\sigma^i(1)\sigma^i(2)\dots\sigma^i(m))$

we prove it by contradiction

Let $i=1$. Then the statement is obviously true.

Suppose that

$$\sigma^{i-1} = (\sigma^{i-1}(1)\sigma^{i-1}(2)\dots\sigma^{i-1}(m))$$

then $\sigma^i = \sigma(\sigma^{i-1}) = \sigma\{\sigma^{i-1}(1)\dots\sigma^{i-1}(m)\}$

Since, here σ sends $\sigma^{i-1}(i)$ to $\sigma^i(1)$,

thus $\sigma^i = (\sigma^{i-1}(1)\dots\sigma^i(m))$

$\implies \sigma^i = (\sigma^{i-1}(1)\dots\sigma^i(m))$

Since $\sigma^i(m) \equiv m+i \pmod m \equiv i \pmod m$ and $\sigma^{i-1}(1) \equiv 1+i-1 \pmod m \equiv i \pmod m$

i.e $\sigma^i(m) = \sigma^{i-1}(1)$

$\implies \sigma^i$ is an m -cycle.

Converse part

Suppose σ^i is an m -cycle and suppose that $(i, m) = d > 1$. (we prove it by contradiction)

then there exists $k, n \in \mathbb{N}$ such that $i=kd$ and $m=nd$,

since, $(\sigma^i)^n = (\sigma^{kd})^n = \sigma^{kdn} = \sigma^{mk} = (\sigma^m)^k = I$

where I is the identity permutation.

Hence $|\sigma^i| \leq n < m$.

which is contradiction, since σ^i is an m -cycle and thus $|\sigma^i| = m$. Thus i is relatively prime to m .

5. **Que. No.05** Let $n \geq 3$. Prove the following in S_n .

- Every permutation of S_n can be written as a product of at most $n - 1$ transpositions.
- Every permutation of S_n that is not a cycle can be written as a product of at most $n - 2$ transpositions.

Proof (a) :

We know that if $k \geq 2$, the cycle (a_1, a_2, \dots, a_k) can be written as $(a_1, a_k)(a_1, a_{k-1}) \dots (a_1, a_2)$ which is $k-1$ transpositions.

Case-I, If $k=1$, then this cycle is the trivial cycle or the identity, which can be written as $1-1=0$ transpositions

Case-II, if $k > 1$,

we know that every permutation $\sigma \in S_n$ can be written as a product of disjoint cycles, thus we can write

$$\sigma = (a_{11}, a_{12}, \dots, a_{1k_1})(a_{21}, a_{22}, \dots, a_{2k_2}) \dots (a_{m1}, a_{m2}, \dots, a_{mk_m})$$

where $k_1 + k_2 + \dots + k_m = n$ and each of these cycle is disjoint.

we know that cycle i can be written as a product of $k_i - 1$ transpositions, and $\sum_{i=1}^m (k_i - 1) = \sum_{i=1}^m k_i - \sum_{i=1}^m 1 = n - m$, this is maximized when m is minimized and the least value of m is 1.

Thus, the largest value of $n-m$ can be $n-1$.

Proof (b) :

From part (a), $\sigma = (a_{11}, a_{12}, \dots, a_{1k_1})(a_{21}, a_{22}, \dots, a_{2k_2}) \dots (a_{m1}, a_{m2}, \dots, a_{mk_m})$ where $\sum_{i=1}^m k_i = n$ and each of cycles is disjoint and also from (a), we still know that cycles i can be written as a product of $k_i - 1$ transpositions and

$\sum_{i=1}^m (k_i - 1) = \sum_{i=1}^m k_i - \sum_{i=1}^m 1 = n - m$, However, since σ is not a cycle. $m \geq 2$, thus $n-m$ is maximized when m is minimized i.e $m=2$ i.e $n-2$ is the maximum value of $n-m$.

Hence every permutation of S_n that is not a cycle can be written as a product of at most $n-2$ transpositions.

6. **Que. No.06** Let σ be a permutation of a set A . We say that σ moves $a \in A$ if $\sigma(a) \neq a$. Let S_A denote the permutations on A .

