Chapter 5 Permutation groups.

Recall a permutation of a set S is a bijective function $\pi: S \longrightarrow S$. The set of all such functions, with composition of functions as their binary operation, forms a group. We will use S_n to denote the group of permutations of an n-element set, S_n is called the <u>symmetric group</u>.

<u>Theorem</u>: S_n is a group with $n!$ elements.

<u>Proof</u>: Exercise.

Some special permutations are called <u>cycles</u>. A <u>cycle</u> $\pi: S \longrightarrow S$ is a permutation satisfying $\exists\, a_1, \ldots, a_k$ such that:

$$\pi_1(a_1) = a_2$$
$$\pi(a_2) = a_3$$
$$\vdots$$
$$\pi(a_k) = a_1$$

and $\pi(s) = s$ for all other $s \in S$.

For example,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix} \in S_5$$

is a cycle, since $\sigma(1)=3, \sigma(3)=4, \sigma(4)=2$ and $\sigma(2)=1$.

We use the notation $\sigma = (1\,3\,4\,2)$.

Example: The permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix} \in S_6$$

is a product of cycles: $\sigma = (1243)(56)$.

Example: Describe the product of cycles $\sigma\tau$ where $\sigma = (1352)$ and $\tau = (256)$ as a function

$$f: \{1,2,3,4,5,6\} \longrightarrow \{1,2,3,4,5,6\}.$$

Solution: Here, σ is

$1 \longmapsto 3$, $3 \longmapsto 5$, $5 \longmapsto 2$, $2 \longmapsto 1$, and τ is

$2 \longmapsto 5$, $5 \longmapsto 6$, $6 \longmapsto 2$.

So we use these rules to calculate what the product $\sigma\tau$ does to each integer. For example:

$$f(1) = \sigma\tau(1) = \sigma(1) = 3$$
$$f(2) = \sigma\tau(2) = \sigma(5) = 2$$
$$f(3) = \sigma\tau(3) = \sigma(3) = 5$$
$$f(4) = \sigma\tau(4) = \sigma(4) = 4$$
$$f(5) = \sigma\tau(5) = \sigma(6) = 6$$
$$f(6) = \sigma\tau(6) = \sigma(2) = 1.$$

or $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 4 & 6 & 1 \end{pmatrix}$

or we can even write:

$$f = (1\ 3\ 5\ 6).$$

<u>Definition</u>: Two cycles $\sigma = (a_1 a_2 a_3 \cdots a_k)$ and $\tau = (b_1 b_2 \cdots b_m)$ are <u>disjoint</u> if $a_i \neq b_j$ for all i, j. I.e. $\{a_1, \dots, a_k\} \cap \{b_1, \dots, b_m\} = \emptyset$.

In general, if we want to talk about permutations of an <u>arbitrary</u> set X (instead of $\{1, \dots, n\}$), we write S_X for the group of permutations of X.

We also sometimes must write

$(a_1, \dots, a_k)$ to denote the cycle $(a_1 \cdots a_k)$

whenever confusion may arise, for example is $(123) \in S_{13}$ the cycle $(1, 2, 3)$ or $(12, 3)$?

Proposition: Let $\sigma, \tau \in S_X$ be disjoint cycles. Then $\tau\sigma = \sigma\tau$.

Proof: Suppose $\sigma = (a_1, \dots, a_k)$ and $\tau = (b_1, \dots, b_\ell)$, we'll show $\tau\sigma(x) = \sigma\tau(x)$ $\forall x \in X$.

We consider 3 cases: $x \notin \{a_1, \dots, a_k, b_1, \dots, b_\ell\}$

$x \in \{a_1, \dots, a_k\}$

$x \in \{b_1, \dots, b_\ell\}$.

Case 1: If $x \notin \{a_1, \dots, a_k, b_1, \dots, b_\ell\}$, then $\sigma(x) = x$ and $\tau(x) = x$, so $\sigma\tau(x) = \tau\sigma(x) = x$.

