Group Theory

Lecture 6, Sunday November 27, 2022
Ari Feiglin

6.1 The Symmetric Group

Definition 6.1.1:

If X is a set, then we define the **symmetric group** of X as:

$$S_X = \{\sigma \colon X \longrightarrow X \mid \sigma \text{ is invertible}\}$$

It is trivial to see that $\mathcal{U}\left(X^X\right) = S_X$ (recall that X^X is a monoid).

Proposition 6.1.2:

If X and Y are sets with the same cardinality, $S_X \cong S_Y$.

Proof:

Suppose $f \colon X \longrightarrow Y$ is a bijection. Then we define an isomorphism $\varphi \colon S_X \longrightarrow S_Y$ by

$$\varphi(\sigma) = f \circ \sigma \circ f^{-1}$$

This is of course well defined since both σ and f are bijections. It is a bijection since for any $\tau \in S_Y$, $f^{-1} \circ \tau \circ f \in S_X$ and $\varphi(f^{-1} \circ \tau \circ f) = \tau$ so it is surjective and since f is bijective, φ is injective. It is a homomorphism since $\varphi(\sigma_1 \circ \sigma_2) = f \circ \sigma_1 \circ \sigma_2 \circ f^{-1} = f \circ \sigma_1 \circ f^{-1} \circ f \circ \sigma_2 \circ f^{-1} = \varphi(\sigma_1) \circ \varphi(\sigma_2)$.

■

So for every X finite of cardinality n:

$$S_X \cong S_n = S_{\{1,\ldots,n\}}$$

And further it can be shown combinatorically that $|S_n| = n!$. The elements of S_n are called *permutations*.
There are a few ways of writing out a permutation, suppose $\sigma \in S_5$ then we can write it out as a table where the top row is $\{1, \ldots, 5\}$ and the bottom row is their image, for example:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 6 & 3 & 9 & 1 & 4 & 8 & 7 & 2 \end{pmatrix}$$

This is caled the tabular representation of a permutation. We can also write this in cycles. If we take 1, it maps to 5 which maps to 1, creating a cyle, so we can write this cycle as $\begin{pmatrix} 1 & 5 \end{pmatrix}$:

$$\sigma = \begin{pmatrix} 1 & 5 \end{pmatrix}\begin{pmatrix} 2 & 6 & 4 & 9 \end{pmatrix}\begin{pmatrix} 3 \end{pmatrix}\begin{pmatrix} 7 & 8 \end{pmatrix}$$

Definition 6.1.3:

A **cycle** is a permutation σ such that there exists elements $k_1, \ldots, k_t$ such that $\sigma(k_i) = k_{i+1}$ for $i < t$ and $\sigma(k_t) = k_1$. And for every other element other than these elements, σ maps it to itself. And two cycles are **disjoint** if the set of values they permute are disjoint.

As said above, we can express a cycle as a tuple:

$$\sigma = \begin{pmatrix} k_1 & k_2 & \ldots & k_t \end{pmatrix}$$

Notice then that a permutation of the form $\begin{pmatrix} k \end{pmatrix}$ is just the identity function. Also notice that the composition of disjoint cycles is commutative since they don't affect each other's permuted elements.

Theorem 6.1.4:

Every (finite) permutation can be written as a unique (up to order) composition of disjoint cycles.

Proof:

We will prove existence by induction on S_n (since every finite symmetry group is isomorphic to some S_n). For $n = 1$, this is trivial since every permutation is the identity function. Suppose this is true for $k < n$, suppose $\sigma \in S_n$. Then we can take the cycle created by 1 (which must exist, since we can exhaust all the elements in $\{1, \ldots, n\}$), let this cycle be σ_1. Then we can create a new permutation defined by $\sigma'(i) = i$ if i is in σ_1's permuted elements and $\sigma(i)$ otherwise. Thus $\sigma = \sigma' \circ \sigma_1$, and since σ' is in a symmetric group isomorphic to some S_k for $k < n$, it has a disjoint cycle decomposition. And therefore so does σ as a whole.
This decomposition must be unique (up to order) because the decomposition is of disjoint cycles, so each cycle represents the cycle its elements take in the permutation. And this is unique, since it is simply $\begin{pmatrix} i & \sigma(i) & \ldots & \sigma^k(i) \end{pmatrix}$. ■

It is immediate then that the set of cycles in S_n generate S_n.