- If A is a finite set then how many elements are moved by a n -cycle $\sigma \in S_A$?
- Let A be an infinite set and let H be the subset of S_A consisting of all $\sigma \in S_A$ such that σ only moves finitely many elements of A . Show that $H \leq S_A$.
- Let A be an infinite set and let K be the subset of S_A consisting of all $\sigma \in S_A$ such that σ moves at most 50 elements of A . Is $K \leq S_A$? Why?

Proof (a):

If A is finite, then σ moves only n elements because σ is n -cycle and the elements

which is not in cycle are fixed.

Proof (b):

We may prove it by One-Step Subgroup Test.

As A is infinite set and $\sigma \in S_A$ moves only finitely many elements of A . Since H consists all $\sigma \in S_A$

$\Rightarrow H$ is non-empty.

Now let, $\sigma \in H \implies \sigma^{-1} \in H$.

So, $\sigma\sigma^{-1} = I \in H$

Now checking for closure property,

Let σ_1 and $\sigma_2 \in H$ be any two permutations such that σ_1 and σ_2 both moves only finitely many elements of A .

Then $\sigma_1\sigma_2$ also moves only finitely many elements of A .

\Rightarrow Closure property holds.

$\Rightarrow H$ is subgroup of A_5 .

Proof (c):

No, K will not be subgroup of S_A

Because, suppose that σ_1 moves at most 50 elements and σ_2 moves at most 50 elements, then $\sigma_1\sigma_2$ (Product of two permutations) might moves more than 50 elements.

\Rightarrow Closure property with respect to function composition is not satisfied in K .

$\Rightarrow K$ is not a subgroup of S_A .

7. **Que. No.07** Show that if σ is a cycle of odd length then σ^2 is a cycle.

Proof : Suppose $\sigma : A \rightarrow A$ is a cycle with odd length. Then we can write σ in a cycle notation as σ

$\sigma = (a_1, a_2, \dots, a_{2k+1})$ where $a_1, a_2, \dots, a_{2k+1} \in A$

On simple calculation, we may show that

$$\sigma^2 = (a_1, a_2, \dots, a_{2k+1})(a_1, a_2, \dots, a_{2k+1})$$

$$\sigma^2 = (a_1, a_3, a_5, \dots, a_{2k+1}, a_2, a_4, \dots, a_{2k})$$

$\implies \sigma^2$ is cycle whenever σ is cycle.

8. **Que. No.08** Let p be a prime. Show that an element has order p in S_n if and only if its cycle decomposition is a product of commuting p -cycles. Show by an explicit example that this need not be the case if p is not prime.

Proof :

\Rightarrow Suppose the order of σ is p (p is prime).

Since order of σ is the lcm of the sizes of the disjoint cycles in the cycle decomposition of σ , So all of these cycle must have sizes that divides p is either 1 or p .

Since 1-cycles are omitted from the notation for the cycle decomposition of σ . Thus the cycle decomposition consists entirely of p -cycles. Thus σ is the product of disjoint commuting p -cycles.

\Leftarrow Suppose σ is the product of disjoint p -cycles. i.e $\sigma = c_1 c_2 c_3 \dots c_r$

then $\sigma^p = (c_1 c_2 c_3 \dots c_r)^p = c_1^p c_2^p c_3^p \dots c_r^p = 1$

(since the p^{th} power of p -cycles in σ are all 1, so their product is 1)

$\sigma^p = 1$

A p -cycle has order p , so no smaller power of σ can be 1. Hence $|\sigma| = p$.

For an example :

Showing these conclusions may fail when p is not a prime.

Let $p=6$, $\sigma = (12)(345)$

$|\sigma| = \text{lcm}(2, 3) = 6$

but σ is not the product of commuting 6-cycles.

9. **Que. No.09** Show that if $n \geq 4$ then the number of permutations in S_n which are the product of two disjoint 2-cycles is $n(n-1)(n-2)(n-3)/8$.

Solution :

Given $n \geq 4$.

Since, Permutations which are the product of two disjoint 2-cycles is of the form $(ab)(cd)$, i.e of length 4.

Hence, there are n choices for a , $(n-1)$ choices for b , $(n-2)$ choices for c and $(n-3)$ choices for d .