Case 2: If $x \in \{a_1, \dots, a_k\}$, then $\sigma(x) = \sigma(a_i)$ for some i and $\sigma(a_i) = a_{i+1}$ unless $i = k$, then $\sigma(a_i) = a_1$. We can say this more cleanly as: $\sigma(a_i) = a_{(i \bmod k)+1}$.
Then using $\tau(a_i) = a_i$ for all i (since σ, τ are disjoint), we compute:

$$\tau\sigma(a_i) = \tau(a_{(i \bmod k)+1}) = a_{(i \bmod k)+1}$$

and

$$\sigma\tau(a_i) = \sigma(a_i) = a_{(i \bmod k)+1}.$$

Case 3 $x \in \{b_1, \dots, b_\ell\}$. The argument is nearly identical to case 2.

Theorem: Every $\sigma \in S_n$ can be written as a product of disjoint cycles.

Proof: Set $X = \{1, 2, \dots, n\}$, and define X_1 to be the set

$$X_1 = \{\sigma(1), \sigma^2(1), \sigma^3(1), \dots \text{etc}\}.$$

The set X_1 is finite since X is finite. Define a disjoint set $X_2 \subset X$ as follows: Let $j_2 \in \{1, 2, \dots, n\}$ be the smallest integer in $X \setminus X_1$. Set

$$X_2 = \{\sigma(j_2), \sigma^2(j_2), \dots\},$$

and similarly define X_i for all $i \geq 3$, stopping when $X \setminus X_i$ is empty. Say there are r disjoint sets when it stops, so

$$X = \dot{\bigcup_{i=1}^{r}} X_i.$$

Define a cycle σ_i by

$$\sigma_i(x) = \begin{cases} \sigma(x) & \text{if } x \in X_i \\ x & \text{if } x \notin X_i. \end{cases}$$

It's a cycle because if j_i is the integer whose iterates define X_i, i.e. if

$$X_i = \{\sigma(j_i), \sigma^2(j_i), \dots\}$$

Then $\sigma_i = (\sigma(j_i), \sigma^2(j_i), \sigma^3(j_i), \dots)$.

Moreover, $\sigma = \sigma_1\sigma_2\cdots\sigma_r$ and since the sets X_i are disjoint, so are the cycles σ_i.

<u>Example</u>. If we choose a random ~~cycle~~ permutation:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 5 & 1 & 6 & 2 \end{pmatrix}$$

it can always be written as a product of cycles using the procedure in the proof. Here, we get:

$$(1\ 4)(2\ 3\ 5\ 6).$$

For this reason, we will always (almost always) assume our permutations of a set S_n are written as disjoint products of cycles.

<u>Transpositions</u>

<u>Def</u>: A <u>transposition</u> is a cyclo of length 2.

<u>Proposition</u>: Any cycle can be written as a product of transpositions.

Proof:

$$(a_1, a_2, \ldots, a_n) = (a_1 a_n)(a_1 a_{n-1}) \cdots (a_1 a_3)(a_1 a_2)$$

Proposition: Any permutation in S_n can be twritten as qproduct of transpositions.

Proof: Write any $\sigma \in S_n$ as a product of disjoint cycles and use the previous formula.

Remark: There is no unique way of writing a permutation as a product of transpositions. For example:

$$(16)(253) = (16)(23)(25)$$

and $$= (16)(45)(23)(45)(25).$$

Lemma: If the identity is written as a product of r transpositions, then r is even.

Proof: Write $id = \tau_1 \tau_2 \cdots \tau_r$ where $r > 1$, and induct. We omit details here and refer to Lemma 5.14 in text.

Here's the induction

Suppose $id = \tau_1 \dots \tau_r$. If $r=1$, this equation is not possible, so suppose $r=2$. Then we're done.

If $r>2$ then the last two transpositions, $\tau_{r-1}\tau_r$, must be of the form:

1. $(ab)(ab) = id$
2. $(bc)(ab) = (ac)(bc)$
3. $(cd)(ab) = (ab)(cd)$
4. $(ac)(ab) = (ab)(bc)$,

where a,b,c,d are distinct elements.

