Chapter 3: Permutation Groups

Permutation of a set A

Definition: A permutation of a set A is a function from A to A that is both one-one and onto.

Permutation group of a set A

Definition: A permutation group of a set A is a set of permutations of A that forms a group under function composition.

Examples:

1. If we define a permutaion α of the set $\{1,2,3,4\}$ by $\alpha(1)=2, \alpha(2)=3, \alpha(3)=1, \alpha(4)=4$
we can write this as $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}$

2. Similarly a permuation β on set $\{1,2,3,4,5\}$ can be defined as $\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{bmatrix}$

Note: Since composition of permutation expressed in array notation is carried out from right to left by going from top to bottom.
for example:

3. $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{bmatrix}$ and $\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 1 & 5 \end{bmatrix}$

$\alpha\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 1 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{bmatrix}$

4.Let S_3 denote the set of all one to one functions from $\{1,2,3\}$ to itself. Then the of elements S_3 are
$e = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$ $\alpha = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$ $\alpha^2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$
$\beta = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$ $\alpha\beta = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$ $\alpha^2\beta = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$
Since $\beta\alpha = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = \alpha^2\beta \neq \alpha\beta$
So S_3 is Non-abelian.

5. Let $A = \{1,2,...,n\}$ be the set. The set of all permutation of A is called symmetric group of degree n and it is denoted by S_n.
Since the elements of S_n are of the form $\alpha = \begin{bmatrix} 1 & 2 & . & . & . & n \\ \alpha(1) & \alpha(2) & . & . & . & \alpha(n) \end{bmatrix}$
Note: Order of S_n is $n!$
Since the elements of S_n are of the form $\alpha = \begin{bmatrix} 1 & 2 & . & . & . & n \\ \alpha(1) & \alpha(2) & . & . & . & \alpha(n) \end{bmatrix}$
So for $\alpha(1)$ we have n choices, once $\alpha(1)$ has been determined, there are $n-1$ possibilities for $\alpha(2)$, since α is one one so $\alpha(1) \neq \alpha(2)$
After choosing $\alpha(n)$, there are exactly $n-2$ possibilities for $\alpha(3)$.
Continuing in this way total elements in S_n is $n.(n-1).(n-2)...3.2.1 = n!$

Cycle Notation: An expression of the form $(a_1, a_2, ...a_m)$ is called a cycle of lenght m or $m-$cycle.
Foe example: Suppose $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 6 & 5 & 1 \end{bmatrix}$ In cycle notation $\alpha = (12346)(5) = (12346)$
Note: 1.Do not write the cycles which have one entry.
2.We can multiply elements of S_n in cycle forms as
$\alpha = (12)(34)(56)$ and $\beta = (1345)(26)$ then $\alpha\beta = (146)(25)$

Properties of Permutations

Theorem: Every permutation of a finite set can be written as cycle or as a product of disjoint cycles.
Proof: Let α be a permutation on $A = \{1, 2, ..., n\}$
To write α in disjoint cycle form
let a_1 be any member of A , $a_2 = \alpha(a_1)$, $a_3 = \alpha(\alpha(a_1)) = \alpha^2(a_1)$ and so on,
continue in this way until $a_1 = \alpha^m(a_1)$ for some m.
Since such an m exists because the sequence $a_1, \alpha(a_1), \alpha^2(a_1)...$ must be finite
so we can write $\alpha = (a_1, a_2, ..., a_m)...$
Let $b_1 \in A$ not an element of the first cycle, and $b_2 = \alpha(b_1)$, $b_3 = \alpha(b_2)$ and so on until we get $b_1 = \alpha^k(b_1)$
This new cycle will have no elements in common with previously constructed cycle.
If so $\alpha^i(a_1) = \alpha^j(b_1)$ for some i and j so that $\alpha^{i-j}(a_1) = b_1$
therefore $b_1 = a_t$ for some t which is contradiction to the choice of b_1
Continueing in this way until we complete all the elements of A so we get
$\alpha = (a_1, a_2, ..., a_m)(b_1, b_2, ...b_k)...(c_1, c_2, ...c_s)$
So every permutation can be written as product of disjoint cycles.

