Week 2

2.1 Cyclic groups

Definition. Let G be a group, with identity element e. The **order** of an *element* $g \in G$, denoted by $|g|$, is the smallest positive integer n such that $g^n = e$; if no such n exists, we say that g has **infinite order** and write $|g| = \infty$.

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

Proposition 2.1.1. *Let G be a group with identity element e. Let g be an element of G. If $g^n = e$ for some $n \in \mathbb{Z}_{>0}$, then $|g|$ divides n.*

Proof. Let $m = |g|$. Suppose $g^n = e$. By the Division Theorem, there exist (uniquely) integers q and $0 \leq r < m$ such that $n = mq + r$. So $g^n = (g^m)^q \cdot g^r$ which implies that $g^r = e$. This forces $r = 0$ (since otherwise this violates the definition of $|g| = m$). Hence $m \mid n$. $\square$

Given an element g in a group G, we define the subset $\langle g \rangle \subset G$ as the set of all integral powers of g:

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}.$$

Recall that

$$|g| = \begin{cases} \min\{n \in \mathbb{Z}_{>0} : g^n = e\} & \text{if } \exists n \in \mathbb{Z}_{>0} \text{ such that } g^n = e, \\ \infty & \text{otherwise.} \end{cases}$$

Proposition 2.1.2. *If $|g| = \infty$, then $\langle g \rangle$ is an infinite set; in fact, the map $\mathbb{Z} \to \langle g \rangle$, $n \mapsto g^n$ is a bijection. If $|g| = m < \infty$, then*

$$\langle g \rangle = \{e, g, g^2, \ldots, g^{m-1}\}.$$

Proof. Suppose $|g| = \infty$. It follows from the definition of $\langle g \rangle$ that the map $\mathbb{Z} \to \langle g \rangle$, $n \mapsto g^n$ is surjective. So we only need to show that it is also injective.

Suppose $g^{n_1} = g^{n_2}$ for some $n_1, n_2 \in \mathbb{Z}$. If $n_1 \neq n_2$, then without loss of generality, we can assume that $n_1 > n_2$. Then we have $g^{n_1 - n_2} = e$ with $n_1 - n_2 \in \mathbb{Z}_{>0}$. But this violates the assumption that $|g| = \infty$. Hence we must have $n_1 = n_2$, showing the required injectivity.

When $|g| = m < \infty$, we want to show that $\langle g \rangle = \{e, g, g^2, \ldots, g^{m-1}\}$. Clearly we have $\langle g \rangle \supset \{e, g, g^2, \ldots, g^{m-1}\}$, so we only need to prove the reverse inclusion. Take an element $g^n \in \langle g \rangle$. Then the Division Theorem implies that there exist integers q and $0 \leq r < m$ such that $n = mq + r$. So $g^n = (g^m)^q \cdot g^r = g^r \in \{e, g, g^2, \ldots, g^{m-1}\}$. This completes the proof. □

Definition. 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 this case, we write $G = \langle g \rangle$, and say that g is a **generator** of G.

Remark. The generator of of a cyclic group might not be unique, i.e. there may exist *different* elements $g_1, g_2 \in G$ such that $G = \langle g_1 \rangle = \langle g_2 \rangle$.

Example 2.1.3.

- $(\mathbb{Z}, +)$ is cyclic, generated by 1 or -1.
- $(\mathbb{Z}_n, +)$ is cyclic, generated by 1, or $k \in \mathbb{Z}_n$ such that $\gcd(k, n) = 1$.
- $(U_m, \cdot)$ is cyclic, generated by $\zeta_m = e^{2\pi \mathbf{i}/m}$, or ζ_m^n for any integer $n \in \mathbb{Z}_m$ such that $\gcd(m, n) = 1$.

Exercise: A finite cyclic group G has order n if and only if each of its generators has order n.

Exercise: The group $(\mathbb{Q}, +)$ is not cyclic.

Example 2.1.4. Let p be a prime. Let $G = (\mathbb{Z}_p, +)$. For all $g \neq 0$ in G, the order of g is p.

Proof. **Exercise.** □

Proposition 2.1.5. *Every cyclic group is abelian*

Proof. Let G be a cyclic group. Then $G = \langle g \rangle$ for some element $g \in G$ and every element is of the form g^n for some $n \in \mathbb{Z}$. Now

$$g^{n_1} \cdot g^{n_2} = g^{n_1 + n_2} = g^{n_2 + n_1} = g^{n_2} \cdot g^{n_1}.$$

So G is abelian. □

Remark. The converse is not true, namely, there are non-cyclic abelian groups (e.g. the *Klein 4-group* $\mathbb{Z}_2 \times \mathbb{Z}_2$).

2.2 Symmetric groups

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

Proposition 2.2.1. *The set S_X of permutations of a set X is a group with respect to $\circ$, the composition of maps.*

Proof.
- 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 $\circ$.

$\square$

Terminology: We call S_X the **symmetric group** on X.

Notation. Let n be a positive integer. Consider the set $I_n := \{1, 2, \ldots, n\}$. Then we denote S_{I_n} by S_n and call it the n**-th symmetric group**.

For $n \in \mathbb{Z}_{>0}$, the group S_n has $n!$ elements.

For $n \in \mathbb{Z}_{>0}$, by definition an element of S_n is a bijective map $\sigma : I_n \longrightarrow I_n$, where $I_n = \{1, 2, \ldots, n\}$. 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 2.2.2. In S_3,

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

is the permutation on $I_3 = \{1, 2, 3\}$ 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 $n \geq 3$, 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.

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

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

where $(i_1 i_2 \cdots i_k)$ denotes the permutation:

$$i_1 \mapsto i_2, i_2 \mapsto i_3, \ldots, i_{k-1} \mapsto i_k, i_k \mapsto i_1$$

and $j \mapsto j$ for all $j \in \{1, 2, \ldots, n\} \backslash \{i_1, i_2, \ldots, i_k\}$. We call $(i_1 i_2 \cdots i_k)$ a **k-cycle** or a **cycle of length k**. Note that 3 is missing from $(15)(246)$, meaning that 3 is fixed by σ.

Proposition 2.2.3. *Every permutation $\alpha \in S_n$ is either a cycle or a product of disjoint cycles.*

Proof. Later. $\square$

Exercise: Disjoint cycles commute with each other.

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