Part IA
Groups

Prof Henry Wilton
Michaelmas 2025
Version 20251203

These are Zixuan's notes for **Part IA – Vectors and Matrices** at the University of Cambridge in 2025. The notes are not endorsed by the lecturers or the University, and all errors are my own.

The latest version of this document is available at academic.micfong.space. Please direct any comments to my CRSid email or use the contact details listed on the site.

This document is typeset using Typst. All figures are created using Inkscape.

Contents

Syllabus and Overview

Michaelmas Term, 2025 [24 Lectures]

Examples of Groups [4 Lectures]

Axioms for groups. Examples from geometry: symmetry groups of regular polygons, cube, tetrahedron. Permutations on a set; the symmetric group. Subgroups and homomorphisms. Symmetry groups as subgroups of general permutation groups. The Möbius group; cross-ratios, preservation of circles, the point at infinity. Conjugation. Fixed points of Möbius maps and iteration.

Lagrange’s Theorem [5 Lectures]

Cosets. Lagrange’s theorem. Groups of small order (up to order 8). Quaternions. Fermat-Euler theorem from the group-theoretic point of view.

Group Actions [4 Lectures]

Group actions; orbits and stabilizers. Orbit-stabilizer theorem. Cayley’s theorem (every group is isomorphic to a subgroup of a permutation group). Conjugacy classes. Cauchy’s theorem.

Quotient Groups [4 Lectures]

Normal subgroups, quotient groups and the isomorphism theorem.

Matrix Groups [3 Lectures]

The general and special linear groups; relation with the Möbius group. The orthogonal and special orthogonal groups. Proof (in $\mathbb{R}^3$) that every element of the orthogonal group is the product of reflections and every rotation in $\mathbb{R}^3$ has an axis. Basis change as an example of conjugation.

Permutations [4 Lectures]

Permutations, cycles and transpositions. The sign of a permutation. Conjugacy in S_n and in A_n. Simple groups; simplicity of A_5.

Lecture 1 · 2025-10-10

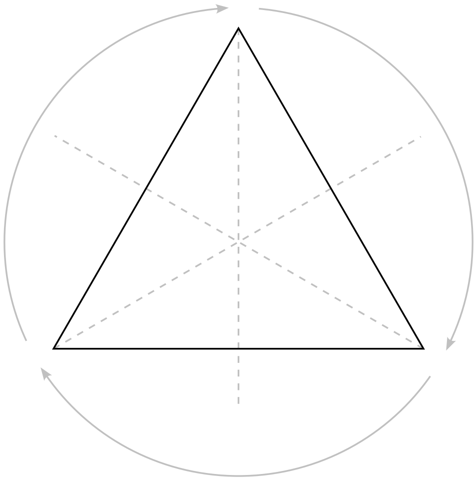
1 Introduction on Groups

One can think about groups in two ways:

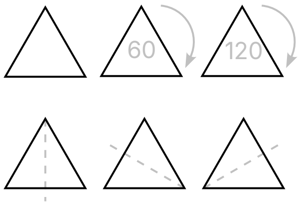
- on the one hand, they are related to algebra,
- on the other hand, they are related to symmetry.

1.1 Motivation

An equilateral triangle has rotational symmetry, reflective symmetry, and the identity symmetry.



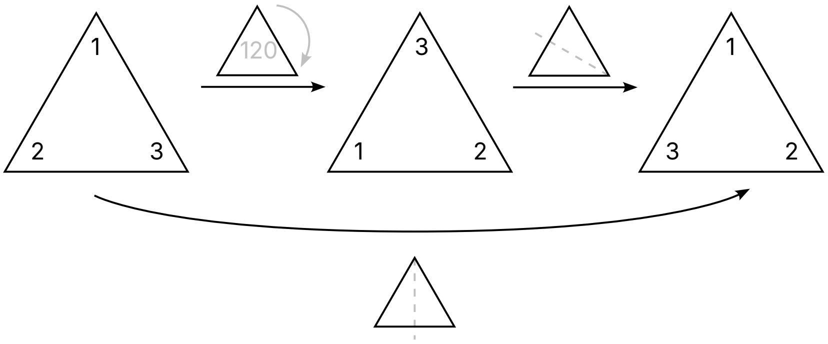
Let us list these symmetries:



So an equilateral triangle has exactly 6 symmetries.

> ***Exercise.*** How many symmetries does a square have? What about a regular pentagon? A regular n-gon?

Things get more interesting when we start to compose (or multiply) symmetries. Note that, after composition of symmetries, our result must also be a symmetry. To find out exactly which one is the end result, we can label the vertices on the triangle.



Here are some important features of symmetries:

- symmtries can be **composed**,
- there is an **identity**,
- every symmetry has an **inverse**,
- comoposition of symmetries is **associative**,

> ***Important.*** The symmetries may not necessarily commute.

We can extend this method to algebra to handle more complex cases, *e.g.* for a 17 - gon.

1.2 Introduction on Groups

Definition 1.1 (Binary operation)

A **binary operation** on a set X is a function $\cdot : X \times X \to X$.

Definition 1.2 (Group)

A group is a triple $(G, \cdot, e)$ where

- G is a set
- $\cdot$ is a binary operation on G,
- $e \in G$

that satisfies the following four axioms:

1. **Closure.** For all $a, b \in G$, $a \cdot b \in G$. [This can be deduced by definition of binary operations.]
2. **Associativity.** For all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3. **Identity.** For all $a \in G$, $a \cdot e = a$.
4. **(Right) Inverse.** For all $a \in G$, there exists $b \in G$ such that $a \cdot b = e$.

Example 1.3

We noticed earlier that the symmetries of an equilateral triangle form a group.

We can also think about the definitions as encompassing algebra with one operation, as shown in the following example.

Exercise. Show that $(\mathbb{Z}, +, 0)$ forms a group.

The definition has some important consequences.

Proposition 1.4

Let $(G, \cdot, e)$ be a group, and $a, b, b', e' \in G$.

1. If $a \cdot b = e$, then $b \cdot a = e$. [right inverses are left inverses.]
2. $e \cdot a = a$ [left identities are right identities.]
3. If $a \cdot b = e = a \cdot b'$, then $b = b'$. [inverses are unique.]
4. If $a \cdot e' = a = a \cdot e$, then $e' = e$. [the identity is unique.]

Proof.

1. Using Definition 1.2, we have

$$\begin{aligned} b &= b \cdot e && \text{by identity} \\ &= b \cdot (a \cdot b) && \text{by assumption} \\ &= (b \cdot a) \cdot b && \text{by associativity} \end{aligned}$$

   By the inverse axiom, there is a $c \in G$ such that $b \cdot c = e$. Multiplying both sides on the right by c, we get

$$\begin{aligned} b \cdot c &= ((b \cdot a) \cdot b) \cdot c \\ &= (b \cdot a) \cdot (b \cdot c) && \text{by associativity} \\ &= (b \cdot a) \cdot e && \text{by construction} \\ &= b \cdot a. && \text{by identity} \end{aligned}$$

2. Using Definition 1.2, and the previous part, there exists $b \in G$ such that $a \cdot b = e = b \cdot a$.

   Now

$$\begin{aligned} e \cdot a &= (a \cdot b) \cdot a \\ &= a \cdot (b \cdot a) && \text{by associativity} \\ &= a \cdot e && \text{by construction} \\ &= a. && \text{by identity} \end{aligned}$$

3. We have

$$\begin{aligned} b' &= e \cdot b' && \text{by part (2)} \\ &= (b \cdot a) \cdot b' && \text{by part (1)} \\ &= b \cdot (a \cdot b') && \text{by associativity} \\ &= b \cdot e && \text{by assumption} \\ &= b. && \text{by identity} \end{aligned}$$

4. Using the inverse axiom from Definition 1.2, and part (1), there is a $b \in G$ such that $b \cdot a = e$.

   Multiplying by b on both sides of $a \cdot e' = a$ gives

$$\begin{aligned} b \cdot a &= b \cdot (a \cdot e') \\ &= (b \cdot a) \cdot e' && \text{by associativity} \\ &= e \cdot e' && \text{by construction} \\ &= e'. && \text{by part (2)} \end{aligned}$$

Since $b \cdot a = e$, we have $e = e'$.