Theorem: If the pair of cycles $\alpha = (a_1, a_2, ...a_m)$ and $\beta = (b_1, b_2, ..., b_n)$ have no entries in common, then $\alpha\beta = \beta\alpha$
Proof: Let α and β are permutaions of the set $S = \{a_1, a_2, ..., a_m, b_1, b_2, ..., b_n, c_1, c_2, ..., c_k\}$
To prove $\alpha\beta = \beta\alpha$
that is to prove $(\alpha\beta)(x) = (\beta\alpha)(x)$ for all $x \in S$
If x is one of the element of α say a_i then
$(\alpha\beta)(a_i) = \alpha(\beta(a_i)) = \alpha(a_i) = a_{i+1}$ since β fixes all the elements of α
Similarly $(\beta\alpha)(a_i) = \beta(\alpha(a_i)) = \beta(a_{i+1}) = a_{i+1}$
Here $\alpha\beta = \beta\alpha$ for all elements of α
Similarly we can prove for all elements of β
Suppose $x = c_i$ then we have $(\alpha\beta)(c_i) = \alpha(\beta(c_i)) = \alpha(c_i) = c_i$
$(\beta\alpha)(c_i) = \beta(\alpha(c_i)) = \beta(c_i) = c_i$
So $\alpha\beta = \beta\alpha$

Theorem: The order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lenghts of the cycles.
Proof: Since a cycle of lenght n has order n.
Let α and β are disjoint cycles of lenght m and n and k be least common multiple of m and n.
So that $k = mx$ and $k = ny$
$(\alpha)^k = (\alpha)^{mx} = (\alpha^m)^x = e^x = e$
Similarly $\beta^k = e$ since α and β are disjoint cycles so α and β commute,
therefore $(\alpha\beta)^k = \alpha^k\beta^k = e.e = e$
Suppose $|\alpha\beta| = t$ so t divides k since if $a^k = e$ then $|a|$ divides k.
As $|\alpha\beta| = t \Rightarrow (\alpha\beta)^t = \alpha^t\beta^t = e \Rightarrow \alpha^t = \beta^{-t}$
Since α and β are disjoint so α^t and β^{-t} are also disjoint but $\alpha^t = \beta^{-t}$ so they must both be identity
So m and n divides t and k ls least common multiple of m and n so k divides t
so $k = t$ therefore order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lenghts of the cycles.

Theorem: Every permutaion in S_n, $n > 1$, is a product of 2-cycles.
Proof: Since identity permutation can be written as (12)(21) product of 2-cycles.
Since every permutation can be wriiten in the form $(a_1a_2...a_k)(b_1b_2...b_t)(c_1c_2...c_s)$
we can write this as $(a_1a_k)(a_1a_{k-1})...(a_1a_2)(b_1b_t)(b_1b_{t-1})...(b_1b_2)...(c_1c_s)...(c_1c_2)$

Note: Identity permutation contains even number of 2-cycles.

Theorem: If a permutation α can be expressed as a product of an even (Odd) number of 2-cycles, then every decomposition of α into a product of 2-cycles must have an even (odd) number of 2-cycles.
that is if $\alpha = \beta_1\beta_2...\beta_r$ and $\alpha = \gamma_1\gamma_2...\gamma_s$, where $\beta's$ and $\gamma's$ are -cycles,
then r and s both even or both odd.
Proof: Let $\alpha = \beta_1\beta_2...\beta_r$ and $\alpha = \gamma_1\gamma_2...\gamma_s$
so $\beta_1\beta_2...\beta_r = \gamma_1\gamma_2...\gamma_s$
$\Rightarrow e = \beta_1\beta_2...\beta_r\gamma_1^{-1}\gamma_2^{-1}...\gamma_s^{-1}$
$\Rightarrow e = \beta_1\beta_2...\beta_r\gamma_1\gamma_2...\gamma_s$ Since identity permutation contains even number of 2-cycles
so $r + s$ is even this is true when both r and s are even or both r and s are odd.

Even Permutation:
Definition: A permutation that can be expressed as a product of an even number of 2-cycles is called an even permutation.
Odd Permutation:
Definition: A permutation that can be expressed as a product of an odd number of 2-cycles is called an odd permutation.

Theorem: The set of even permutations in S_n forms a subgroup of S_n.
Proof: Let α and β be two even permutations so number of 2-cycles in α and β are even say r and s.
So that $\alpha\beta$ contains $r+s$ number of 2-cycles. As r and s are even so $r+s$ is even. So $\alpha\beta$ is even permutation.
Set of even permutation is closed.
Since set of even permutations is subset of S_n so associativity holds.
Since identity permutation is even permutation so identity exists.
And inverse of even permutation is even.
Therefore set of even permutations forms a group and it is a subset of S_n so it is a subgroup of S_n.

Alternating group of degree n
Definition: The group of even permutations of n symbols is denoted by A_n and is called alternating group of degree n.

Theorem: For $n > 1$, A_n has order $n!/2$
Proof: Let α be an odd permutation. So $(12)\alpha$ is an even permutation and $(12)\alpha \neq (12)\beta$ when $\alpha \neq \beta$. Thus there are atleast as many even permutation as odd ones. On the other hand for each even permutation α the permutation $(12)\alpha$ is odd and $(12)\alpha \neq (12)\beta$ when $\alpha \neq \beta$. Thus there are atleast as many odd permutation as even ones. So there are equal number of even and odd permutation. Since $|S_n| = n!$ so $A_n = n!/2$.