2. Examples of Groups

2.1. **Some infinite abelian groups.** It is easy to see that the following are infinite abelian groups:

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

where $\mathbb{R}$ is the set of real numbers and $\mathbb{C}$ is the set of complex numbers,

$$(\mathbb{Q}^*,\,\cdot\,),\ (\mathbb{R}^*,\,\cdot\,),\ (\mathbb{C}^*,\,\cdot\,),$$

where the star means "without 0",

$$(\mathbb{Q}^+,\,\cdot\,),\ (\mathbb{R}^+,\,\cdot\,),$$

where the plus-sign means "just positive numbers", and

$$(\mathbb{U},\,\cdot\,),$$

where $\mathbb{U} = \{z \in C : |z| = 1\}$.

Let $2^{\mathbb{Z}} := \{2^x : x \in \mathbb{Z}\} = \{1, 2, \frac{1}{2}, 4, \frac{1}{4}, 8, \frac{1}{8}, \dots\}$, then $(2^{\mathbb{Z}},\,\cdot\,)$ is a group:

(0) Multiplication is associative (and even commutative): For all $x, y, z \in \mathbb{Z}$ we have

$$2^x \cdot \big(2^y \cdot 2^z\big) = 2^{x+(y+z)} = 2^{(x+y)+z} = \big(2^x \cdot 2^y\big) \cdot 2^z\,.$$

(1) $2^0 = 1$ is the neutral element: For all $x \in \mathbb{Z}$ we have

$$2^0 \cdot 2^x = 2^x \cdot 2^0 = 2^{x+0} = 2^x\,.$$

(2) Every element in $2^{\mathbb{Z}}$ has an inverse: For all $x \in \mathbb{Z}$ we have

$$2^{-x} \cdot 2^x = 2^x \cdot 2^{-x} = 2^{x+(-x)} = 2^0\,.$$

The groups $(2^{\mathbb{Z}},\,\cdot\,)$ and $(\mathbb{Z},+)$ are essentially the same groups. To see this, let

$$\begin{array}{rccc} \varphi: & \mathbb{Z} & \longrightarrow & 2^{\mathbb{Z}} \\ & x & \longmapsto & 2^x \end{array}$$

It is easy to see that φ is a bijection (*i.e.*, a one-to-one mapping which is onto) between $\mathbb{Z}$ and $2^{\mathbb{Z}}$. Further, $\varphi(x+y) = 2^{x+y} = 2^x \cdot 2^y = \varphi(x) \cdot \varphi(y)$, and $\varphi(0) = 2^0 = 1$. So, the image under φ of $x + y$ is the same as the product of the images of x and y, and the image of the neutral element of the group $(\mathbb{Z},+)$ is the neutral element of the group $(2^{\mathbb{Z}},\,\cdot\,)$. Thus, the only difference between $(2^{\mathbb{Z}},\,\cdot\,)$ and $(\mathbb{Z},+)$ is that the elements as well as the operations have different names. This leads to the following:

Definition. Let $(G_1,\,\circ\,)$ and $(G_2,\,\bullet\,)$ be two groups. If there exists a bijection φ between G_1 and G_2 such that for all $x, y \in G_1$ we have

$$\varphi(x \circ y) = \varphi(x) \bullet \varphi(y)\,,$$

then the groups $(G_1,\,\circ\,)$ and $(G_2,\,\bullet\,)$ are called **isomorphic**, denoted by $G_1 \cong G_2$, and the mapping φ is called an **isomorphism**.

In other words, two groups are isomorphic if they are essentially the same groups (up to renaming the elements and the operation). In particular, all groups with 1 element are isomorphic.

2.2. **Some infinite non-abelian groups.** Let $\mathrm{M}(n)$ be the set of all n by n matrices with real numbers as entries. Notice that $\big(\mathrm{M}(n),\,\cdot\big)$ is *not* a group, even though there exists a unique neutral element, namely the n by n **identity matrix**

$$I_n := \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Let $\mathrm{GL}(n) := \big\{A \in \mathrm{M}(n) : \det(A) \neq 0\big\}$, then $\big(\mathrm{GL}(n),\,\cdot\big)$ is a group, the so-called **general linear group**. It is easy to see that $\mathrm{GL}(1)$ is isomorphic to $(\mathbb{R}^*,\,\cdot)$, but for $n > 1$, $\mathrm{GL}(n)$ is a non-abelian group, consider for example

$$\begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 3 & 1 \end{pmatrix} = \begin{pmatrix} 6 & 3 \\ 6 & 2 \end{pmatrix},$$
$$\begin{pmatrix} 0 & 1 \\ 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 3 & 8 \end{pmatrix}.$$

The so-called **special linear group** is $\mathrm{SL}(n) := \big\{A \in \mathrm{GL}(n) : \det(A) = 1\big\}$, where the operation is again matrix-multiplication. It is easy to see that $\mathrm{SL}(1)$ is isomorphic to $\big(\{1\},\,\cdot\big)$, but for $n > 1$, $\mathrm{SL}(n)$ is non-abelian group.