Notation. By Proposition 1.4, inverses are unique. Therefore, if $a \cdot b = e$, we may write

$$b = a^{-1}.$$

Lecture 2 · 2025-10-13

Part (1) of Proposition 1.4 tells us that

$$a \cdot a^{-1} = e = a^{-1} \cdot a,$$

which tells us the following.

Corollary 1.5

For a in a group $(G, \cdot, e)$, we have

$$\left(a^{-1}\right)^{-1} = a.$$

Notation. It makes sense to extend this notation. For any $a \in G$,

- $a^0 = e$
- $a^n = a^{n-1} \cdot a$ for any $n \in \mathbb{Z}^+$
- $a^{-n} = \left(a^{-1}\right)^n$ for any $n \in \mathbb{Z}^+$

Exercise. Show that, if G is a group, then for $a \in G$ and $m, n \in \mathbb{Z}$,

$$a^m \cdot a^n = a^{m+1} \quad \text{and} \quad (a^n)^m = a^{nm}.$$

Recall that it is **not** necessarily true that $a \cdot b = b \cdot a$ in a group G. Hence, it is also **not** necessarily true that $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$.

Proposition 1.6

Let $(G, \cdot, e)$ be a group and $a, b \in G$. Then

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}.$$

Proof. We have

$$\begin{aligned}(a \cdot b)^{-1} \cdot \left(b^{-1} \cdot a^{-1}\right) &= \left(a \cdot \left(b \cdot b^{-1}\right)\right) \cdot a^{-1} \\ &= (a \cdot e) \cdot a^{-1} \\ &= a \cdot a^{-1} \\ &= e.\end{aligned}$$

Since inverses are unique, the result follows.

Definition 1.7 (Abelian group)

If $(G, \cdot, e)$ is a group and $a \cdot b = b \cdot a$ for all $a, b \in G$, then the group is called **abelian**.

Definition 1.8 (Trivial group)

If $G = \{e\}$ and $e \cdot e = e$, then $(G, \cdot, e)$ is called the **trivial group**.

1.3 Familar Examples from Arithmetic

Example 1.9

1. $(\mathbb{Z}, +, 0), (\mathbb{Q}, +, 0), (\mathbb{R}, +, 0), (\mathbb{C}, +, 0)$ are all abelian groups. The inverse of x is $-x$ in each case.
2. $(\mathbb{N}, +, 0)$ is not a group due to a lack of inverses.
3. $(\mathbb{Q}^*, \times, 1)$ is an abelian group. Note that $(\mathbb{Q}, \times, 1)$ is not a group since 0 has no inverse.

   Similarly, $(\mathbb{R}^*, \times, 1)$ and $(\mathbb{C}^*, \times, 1)$ are abelian groups.

1.4 Finite Groups

Most of the groups above are infinite.

Definition 1.10 (Order of a group)

The **order** of a group $(G, \cdot, e)$ is the number of elements of G, denoted by $|G|$.

If $|G| < \infty$, then $(G, \cdot, e)$ is **finite**.

Example 1.11

1. For a specific $n \in \mathbb{N}$, let

   $$C_n = \{z \in \mathbb{C} : z^n = 1\}$$

   then $(C_n, \times, 1)$ is an abelian group.
2. Let $\mathbb{Z}_n = \{0, 1, ..., n - 1\}$. For $a, b \in \mathbb{Z}$, let $a +_n b = (a + b) \bmod n$. Then $(\mathbb{Z}_n, +_n, 0)$ is an abelian group.

Lecture 3 · 2025-10-15

1.5 Symmetric Groups

We need to introduce some definitions before we introduce the notion of a symmetric group.

Definition 1.12 (Bijection)

Let X, Y be sets. A **bijection** is a map $f : X \to Y$ that has an inverse $g : Y \to X$ such that

$$f \circ g = \mathrm{id}_X \quad \text{and} \quad g \circ f = \mathrm{id}_Y.$$

i.e. $g \circ f(x) = x$ for all $x \in X$, and $f \circ g(y) = y$ for all $y \in Y$.

Definition 1.13 (Permuation)

A bijection $X \to X$ is called a **permutation**.

Definition 1.14 (Symmetric group)

$\mathrm{Sym}(X)$ is defined to be the set of permutations of a set X.

We will prove that this is a group in Proposition 1.16.

Recall that $g \circ f(x) = g(f(x))$.

Lemma 1.15 (Composition is associative)

Consider the following maps of sets:

$$W \xrightarrow{f} X \xrightarrow{g} Y \xrightarrow{h} Z.$$

Then $(h \circ g) \circ f = h \circ (g \circ f)$.

Proof. For any $w \in W$,

$$\begin{aligned}((h \circ g) \circ f)(w) &= (h \circ g)(f(w)) \\ &= h(g(f(w))) \\ &= h(g \circ f(w)) \\ &= (h \circ (g \circ f))(w).\end{aligned}$$

This makes it easy to see that $\mathrm{Sym}(X)$ is a group.

Proposition 1.16

For any set X, $(\mathrm{Sym}(X), \circ, \mathrm{id}_X)$ is a group.

Proof.

- Closure is automatic, since the composition of two permutations is still a permutaion.
- Associativity follows from Lemma 1.15.

- The identity map is the identity element.
- Inverses exist by definition of a bijection.

Therefore the result follows.

Definition 1.17

If $X = \{1, ..., n\}$, then we write $S_n = \mathrm{Sym}(X)$

Example 1.18

1. S_3 is the group of ways to rearrange three flower pots on a windowsill.
2. S_{52} is the group of ways to shuffle a deck of cards.

Proposition 1.19

The order of S_n is $n!$.

Notation. Writing $(G, \cdot, e)$ is cumbersome. Henceforth, we will just write G.

If we want to emphasize that e is the identity element of G, we will write e_G for e. Likewise, we can also write $\cdot_G$ for the operation on G.

1.6 Subgroups

Sometimes, we want to restrict our attention to smaller groups. For instance, $\mathbb{Z}$ inside $\mathbb{R}$, the rotations of a triangle instead of all symmetries.

Definition 1.20 (Subgroup)

Let G be a group and $H \subseteq G$. If we have

1. $e \in H$,
2. $a \cdot b \in H$ for all $a, b \in H$,
3. $a^{-1} \in H$ for all $a \in H$.

Then we say that H is a **subgroup** of G. We write $H \leqslant G$.

Remark. If G is a group, and $H \leqslant G$, then H is also a group.

Example 1.21 (Example of subgroups)

1. Every group G is a subgroup of itself.
2. For any group G, $1_G = \{e_G\}$ is the trivial subgroup of G.
3. $\mathbb{Z} \leqslant \mathbb{Q} \leqslant \mathbb{R} \leqslant \mathbb{C}$.

4. For $n = 0, 1, 2, 3, \ldots$, let $n\mathbb{Z} \overset{\text{def}}{=} \{nk : k \in \mathbb{Z}\} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$.