So there are $n(n-1)(n-2)(n-3)$ possible ways to write to write such a cycle. Since disjoint cycles commutes there, so there are 8 different ways that differently represent the same cycle(As i mentioned it in sol. of Que.2)

Hence total number of Permutation in S_n which are the product of two disjoint

2-cyles is $\frac{(n)(n-1)(n-2)(n-3)}{8}$.

10. **Que. No.10** Let $b \in S_7$ and suppose $b^4 = (2143567)$. Find b .

Solution :

$$\because b \in S_7$$

$$|b| = 7$$

$$\Rightarrow b^7 = I$$

$$\text{So } b = Ib = (b^7).b = b^8 = (b^4)^2$$

$$\Rightarrow b = b^4.b^4$$

$$\begin{aligned} \Rightarrow b &= (2143567)(2143567) \\ &= (2457136). \end{aligned}$$

As given that $b^4 = (2143567)$.

11. **Que. No.11** Let $b = (123)(145)$. Write b^{99} in disjoint cycle form.

Solution :

Since $b = (123)(145) = (14523)$. So order of b is 5.

(In case of single cycle. The order of permutation is the degree of permutation is the lengths of the set.)

Now since $|b| = 5$, then $b^5 = I$.

So we can write $b^{99} = (b^5)^{19} \cdot b^4 = Ib^4 = b^4 = b^{-1}$.

Since $b = (14523) \Rightarrow b^4 = b^{-1} = (32541) = (132541)$

so $b^{99} = (13254)$ or $(154)(132)$.

12. **Que. No.12** Find three elements σ in S_9 with the property that $\sigma^3 = (157)(283)(469)$.

Solution :

Let $1 = a_1, 2 = a_2, 3 = a_3, 4 = a_4, 5 = a_5, 6 = a_6, 7 = a_7$ and $8 = a_8$.

Now we have to find σ such that $\sigma^3 = (a_1 a_5 a_7)(a_2 a_8 a_3)(a_4 a_6 a_9)$

then $\sigma_1 = (a_1 \dots a_5 \dots a_7 \dots)$

$\sigma_1 = (a_1 a_2 \dots a_5 a_8 \dots a_7 a_3 \dots)$

$\sigma_1 = (a_1 a_2 a_4 a_5 a_8 a_6 a_7 a_3 a_9)$

$\sigma_1 = (1 2 4 5 8 6 7 3 9)$.

Similarly we can find other two elements

$\sigma_2 = (a_1 \dots a_5 \dots a_7 \dots)$

$\sigma_2 = (a_1 a_3 \dots a_5 a_2 \dots a_7 a_8 \dots)$

$\sigma_2 = (a_1 a_3 a_9 a_5 a_2 a_4 a_7 a_8 a_6)$

$\sigma_2 = (1 3 9 5 2 4 7 8 6)$.

and

$\sigma_3 = (a_2 \dots a_8 \dots a_3 \dots)$

$\sigma_3 = (a_2 a_1 a_4 a_8 a_5 a_6 a_3 a_7 a_9)$

$\sigma_3 = (2 1 4 8 5 6 3 7 9)$.

13. **Que. No.13** Show that if H is a subgroup of S_n , then either every member of H is an even permutation or exactly half of the members are even.

Solution :

Let $H \subset S_n$ be any subgroup.

Now, we define $\overline{H} = \{\sigma \in H \mid \sigma \text{ is even}\}$

Claim: \overline{H} is subgroup of H .

Let $f, g \in \overline{H}$, Since f, g are even, so f^{-1} is also even.

since the product of even permutations are still even, so we have $f \circ g^{-1}$ is even.

So, here there are only two possibilities either $\overline{H} = H$ or $\overline{H} \subsetneq H$

Case-I, if $\overline{H} = H$, then we are done.

Case-II, if $\overline{H} \neq H$, then we need to show that $|\overline{H}| = \frac{|H|}{2}$

Since $\overline{H} \neq H$, it implies that there exists at least one odd permutations $\sigma \in H$

Now consider $f: \overline{H} \rightarrow \frac{H}{H}$ defined by $f(h) = \sigma.h$ for any $h \in \overline{H}$.

since σ is odd and h is even

$\Rightarrow \sigma.h$ is odd.