In case 1, $id = \tau_1 \dots \tau_r$
$= \tau_1 \dots \tau_{r-2}$, which is even length by induction, so $r-2$ even $\Rightarrow r$ even.

In case 2, replace
$$id = \tau_1 \cdots \tau_r = \tau_1 \cdots \tau_{r-2}(bc)(ab).$$
with
$$id = \tau_1 \cdots \tau_{r-2}(ac)(bc)$$

in case 3, $id = \tau_1 \cdots \tau_{r-2}(ab)(cd)$

in case 4, $id = \tau_1 \cdots \tau_{r-2}(ab)(bc)$

In each case, the last occurence of a in the product is now in position $r-1$ instead of $r-2$.

Repeating these substitutions, one of two things happens:

(i) Either we end up with the only occurence of a being in position 1, in which case the product of transpositions cannot be the identity (since it moves 1), or

(ii) At some point we're in case (i), where we have two identical adjacent transpositions that cancel and leave us with a product of length $r-2$. But then induction $\Rightarrow$ $r-2$ even, so r is even.

Since Case (i) is impossible, we're in Case (ii) every time. Therefore r is even.

Proposition: Suppose that $\sigma_1, \dots, \sigma_m$ and $\tau_1, \dots, \tau_n$ are transpositions. If

$$\sigma_1 \cdots \sigma_m = \tau_1 \cdots \tau_n$$

then $m \equiv n \mod 2$ (ie. they're either both even or both odd).

Proof: Suppose that

$$\sigma_1 \cdots \sigma_m = \tau_1 \cdots \tau_n,$$

where m is even. We must show that n is also even.

Since a transposition is its own inverse, $\sigma_m \cdots \sigma_1$ is the inverse of σ, so

$$id = \sigma \cdot \sigma_m \cdots \sigma_1 = \tau_1 \cdots \tau_n \cdot \sigma_m \cdots \sigma_1$$

so $m+n$ must be even, by the previous lemma. If m is even, this forces n to be even, if m is odd this forces n to be odd.

Definition: Define a permutation $\sigma \in S_n$ to be <u>even</u> if it can only be written as a product of an even number of transpositions. Call $\sigma \in S_n$ odd if it can only be written as a product of an odd number of transpositions.

Definition: Set

$$A_n = \{\sigma \in S_n \mid \sigma \text{ is even}\}.$$

<u>Proposition</u>: A_n is a subgroup of S_n, called the <u>alternating group</u> on n letters.

<u>Proof</u>: If σ and τ are even permutations, then $\sigma\tau$ must also be an even permutation. Moreover, id is an even permutation and so $id \in A_n$.

Last, if $\sigma \in A_n$ and

$$\sigma = \sigma_1 \cdots \sigma_r \text{, a product of } r \text{ transpositions with } r \text{ even,}$$

then $\sigma^{-1} = \sigma_r \cdots \sigma_1$ is also even, so $\sigma^{-1} \in A_n$.

<u>Proposition</u>: The group S_n contains the same number of even permutations as odd permutations for all $n \geq 2$. Thus $|A_n| = \frac{n!}{2}$ for $n \geq 2$.

<u>Proof</u>: Let $A_n \subset S_n$ be the set of ~~odd~~ even permutations, and $C_n \subset S_n$ the odd ones.

Fix a transposition $\sigma \in S_n$, and define a map

$$f_\sigma : A_n \longrightarrow B_n$$

by $f_\sigma(\tau) = \sigma\tau$. Then if τ is even, $\sigma\tau$ is odd, and we will show it is a bijection.