Definition 6.1.5:

We define the **sign** function to be a function:

$$\operatorname{sgn}\colon S_n \longrightarrow \{-1, 1\}$$

Where $\operatorname{sgn}(\sigma) = (-1)^k$ where $k = |\{(i,j) \mid i < j, \sigma(i) > \sigma(j)\}|$. Essentially the sign function indicates whether or not the number of times σ reverses the order of numbers is even or odd.

Similarly, we can define

$$\delta_{ij} = \begin{cases} +1 & \sigma(i) < \sigma(j) \\ -1 \sigma(i) > \sigma(j) & \end{cases}$$

and then

$$\operatorname{sgn}(\sigma) = \prod_{i<j} \delta_{ij}$$

We can also think of the sign function geometrically: if we draw a line between k and $\sigma(k)$ in σ's tabular form, counting the number of intersections between these lines and raising -1 to that power gives $\operatorname{sgn}(\sigma)$. This is because two lines orignating from i and j where $i < j$ intersect if and only if $\sigma(i) > \sigma(j)$.

Proposition 6.1.6:

The sign function is a homomorphism between S_n and $\{\pm 1\}$.

$\{\pm 1\}$ is a group under multiplication, and it is isomorphic to Euler(3).

Proof:

Suppose $\sigma, \tau \in S_n$. For every $1 \leq i < j \leq n$ there are four possibilities:

(1) τ preserves the order and σ preserves the order of their images.

(2) τ preserves the order and σ does not preserve the order of the images.

(3) τ does not preserve the order, σ does.

(4) τ does not preserve the order, σ does not.

If we focus on the product definition of sign: the first and fourth options provides a $+1$ (since order is preserved, for the fourth option the order is reversed twice, so at the end it is preserved). And the second and third options provide a -1. So if we use δ_{ij}^{σ} as the indicator for σ, the first option corresponds to $\delta_{ij}^{\sigma} = \delta_{ij}^{\tau} = 1$, and so on. And so we can see that:

$$\delta_{ij}^{\sigma\circ\tau} = \delta_{ij}^{\sigma} \cdot \delta_{ij}^{\tau}$$

And therefore:

$$\operatorname{sgn}(\sigma \circ \tau) = \prod_{i<j} \delta_{ij}^{\sigma\circ\tau} = \prod_{i<j} \delta_{ij}^{\sigma} \cdot \delta_{ij}^{\tau} = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau)$$

as required.

■

Definition 6.1.7:

A permutation is **even** if its sign is 1 and **odd** if its sign is -1.

Definition 6.1.8:

A **transposition** is a cycle of length 2.

Since all a transposition does is permute two elements, one of which must be greater than the other, the sign of a transposition is -1, and thus every transposition is odd.
Notice that for a cycle $\begin{pmatrix} k_1 & \dots & k_t \end{pmatrix}$, this can be written the composition of transpositions:

$$\begin{pmatrix} k_1 & \dots & k_t \end{pmatrix} = \begin{pmatrix} k_1 & k_2 \end{pmatrix}\begin{pmatrix} k_2 & k_3 \end{pmatrix}\cdots\begin{pmatrix} k_{t-1} & k_t \end{pmatrix}$$

Since for k_i, it gets swapped to k_{i+1} in the ith transposition in this decomposition, and k_{i+1} is not in any of the subsequent transpositions. It can also be written as:

$$\begin{pmatrix} k_1 & k_t \end{pmatrix}\begin{pmatrix} k_1 & k_{t-1} \end{pmatrix}\cdots\begin{pmatrix} k_1 & k_2 \end{pmatrix}$$

Since k_i is mapped to k_1, which is mapped to k_{i+1} in the next transposition, which is not in any of the other transpositions. For k_1, it is mapped back and fourth until the final transposition when it is mapped to k_t. And since the sign function is a homomorphism:

$$\operatorname{sgn}\left(\begin{pmatrix} k_1 & \dots & k_t \end{pmatrix}\right) = (-1)^{t-1}$$

So even length cycles are odd, and odd length cycles are even (the identity cycle is considered odd length, since it is actually of the form (i)).
Also notice that we showed that cycles can be written as a product of transpositions, so the set of transpositions also generates S_n. And the sign of a permutation equals to the parity of the number of transpositions in its decomposition into transpositions.

Note:

For any $n \geq 3$, S_n is not abelian. This much should not be surprising.