   Now we have

   - $0 \in n\mathbb{Z}$
   - Let $x = nk, y = nl \in n\mathbb{Z}$. Then $x + y = n(k + l) \in n\mathbb{Z}$
   - Let $x = nk \in n\mathbb{Z}$. Then $-x = -nk = n(-k) \in n\mathbb{Z}$

   Therefore, $n\mathbb{Z} \leqslant \mathbb{Z}$. In fact, these are all of the subgroups $\mathbb{Z}$.

Definition 1.22 (Proper subgroup)

Let G be a group. Then H is a proper subgroup of G if $H \leqslant G$, $H \neq G$ and $H \neq 1_G$.

Proposition 1.23

If $H \leqslant \mathbb{Z}$, then $H = n\mathbb{Z}$ for some $n = \mathbb{Z}_{\geqslant 0}$.

Proof. For the trivial case $H = \{0\}$, we can construct it by $H = 0\mathbb{Z}$.

Otherwise, if $H \neq \{0\}$, we may choose $n \in H \setminus \{0\}$ to be the smallest positive $n \in H$. [Note that, if $x \in H$ and $x < 0$, then $-x \in H$ and $-x > 0$. Therefore, unless $H = \{0\}$, H contains a positive element.]

By induction, we see that $nk \in H$ for all $k = \mathbb{Z}^+$. By the closure of inverses, we conclude that $nk \in H$ for all $k \in \mathbb{Z}$. Hence $n\mathbb{Z} \leqslant H$.

It remains to prove that $n\mathbb{Z} = H$. We shall prove this by contradiction. Suppose that $n\mathbb{Z} \neq H$, so there exists some $x \in H$ such that $x \notin n\mathbb{Z}$. Dividing by n and taking remainders, we get

$$x = nq + r$$

for some $q \in \mathbb{Z}$ and $0 < r < n$.

But now $r = x - nq$, so $r \in H$. However, we have $0 < r < n$ which contradicts with our construction of n. ※

Lecture 4 · 2025-10-17

Proposition 1.24

If $H, K \leqslant G$, then

$$H \cap K \leqslant G.$$

Similarly, for any family of subgroups $H_i \leqslant G$, we have

$$\bigcap_i H_i = \{a \in G : \forall i, a \in H_i\} \leqslant G.$$

Definition 1.25 (Generated subgroup and generated set)

Let G be a group, and X be a subset of G. Then

$$\langle X\rangle = \bigcap_{X\subseteq H\leqslant G} H$$

which is the intersection of all the subgroups of G that contain X, and is called the **subgroup generated by** X.

If $G = \langle X\rangle$, we say X **generates** G, or X is a **generating set** for G.

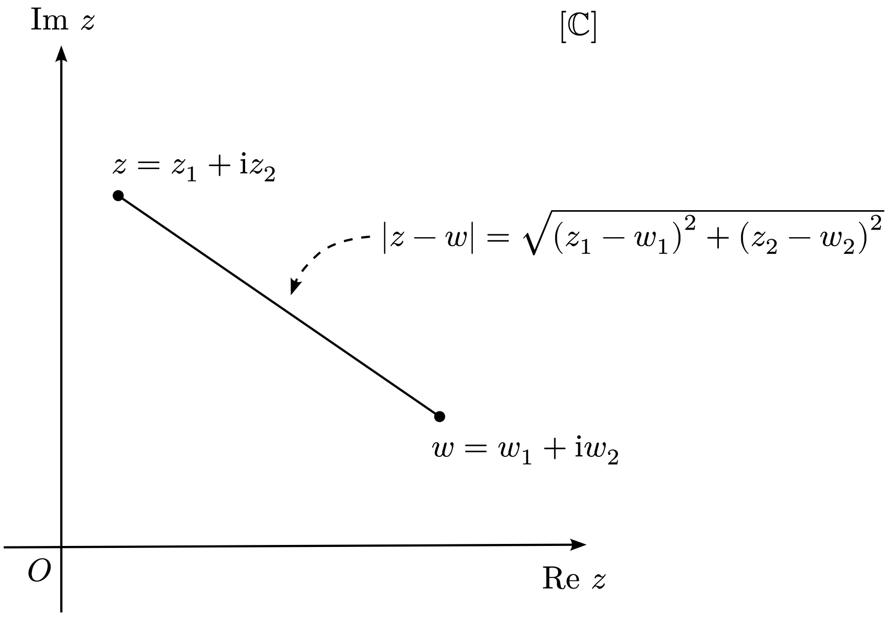
Intuitively, $\langle X\rangle$ is the *smallest* subgroup containing X. If X generates G, it means that every $g \in G$ can be written as

$$g = x_1^{\pm 1}x_2^{\pm 1}x_3^{\pm 1}...x_n^{\pm 1}$$

for some $n \geqslant 0$, where all $x_i \in X$. [Note that x_i and x_j can be repetitive elements from X.]

1.7 Geometric Examples of Subgroups

Let $\mathbb{C}$ be the plane, equipped with the usual notion of distance.


Im z
[$\mathbb{C}$]
$z = z_1 + \mathrm{i}z_2$
$|z-w| = \sqrt{(z_1-w_1)^2+(z_2-w_2)^2}$
$w = w_1 + \mathrm{i}w_2$
O
Re z

Definition 1.26 (Isometry)

For any $X \subseteq \mathbb{C}$ an **isometry** of X is a bijection

$$f : X \to X$$

that preserves distance:

$$|f(x) - f(y)| = |x - y|.$$

Proposition 1.27 (Isometry groups in $\mathbb{C}$)

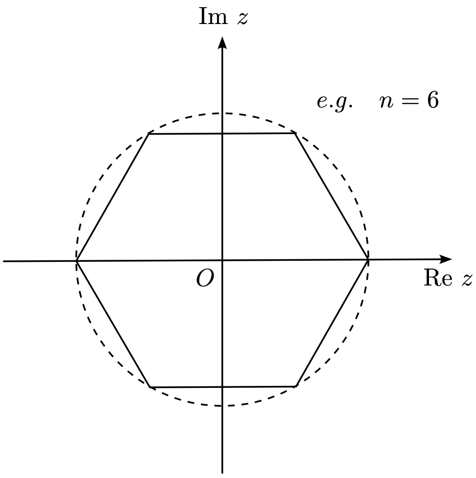
Let $X \subseteq \mathbb{C}$. The set of isometries of X, $\mathrm{Isom}(X)$, is a subgroup of $\mathrm{Sym}(X)$. In particular, $\mathrm{Isom}(X)$ is a group.

Proof. Let us check Definition 1.20. Let $f, g \in \mathrm{Isom}(X)$ and $x, y \in X$.

- Clearly, $\mathrm{id}_X \in \mathrm{Isom}(X)$.
- Since f and g are isometries,
$$\begin{aligned}|f(g(x)) - f(g(y))| &= |g(x) - g(y)| \\ &= |x - y|.\end{aligned}$$
So $f \circ g \in \mathrm{Isom}(X)$.
- Let $x' = f^{-1}(x), y' = f^{-1}(y)$. Then
$$|x'y'| = |f(x') - f(y')|$$
because f is an isometry. So
$$\left|f^{-1}(x)f^{-1}(y)\right| = \left|f\left(f^{-1}(x)\right) - f\left(f^{-1}(y)\right)\right| = |x - y|$$
and $f^{-1} \in \mathrm{Isom}(X)$ as required.

Definition 1.28 (Dihedral groups)

Let $X_n \in \mathbb{C}$ be the n-gon with vertices $\left\{e^{\frac{2\pi ik}{n}} : k = 0, ..., n-1\right\}$ for $n \geqslant 3$.



Define the ***n*th dihedral group** to be
$$D_{2n} = \mathrm{Isom}(X_n).$$

Example 1.29

D_6 is the symmetry group of an equilateral triangle, as seen in Section 1.1.