First, f_σ is onto since if τ is an odd permutation, then $\sigma^{-1}\tau$ is even and

$$f_\sigma(\sigma^{-1}\tau) = \sigma(\sigma^{-1}\tau) = \tau.$$

The map f_σ is 1-1 since

$$f_\sigma(\tau) = f_\sigma(\tau') \Rightarrow \sigma\tau = \sigma\tau'$$
$$\Rightarrow \tau = \tau'.$$

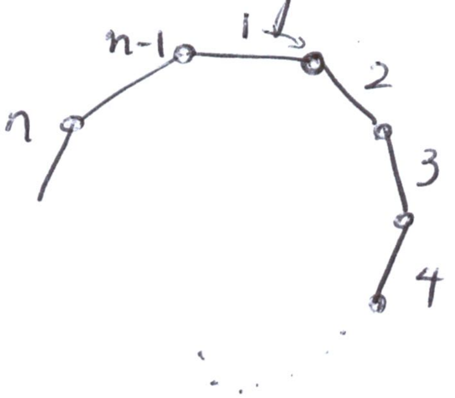
Another special subgroup of S_n is the <u>dihedral group</u> D_n.

<u>Definition</u>: The n^{th} dihedral group is denoted D_n and is the group of rigid motions of a regular n-gon.

The group D_n is naturally a subgroup of S_n: For each rigid motion, label the vertices of D_n with numbers $\{1, \ldots, n\}$. Then the rigid motion gives a permutation of $\{1, \ldots, n\}$, i.e. it's an element of S_n.

Theorem: D_n is a subgroup of order $2n$.

Proof: Consider a regular n-gon:



A rigid motion can move the vertex '1' to n possible positions, either 1, 2, 3, ... etc. After choosing where to send vertex 1, we choose where to send vertex '2'. If 1 is sent to vertex k, then 2 can go to either $k+1$ or $k-1$. Either one of these choices completely determines the positions of the remaining vertices. Thus there are $2n$ elements.

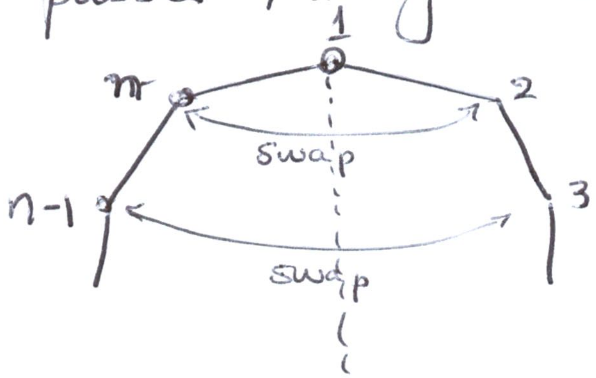
Two specific elements of D_n are given names:

r is the cycle $(1\ 2\ 3 \dots n)$, it is a rotation of the figure by $\frac{2\pi}{n}$.

S is the permutation

$(n, 2)(n-1, 3)(n-2, 4) \dots$

s corresponds to reflecting in the line that passes through vertex 1:



<u>Theorem</u>: The group $D_n \subset S_n$ consists of all products of the two elements s and r, satisfying the relations

$$r^n = 1$$
$$s^2 = 1$$
$$srs = r^{-1}.$$

<u>Proof</u>: There are n rotations, by angles

$$0, \frac{2\pi}{n}, 2\cdot\frac{2\pi}{n}, 3\cdot\frac{2\pi}{n}, \dots, (n-1)\frac{2\pi}{n}.$$

These are given by powers of r, namely

$r^0, r^1, r^2, \dots, r^{n-1}$, and $r^n = 1$ since rotation by 2π gives the identity.

There are also n axes of symmetry, when n is odd ~~so let~~ one passing through each vertex, label their reflections $s_1, s_2, \dots, s_n$. Set $s = s_1$

We can produce a reflection s_k for any $1 \leq k \leq n$ by using only r and $s = s_1$, as follows: First we rotate vertex k to position 1 by doing r^{-k}, then reflect in vertex 1 by doing $s = s_1$. So we have done $s_1 r^{-k}$. Now rotate back:

$$r^k s_1 r^{-k} = s_k.$$

This means that products of r and s alone give all elements of D_n. That $s^2 = 1$ is obvious, and we leave $srs = r^{-1}$ to the exercises, as well as the case of n even.

Questions:

1, 2 (a)-(d), (m)-(p), 3, 13, 14, 17-24.