$\Rightarrow \sigma.h \in \frac{H}{H}$

To prove that $\overline{H} = \frac{|H|}{2}$, We need to prove f is 1-1 and onto.

for 1-1

let $h_1, h_2 \in H$ such that $h_1 = h_2$.

since $h_1 = h_2$

$\Rightarrow \sigma h_1 = \sigma h_2 \Rightarrow f(h_1) = f(h_2) \Rightarrow f$ is 1-1.

and for onto

since $f^{-1}: \frac{H}{H} \rightarrow \overline{H}$ is given by $f^{-1}(h) = \sigma^{-1}h'$ for every $h' \in \frac{H}{H}$.

So f is both 1-1 and onto

$\Rightarrow |\overline{H}| = \left| \frac{H}{H} \right|$, hence $|\overline{H}| = \frac{|H|}{2}$

14. **Que. No.14** Suppose that H is a subgroup of S_n of odd order. Prove that H is a subgroup of A_n . rate S_n .

Proof :

Let H be a subgroup of S_n of odd order.

i.e $|H| = \text{odd order}$

We may prove it by contradiction.

To the contrary, suppose $H \not\subseteq A_n$, then

suppose $\exists \sigma \in H$ such that σ is an odd permutation.

Let $H = \underbrace{\{\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_p\}}_{\text{Odd}} \cup \underbrace{\{\beta_1, \beta_2, \beta_3, \dots, \beta_q\}}_{\text{Even}}$

$\therefore \sigma H = \underbrace{\{\sigma\alpha_1, \sigma\alpha_2, \sigma\alpha_3, \dots, \sigma\alpha_p\}}_{\text{Even}} \cup \underbrace{\{\sigma\beta_1, \sigma\beta_2, \sigma\beta_3, \dots, \sigma\beta_q\}}_{\text{Odd}}$

$= H$

$\implies p = q$

$\implies |H| = 2p = 2q = \text{even}$

Which is a contradiction.

$\implies H \subset A_n$

15. **Que. No.15** Prove that the smallest subgroup of S_n containing (12) and $(12 \dots n)$ is S_n . In other words, these generate S_n .

Proof :

Let $\sigma = (12)$ and $\tau = (123 \dots n)$

Suppose H is subgroup of S_n which contains both $\sigma = (12)$ and $\tau = (123\dots n)$.

Now, we need to show that $H = S_n$.

Clearly, we have $H \subseteq S_n$. Since subgroups in particular are subsets.

Since we know that S_n is generated by (n-1) transpositions $(12)(23)(34)(45)\dots(n-1\ n)$.

Now, I want to show that (12) and $(123\dots n)$ generates these (n-1) transposition.

Consider, $\tau\sigma\tau^{-1}$

$$(12\dots n)(12)(12\dots n)^{-1} = (23)$$

$$(12\dots n)(23)(12\dots n)^{-1} = (34)$$

$$(12\dots n)(34)(12\dots n)^{-1} = (45)$$

.....

$$(12\dots n)(n-2\ n-1)(12\dots n)^{-1} = (n-1\ n)$$

$$(12\dots n)(n-1\ n)(12\dots n)^{-1} = (n\ 1)$$

Now i prove it by induction...

for $n = 1$, it is obviously true.

We assume that it is true for $n = k$, then

$$(12\dots k)(k-1\ k)(12\dots k)^{-1} = (k\ 1)$$

Now, we wish to show that it is true for $n = k+1$

$$(1, 2, \dots, k, k+1)(k, k+1)(1, 2, \dots, k, k+1)^{-1}$$

$$= (1, 2, \dots, k, k+1)(k+1, k)(k+1, k, \dots, 3, 2, 1)$$

$$= 6(1, 2, \dots, k, k+1)(k+1)(k, \dots, 3, 2, 1)$$

$$= (1, 2, \dots, k, k+1)(k, \dots, 3, 2, 1)$$

$$= (k)(k-1)\dots(3)(2)(1)(1, k+1)$$

$$= (k+1, 1)$$

So, it is true for $n=k+1$

$\Rightarrow (12)$ and $(123\dots n)$ generates S_n

Which shows that $S_n \subseteq H$.

Thus $h = S_n$

16. **Que. No.16** Prove that for $n \geq 3$ the subgroup generated by the 3-cycles is A_n .