We can fast-forward to take a look at Theorem 1.32:

For a dihedral group, we have $|D_{2n}| = 2n$ for $n \geqslant 3$.

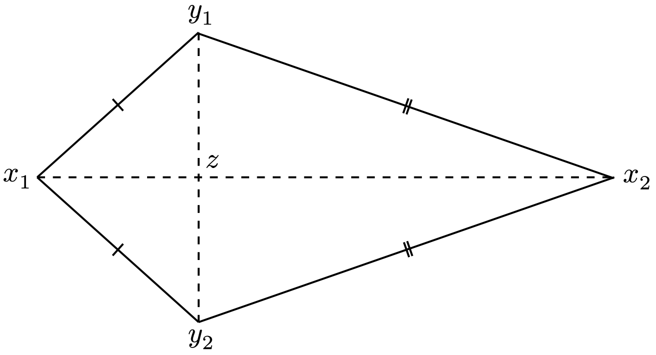
The proof will also give us a good desciption of all the elements. But first, we need some geometric lemmas.

Lemma 1.30 (Kite lemma)

Let $x_1, x_2, y_1, y_2 \in \mathbb{C}$. If

$$|y_1 - x_1| = |y_2 - x_1| \quad \text{and} \quad |y_1 - x_2| = |y_2 - x_2|,$$

then $(x_2 - x_1)$ is perpendicular to $(y_2 - y_1)$.



Proof. By symmetry,

$$\angle x_1 z y_1 = \angle x_1 z y_2.$$

But y_1y_2 is a straight line, so $y_1y2 \perp x_1x_2$.

Lecture 5 · 2025-10-20

Lemma 1.31 (3 point lemma)

Let $X \subseteq \mathbb{C}$ and $f \in \text{Isom}(X)$. If there are non-collinear points $x_1, x_2, x_3 \in X$ such that $f(x_i) = x_i$ for $i = 1, 2, 3$, then $f = \text{id}_x$.

Proof. The proof is by contradiction. Suppose that $f(y) \neq y$ for some $y \in X$. Then

$$\begin{aligned} |f(y) - x_i| &= |f(y) - f(x_i)| && \text{by hypothesis} \\ &= |y - x_i| && \text{since } f \in \text{Isom}(X) \end{aligned}$$

for $i = 1, 2, 3$.

Now apply Lemma 1.30, with $y_1 = y$, $y_2 = f(y)$, then we get

$$x_2 - x_1 \perp y_2 - y_1 = f(y) - y.$$

Similarly,

$$x_3 - x_1 \perp f(y) - y.$$

Hence, x_1, x_2, x_3 are collinear, contradicting the hypothesis.

> ***Remark.*** There is equally an $n+1$-point lemma valid in $\mathbb{R}^n$.

Now, to prove the theorem we stated above, we define two elements of D_{2n}:

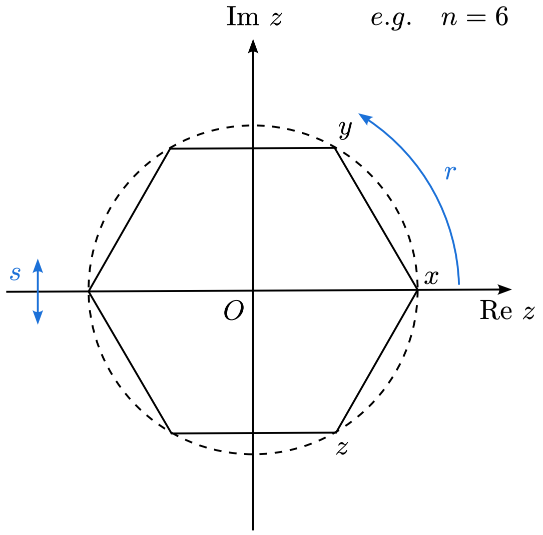
$$\begin{aligned} r(z) &= \frac{e^{2\pi i}}{n} z \qquad \text{(a rotation)} \\ s(z) &= \overline{z} \qquad \text{(a reflection)} \end{aligned}$$

Theorem 1.32

For a dihedral group, we have $|D_{2n}| = 2n$ for $n \geqslant 3$, and we have

$$D_{2n} = \left\{e, r, ..., r^{n-1}, s, rs, ..., r^{n-1}s\right\}.$$

In particular, $\{r, s\}$ generates D_{2n}.



Proof. This will be a long proof.

> ***Outline.***
> 1. We show that $r, s \in D_{2n}$.
> 2. We show that $D_{2n} = \left\{e, r, ..., r^{n-1}, s, rs, ..., r^{n-1}s\right\}$ by showing
>   - that $\left\{e, r, ..., r^{n-1}, s, rs, ..., r^{n-1}s\right\} \subseteq D_{2n}$, and
>   - that $D_{2n} \subseteq \left\{e, r, ..., r^{n-1}, s, rs, ..., r^{n-1}s\right\}$.
> 3. We show that there are no duplicate elements in $\left\{e, r, ..., r^{n-1}, s, rs, ..., r^{n-1}s\right\}$.

STEP 1: $r, s \in D_{2n}$

Let the polygon be X_n. First, we show that $r, s \in D_{2n}$.

- **For r:**

  Indeed, For any $x, y \in \mathbb{C}$, then

$$\begin{aligned} |r(x)-r(y)| &= \left|e^{\frac{2\pi i}{n}}x - e^{\frac{2\pi i}{n}}y\right| \\ &= \left|e^{\frac{2\pi i}{n}}\right||x-y| \\ &= |x-y|. \end{aligned}$$

so r is indeed an isometry. Also,

$$re^{\frac{2\pi ik}{n}} = e^{\frac{2\pi i(k+1)}{n}}$$

so r sends vertices of X_n to vertices, and hence preserves X_n.

- **For s:**

  Similarly for any $x, y \in \mathbb{C}$, we have

  $$\begin{aligned} |s(x)-s(y)| &= |\overline{x}-\overline{y}| \\ &= |\overline{x-y}| \\ &= |x-y|. \end{aligned}$$

  so s is indeed an isometry. Also,

  $$se^{\frac{2\pi ik}{n}} = e^{-\frac{2\pi ik}{n}}$$

  so s sends vertices of X_n to vertices, and hence preserves X_n.

STEP 2: $D_{2n} = \left\{e, r, ..., r^{n-1}, s, rs, ..., r^{n-1}s\right\}$

We have shown that $\{r, s\} \in D_{2n}$. Therefore, by induction,

$$\left\{e, r, ..., r^{n-1}, s, rs, ..., r^{n-1}s\right\} \subseteq D_{2n}.$$

To see that this is all the elements, let $f \in D_{2n}$. We aim to prove that $f \in \left\{e, r, ..., r^{n-1}, s, rs, ..., r^{n-1}s\right\}$. We shall apply Lemma 1.31 to complete this proof.

Consider $x = 1$, $y = e^{\frac{2\pi i}{n}}$ and $z = e^{-\frac{2\pi i}{n}}$.

- **For x:**

  Since $f \in D_{2n}$, $f(x)$ is a vertex of X_n. So

  $$f(x) = e^{\frac{2\pi ik}{n}}$$

  for some $k \in \{0, 1, ..., n-1\}$. We will try to *undo* f using r and s.

  Therefore,

  $$r^{-k} \circ f(x) = 1 = x.$$

- **For y and z:**

  Now, $r^{-k} \circ f \subseteq D_{2n}$, so

  $$\begin{aligned} \left|r^{-k} \circ f(y) - x\right| &= \left|r^{-k} \circ f(y) - r^{-k} \circ f(x)\right| \\ &= |y-x| \end{aligned}$$

and hence $r^{-k} \circ f(y) = y$ or z.