The so-called **orthogonal group** is $\mathrm{O}(n) := \big\{A \in \mathrm{M}(n) : AA^t = I_n\big\}$. It is easy to see that $\mathrm{O}(1)$ is isomorphic to $\big(\{-1, 1\},\,\cdot\big)$, but for $n > 1$, $\mathrm{O}(n)$ is a non-abelian group.

The so-called **special orthogonal group** is $\mathrm{SO}(n) := \big\{A \in \mathrm{O}(n) : \det(A) = 1\big\}$. It is easy to see that $\mathrm{SO}(1)$ is isomorphic to $\big(\{1\},\,\cdot\big)$. Further, each $A \in \mathrm{SO}(2)$ is of the form

$$A = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$$

for some $\alpha \in \mathbb{R}$, and therefore, the matrices in $\mathrm{SO}(2)$ are just rotations and the group $\mathrm{SO}(2)$ is abelian. In fact, $\mathrm{SO}(2)$ is isomorphic to $(\mathbb{U},\,\cdot)$. But for $n > 2$, $\mathrm{SO}(n)$ is a non-abelian group, consider for example the matrices

$$\begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}.$$

2.3. **Some finite abelian groups.** For a positive integer n, consider the set $C_n := \{a^0, a^1, \dots, a^{n-1}\}$. On C_n define a binary operation as follows:

$$a^\ell a^m = \begin{cases} a^{\ell+m} & \text{if } \ell + m < n, \\ a^{(\ell+m)-n} & \text{if } \ell + m \geq n. \end{cases}$$

For every positive integer n, C_n is an abelian group: First note that every $x \in \mathbb{Z}$ is of the form $x = sn + r$, where $s \in \mathbb{Z}$ and $r \in \{0, 1, \dots, n-1\}$, and we write $x \equiv r \pmod{n}$. In fact, $a^\ell a^m = a^r$, where $\ell + m \equiv r \pmod{n}$. Thus, $a^k\big(a^\ell a^m\big) = \big(a^k a^\ell\big)a^m = a^r$, where r is such that $k + \ell + m \equiv r \pmod{n}$, and $a^m a^\ell = a^\ell a^m$, which implies that the operation is associative and commutative.

The element a^0 is a neutral element, since $a^0 a^m = a^{0+m} = a^m$. Further, for all $s \in \mathbb{Z}$ we have $a^n = a^{sn} = a^0$, since $sn \equiv 0 \pmod{n}$. The inverse of $a^m \in C_n$ is a^{n-m}, since $a^m a^{n-m} = a^{m+(n-m)} = a^n = a^0$.

Definition. The group C_n is called the **cyclic group** of order n (since $|C_n| = n$).

2.4. **Some finite non-abelian groups.** Let X, Y and Z be three sets and let $f : X \to Y$ and $g : Y \to Z$ be two functions. The composition of f and g is a function from X to Z defined as follows:

$$(g \circ f)(x) := g\big(f(x)\big)\,.$$

Let $X = \{1, 2, \dots, n\}$ be a finite set and let S_n be the set of all bijections $\sigma : X \to X$. The composition "$\circ$" of two bijections $\sigma, \tau : X \to X$ is again a bijection, and therefore, "$\circ$" is a binary operation on S_n.

The operation "$\circ$" is associative:
For every $x \in X$ and any $\sigma, \tau, \pi \in S_n$ we have

$$\big((\sigma \circ \tau) \circ \pi\big)(x) = \big(\sigma \circ \tau\big)\big(\pi(x)\big) = \sigma\big(\tau\big(\pi(x)\big)\big)$$
$$\big(\sigma \circ (\tau \circ \pi)\big)(x) = \sigma\big((\tau \circ \pi)(x)\big) = \sigma\big(\tau\big(\pi(x)\big)\big)$$

The identity mapping is a bijection and a neutral element of S_n, and the inverse mapping of a bijection is also a bijection. So, S_n has a neutral element and each $\sigma \in S_n$ has an inverse, denoted by σ^{-1}, and therefore, S_n is a group.

Definition. The group S_n is called the **symmetric group** of degree n, or the **permutation group** of degree n.

Notice that $|S_n| = n!$, so, except for $n = 1$ and $n = 2$, the order of S_n is strictly greater than n. Let us consider S_n for small values of n.

S_1: $|S_1| = 1$, namely the identity mapping $\iota : 1 \mapsto 1$. Since every group with just one element is isomorphic to C_1, we have $S_1 \cong C_1$.