Proof :

Since every 3-cycle is an even permutation, then every 3-cycle of S_n is in A_n .

Now, Let $\tau \in A_n \Rightarrow \tau$ is an even permutation.

$\Rightarrow \tau$ is a product of an even no. of transposition.

However, $(a_1a_2)(a_3a_4) = (a_1a_2a_3)(a_2a_3a_4)$

And $(a_1a_2)(a_1a_3) = (a_1a_3a_2)$

Consequently, every product of two transposition(whether they share an element or not) can be written as a product of 3-cycles.

Hence, τ can be written as a product of 3-cycles.

\Rightarrow For any $n \geq 3$, the subgroup generated by 3-cycle is A_n .

17. **Que. No.17** Prove that if a normal subgroup of A_n contains even a single 3-cycle

it must be all of A_n .

Proof :

Let $N \subset A_n$ be Normal subgroup and suppose that $(abc) \in N$. Let $\sigma' \in A_n$ be an arbitrary 3-cycles.

Then $\sigma' = \tau(abc)\tau^{-1}$ for some $\tau \in S_n$.

Now here, there are two possibility either $\tau \in A_n$ or $\tau \notin A_n$.

Case -I, If $\tau \in A_n$ then $\sigma' \in N$ and we are done.

Case -II, If $\tau \notin A_n$ then $\tau' = \tau(ab)$ is in A_n and $\tau' = \tau(acb)\tau'^{-1}$ is once again in N .

\Rightarrow If $N \subseteq A_n$ and contains a 3-cycle. Then $N=A_n$.

18. **Que. No.18** Prove that A_5 has no non-trivial proper normal subgroups. In other words show that A_5 is a simple group.

Solution :

Order of $A_5 = |A_5| = \frac{5!}{2} = 60 = 2^2 \cdot 3 \cdot 5$.

Let N be proper normal subgroup of A_5 , then

$|N| = 2, 3, 4, 5, 6, 10, 12, 15, 20, 30$.

Total no. of 5 order elements in $A_5 = \frac{{}^5P_5}{5} = 24$,

Total no. of elements of 3 order in $A_5 = \frac{{}^5P_3}{5} = 20$,

And total no. of 15-order elements in $A_5 = 0$.

Let us assume that $|H| = 3, 6, 12, 15$

then $|\frac{A_5}{H}| = 20, 10, 5, 4$

so $\gcd\left(3, |\frac{A_5}{H}|\right) = 1$

\Rightarrow H would contain all 20 elements of order 3.

Which is a contradiction.

{ As, Theorem says that If H be Normal subgroup of a finite group G . And if

$\gcd\left(|x|, |\frac{G}{H}|\right) = 1$, then $x \in G$ }.

Similarly, suppose that $|H| = 5, 10, 20$

then $|\frac{A_5}{H}| = 12, 6, 3$

\Rightarrow H would contain all 24 elements of order 5.

which is a contradiction.

Let $|H| = 30$, then $|\frac{A_5}{H}| = 2$.

So again $\gcd\left(3, |\frac{A_5}{H}|\right) = 1$ and $\gcd\left(5, |\frac{A_5}{H}|\right) = 1$.

\Rightarrow H would contain all $20+24 = 44$ elements.

we get again a contradiction.

And finally, let us assume that, $|H|= 2$ or 4 .

$$\implies \left| \frac{A_5}{H} \right| = 30, 15$$

Since, we know that any group of order 30 or 15 has an element of order 15.

or As, if $\left| \frac{A_5}{H} \right| = 15 = 3 \times 5 = p \times q$ where $p=3$ and $q=5$.

(Theorem : If G is a group of order pq , where p and q are primes, $p < q$ and $p \nmid q$, then G is cyclic.)

$\Rightarrow G$ has at least one element of order 15.

Which is again contradiction,

because A_5 contains no such element, neither does $\frac{A_5}{H}$.

This proves that A_5 is simple.

19. **Que. No.19** Show that $Z(S_n)$ is trivial for $n \geq 3$.

Solution :

Let $\sigma \in S_n$ be a non-identity element then there exists two distinct $a, b \in \{1, 2, 3, \dots, n\}$ with $\sigma(a) = b$.

Since $n \geq 3$, Now choosing $k \in \{1, 2, 3, \dots, n\}$ such that $k \neq a$ and $k \neq b$.