For the same reasons, $r^{-k} \circ f(z) = y$ or z. Therefore, there are two cases:

1. $r^{-k} \circ f(y) = y$ and $r^{-k} \circ f(z) = z$,
2. $r^{-k} \circ f(y) = z$ and $r^{-k} \circ f(z) = y$.

- **Case 1.** $r^{-k} \circ f$ forms x, y, z.

  Since x, y, z are not collinear,

  $$r^{-k} \circ f = \mathrm{id}_X$$

  by Lemma 1.31. Hence, $f = r^k$.

- **Case 2.** We have

  $$\begin{aligned} r^{-k} \circ f(x) &= x = s(x), \\ r^{-k} \circ f(y) &= z = s(y), \\ r^{-k} \circ f(z) &= y = s(z). \end{aligned}$$

  Therefore,

  $$\begin{aligned} s^{-1} \circ r^{-k} \circ f(x) &= s^{-1} \circ s(x) = x, \\ s^{-1} \circ r^{-k} \circ f(y) &= s^{-1} \circ s(y) = y, \\ s^{-1} \circ r^{-k} \circ f(z) &= s^{-1} \circ s(z) = z. \end{aligned}$$

  Simiarly to **Case 1**, by the Lemma 1.31, we get

  $$s^{-1} \circ r^{-k} \circ f = \mathrm{id}_X .$$

  Hence, $f = r^k s$ as required.

This proves that

$$D_{2n} = \left\{e, r, ..., r^{n-1}, s, rs, ..., r^{n-1}s\right\}.$$

STEP 3: DUPLICATE CHECK

Now, we need to check that this list does not contain duplicate elements, so that $|D_{2n}| = 2n$.

First, if $0 \leqslant k, l \leqslant n$ such that

$$r^k = r^l,$$

then

$$\mathrm{e}^{\frac{2\pi i k}{n}} = r^k(1) = r^l(1) = \mathrm{e}^{\frac{2\pi i l}{n}},$$

so $k = l$.

Now, if $r^k = s$ then

$$\mathrm{e}^{2\pi i \frac{k}{n}} = r^{k(1)} = s(1) = 1,$$

so $k = 0$ and $s = r^0 = \mathrm{id}_X$.

But then $z = s(y) = \mathrm{id}_{X(y)} = y$, which is a contradiction. Therefore, $s \neq r^k$ for any k.

Now, if $r^k = r^l s$, then $s = r^k - l$, contradicting the previous case.

Finally, if there exists $0 \leqslant k, l < n$ such that $r^k s = r^l s$, then multiplying by inverses to the right by s^{-1} gives

$$r^k = r^l \Rightarrow k = l$$

as above.

To understand the group operations on D_{2n}, we need to understand the different ways to multiply r and s.

Lemma 1.33 (Dihedral Relation)

For $r, s \in D_{2n}$ where r represents the rotation and s represents the reflection, we have

$$sr = r^{-1}s.$$

Proof. By Lemma 1.31, it suffices to check that the two expressions do the same thing to x, y, z. Indeed, with $x = 1$, $y = e^{\frac{2\pi i}{n}}$ and $z = e^{-\frac{2\pi i}{n}}$,

$$\begin{aligned} sr(z) &= \overline{e^{-\frac{2\pi ik}{n}}} &&= e^{\frac{2\pi ik}{n}} &&= r^{-1}(y) = r^{-1}s(z), \\ sr(y) &= \overline{e^{\frac{2\pi ik}{n}}} &&= e^{-\frac{2\pi ik}{n}} &&= r^{-1}(z) = r^{-1}s(y), \\ sr(x) &= \overline{1} &&= e^{1} &&= r^{-1}(x) = r^{-1}s(x). \end{aligned}$$

Lecture 6 · 2025-10-22

2 Homomorphism and Isomorphism

2.1 Introduction on Homomorphisms and Isomorphisms

Some groups are not set-theoretically *equal*, but nonetheless have the same structure. *e.g.* Sym({A deck of cards}) and Sym({52 undergraduate mathematiicians}). We wish to encompass this underlying strucutre.

Definition 2.1 (Homomorphism)

A map between groups

$$\varphi : G \to H$$

is called a **homomorphism** if

$$\varphi(g \cdot g') = \varphi(g) \cdot \varphi(g')$$

for all $g, g' \in G$.

Example 2.2

1. For any two groups G and H, the map

$$\varphi : G \to H \quad \text{with} \quad g \mapsto e_H$$

for all $g \in G$ is a homomorphism, called the **trivial homomorphism**.

3. If $H \leqslant G$, then the map

$$i : H \to G \quad \text{with} \quad h \mapsto h$$

is the **inclusion homomorphism**.

4. Recall that $C_n = \{z \in \mathbb{C} : z^n = 1\}$.

> ***Exercise.*** Show that if $n \mid m$, then
>
> $$\varphi : C_m \to C_n \quad \text{with} \quad z \mapsto z^{\frac{m}{n}}$$
>
> is a homomorphism.

5. Since $\det(AB) = \det(A)\det(B)$, the determinant function

$$\det : GL_2(\mathbb{R}) \to (\mathbb{R}^*, \times) \quad \text{with} \quad A \mapsto \det(A)$$

is a homomorphism.

Lemma 2.3

If $\varphi : G \to H$ is a homomorphism, then

1. $\varphi(e_G) = e_H$.
2. $\varphi\left(g^{-1}\right) = \varphi(g)^{-1}$ for all $g \in G$.

Proof.

1. We have

$$\begin{aligned}\varphi(e_G) \cdot \varphi(e_G) &= \varphi(e_G \cdot e_G)\\ &= \varphi(e_G).\end{aligned}$$

   Note that $\varphi(e_G)$, being multiplied by a group element and yielding itself, must be the identity element e_H. This is by Proposition 1.4 (4).

2. We have

$$\begin{aligned}\varphi(g) \cdot \varphi\left(g^{-1}\right) &= \varphi\left(g \cdot g^{-1}\right)\\ &= \varphi(e_G)\\ &= e_H.\end{aligned}$$

   Thus, by Proposition 1.4 (3), we have $\varphi\left(g^{-1}\right) = \varphi(g)^{-1}$.

To discuss the notion of two groups being “structurally the same”, we can do this using isomorphisms.

Definition 2.4 (Isomorphism)

If a homomorphism

$$\varphi : G \to H$$

is a bijection, then φ is an **isomorphism**. In this case, we write

$$G \cong H.$$

From the perspective of group theory, isomorphic groups are considered *the same*.

Example 2.5

1. Recall that $C_n = \{z \in \mathbb{C} : z^n = 1\}$ with operation $\times$, and $\mathbb{Z}_n = \{0, 1, \ldots, n - 1\}$ with operation $+_n$. Let

$$\varphi : \mathbb{Z}_n \to C_n \quad \text{with} \quad k \mapsto \mathrm{e}^{\frac{2\pi i k}{n}}.$$

   Clearly, φ is bijective. Further more, for any $k, l \in \mathbb{Z}$,

$$k + l = np + (k +_n l)$$

   for some $p \in \mathbb{Z}$, so

$$\begin{aligned}
\varphi(k +_n l) &= \mathrm{e}^{\frac{2\pi\mathrm{i}}{n}(k+_n l)} && \text{by the definition of } \varphi \\
&= \mathrm{e}^{\frac{2\pi\mathrm{i}}{n}(np)}\mathrm{e}^{\frac{2\pi\mathrm{i}}{n}(k+_n l)} && \text{multiply by 1 in a fancy way} \\
&= \mathrm{e}^{\frac{2\pi\mathrm{i}}{n}(np+k+_n l)} \\
&= \mathrm{e}^{\frac{2\pi\mathrm{i}}{n}(k+l)} \\
&= \mathrm{e}^{\frac{2\pi\mathrm{i}}{n}(k)}\mathrm{e}^{\frac{2\pi\mathrm{i}}{n}(l)} \\
&= \varphi(k)\cdot\varphi(l). && \text{by the definition of } \varphi
\end{aligned}$$

Therefore, φ is indeed an homomorphism, and hence an isomorphism. That is,

$$\mathbb{Z}_n \cong C_n$$

for all n.

