Week 5

Defn. (Dihedral group)

The group of symmetrics of the regular n-gon is called the n-th dihedral group, denoted by D_n.

Examples

1. $D_3 = S_3 = \{\rho_0, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\} = \{e, (123), (132), (23), (13), (12)\}$.

2. $D_4 = \{\rho_0, \rho_1, \rho_2, \rho_3, \mu_1, \mu_2, \delta_1, \delta_2\}$

$= \{e, (1234), (13)(24), (1432), (12)(34), (14)(32), (13), (24)\}$.

Note： In $D_3, (23) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$,

In $I_n D_4, (13)(24) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ and $(13) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$.

Defn. If A is a set, then a subgroup of S_A is <u>transitive</u> on A if for each $a, b \in A$ there exists a permutation $\sigma \in H$ such that $\sigma(a) = b$.

Fact Let $A = \{1,2,3\}$. Then the subgroup $\{e, (123), (132)\}$ is transitive on A.

($\{e, (123), (132)\}$ is a cyclic subgroup of S_3.)

(＊) Let A be a nonempty set and σ be a permutation. Then σ gives a natural partition of A with the property that $a, b \in A$ are in the same cell if and only if $\exists n \in Z$ such that $\sigma^n(a) = b$.

Note： If n is negative, $\sigma^n(a)=b$ iff $\sigma^{-n}(b)=a$.

Example 1

Let $A=\{1,2,3,4,5,6,7,8\}$ and $\sigma=(136)(28)(475)$. Then we have the partition：

$\{1,3,6\}$, $\{2,8\}$, $\{4,7,5\}$

Fact The partition can be obtaind by using the equivalence relation ~ on A defined by $a \sim b$ if and only if $\exists \ n \in Z$ such that $\sigma^n(a)=b$.

Defn. (Orbit of σ in A)

Let σ be a permutation of A. The equivalence classes in A determined by the equivalence relation " $a \sim b$ " if and only if $\exists \ n \in Z$ such that $\sigma^n(a)=b$ " are the orbits of σ in A.

Example 2

The orbits of $\sigma=(136)(28)(475)$ in $\{1,2,3,4,5,6,7,8\}$ are $\{1,3,6\},\{2,8\}$ and $\{4,7,5\}$.

Defn. (Cycle)

A permutation $\alpha \in S_n$ is a cycle if it has at most one orbit in A more than one element.

Clearly, $(136)(28)(475)$ is not a cycle since the permutation has three orbits with more than one element in $\{1,2,3,4,5,6,7,8\}$. On the other hand, (13245) is a cycle in S_8 since (13245) has four orbits in $\{1,2,3,4,5,6,7,8\}$, namely $\{1,2,3,4,5\},\{6\},\{7\}$ and $\{8\}$ but only one of then has more than one element.

Theorem

Every permutation of a finite set is a product of disjoint cycles.

Proof.

We can obtain the product recursively. First, let A be the finite set and $A=\{a_1,a_2,\cdots,a_n\}$, also let σ be a permutation of A. Start with a_1, we have the first cycle $(a_1\sigma(a_1)\cdots\sigma^{t-1}(a_1))$ where t is the smallest positive integer satisfying $\sigma^t(a_1)=a_1$. Then, let i be the smallest index such that $a_i\notin\{a_1,\sigma(a_1),\cdots,\sigma^{t-1}(a_1)\}$ and the second cycle is $(a_i\sigma(a_i)\cdots\sigma^{s-1}(a_i))$ where s is the smallest positive integer satisfying $\sigma^s(a_i)=a_i$. Continuing this process, we have a cycle product of σ, moreover, they are disjoint cycles. ▓

Defn. (Transposition)

A cycle of length 2 is a transposition.

Lemma $(a_1a_2a_3\cdots a_n)=(a_1a_n)(a_1a_{n-1})\cdots(a_1a_2)$.

Example $(123465)=(15)(16)(14)(13)(12)$.

Corollary Any permutation of a finite set of at least two elements is a product of transpositions.

Defn.

A permutation of a finite set is even (or odd) according to whether it can be expressed as a product of an even (or odd) number of transpositions.

Theorem A permutation of a finite set can not be both even and odd.

Proof.

Let $A=\{a_1,a_2,\cdots,a_n\}$ and σ be a permutation of A. Then σ can be represented by a permutation matrix $B=(b_{i,j})$ where $b_{i,j}=1$ if $\sigma(a_i)=a_j$ and $b_{i,j}=0$ otherwise. Clearly, in B, each row and each column "1" occurs exactly once. This implies that $\det(B)$ is equal to 1 or -1 but not both. On the other hand,

since $\sigma = \prod (a_{i'} a_{j'})$ where $i', j' \in \{1,2,\cdots,n\}$ and the product has t transpositions. Therefore, B can be obtained by permuting the $n \times n$ identity matrix B using $(a_{i'} a_{j'})$ recursively. This implies $\det(B)$ is equal to 1 if t is even and $\det(B) = -1$ if t is odd where t is the number of transpositions. Hence the proof follows.
▓

Note： The proof of the above theorem can also be obtained by showing that the number of orbits of σ and $(i, j)\sigma$ differ by 1.

Example： $\sigma = (16)(253)$, $(34)(16)(253) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 3 & 4 & 1 \end{pmatrix} = (16)(2543)$

The orbits of σ in $\{1,2,3,4,5,6\}$ are $\{1,6\}, \{4\}, \{2,5,3\}$, and the orbits of $(34)\sigma$ are $\{1,6\}$ and $\{2,5,4,3\}$.

Theorem (Alternating group)

If $n \geq 2$, then the collection of all even permutations of $\{1,2,\cdots,n\}$ forms a subgroup A_n of order $\frac{n!}{2}$ of the symmetric group S_n.

Proof.

Let O_n denote the set of odd permutations in S_n. Then $S_n = A_n \cup O_n$. Since $A_n \cap O_n = \phi$, $|A_n| + |O_n| = n!$. Now, it suffices to show that $|A_n| = |O_n|$ or equivalenty there exists a bijection from A_n onto O_n.

Define a mapping $f : A_n \to O_n$ by $f(\alpha) = \alpha \circ (12)$ for each $\alpha \in A_n$. Since $(12) \circ (12) = e$ (identity), $f(\alpha) = f(\beta)$ implies that $\alpha = \beta$. Hence f is 1-1. Moreover, for each $\gamma \in O_n$, $\gamma \circ (12)$ is an even permutation and thus $\gamma \circ (12) \in A_n$. By the fact that $f(\gamma \circ (12)) = \gamma$, we have shown f is onto. Thus f is a bijection. This concludes the proof. ▓

Note： A_n plays an important role in proving that there are no formulas involving just radicals for solution of polynomial equations of degree n for $n \geq 5$. (A_5 is simple and S_5 is not solvable.)