# 1. Groups

## Quick Review of Group Theory

### Key definitions

**Definition:** A group is a set

$$G$$

together with a map

$$m : G \times G \to G$$

satisfying the following axioms:

1. There is an element $e \in G$ such that $m(e, x) = m(x, e) = x$ for all $x \in G$.
2. For all $x, y, z \in G$, we have $m(x, m(y, z)) = m(m(x, y), z)$.
3. For all $x \in G$, there is $y \in G$ such that $m(x, y) = m(y, x) = e$.

We usually just write $ab$ or $a + b$ for $m(a, b)$; and we usually write $G$, rather than $(G, m)$ when speaking about a group.

One can weaken these axioms in various ways and obtain an equivalent definition.

For any group $G$ and $x \in G$:

- there is only one element $e$ satisfying axiom (1).
- the regrouping in axiom (2) extends to arbitrary many elements, so the product $a_1 a_2 \cdots a_n$ is well defined for any set of elements $a_1, a_2, \ldots, a_n \in G$.
- the inverse $y$ for $x$ required by axiom (3) is unique.

**Definition:** If $G$ is a group and $ab = ba$ for all $a, b \in G$ then $G$ is called *abelian*.

**Definition:** If $G$ is a group and $g \in G$ then the *order* of $g$ is the smallest positive integer $n$ such that $g^n = e$ (or infinity, if no such $n$ exists).

**Definition:** If $G$ is a group, and $H$ is a nonempty subset of $G$ which is a group when the multiplication of $G$ is restricted to $H$, then $H$ is called a *subgroup* of $G$. $H$ is a subgroup if: - for all $a, b \in H$, $ab \in H$, - if $a \in H$, then $a^{-1} \in H$.

**Definition:** If $G$ and $H$ are groups, and $f : G \to H$ is a function, then $f$ is called a *homomorphism* if $f(ab) = f(a)f(b)$ for all $a, b \in G$ and and *isomorphism* if it is a bijective homomorphism. The *kernel* of a homomorphism $f$ is the subgroup of $G$ consisting of elements $g$ such that $f(g) = e$. The *image* of a homomorphism $f$ is the subgroup of $H$ consisting of elements $h \in H$ such that $h = f(g)$ for some $g \in G$.

**Definition:** If $G$ is a group and $X$ is a set, then a map $m : G \times X \to X$ is called a (left) action of $G$ on $X$ if $m(e,x) = x$ for all $x \in X$ and $m(a, m(b,x)) = m(ab, x)$ for all $a, b \in G$ and $x \in X$. We usually write $ax$ for $m(a,x)$.

**Examples**

1. The integers, rational numbers, real numbers, and complex numbers are all groups under addition.
2. The nonzero rational numbers, real numbers, and complex numbers are all groups under multiplication.
3. For $n > 0$, the set $\mathbb{Z}/n\mathbb{Z}$ of integers modulo $n$ are a group under addition.
4. The subset of $\mathbb{Z}/n\mathbb{Z}$ consisting of elements $a$ that are invertible (i.e. such that the congruence $ax \equiv 1 \pmod{n}$ has a solution) form a group under multiplication. This group is called $(\mathbb{Z}/n\mathbb{Z})^{\times}$. If $n = p$ is prime, then $(\mathbb{Z}/p\mathbb{Z})^{*}$ consists of the $p-1$ nonzero congruence classes.
5. The invertible $n \times n$ matrices $\mathrm{GL}_n(F)$ where $F$ is any of $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ form a group under matrix multiplication. These groups come with actions on $F^n$ given by matrix multiplication.
6. For any set $X$, the set of bijective maps $X \to X$ form a group under composition of functions. This group is called the *symmetric group* $S(X)$ on $X$. If there is a bijection from $X$ to $Y$, then $S(X)$ and $S(Y)$ are isomorphic. If $X =$
   $1, 2, 3, \ldots, n$ then $S(X)$ is usually written $S_n$ and is called the symmetric group on $n$ elements. Notice that $S(X)$ comes with an action on $X$ given by $(f, x) \mapsto f(x)$.
7. If $X$ is a regular $n - gon$ in the plane, the group of rigid motions $f$ of the plane such that $f(X) = X$ form a group under composition called the Dihedral group. Dummit and Foote call this group $D_{2n}$ since it has $2n$ elements, but others call it $D_n$ since it is the symmetries of an $n$-gon. The elements of $D_{2n}$ consist of

   $$\{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$$

   and the group law is determined by the rules $r^i r^j = r^{i+j}$ with exponents read modulo $n$, $s^2 = 1$, and $sr = r^{-1}s$. The group $D_{2n}$ comes with an action on the $n$ vertices of $X$ by $(f, v) \mapsto f(v)$ and on the $n$ sides of $v$ by $(f, s) = f(s)$.

## Cyclic Groups

**Definition:** A group $G$ is cyclic if there is an element $g \in G$ such that the homomorphism

$$\phi_g : \mathbb{Z} \to G$$

defined by $\phi_g(n) = g^n$ is surjective.

**Proposition:** Let $H \subset \mathbb{Z}$ be a propersubgroup. Then either $H = \{0\}$ or there is a unique $n > 0$ such that $H = n\mathbb{Z}$.

**Corollary:** A cyclic group is isomorphic either to $\mathbb{Z}$ or to $\mathbb{Z}/n\mathbb{Z}$ for some integer $n > 0$.

**Properties of order:** Let $G$ be a group and $x \in G$.

1. If $x^a$ has infinite order for some $a$, so do all nonzero powers of $x$.
2. If $x^a = e$ and $x^b = e$ then $x^{\gcd(a,b)} = e$.
3. If $x^a = e$ then the order of $x$ divides $a$.
4. If $x$ has order $a$, then $x^k$ has order $a/\gcd(a,k)$.
5. If $G$ is cyclic of order $n$ generated by $x$, then $x^a$ generates $G$ if and only if $\gcd(a,n) = 1$.

**Proposition:** The subgroups of $G = \mathbb{Z}/n\mathbb{Z}$ are in bijection with the divisors of $n$. If $d$ is a divisor of $n$, then the unique subgroup of $G$ of order $d$ is generated by $n/d$.

## Euclid's Algorithm and Congruences

**Theorem:** Let $a$ and $b$ be nonzero integers. Then there exist integers $x$ and $y$ such that

$$ax + by = d$$

where $d$ is the greatest common divisor of $a$ and $b$.

**Theorem:** Let $n$ be a positive integer. The congruence equation

$$ax \equiv b \pmod{n}$$

has solutions if and only if $d = \gcd(a,n)$ divides $b$. If this condition is satisfied, it has $d$ solutions of the form

$$x_0 + k\frac{n}{d} \quad k = 0, \ldots, d-1$$

where $x_0$ is a representative for the unique solution to the congruence

$$\frac{a}{d}x_0 \equiv \frac{b}{d} \pmod{\frac{n}{d}}.$$

**Remark:** Notice that the congruence equation problem is equivalent to finding $x$ and $y$ so that

$$ax + ny = b.$$