2. The exponential map

$$\exp : (\mathbb{R}, +, 0) \to \left(\mathbb{R}^+, \times, 1\right) \quad \text{with} \quad x \mapsto \mathrm{e}^x$$

is a homomorphism, because

$$\begin{aligned}
\exp(x+y) &= \mathrm{e}^{x+y} \\
&= \mathrm{e}^x\mathrm{e}^y \\
&= \exp(x)\times\exp(y).
\end{aligned}$$

Since $\exp^{-1} \equiv \log$, exp is also a bijection. Hence exp is an isomorphism.

The following lemma justifies the claim that we may think of isomorphic groups as "the same".

Lemma 2.6

1. If $\varphi : G \to H$ is a isomorphism, so is φ^{-1}.
2. If $G \overset{\varphi}{\to} H \overset{\psi}{\to} K$, are homomorphisms, so is $\psi \circ \varphi$.
3. $\cong$ is an equivalence relation.

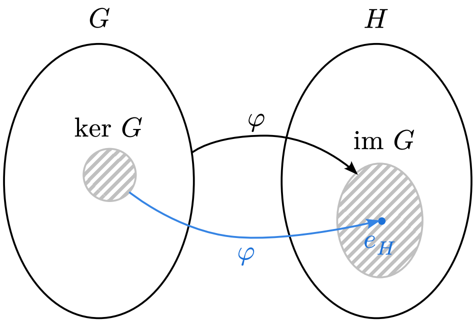
Exercise. Prove this lemma.

We have seen that every subgroup leads to an inclusion homomorphism. This is conversely true, that homomorphism leads to subgroups.

Definition 2.7 (Image and Kernel)

Let $\varphi : G \to H$ be a homomorphism.

1. The **image** of φ is $\operatorname{im}\varphi = \{h \in H : \exists g \in G, h = \varphi(g)\}$.
2. The **kernel** of φ is $\ker\varphi = \left\{g \in G : \varphi(g) = e_H\right\}$.



Proposition 2.8

If $\varphi : G \to H$ is a homomorphism, then

1. $\operatorname{im}\varphi \leqslant H$, and
2. $\ker\varphi \leqslant G$.

Proof.

1. - In Lemma 2.3, we showed that $e_H = \varphi(e_G) \in \operatorname{im}\varphi$.
   - For $\varphi(g_1), \varphi(g_2) \in \operatorname{im}\varphi$, we have
   $$\varphi(g_1) \cdot \varphi(g_2) = \varphi(g_1 \cdot g_2) \in \operatorname{im}\varphi.$$
   - For $g \in G$,
   $$\varphi(g)^{-1} = \varphi\left(g^{-1}\right) \in \operatorname{im}\varphi.$$

   Therefore $\operatorname{im}\varphi \leqslant H$.
2. - $\varphi(e_G) = e_H \Rightarrow e_G \in \ker\varphi$.
   - For $g_1, g_2 \in \ker\varphi$,
   $$\begin{aligned}\varphi(g_1 \cdot g_2) &= \varphi(g_1) \cdot \varphi(g_2) \\ &= e_H \cdot e_H \\ &= e_H.\end{aligned}$$
   So $g_1 \cdot g_2 \in \ker\varphi$.
   - For $g \in \ker\varphi$, we have
   $$\varphi\left(g^{-1}\right) = \varphi(g)^{-1} = e_H^{-1} = e_H.$$
   So $g^{-1} \in \ker\varphi$.

   Therefore $\ker\varphi \leqslant G$.

Proposition 2.9

Let $\varphi : G \to H$ be a homomorphism.

1. φ is surjective if and only if $\operatorname{im}\varphi = H$.
2. φ is injective if and only if $\ker\varphi = 1_G$.

Lecture 7 · 2025-10-24

Proof.

1. This is immediate from the definition of surjectivity and image.
2. Indeed, if φ is injective, then
$$\ker\varphi = \varphi^{-1}(e_H).$$
This has at most one element, and since $e_G \in \ker\varphi$, we have $\ker\varphi = \{e_G\} = 1_G$.
Conversely, suppose $\ker\varphi = 1_G$. If $\varphi(g_1) = \varphi(g_2)$, then
$$\varphi\left(g_1 g_2^{-1}\right) = \varphi(g_1)\varphi(g_2)^{-1} = e_H.$$
This calculation shows that $g_1 g_2^{-1} \in \ker\varphi$, so $g_1 g_2^{-1} = e_G$ by assumption, and hence $g_1 = g_2$. Thus φ is injective.

Proposition 2.10

By Proposition 2.9, a homomorphism $\varphi : G \to H$ is an isomorphism if and only if $\operatorname{im}\varphi = H$ and $\ker\varphi = 1_G$.

2.2 Cyclic Groups

The groups $C_n \cong \mathbb{Z}_n$ that we have seen are examples of *cyclic groups*.

Definition 2.11 (Cyclic Group)

A group G is **cyclic** if there exists an element $g \in G$ such that
$$G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}.$$
Such an element g is called a **generator** of G.

Example 2.12

1. $C_n = \{z \in \mathbb{C} : z^n = 1\}$ is cyclic, with generator $e^{\frac{2\pi i}{n}}$.
2. $(\mathbb{Z}, +)$ is cyclic, with generator 1.
3. $\mathbb{Z}_n$ is cyclic, since $\mathbb{Z}_n \cong C_n$.

Theorem 2.13

If G is cyclic, then either

- $G \cong C_n$ for some $n \in \mathbb{Z}$, or
- $G \cong \mathbb{Z}$.

Proof. Let G be a cyclic group with generator g. Let

$$S = \left\{k \in \mathbb{Z}^+ : g^k = e\right\},$$

and let

$$n = \begin{cases} \min S & \text{if } S \neq \varnothing \\ \infty & \text{if } S = \varnothing \end{cases}.$$

Case 1. If $n = \infty$, Define

$$\varphi : \mathbb{Z} \to G \quad \text{with} \quad k \mapsto g^{|k|}$$

We need to show that φ is an isomorphism. Since

$$\varphi(k + l) = g^{k+l} = g^k g^l = \varphi(k)\varphi(l),$$

φ is certainly a homomorphism.

By the definition of cyclic groups, φ is surjective.

To prove that φ is injective, for the purpose of contradiction, suppose that $0 \neq k \in \ker\varphi$. Since $\ker\varphi \leqslant \mathbb{Z}$, we may replace k by $-k$ if necessary, and assume $k > 0$. Then $k \in S \Rightarrow S \neq \varnothing$, which is a contradiction because $n \in \infty$. ※

Therefore, $\ker\varphi = \{0\}$ so φ is injective. Hence, φ is an isomorphism and $G \cong \mathbb{Z}$.

Case 2. If $n < \infty$, define

$$\varphi : \mathbb{Z}_n \to G \quad \text{with} \quad k \mapsto g^k.$$

Since $k + l = qn + \left(k +_n l\right)$ for some $q \in \mathbb{Z}$, we have

$$\begin{aligned} \varphi(k)\varphi(l) &= g^k g^l \\ &= g^{k+l} \\ &= g^{qn+(k+_n l)} \\ &= g^{k+_n l} \\ &= \varphi\left(k +_n l\right). \end{aligned}$$

Thus, φ is a homomorphism.

