# MAT347: Groups, Rings and Fields

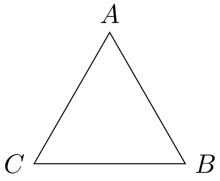
QiLin Xue

Fall 2021

## Contents

# 1 Group Theory

Group theory and symmetry are closely related. Consider the following equilateral triangle made up of some stiff material, allowing it to perform rigid motion.



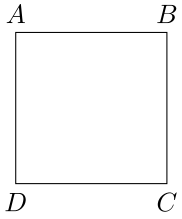
There are six symmetries:

- rotations $2\pi/3 : A \to C \to B \to A$
- rotations $4\pi/3 : A \to B \to C \to A$
- reflections $C \leftrightarrow B, C \leftrightarrow A$, or $A \leftrightarrow B$
- identity transformation: $A \to A, B \to B, C \to C$ : denoted as either id or $e$.

Let $\rho$ be a rotation through $2\pi/3$ and $\sigma$ a reflection $C \leftrightarrow B$. We want to compose them as $\rho\sigma$, which takes $ABC \to ACB \to CBA$. Therefore, $A \leftrightarrow C$, so this becomes another reflection. Similarly, $\sigma\rho$ takes $ABC \to CAB \to BAC$, which results in an overall $A \leftrightarrow B$, resulting in another but *different* reflection.

Here, $\sigma$ and $\rho$ are symmetries. Applying these to a triangle will still give us a triangle, so it makes sense that their composition will be a symmetry as well. However, the order of composition may make a difference. Some terminology: if $\sigma\rho = \rho\sigma$, we say the two elements **commute**.

For a square, there are eight symmetries:



Namely, the identity $e$, 3 rotations, and 4 reflections. Note that in each symmetry, $\alpha$ has an inverse $\alpha^{-1}$ with the property that $\alpha\alpha^{-1} = e = \alpha^{-1}\alpha$.

**Definition**: A **group** is a set $G$ with a composition:

$$\begin{aligned} G \times G &\to G \\ (g, h) &\mapsto gh \sim g \circ h \end{aligned}$$

satisfying:

1. Associativity: $(gh)k = g(hk)$
2. Identity: $\exists e \in G$ such that $eg = ge = g, \forall g \in G$
3. For every $g \in G, \exists g^{-1} \in G$ such that $g^{-1}g = gg^{-1} = e$

We can look at some examples.

- $\mathbb{Z}$ with $+$ is a group, where $e = 0$ and $n^{-1} = -n$. Likewise, this is true for any field.
- The multiplicative group $F^{\times} = F \setminus \{0\}$ has identity $1$ and the inverse of $x$ is $x^{-1} = 1/x$.
- $\mathbb{Z}/n\mathbb{Z}$ (addition modulo $n$)
- $SL(n, F)$ (special linear group) = all $n \times n$ matrices over a field $F$ whose determinant equals $1$.
- $GL(n, F)$ (general linear group) = all invertible $n \times n$ matrices
- $SO(n, F)$ (special orthogonal group) = $\{A \in SL(n, F) | A^T = A^{-1}\}$

**Example 1:** $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$ is one of the simplest groups where addition is done under modulo $n$. That is, if $n = 8$ we have $5 + 7 = 12 \equiv 4$.
*Notation:* we can write elements with a bar at the top. For example, $\bar{5} + \bar{7} = \bar{4}$. Note that $\bar{k}^{-1} = \overline{-k} = \overline{n-k}$.

An alternative way to express elements is through the bijection:

$$\bar{k} \leftrightarrow e^{2\pi ik/n},$$

and the group operation is multiplication in $\mathbb{C}^{\times}$. Here, $\mathbb{Z}/n\mathbb{Z}$ is known as a cyclic group.

We often denote the **cyclic group** of order $n$ by $C_n$. The **order** of a group $G$ is its cardinality, denoted as $|G|$ or $\text{ord}(G)$. Using this notation,

$$\begin{aligned} |C_n| &= n \\ |\text{triangle group}| &= 6 \\ |\text{rigid motions of square}| &= 8 \\ |(\mathbb{R}, +)| &= \infty. \end{aligned}$$

**Example 2:** The **quaternion group** is written as

$$\mathbb{H} = \{\pm 1, \pm i, \pm j, \pm k\}, \qquad |\mathbb{H}| = 8, \tag{1.1}$$

with $1 = \text{id}$, and the group operation is given by

$$\begin{aligned} ij &= -ji = k \\ jk &= -kj = i \\ ki &= -ik = j \\ i^2 &= j^2 = k^2 = -1. \end{aligned}$$

Note that $\mathbb{H}$ sometimes refers to

$$\{a1 + bi + cj + dk | a, b, c, d \in \mathbb{R}\},$$

which is closely related but not the same. We will be working with the first definition.

