Math 2070 Week 2

Groups

Definition 2.1. Let G be a group, with identity element e.
The **order** of G is the number of elements in G.
The **order** $\operatorname{ord} g$ of an *element* $g \in G$ is the smallest $n \in \mathbb{N}$ such that $g^n = e$. If no such n exists, we say that g has **infinite order**.

Theorem 2.2. *Let G be a group with identity element e. Let g be an element of G. If $g^n = e$ for some $n \in \mathbb{N}$, then $\operatorname{ord} g$ is finite, and moreover $\operatorname{ord} g$ divides n.*

Proof of Theorem 2.2. Shown in class. □

Exercise 2.3. If G has finite order, then every element of G has finite order.

Definition 2.4. A group G is **cyclic** if there exists $g \in G$ such that every element of G is equal to g^n for some integer n. In which case, we write: $G = \langle g \rangle$, and say that g is a **generator** of G.
Note: The generator of of a cyclic group might not be unique.

Example 2.5. $(U_m, \cdot)$ is cyclic.

Exercise 2.6. A finite cyclic group G has order (i.e. size) n if and only if each of its generators has order n.

Exercise 2.7. $(\mathbb{Q}, +)$ is not cyclic.

2.1 Permutations

Definition 2.8. Let X be a set. A **permutation** of X is a bijective map $\sigma : X \longrightarrow X$.

Claim 2.9. *The set S_X of permutations of a set X is a group with respect to $\circ$, the composition of maps.*

Proof of Claim 2.9.

- Let σ, γ be permutations of X. By definition, they are bijective maps from X to itself. It is clear that $\sigma \circ \gamma$ is a bijective map from X to itself, hence $\sigma \circ \gamma$ is a permutation of X. So $\circ$ is a well-defined binary operation on S_X.
- For $\alpha, \beta, \gamma \in S_X$, it is clear that $\alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma$.
- Define a map $e : X \longrightarrow X$ as follows:
  $$e(x) = x, \quad \text{for all } x \in X.$$
  It is clear that $e \in S_X$, and that $e \circ \sigma = \sigma \circ e = \sigma$ for all $\sigma \in S_X$. Hence, e is an identity element in S_X.
- Let σ be any element of S_X. Since $\sigma : X \longrightarrow X$ is by assumption bijective, there exists a bijective map $\sigma^{-1} : X \longrightarrow X$ such that $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = e$. So σ^{-1} is an inverse of σ with respect to the operation $\circ$.

□

Terminology: We call S_X the **Symmetric Group** on X.
Notation: If $X = \{1, 2, \ldots, n\}$, where $n \in \mathbb{N}$, we denote S_X by S_n.
For $n \in \mathbb{N}$, the group S_n has $n!$ elements.
For $n \in \mathbb{N}$, by definition an element of S_n is a bijective map $\sigma : X \longrightarrow X$, where $X = \{1, 2, \ldots, n\}$. We often describe σ using the following notation:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$$

Example 2.10. In S_3,

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

is the permutation on $\{1, 2, 3\}$ which sends 1 to 3, 2 to itself, and 3 to 1, i.e. $\sigma(1) = 3, \sigma(2) = 2, \sigma(3) = 1$.
For $\alpha, \beta \in S_3$ given by:

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

we have:

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

(since, for example, $\alpha \circ \beta : 1 \overset{\beta}{\mapsto} 2 \overset{\alpha}{\mapsto} 3$.).

We also have:

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

Since $\alpha\beta \neq \beta\alpha$, the group S_3 is non-abelian.

In general, for $n > 2$, the group S_n is non-abelian (**Exercise:** Why?).

For the same $\alpha \in S_3$ defined above, we have:

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

and:

$$\alpha^3 = \alpha \cdot \alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$$

Hence, the order of α is 3.

2.2 Dihedral Group

Consider the subset $\mathcal{T}$ of transformations of $\mathbb{R}^2$, consisting of all rotations by fixed angles about the origin, and all reflections over lines through the origin.

Consider a regular polygon P with n sides in $\mathbb{R}^2$, centered at the origin. Identify the polygon with its n vertices, which form a subset $P = \{x_1, x_2, \ldots, x_n\}$ of $\mathbb{R}^2$. If $\tau(P) = P$ for some $\tau \in \mathcal{T}$, we say that P is **symmetric** with respect to τ.

Intuitively, it is clear that P is symmetric with respect to n rotations $\{r_0, r_1, \ldots, r_{n-1}\}$, and n reflections $\{s_1, s_2, \ldots, s_n\}$ in $\mathcal{T}$.

IMAGE (Public Domain, Link)

Theorem 2.11. *The set $D_n := \{r_0, r_1, \ldots, r_{n-1}, s_1, s_2, \ldots, s_n\}$ is a group, with respect to the group operation defined by $\tau * \gamma = \tau \circ \gamma$ (composition of transformations).*

Terminology: D_n is called a **dihedral group** .

2.3 More on S_n

Consider the following element in S_6:

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

We may describe the action of $\sigma : \{1, 2, \ldots, 6\} \longrightarrow \{1, 2, \ldots, 6\}$ using the notation:

$$\sigma = (15)(246),$$

where $(n_1 n_2 \cdots n_k)$ represents the permutation:

$$n_1 \mapsto n_2 \ldots n_i \mapsto n_{i+1} \cdots \mapsto n_k \mapsto n_1$$

Viewing permutations as bijective maps, the "multiplication" $(15)(246)$ is by definition the composition $(15) \circ (246)$.

We call $(n_1 n_2 \cdots n_k)$ a k-**cycle** . Note that 3 is missing from $(15)(246)$. This corresponds to the fact that 3 is fixed by σ.

Exercise 2.12. In S_n, for any positive integer $k \leq n$, every k-cycle has order k.

Claim 2.13. *Every non-identity permutation in S_n is either a cycle or a product of disjoint cycles.*

Proof of Claim 2.13. Discussed in class. □

Exercise 2.14. Disjoint cycles commute with each other.

A 2-cycle is often called a **transposition**, for it switches two elements with each other.

Claim 2.15. *Each element of S_n is a product of (not necessarily disjoint) transpositions.*

Sketch of proof:

Show that each permutation not equal to the identity is a product of cycles, and that each cycle is a product of transpositions:

$$(a_1 a_2 \ldots a_k) = (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_3)(a_1 a_2)$$

Example 2.16.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 6 & 1 & 2 \end{pmatrix} = (15)(246)$$
$$= (15)(26)(24)$$
$$= (15)(46)(26)$$

Note that a given element σ of S_n may be expressed as a product of transpositions in different ways, but:

Claim 2.17. *In every factorization of σ as a product of transpositions, the number of factors is either always even or always odd.*

Proof of Claim 2.17. **Exercise.** One approach: Show that there is a unique $n \times n$ matrix, with either 0 or 1 as its coefficients, which sends each standard basis vector $\vec{e}_i$ in $\mathbb{R}^n$ to $\vec{e}_{\sigma(i)}$. Then, use the fact that the determinant of the matrix corresponding to a transposition is -1, and that the determinant function of matrices is multiplicative. □

2.4 WeBWorK

1. **WeBWorK**
2. **WeBWorK**
3. **WeBWorK**
4. **WeBWorK**
5. **WeBWorK**
6. **WeBWorK**