To prove that φ is surjective, since G is cyclic, every element can be written as g^k for some $k \in \mathbb{Z}$. By the division algorithm, we can write $k = qn + r$ for some $q \in \mathbb{Z}$ and $r \in \mathbb{Z}_n$. Therefore,

$$g^k = g^{nq+r} = (g^n)^q g^r = g^r = \varphi(r).$$

This proves that φ is surjective.

To prove injectivity, suppose that $\varphi(k) = e$ for some $k \in \mathbb{Z}_n$ [this is equivalent to saying $k \in \ker \varphi$]. Then $k \in S$ or $k = 0$. Since n is minimal in S, and that $n > 0$ and $\varphi(n) = e$, it follows that $k = 0$, because $k < n$. Therefore, $\ker \varphi = \{0\}$ and φ is injective.

Therefore,

$$G \cong \mathbb{Z}_n \cong C_n.$$

Because of this theorem, we will write C_n for any cyclic group of order n, and $C_\infty \cong \mathbb{Z}$.

Definition 2.14 (Order of an element of a group)

For any group G, and element $g \in G$, let

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

Note that $\langle g \rangle$ is cyclic, so $\langle g \rangle \cong C_n$ for some $n \in \mathbb{Z}^+ \cup \{\infty\}$. This number n is called the **order** of g, denoted by $o(g)$.

2.3 Dihedral Groups, Revisited

Remark. Whenever $x, y \in G$ satisfy the dihedral relation

$$xy = yx^{-1},$$

Then, for any $l > 0$, we have

$$yx^{-l} = (yx)x^{1-l} = xyx^{1-l} = \ldots = x^l y$$

by induction on l.

If $y^2 = e$, we also have

$$yx^l = y\left(x^l y\right)y = y\left(yx^{-l}\right)y = x^{-l}y.$$

In summary, we have shown that

$$yx^l = x^{-l}y$$

for all $l \in \mathbb{Z}$.

Lemma 2.15

Let G be a group, that for some $a, b \in G$, the following relations hold:

1. $a^n = e$ for some $n \geqslant 3$
2. $b^2 = e$
3. $ab = ba^{-1}$

Then $\varphi\left(r^k\right) = a^k$ and $\varphi\left(r^k s\right) = a^k b$ defines a homomorphism $\varphi : D_{2n} \to G$ that sends the generators r, s of D_{2n} to a, b respectively.

Proof. There are 4 cases to check:

1. $\varphi\left(r^k\right)\varphi\left(r^l\right) = a_k a^l = a^{k+l} = a^{k+_n l} = \varphi\left(r^{k+l}\right)$
2. $\varphi\left(r^k\right)\varphi\left(r^l s\right) = a^k a^l b = a^{k+l} b = a^{k+_n l} b = \varphi\left(r^{k+l} s\right)$
3. $\varphi\left(r^k s\right)\varphi\left(r^l\right) = a^k b a^l = a^k a^{-l} b = a^{k-l} b = \varphi\left(r^{k-l} s\right) = \varphi\left(r^k s r^l\right)$
4. $\varphi\left(r^k s\right)\varphi\left(r^l s\right) = a^k b a^l b = a^k a^{-l} b^2 = a^{k-l} = \varphi\left(r^{k-l}\right) = \varphi\left(r^{k-l} s s\right) = \varphi\left(r^k s r^l s\right)$

Proposition 2.16

Suppose G has generating set

$$\{a, b\}$$

satisfying:

1. $a^n = e$ for some $n \geqslant 3$
2. $b^2 = e$
3. $ab = ba^{-1}$
4. $|G| = 2n$

Then $G \cong D_{2n}$.

Proof. By Lemma 2.15, there is a homomorphism

$$\varphi : D_{2n} \to G$$

sending $r \mapsto a$ and $s \mapsto b$. Since a and b generate G, φ is surjective. Also, since $\left|D_{2n}\right| = |G| = 2n$, φ is bijective. Therefore, φ is an isomorphism, and $G \cong D_{2n}$.

Lecture 8 · 2025-10-27

3 Lagrange's Theorem

This very important theorem helps us to think about the orders of a groups and subgroups.

Theorem 3.1 (Lagrange's Theorem, Weak Version)

If $H \leqslant G$ and $|G| \leqslant \infty$, then $|H| \mid |G|$.

The idea of this theorem is to somehow partition the group G into cosets of H.

3.1 Cosets

Definition 3.2 (Left Cosets)

Let $H \leqslant G$ and $g \in G$. The corresponding **left coset** is

$$gH \overset{\text{def}}{=} \{gh : h \in H\} \subseteq G$$

The set of all left cosets of H in G is denoted by

$$G/H = \{gH : g \in G\}.$$

Remark. We may similarly define **right cosets**

$$Hg \overset{\text{def}}{=} \{hg : h \in H\} \subseteq G.$$

The set of right cosets of H in G is denoted by

$$H \setminus G = \{Hg : g \in G\}.$$

Lemma 3.3

If $H \leqslant G$, the left cosets **partition** G. That is,

1. $G = \bigcup_{gH \in G/H} gH$
2. If $g_1H \cap g_2H \neq \varnothing$, then $g_1H = g_2H$ for any $g_1H, g_2H \in G/H$.

Proof.

1. For any $g \in G$, we have $g \in gH$ since $e \in H$. Thus, $g \in \bigcup_{gH \in G/H} gH$. Hence, $G \subseteq \bigcup_{gH \in G/H} gH$. The reverse inclusion is obvious. Hence the equality holds.
2. Suppose $g_1H \cap g_2H \neq \varnothing$, so there is a k in the intersection. Then,

$$k = g_1h_1 = g_2h_2$$

for some $h_1, h_2 \in H$. Thus,

$$g_1 = g_2h_2h_1^{-1}.$$

Since H is a group, $h_2h_1^{-1} \in H$. Thus

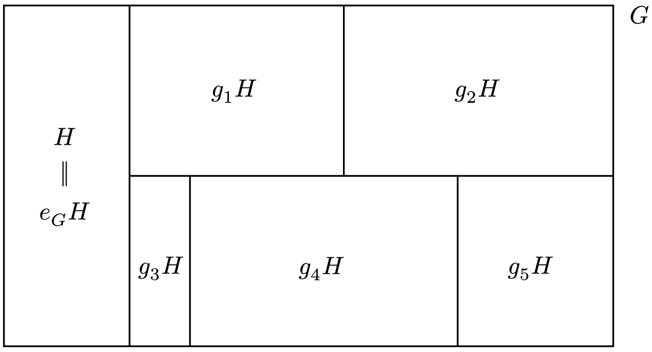
$$g_1 \in g_2H.$$

Furthermore, for any $h \in H$,

$$g_1h = g_2\left(h_1h_1^{-1}\right)h \in g_2H.$$

Hence $g_1H \subseteq g_2H$. By symmetry, we have the reverse inclusion. Thus, the equality holds.

A schematic picture of the lemma above is shown below.



However, we can say more about the sizes of the cosets.

Lemma 3.4

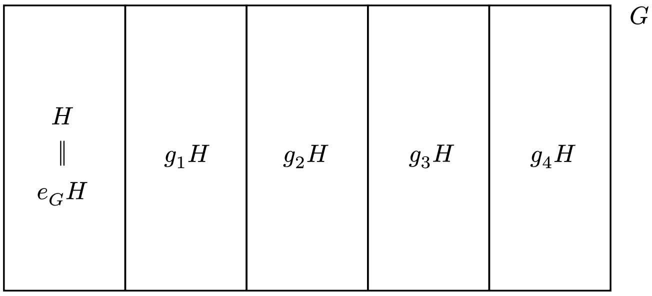
Let $H \leqslant G$, then there is a bijection

$$H \to gH$$

for any $g \in G$. In particular, $|gH| = |H|$.