Recall that in our triangle group, we can find a smaller group (cyclic of order 3) $\{e, \rho, \rho^2\}$ that also forms a group. This is known as a **subgroup.**

**Definition**: A nonempty subset $H$ of a group $G$ is a subgroup and we write $H \leq G$, if H is a group using the same operations as G. This means that if $h, k \in H$, then $hk \in H$ and $h^{-1} \in H$.

**Proposition 1:** If $\emptyset \neq H \subseteq G$, then $H \leq G$ if and only if $hk^{-1} \in H, \forall h, k \in H$.

As a non-example, if $F$ is a field, then $F^{\times} = F \setminus \{0\}$ is a non-empty subset of $F$ and is also a group, but it is not a subgroup of $F^{+}$, since the group operation is different.

**Example 3:** Recall that in $\mathbb{H}$, we have $i, i^2 = -1, i^3 = -i, i^4 = 1$, so $\{1, i, -1, -i\}$ is a cyclic subgroup of order $4$. Sometimes, we write this as $\langle i \rangle$, which is the group **generated** by $i$.

A direct corollary is that if $g_1, \ldots, g_m \in G$, then $\langle g_1, \ldots, g_m \rangle$ is the smallest subgroup of $G$ that contains $g_1, \ldots, g_m$. Here, $g_1, \ldots, g_m$ are known as the **generators** of the subgroup, but are not uniquely determined.

**Definition**: Let $G$ be a group and $H \leq G$. Consider sets of the form

$$Hg = \{hg | h \in H\}$$

for some fixed $g \in G$. This is a **coset** of H. And in particular, it is a **right coset**.

Let us investigate properties of cosets. Consider $Hg$ and $Hg'$ for some $g, g' \in G$. These cosets might be disjoint, but we will first look at the case in which they intersect. In other words, $hg = h'g'$ for some $h, h' \in H$. Multiplying both sides by $h^{-1}$, we have

$$g = h^{-1}h'g' \in Hg',$$

since $h^{-1}h' \in H$. Similarly, we have $g' \in Hg$.

Now consider an arbitrary element of $Hg$, which we write as $kg$, with $k \in H$. Then:

$$kg = kh^{-1}h'g' \in Hg'.$$

This is true for all $k \in Hg$, so $Hg \subseteq Hg'$. By symmetry, we also have $Hg' \subseteq Hg$, so $Hg = Hg'$. This leads us to an important result,

> **Proposition 2:** The (right) cosets of $H$ partition $G$, so
>
> $$G = \bigsqcup Hg,$$
>
> where $\{g_i\}$ are representative elements of disjoint cosets.

Recall that for a fixed $g$, if $hg = h'g$, then $h = h'$. This means in $Hg$, each $h \in H$ gives a different element $hg$, so

$$|Hg| = |H|.$$

Therefore,

$$|G| = (\# \text{ of distinct right cosets}) \cdot |H|.$$

This proves Lagrange's Theorem,

> **Theorem:** If $|G| < \infty$ and $H \leq G$, then $|H|$ divides $|G|$.

We write

$$\frac{|G|}{|H|} = [G : H],$$

which is the **index** of $H$ in $G$. Therefore,

$$|G| = [G : H]|H|.$$

This also works for infinite groups, if $G$ and $H$ are infinite. We can use this to quickly classify subgroups. For example, if $|G| = 13$, the only subgroups of $G$ are $|e|$ and $G$.

> **Example 4:** Let $G = \mathbb{Z}$ and $H = 2\mathbb{Z}$ is the group of even integers, then the distinct cosets are:
>
> - $H + 0 = H$ are the even integers
> - $H + 1$ are the odd integers, so
>
> $$\mathbb{Z} = 2\mathbb{Z} \bigsqcup (2\mathbb{Z} + 1),$$
>
> so $[\mathbb{Z} : 2\mathbb{Z}] = 2$.

Note that everything above is also true for left cosets. How then, do left and right cosets interact?

To motivate this, we look at the triangle group and consider the subgroup $H = \{e, \sigma_A\}$. Then the distinct right cosets are:

- $He = H = \{e, \sigma_A\}$
- $H\rho = \{\rho, \sigma_B\}$
- $H\rho^2 = \{\rho^2, \sigma_C\}$

Similarly, the distinct left cosets are:

- $eH = H = \{e, \sigma_A\}$
- $\rho H = \{\rho, \sigma_C\}$

- $\rho^2 H = \{\rho^2, \sigma_B\}$

In general, $gH \neq Hg$.

**Definition**: An **action** of a group $G$ on a set $X$ is a map

$$\begin{aligned} G \times X &\to X \\ (g, x) &\mapsto g \cdot x = gx, \end{aligned}$$

subject to
(i) $(gh) \cdot x = g(h \cdot x)$
(ii) $e \cdot x = x$

If $G$ is a group, then it acts on itself. Specifically,

$$(g, x) \mapsto g \cdot x = gx,$$

where we used the group product. This is known as the **left translation** or the **left regular action.**

We can also define the **right regular action** As

$$(g, x) = xg^{-1}.$$

Finally, we can define how $G$ acts on $G$ by

$$(g, x) = gxg^{-1},$$

and is reminiscent of the change of basis formula in multivariable calculus. This action is called **conjugation.**

**Example 5:** Let $G = SO(3)$, and $X = S^2$. We have that $G$ acts on $X$ by rotation. Let

$$H = \begin{pmatrix} \cos\theta & \sin\theta & 0 \\ -\sin\theta & \cos\theta & 0 \\ 0 & 0 & 1, \end{pmatrix},$$

which are rotations about the $z$ axis and also acts on $X$.

