Week 1

1.1 Groups

Definition. A **group** is a set G equipped with a binary operation

$$* : G \times G \longrightarrow G$$

(called the **group operation** or "**product**" or "**multiplication**") such that the following conditions are satisfied:

- The group operation is **associative**, i.e.

  $$(a * b) * c = a * (b * c)$$

  for all $a, b, c \in G$.

- There is an element $e \in G$, called an **identity element**, such that

  $$a * e = e * a = a,$$

  for all $a \in G$.

- For every $a \in G$ there exists an element $a^{-1} \in G$, called an **inverse** of a, such that

  $$a^{-1} * a = a * a^{-1} = e.$$

Remark. We often write $a \cdot b$ or simply ab to denote $a * b$.

Definition. If $ab = ba$ for all $a, b \in G$, we say that the group operation is **commutative** and that G is an **abelian group**; otherwise we say that G is **nonabelian**.

Remark. When the group is abelian, we often use $+$ to denote the group operation.

Definition. The **order** of a group G, denoted by $|G|$, is the number of elements in G. We say that G is **finite** (resp. **infinite**) if $|G|$ is finite (resp. infinite).

Example 1.1.1. The following sets are groups, with respect to the specified group operations:

- $G = \mathbb{Q}$, where the group operation is the usual addition $+$ for rational numbers. The identity is $e = 0$. The inverse of $a \in \mathbb{Q}$ with respect to $+$ is $-a$. This is an infinite abelian group.

- $G = \mathbb{Q}^\times = \mathbb{Q}\backslash\{0\}$, where the group operation is the usual multiplication for rational numbers. The identity is $e = 1$, and the inverse of $a \in \mathbb{Q}^\times$ is $a^{-1} = \frac{1}{a}$. This group is also infinite and abelian.

  Note that $\mathbb{Q}$ is *not* a group with respect to multiplication. For in that case, we have $e = 1$, but $0 \in \mathbb{Q}$ has no inverse $0^{-1} \in \mathbb{Q}$ such that $0 \cdot 0^{-1} = 1$.

Exercise: Verify that the following sets are groups under the specified binary operations:

- $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$.

- $(\mathbb{R}^\times = \mathbb{R}\backslash\{0\}, \cdot)$, $(\mathbb{C}^\times = \mathbb{C}\backslash\{0\}, \cdot)$

- $(U_m, \cdot)$, where $m \in \mathbb{Z}_{>0}$,
$$U_m = \{1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{m-1}\}$$
  and $\zeta_m = e^{2\pi \mathbf{i}/m} = \cos(2\pi/m) + \mathbf{i}\sin(2\pi/m) \in \mathbb{C}$.

- The set of bijective functions $f : \mathbb{R} \longrightarrow \mathbb{R}$, where $f * g := f \circ g$ (i.e. composition of functions).

- More generally, one can consider any nonempty set X. Then the set
$$S_X := \{\sigma : X \to X : \sigma \text{ is bijective}\}$$
  of all bijective maps from X onto X is a group under composition of maps.

Example 1.1.2. The set $G = \mathrm{GL}(2, \mathbb{R})$ of real 2×2 matrices with nonzero determinants is a group under matrix multiplication, with identity element:
$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$
In the group G, we have:
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Note that there are matrices $A, B \in \mathrm{GL}(2, \mathbb{R})$ such that $AB \neq BA$. Hence $\mathrm{GL}(2, \mathbb{R})$ is nonabelian (and infinite).

More generally, for any $n \in \mathbb{Z}_{>0}$, the set $\mathrm{GL}(n, \mathbb{R})$ of $n \times n$ real matrices M, such that $\det M \neq 0$, is a group under matrix multiplication, called the **General Linear Group**. The group $\mathrm{GL}(n, \mathbb{R})$ is nonabelian for $n \geq 2$.

Exercise: The set $\mathrm{SL}(n, \mathbb{R})$ of real $n \times n$ matrices with determinant 1 is a group under matrix multiplication, called the **Special Linear Group**.

Example 1.1.3. Let $n \in \mathbb{Z}_{>0}$. Consider the finite set

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}.$$

We define a binary operation $+_n$ on $\mathbb{Z}_n$ by

$$a +_n b = \begin{cases} a + b & \text{if } a + b < n, \\ a + b - n & \text{if } a + b \geq n. \end{cases}$$

for any $a, b \in \mathbb{Z}_n$.

Exercise: Then $(\mathbb{Z}_n, +_n)$ is a finite abelian group. (By abuse of notation, we will usually use the usual symbol $+$ to denote the additive operation for this group.)

Proposition 1.1.4. *The identity element e of a group G is unique.*

Proof. Suppose there is an element $e' \in G$ such that $e'g = ge'$ for all $g \in G$. Then, in particular, we have:

$$e'e = e$$

But since e is an identity element, we also have $e'e = e'$. Hence, $e' = e$. $\square$

Proposition 1.1.5. *Let G be a group. For all $g \in G$, its inverse g^{-1} is unique.*

Proof. Suppose there exists $g' \in G$ such that $g'g = gg' = e$. By the associativity of the group operation, we have:

$$g' = g'e = g'(gg^{-1}) = (g'g)g^{-1} = eg^{-1} = g^{-1}.$$

Hence, g^{-1} is unique. $\square$

Let G be a group with identity element e. For $g \in G$, $n \in \mathbb{N}$, let:

$$\begin{aligned} g^n &:= \underbrace{g \cdot g \cdots g}_{n \text{ times}}. \\ g^{-n} &:= \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{n \text{ times}} \\ g^0 &:= e. \end{aligned}$$

Proposition 1.1.6. *Let G be a group.*

1. *For all $g \in G$, we have:*
$$(g^{-1})^{-1} = g.$$

2. *For all $a, b \in G$, we have:*
$$(ab)^{-1} = b^{-1}a^{-1}.$$

3. *For all $g \in G$, $n, m \in \mathbb{Z}$, we have:*
$$g^n \cdot g^m = g^{n+m}.$$

Proof. **Exercise.** $\square$