Abstract Algebra
Lecture 3
Wednesday, 9/8/2010

1 Dihedral Groups

Recall: Dihedral groups are groups of symmetries of rigid regular n-gons in the plane.

Choose a regular n-gon, such as the square. Find the center point, and choose one line of symmetry that passes through that point. Call this line L_0. Then, each L_k is found from L_0 by rotating $\frac{k\pi}{n}$. (We use modular arithmetic, such that, for the square, L_0 and L_4 are the same line, from opposite sides.) We denote reflection about the line L_k by σ_k. We use ρ_k to denote rotation by $\frac{2\pi k}{n}$.

We can then describe the group D_4 with generators and relations:

$$D_4 =< \rho_0, \rho_1, \rho_2, \rho_3, \sigma_0, \sigma_1, \sigma_2, \sigma_3 >$$

subject to the relations

$$\rho_i \rho_j = \rho_{i+j}$$
$$\rho_i \sigma_j = \sigma_{i+j}$$
$$\sigma_i \rho_j = \sigma_{i-j}$$
$$\sigma_i \sigma_j = \rho_{i-j}$$

all mon n. We could use shorthand to say $D =< \rho_i, \sigma_i | R >$.

Recall: The group

$$\mathcal{D}_{2n} =< r, s | r^n = s^2 = 1, rs = sr^{-1} >$$

These groups feel the same. If r represents an arbitrary rotation, and s represents a flip, then just these two generators and two relations describe the same group as D_2.

2 Symmetric Groups

Defn: Let $\varphi : A \to B$ be a map of sets. Then
1. φ is injective if it is one-to-one, i.e. $\varphi(a_1) = \varphi(a_2) \Rightarrow a_1 = a_2$.
2. φ is surjective if it is onto, i.e. $\forall b \in B, \exists a \in A$ s.t. $\varphi(a) = b$.
3. φ is bijective if it is injective and surjective.
4. φ is a permutation of A if $\varphi : A \to A$ is a bijection.

Ex: Let $A = \{1, 2, 3, 4\}$. Let α be the permutation

$$\alpha(1) = 2, \alpha(2) = 3, \alpha(3) = 1, \alpha(4) = 4.$$

We can also display this information as

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

Defn: For any set A, the group of permutations of A, denoted by S_A, is

$$S_A = \{\alpha : A \to A | \alpha \text{ perm}\}.$$

S_A is a group with group structure (operation) $\alpha \star \beta = \alpha \circ \beta$ of composition.

Defn: In the case that $A = \{1, 2, 3, \ldots, n\}$, then S_A is written S_n, and is called the Symmetric Group of degree n.

Ex: S_3 is non Abelian. The elements of S_3 are

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

These three elements can generate everything else. For example,

$$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \alpha^2\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

And note that $\beta\alpha \neq \alpha\beta$.

Ex: We can think of the dihedral group D_4 as a subgroup of S_4. If we label the vertices of the square 1 through 4, then the actions of the elements of the dihedral group can instead be viewed as simple arrangements of the vertices - an action that can be performed by elements of the symmetric group. For example

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

And, this should obey our relations from the dihedral group. For example:

$$\rho_1\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \sigma_2$$

as desired.

3 Cycle Notation

However, this matrix/array notation is still very clunky. So we use cycle notation instead. This was first introduced Augustin Cauchy in 1815.

Ex: Consider $\alpha \in S_6$

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

Instead, we use notation representing the cycles in which numbers progress while under the permutation α:

$$\alpha = (145)(26)(3) = (514)(62)(3) = \text{etc.}$$

Defn: An expression of the form $(a_1 \dots a_m)$ is a cycle of length m, also called an m-cycle.

Ex: For example, we can revisit the symmetric group S_3:

$$S_3 = \{(1), (12), (13), (23), (123), (132)\}$$

Note that when a number is excluded (as in the first cycle representing the identity notated above) it is assumed to map to itself. We could have just as legitimately represented the identity as (2) or (3).

Theorem: Every permutation of a finite set can be written as a product of disjoint cycles.

Proof: In the book. ∎

Theorem: Disjoint cycles commute. Let $\alpha = (a_1 \dots a_m)$ and $\beta = (b_1 \dots b_n)$. If $a_i \neq b_j$ for all i, j, then $\alpha\beta = \beta\alpha$.

Ex: Let $\alpha, \beta \in S_4$. Let $\alpha = (13)$ and $\beta = (24)$. Then

$$\alpha\beta = (13)(24) = (24)(13) = \beta\alpha.$$

By inspection of looking at where each element gets sent under each of the two composed cycle operations. Note that $\alpha\beta \in S_4$, both because it is a group and is therefore closed, and also because the composition of two bijections is always a bijection.

Theorem: A cycle of length n has order n.

Proof: In the homework. ∎

Theorem: Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be disjoint cycles. Then $|\alpha_1 \cdots \alpha_n| = \text{lcm}\{|\alpha_i|, i = 1, n\}$.

Theorem: Every permutation in S_n is a product of 2-cycles, not necessarily disjoint!

Ex:

- $(1) = (12)(12)$.
- $(123) = (13)(12)$.
- $(1234) = (14)(13)(12) = (43)(42)(41) = (4123)$.
- $(a_1 \ldots a_n) = (a_1 a_n)(a_1 a_{n-1}) \cdots (a_1 a_3)(a_1 a_2)$.

Note that these decompositions are not necessarily unique.

Theorem: If $\alpha = \beta_1 \ldots \beta_r$, and $\alpha = \gamma_1 \ldots \gamma_s$ where β_i, γ_i are 2-cycles, then r and s are both even or both odd.

Defn: An even permutation is a permutation that can be written as a product of an even number of 2-cycles. Similarly, and odd permutation can be written as a product of an odd number of 2-cycles.

Theorem: The set of even permutations in S_n form a group.

Defn: This group is called the Alternating Group, denoted $A_n < S_n$.

Note: The same cannot be said for the odd permutations, because the identity is an even permutation.

Note: There are exactly half as many elements in the alternating group as there are in the symmetric group, i.e. $|A_n| = \frac{n!}{2}$.