S_2: $|S_2| = 2$, namely the identity mapping ι and the permutation $\sigma : \begin{cases} 1 & \mapsto & 2 \\ 2 & \mapsto & 1 \end{cases}$.
Since every group with just two elements is isomorphic to C_2, we have $S_2 \cong C_2$.

S_3: $|S_3| = 6$. Consider the permutations $\sigma : \begin{cases} 1 & \mapsto & 2 \\ 2 & \mapsto & 1 \\ 3 & \mapsto & 3 \end{cases}$ and $\tau : \begin{cases} 1 & \mapsto & 1 \\ 2 & \mapsto & 3 \\ 3 & \mapsto & 2 \end{cases}$.

Now,

$$(\sigma \circ \tau)(1) = \sigma\big(\tau(1)\big) = \sigma(1) = 2\,,$$
$$(\tau \circ \sigma)(1) = \tau\big(\sigma(1)\big) = \tau(2) = 3\,,$$

thus, S_3 is a non-abelian group. In fact, for every $n \geq 3$, S_n is a non-abelian group.

Let us now consider a special class of groups, namely the group of rigid motions of a two or three-dimensional solid.

Definition. A **rigid motion** of a solid S is a bijection $\varphi : S \to S$ which has the following property: The solid S can be moved through 3-dimensional Euclidean space in such a way that it does not change its shape and when the movement stops, each point $p \in S$ is in position $\varphi(p)$.

Since rigid motions are special kinds of bijections, for every solid S, the set of all rigid motions of S together with composition (as operation) is a group. In this course we will investigate in depth the groups of rigid motions of the five Platonic solids, which are tetrahedron, cube, octahedron, dodecahedron, and icosahedron. But first, let us consider a simpler solid, namely a regular n-sided polygon.

DEFINITION. The group of rigid motions of a regular n-sided polygon (for $n \geq 3$) is called the **dihedral group** of degree n and is denoted by D_n.

Let us consider first D_3: D_3 has 6 elements, namely the identity ι, two non-trivial rotations say ρ_1 and ρ_2, and three reflections say σ_1, σ_2, and σ_3. If we label the vertices of the regular triangle with 1, 2, and 3, then every permutation of $\{1, 2, 3\}$ corresponds to an element of D_3, and since $|D_3| = 6 = |S_3|$, $D_3 \cong S_3$. In particular, D_3 is a non-abelian group. In fact, for every $n \geq 3$, D_n is a non-abelian group.

2.5. **Representing finite groups by multiplication tables.** Let $S = \{a, b, c, \dots\}$ be a finite set with some binary operation "$\circ$". Then the following table is the so-called multiplication table of S:

$\circ$	a	b	c	$\cdots$
a	$a \circ a$	$a \circ b$	$a \circ c$	$\cdots$
b	$b \circ a$	$b \circ b$	$b \circ c$	$\cdots$
c	$c \circ a$	$c \circ b$	$\cdots$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

For example, the multiplication table of $C_4 = \{e, a, a^2, a^3\}$, where $e = a^0$, is as follows:

$\circ$	e	a	a^2	a^3
e	e	a	a^2	a^3
a	a	a^2	a^3	e
a^2	a^2	a^3	e	a
a^3	a^3	e	a	a^2

A multiplication table of a group is often called its **Cayley table**. Note that not every multiplication table is a Cayley table (see Hw3.Q11).

2.6. **Products of groups.** Let $(G, *_G)$ and $(H, *_H)$ be any groups (not necessarily finite groups), then

$$G \times H := \big\{ \langle x, y \rangle : x \in G \text{ and } y \in H \big\} .$$

On the set $G \times H$ we define an operation "$\circ$" as follows:

$$\langle x_1, y_1 \rangle \circ \langle x_2, y_2 \rangle := \langle x_1 *_G x_2, y_1 *_H y_2 \rangle .$$

It is easy to verify that $(G \times H, \circ)$ is a group and that it is abelian if and only if G and H are both abelian (see Hw3.Q12).

Let us consider the abelian group $C_2 \times C_2$: By definition we have $|C_2 \times C_2| = |C_2| \cdot |C_2| = 4$. Let $C_2 = \{a^0, a^1\}$ and let $e = \langle a^0, a^0 \rangle$, $x = \langle a^0, a^1 \rangle$, $y = \langle a^1, a^0 \rangle$, and $z = \langle a^1, a^1 \rangle$. In this notation, $C_2 \times C_2$ has the following Cayley table:

$\circ$	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

It is easy to see that $C_2 \times C_2$ is not isomorphic to C_4 and we will see later that these two groups are essentially the only groups of order 4. If p and q are positive integers such that $\gcd(p, q) = 1$, then $C_p \times C_q \cong C_{pq}$ (see Hw3.Q14.a), but in general, $C_p \times C_q$ is not isomorphic to C_{pq}, *e.g.*, let $p = q = 2$ (see also Hw3.Q14.b).