For $n \geq 2$, sgn is surjective (since there exists transpositions in S_n for $n \geq 2$, S_1 only contains the identity). And we define:

$$A_n = \operatorname{Ker}(\operatorname{sgn}) = \{\sigma \in S_n \mid \sigma \text{ even}\}$$

And so by the first isomorphism theorem:

$$S_n/A_n \cong \{\pm 1\} \implies |A_n| = \frac{S_n}{2}$$

Notice that the order of a cycle of length t is t. This is a direct result of the definition of a cycle.

Proposition 6.1.9:

A_n is generated by the set $\left\{\begin{pmatrix} a & b \end{pmatrix}\begin{pmatrix} c & d \end{pmatrix}\right\}$ where $a \neq b$ and $c \neq d$.

This is obvious since every permutation in A_n can be written as a product of an even number of transpositions.
There are three types of this product of transpositions: the identity, the product of two disjoint transpositions, and the product of two transpositions which intersect at only one point. Notice that the last type is a product of the form $\begin{pmatrix} a & b \end{pmatrix}\begin{pmatrix} b & c \end{pmatrix} = \begin{pmatrix} a & b & c \end{pmatrix}$. So A_n is generated by the set of disjoint products of two transpositions and cycles of length three. Notice that:

$$\begin{pmatrix} k_1 & k_2 & k_3 \end{pmatrix}\begin{pmatrix} k_1 & k_2 & k_4 \end{pmatrix} = \begin{pmatrix} k_1 & k_3 \end{pmatrix}\begin{pmatrix} k_2 & k_4 \end{pmatrix}$$

And so every product of two disjoint transpositions can be written as the product of two cycles of length 3. Therefore A_n is generated by the set of cycles of length 3, thus we have proven the following proposition:

Proposition 6.1.10:

A_n is generated by the set of cycles of length 3.

Definition 6.1.11:

The **periodic structure** of a permutation is a multiset which encodes the number of cycles of each length there are in its disjoint cycle decomposition. So for example if the decomposition of a permutation is $\sigma_1 \cdots \sigma_t$ where σ_i are disjoint (non trivial) cycles, the periodic structure is:

$$\left\{[n]^k \;\middle|\; k = |\{i \mid |\sigma_i| = n\}|, k > 0\right\}$$

Definition 6.1.12:

Two elements $a, b \in G$ are **conjugates** are if there exists a $g \in G$ such that $b = gag^{-1}$.

It is trivial to see that this is an equivalence relation. In an abelian group, this relation is the trivial relation.
Notice that the inverse of a cycle $\begin{pmatrix} k_1 & \dots & k_t \end{pmatrix}$ is $\begin{pmatrix} k_t & k_{t-1} & \dots & k_1 \end{pmatrix}$ which is just the reverse order of the permutation.

Theorem 6.1.13:

Elements of S_n are conjugates if and only if they have the same periodic structure.

Proof:

Suppose σ is a cycle $\sigma = \begin{pmatrix} k_1 & \dots & k_n \end{pmatrix}$ then for any permutation g:

$$g\sigma g^{-1} = \begin{pmatrix} g(k_1) & \dots & g(k_n) \end{pmatrix}$$

since σg^{-1} only affects elements of the for $g(k_i)$, which converts them to $g\sigma g^{-1}(g(k_i)) = g\sigma(k_i) = g(k_{i+1})$. So the conjugate of a cycle is a cycle of the same length (since g is bijective, $g(k_i)$ are distinct).
So if σ is a permutation with a decomposition $\sigma_1 \cdots \sigma_t$, then:

$$g\sigma g^{-1} = g\sigma_1 \cdots \sigma_t g^{-1} = g\sigma_1 g^{-1} g\sigma_2 g^{-1} \cdots g\sigma_t g^{-1}$$

And since $g\sigma_i g^{-1}$ is a cycle of the same length as σ_i, the periodic structure of $g\sigma g^{-1}$ is the same as that of σ.
Now suppose σ and τ have the same periodic structures, suppose σ and τ have the following decompositions:

$$\sigma = \sigma_1 \cdots \sigma_n$$
$$\tau = \tau_1 \cdots \tau_n$$

Where σ_i and τ_i have the same length (since σ and τ have the same periodic structure). So we can define g such that if $\sigma_i = \begin{pmatrix} k_1 & \dots & k_t \end{pmatrix}$ and $\tau_i = \begin{pmatrix} j_1 & \dots & j_t \end{pmatrix}$, g maps k_i to j_i. So then we have that $g\sigma g^{-1}(j_i) = g\sigma(k_i) = g(k_{i+1}) = j_{i+1} = \tau(j_i)$. So $g\sigma g^{-1} = \tau$, so σ and τ are conjugates.

■