Abstract Algebra Assignment (3): Basic Concepts of Permutations

Mostafa Hassanein

25 November 2023

1.

Proof. We use strong induction on m.

Base case ($m = 1$):

$L.H.S. = (p_1)^{-1} = R.H.S.$

Inductive step ($m > 1$):

We assume P(n) is true for all $1 \leq n \leq m$ and use it to prove P(m+1). For $m + 1$, we have:

$$
\begin{aligned}
L.H.S. = (p_1 \circ p_2 \circ ... \circ p_m \circ p_{m+1})^{-1} &= ((p_1 \circ p_2 \circ ... \circ p_m) \circ p_{m+1})^{-1} \\
&= p_{m+1}^{-1} \circ (p_1 \circ p_2 \circ ... \circ p_m)^{-1} \\
&= p_{m+1}^{-1} \circ (p_m^{-1} \circ p_{m-1}^{-1} \circ ... \circ p_1^{-1}) \quad \text{(Because P(2) is true)} \\
&= p_{m+1}^{-1} \circ p_m^{-1} \circ p_{m-1}^{-1} \circ ... \circ p_1^{-1} \quad \text{(Because P(m) is true)} \\
&= R.H.S.
\end{aligned}
$$

□

2.

Proof. Given a permutation p of n symbols, we can be express the permutation as a product of k disjoint cycles. We can also express any cycle of length l as a product of $l - 1$ transpositions. Therefore, we can express any permutation as a product of t transpositions, where:

$$
\begin{aligned}
t &= \sum_{i=1}^{k} (l_i - 1) \\
&= \sum_{i=1}^{k} l_i - \sum_{i=1}^{k} 1 \\
&= n - k
\end{aligned}
$$

Therefore, $p = t_1 t_2 ... t_(n - k)$.
Adding any pair transpositions that are inverses of each other will leave the permutation the same. So, p can be expressed as $(n - k) + 2a$ transpositions, where $a \in Z^+$. Since adding an even number does not change the parity, then the parity depends only on the value of $n - k$ which is unique to the permutation p.

□

3.

Proof. Since A_n is a subset of S_n, we need only prove that A_n is a subgroup of S_n.

i. Closure: The product 2 even permutations is even, therefore A_n is closed.

ii. Associativity: Associativity is satisfied for S_n so it is also satisfied for A_n.

iii. Identity: The identity permutation can be expressed as a product on n disjoint cycles.
$\Rightarrow$ The identity permutation can be expressed as a product of $n - n = 0$ transpositions.
$\Rightarrow$ The identity permutation is even.
$\Rightarrow$ The identity permutation belongs to A_n.

iv. Inverse: For any permutation $p = p_1 \circ p_2 \circ ... \circ p_m$, we have $p^{-1} = p_m^{-1} \circ p_{m-1}^{-1} \circ ...p_1^{-1}$.
$\Rightarrow$ The inverse of an even permutation is also even.
$\Rightarrow \forall a \in A_n \; \exists a^{-1} : \; a \circ a^{-1} = id.$

i, ii, iii, iv $\Rightarrow A_n$ is a subgroup of S_n.

Next, to show that $|A_n| = n!/2$, it suffices to show that the number of even permutation $|A_n|$ is equal to the number of odd permutations $|B_n|$.

We use the fact that the product of an odd permutation with an even permutation is an odd permutation to construct a bijection from A_n to B_n and thus conclude that they must have the same number of elements.

Let τ be any transposition in S_n (we know that one exists assuming $n > 1$), then τ is an odd permutation; and let $f : A_n \to B_n$ be a function defined as $f(a) = \tau \circ a$.

Injectivity: $f(a_1) = f(a_2) \Rightarrow \tau \circ a_1 = \tau \circ a_2$
$\Rightarrow \tau^{-1} \circ (\tau \circ a_1) = \tau^{-1} \circ (\tau \circ a_2)$
$\Rightarrow (\tau^{-1} \circ \tau) \circ a_1 = (\tau^{-1} \circ \tau) \circ a_2$
$\Rightarrow a_1 = a_2$
$\Rightarrow$ f is injective.

Surjectivity: Let $b \in B_n \Rightarrow (\tau^{-1} \circ b)$ is an even permutation and $f(\tau^{-1} \circ b) = \tau \circ (\tau^{-1} \circ b) = (\tau \circ \tau^{-1}) \circ b = b$
$\Rightarrow$ f is surjective.

f is injective and surjective $\Rightarrow$ f is bijective. $\square$

4.