Let $\tau = (ak)$. Then

$$\tau(\sigma(a)) = \tau(b) = k \text{ and } \sigma(\tau(a)) = \sigma(a) = b$$

$$\text{since } k \neq b \Rightarrow \tau(\sigma(a)) \neq \sigma(\tau(a)).$$

Hence for every non-identity permutation in S_n , there exists some element not commuting with it.

Therefore $Z(S_n)$ must be trivial.

20. **Que. No. 20** Show that two permutations in S_n are conjugate if and only if they have the same cycle structure or decomposition. Given the permutation $x = (12)(34)$, $y = (56)(13)$, find a permutation a such that $a^{-1}xa = y$.

Proof :

For any σ and any $d \leq n$, we have

$$\sigma(12\dots d)\sigma^{-1} = (\sigma(1)\sigma(2)\dots\sigma(d))$$

This shows that any conjugate of d -cycle is again d -cycle.

Since every permutation is a product of disjoint cycles, it follows that the cycle structure of conjugate permutations are the same.

In other direction,

Let $\tau = (a_1a_2\dots a_r)(a_{r+1}a_{r+2}\dots a_s)\dots(a_l\dots a_m)$ and

$$\tau' = (a'_1a'_2\dots a'_r)(a'_{r+1}a'_{r+2}\dots a'_s)\dots(a'_l\dots a'_m)$$

be two permutations having the same cycle structure.

Define $\sigma \in S_n$ by $\sigma(a'_i) = a_i$ for $i = 1, 2, \dots, m$ then

$$\sigma\tau\sigma^{-1} = \sigma(a_1a_2\dots a_r)\sigma^{-1}\sigma(a_{r+1}a_{r+2}\dots a_s)\sigma^{-1}\dots\sigma(a_l\dots a_m)\sigma^{-1}$$

$$= (a'_1a'_2\dots a'_r)(a'_{r+1}a'_{r+2}\dots a'_s)\dots(a'_l\dots a'_m)$$

$$= \tau'$$

This shows that τ and τ' are conjugate.

Now, Given the permutation $x = (12)(34)$, $y = (56)(13)$

Since that $a^{-1}xa = y$.

$$\therefore xa = ay \Rightarrow x = aya^{-1}.$$

$$\Rightarrow ((12)(34)) = a((56)(13))a^{-1}$$

$$\Rightarrow ((12)(34))(5)(6) = a((56)(13)(2)(4))a^{-1}$$

$$. \qquad \qquad \qquad = (a(5)a(6))(a(1)a(3))a(2)a(4)$$

$$\Rightarrow 1 = a(5), 2 = a(6), 3 = a(1), 4 = a(3) \text{ and } 5 = a(2), 6 = a(4)$$

$$\Rightarrow a = \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 6 & 1 & 2 \end{array}$$

$$\Rightarrow a = (134625)$$

Checking for a, $a = (134625)$ and $a^{-1} = (526431) = (152643)$

$$\therefore a^{-1}xa = (134625)((12)(34))(152643)$$

$$= (13)(2)(4)(56) = (13)(56) = \text{RHS, Hence done.}$$

Acknowledgement

This problem & solution is part of my INSPIRE(DST) summer work, which has been done at Ambekar University, Delhi. I thank my supervisor Prof. Geetha Venkataraman who gave me this opportunity for this summer internship and also for her fruitful guidelines and discussion. I also thank DST(Department of Science and Technology) Govt. of India, India for the financial Grant.

References

- [1] Joseph A. Gallian : *Contemporary Abstract Algebra*, Ch-5, Brooks/Cole, Cengage Learning, ISBN: 978-0-547-16509-7, 7th Ed. (2010)
- [2] VK Khanna & SK Bhamri : *A course in abstract algebra*, 1998
- [3] David S. Dummit & Richard M. Foote : *Abstract Algebra*, Ch-1, John Wiley & Sons, Inc, ISBN: 0-471-43334-9, 3rd Ed. (2004).
- [4] I. N. Herstein : *Topics in Algebra*, John Wiley & Sons, Ch-2, 2nd Ed (1975).
- [5] John B. Fraleigh : *A First Course in Abstract Algebra*