**Definition**: If $G$ acts on $X$ and $x \in X$, then the **orbit** of $x$ under $G$ is the set of all points $x$ is taken to by elements of $G$, written as:

$$G \cdot x = \{g \cdot x \mid g \in G\}.$$

Therefore, the orbits of $SO(2)$ on the sphere are the lines of latitudes and the poles $N$ and $S$. Similarly, the orbit of $SO(3)$ is the whole sphere.

Consider the orbit of $N$. Recall that $H$ fixes $N$. Recall that the leftcoset is

$$gH = \{gh | h \in H\}.$$

Since $h$ fixes $N$, $ghN = gN$. Every element of $gH$ takes $N$ to the same point $gN$. Suppose that $gH$ and $g'H$ are cosets such that $gHN = g'HN$, which implies $gN = g'N$, or $(g')^{-1}gN = N$. We can say that $g'^{-1}g = h$. Therefore, the points on the sphere are in a 1-1 correspondence with the left cosets of $H$.

**Definition**: If $G$ acts on $X$ and $x \in X$ then the **stabilizer** of $x$ in $G$ is

$$\text{Stab}_G(x) = \{g \in G | gx = x\}$$

## Cayley's Theorem

If we have $G$ acting on $X$, then there is an isomorphism

$$\varphi : G \to S_X \cong S_n,$$

where $n = |X|$. For example, let $H \leq G$ and $X = G/H$ where $G$ acts by left translation. This is transitive, and

$$\ker \varphi = \bigcap_x xHx^{-1}.$$

For the specific case where $H = \{e\}$. Therefore,

$$\ker \varphi = \{e\}$$

and $\varphi$ us 1-1 and

$$\varphi : G \to S_X$$

is an isomorphism, from $G$ to $\operatorname{Im} f$, a subgroup of $S_X$.

**Theorem**: Every group is isomorphic to a subgroup of $S_n$ for some $n$.

Consider another example, where $G$ acts on itself by conjugation,

$$g \cdot x = gxg^{-1} = C_g(x).$$

This is no longer transitive (or else everything is conjugate to everything else). The orbits are the conjugacy classes and are disjoint, since conjugacy is an equivalence relation. Note that if $z \in Z(G)$, then

$$gzg^{-1} = z$$

for all $g$. Therefore, $\{z\}$ is a conjugacy class with one element if and only if $z \in Z(G)$. If $G$ is abelian, then $Z(G) = G$ and every element is its own conjugacy class.

Because conjugacy is an equivalence relation,

$$G = \bigsqcup (\text{conjugacy classes}).$$

If $\{e = z_1, \ldots, z_k\} = Z(g)$ and $g_1, g_2, \ldots, g_m$ are representatives of the non-central conjugacy classes, we can write

$$C(g_i) = \{gg_ig^{-1} | g \in G\}.$$

Then,

$$G = \left(\bigsqcup \{z_i\}\right) \sqcup \left(\bigsqcup C(g_i)\right),$$

which if you have gone past kindergarten math, you can count

$$|G| = |Z(G)| + \sum_i |C(g_i)|.$$

This leads to the **class equation**. We first need to state the **orbit-stabilizer** theorem,

**Theorem**: For all $x \in X$, the map

$$\begin{aligned} G/\text{Stab}(x) &\to G \cdot x \\ g\text{Stab}(x) &\mapsto g \cdot x, \end{aligned}$$

is a well-defined bijection. Thus,

$$|G \cdot x| = [G : \text{Stab}(x)]$$

and if $|G| < \infty$, then

$$|G \cdot x| = |G|/|\text{Stab}(x)|$$

**Theorem**: The better **class equation** is

$$|G| = |Z| + \sum_{i=1}^{n} [G : Z(g_i)]$$

We can apply this to $S_3$. The center is $Z(S_3) = \{e\}$. The index of a 2-cycle is 3 and the index of a 3-cycle is 2. Therefore,

$$|S_3| = 1 + 2 + 3 = 6.$$

We introduce $p$ groups,

**Definition**: A finite group $G$ is a $p$-group if $|G| = p^n$ for some $n \in \mathbb{Z}_{\geq 0}$.

There is an interesting theorem,

**Theorem**: If $G$ is a non-trivial $p$-group, then $Z(G)$ is non-trivial.

*Proof.* Note that

$$|Z| = |G| - \sum [G : Z(g_i)],$$

but both terms are powers of $p$, so

$$|Z| \equiv 0 \pmod{p}.$$

□