There are $4! = 24$ permutation for S_4:

$\boldsymbol{P_x}$	$\lvert\boldsymbol{P_x}\rvert$	***Parity***
$P_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = (1)(2)(3)(4)$	1	*Even*
$P_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = (3\ 4)$	2	*Odd*
$P_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} = (2\ 3)$	2	*Odd*
$P_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} = (2\ 3\ 4) = (2\ 3)(2\ 4)$	3	*Even*
$P_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = (2\ 4\ 3) = (2\ 4)(2\ 3)$	3	*Even*
$P_6 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (2\ 4)$	2	*Odd*
$P_7 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (1\ 2)$	2	*Odd*
$P_8 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1\ 2)(3\ 4)$	2	*Even*
$P_9 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = (1\ 2\ 3) = (1\ 2)(1\ 3)$	3	*Even*
$P_{10} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1\ 2\ 3\ 4) = (1\ 2)(1\ 3)(1\ 4)$	4	*Odd*
$P_{11} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = (1\ 2\ 4\ 3) = (1\ 2)(1\ 4)(1\ 3)$	4	*Odd*
$P_{12} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = (1\ 2\ 4) = (1\ 2)(1\ 4)$	3	*Even*
$P_{13} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = (1\ 3\ 2) = (1\ 3)(1\ 2)$	3	*Even*
$P_{14} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = (1\ 3\ 4\ 2) = (1\ 3)(1\ 4)(1\ 2)$	4	*Odd*
$P_{15} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = (1\ 3)$	2	*Odd*
$P_{16} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (1\ 3\ 4) = (1\ 3)(1\ 4)$	3	*Even*
$P_{17} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1\ 3)(2\ 4)$	2	*Even*
$P_{18} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = (1\ 3\ 2\ 4) = (1\ 3)(1\ 2)(1\ 4)$	4	*Odd*
$P_{19} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = (1\ 4\ 3\ 2) = (1\ 4)(1\ 3)(1\ 2)$	4	*Odd*
$P_{20} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} = (1\ 4\ 2) = (1\ 4)(1\ 2)$	3	*Even*
$P_{21} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = (1\ 4\ 3) = (1\ 4)(1\ 3)$	3	*Even*
$P_{22} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} = (1\ 4)$	2	*Odd*
$P_{23} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} = (1\ 4\ 2\ 3) = (1\ 4)(1\ 2)(1\ 3)$	4	*Odd*
$P_{24} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (1\ 4)(2\ 3)$	2	*Even*

The parity of a permutation is the parity of the number of transpositions required to represent the permutation.

The order of a permutation is the smallest positive integer m such that $P^m = I$. It can be computed by first factoring the permutation as a product of disjoint cycles, then the order m of the permutation becomes the L.C.M. of orders of these cycles.

The elements of A_4 are those permutations of S_4 with an even parity, and they form a subgroup of S_4.

5.

i.

Proof. A transposition is a permutation that exchanges 2 elements and leaves all the other elements unchanged. Let τ be a transposition that exchanges the 2 elements x and y, so that x becomes y and y becomes x. When applying τ twice to x, the first application will move x into y and the second application will move y to x, so that x moves to x. Similarly for y, the first application will move y into x and the second application will move x to y, so that y moves to y. This implies that $\tau\tau = I$, which imply that $\tau = \tau^{-1}$

□

ii.

Proof. The identity permutation on n symbols moves each symbol into itself.
$\Rightarrow$ The identity permutation has n disjoint cycles each of length 1.

We also have that any cycle of length n can be expressed as a product of $n-1$ transpositions.
$\Rightarrow$ Any cycle of length 1 can be expressed as a product of 0 transpositions.

$\Rightarrow$ The identity permutation can be written as a product of $n * 0 = 0$ transpositions.
$\Rightarrow$ The identity permutation is an even permutation.

□

7.

i.

$P_1 = (1\ 3\ 5)(2\ 4)(6\ 8\ 7)$
$|P_1| = LCM(3, 2, 3) = 6$

ii.

$P_2 = (1\ 4\ 2)(5\ 6)$
$|P_2| = LCM(3, 2) = 6$

iii.

$P_3 = (1\ 3\ 5\ 8)(2\ 7)(4\ 6\ 9)$
$|P_3| = LCM(4, 2, 3) = 12$

iv.

$P_4 = (1\ 3\ 4)(5\ 7)$
$|P_4| = LCM(3, 2) = 6$

8.

i.

Inversions of $\langle 3, 1, 4, 2\rangle = \{(3, 1), (3, 2), (4, 2)\}$

Inversions of $\langle 1, 2, 4, 5, 6, 7, 8, 3\rangle = \{(4, 3), (5, 3), (6, 3), (7, 3), (8, 3)\}$

Inversions of $\langle 4, 5, 3, 2, 1, 8, 6, 7, 9\rangle = \{(4, 1), (4, 2), (4, 3), (5, 1), (5, 2), (5, 3), (3, 1), (3, 2), (2, 1), (8, 6), (8, 7)\}$