Proof. The map $H \to gH$ defined by $h \mapsto gh$ has inverse $gH \to H$ defined by $gh \mapsto g^{-1}(gh) = h$. Hence it is a bijection.

So the schematic picture above can be redrawn, where each coset has the same size as H.



Definition 3.5 (Index of a Subgroup)

Let $H \leqslant G$. The **index** of H in G is defined as

$$[G : H] \overset{\text{def}}{=} |G/H|.$$

Theorem 3.6 (Lagrange's Theorem)

If $H \leqslant G$ and $|G| \leqslant \infty$, then

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

Proof. Since left cosets partition G,

$$|G| = \sum_{gH \in G/H} |gH| = \sum_{gH \in G/H} |H| = [G : H] \cdot |H|$$

3.2 Consequences of Lagrange's Theorem

Corollary 3.7

If $|G| < \infty$ and $g \in G$, then

$$o(g) \mid |G|.$$

Proof. Recall that $o(g) = |\langle g \rangle|$ and $|\langle g \rangle| \mid |G|$ by Lagrange's Theorem.

Corollary 3.8

If $|G| < \infty$ and $y \in G$, then $g^{|G|} = e_G$.

Proof. Corollary 3.7 says that $|G| = ko(g)$ for some $k \in \mathbb{Z}$, so

$$g^{|G|} = g^{ko(g)} = \left(g^{o(g)}\right)^k = e_G^k = e_G.$$

Corollary 3.9

If $|G|$ is prime, then G is cyclic, and any element $g \neq e$ generates it.

Proof. Choose any $g \neq e$. Then

$$o(g) \mid G.$$

So, since $|G|$ is prime, either $o(g) = 1$ or $o(g) = |G|$. Since $g \neq e$, we must have $o(g) = |G|$. Therefore,

$$G = \langle g \rangle.$$

So g generates G, and hence G is cyclic.

3.3 Applications of Lagrange's Theorem

Lagrange's theorem 3.6 implies an important result in number theory.

Definition 3.10 (Euler totient function)

The **Euler totient function**

$$\varphi(n) = \#\{x \in Z_n : \gcd(x, n) = 1\}.$$

Let $\times_n$ denote multiplication modulo n on $\mathbb{Z}_n$, which is associative with identity 1.

Lecture 9 · 2025-10-29

Recall that by the division algorithm, $x \in \mathbb{Z}_n$ has a multiplicative inverse modulo n, iff there are $y, m \in \mathbb{Z}$ such that

$$\begin{aligned} xy + mn &= 1 \\ \Leftrightarrow \gcd(x, n) &= 1. \end{aligned}$$

Hence,

$$\mathbb{Z}_n^* := \{x \in \mathbb{Z}_n : \gcd(x, n) = 1\}$$

is a group with operation $\times_n$.

Theorem 3.11 (Fermat-Euler Theorem)

Let $x, n \in \mathbb{Z}$. If $\gcd(x, n) = 1$, then

$$x^{\varphi(n)} \equiv 1 \operatorname{mod} n.$$

Proof. By Corollary 3.8, we have

$$x^{|\mathbb{Z}_n^*|} = 1 \operatorname{mod} n.$$

And by definition

$$|\mathbb{Z}_n^*| = \varphi(n).$$

4 Group Actions

Groups become groups of symmetries when they *act*.

4.1 Introduction

Definition 4.1 (Group Action)

An **action** of a group G on a set X is a function

$$G \times X \to X$$

with

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

such that

1. $e_G x = x$ for all $x \in X$,
2. $(g_1 g_2)x = g_1(g_2 x)$ for all $g_1, g_2 \in G$ and $x \in X$.

Notation. We write $G \curvearrowright X$ to indicate that G acts on X.

Example 4.2

1. For any group G, there is a **trivial action** of G on any set X defined by $gx = x$ for all $g \in G$ and $x \in X$.
2. $\mathrm{Sym}(X) \curvearrowright X$ by $fx = f(x)$.
3. If $G \curvearrowright X$ and $H \leqslant G$ then $H \curvearrowright X$ by restriction.

   In particular, $\mathrm{Isom}(\mathbb{C}) \curvearrowright \mathbb{C}$ since $\mathrm{Sym}(\mathbb{C}) \leqslant \mathrm{Isom}(\mathbb{C})$.
4. Similarly, dihedral groups D_{2n} acts on X_n (the regular n-gon). It also acts on the set of vertices of the regular n-gons.
5. Every group G acts on itself by left multiplication: $g\gamma = g \cdot \gamma$ for all $g, \gamma \in G$.

   This is called the **left regular action** of G.

Theorem 4.3

An action of a group G on a set X is the same as a homomorphism $\varphi : G \to \mathrm{Sym}(X)$.

Proof. We will show the two directions separately.

Suppose $G \curvearrowright X$. Consider $t_g : X \to X$ defined by $x \mapsto gx$ for all $g \in G$. Then

$$\begin{aligned} t_{g^{-1}}\Big(t_g(x)\Big) &= t_{g^{-1}}(gx) \\ &= g^{-1}(g(x)) \\ &= \left(g^{-1} \cdot g\right)(x) \\ &= x. \end{aligned}$$

So $t_{g^{-1}} \cdot t_g = \mathrm{id}_X$. Similarly, $t_g \cdot t_{g^{-1}} = \mathrm{id}_X$. Thus t_g is invertible, so $t_g \in \mathrm{Sym}(X)$. Therefore, we can define a homomorphism $\varphi : G \to \mathrm{Sym}(X)$ by $g \mapsto t_g$.

We shall now prove that φ is a homomorphism. For any $g, h \in G$ and $x \in X$, we have

$$t_g \circ t_h(x) = t_g(hx) = g(hx) = (g \cdot h)x = t_{g \cdot h}(x).$$

Thus, $t_g \circ t_h = t_{g \cdot h}$, so $\varphi(g \cdot h) = \varphi(g) \circ \varphi(h)$. Hence, φ is a homomorphism.

Conversely, given a homomorphism

$$\varphi : G \to \mathrm{Sym}(X),$$

we may define an action $G \curvearrowright X$ by

$$gx := \varphi(g)(x).$$

Let us check the two properties of an action.

1. For any $x \in X$,

$$e_G x = \varphi(e_G)(x) = \mathrm{id}_X(x) = x.$$

2. For any $g_1, g_2 \in G$ and $x \in X$,

$$(g_1 g_2)x = \varphi(g_1 g_2)(x) = (\varphi(g_1) \circ \varphi(g_2))(x) = \varphi(g_1)(\varphi(g_2)(x)) = g_1(g_2 x).$$

Thus, the two properties hold, so we have an action of G on X.

Theorem 4.4 (Cayley's theorem)

Every group G is isomorphic to a subgroup of some $\mathrm{Sym}(X)$.

Furthermore, if $|G| < \infty$, we may choose X with $|X| < \infty$.

Proof. Let $X = G$. Consider the left regular action of G on itself. By the previous theorem, this corresponds to a homomorphism

$$\varphi : G \to \mathrm{Sym}(X).$$

Let $H = \operatorname{im} \varphi \leqslant \mathrm{Sym}(X)$. We may think of φ as a surjective homomorphism from G to H.

> ***Claim.*** $\ker \varphi = \{e\}$.

> ***Proof.*** Indeed, if $g \in \ker \varphi \Rightarrow \varphi(g) = \mathrm{id}_X \Leftrightarrow g\gamma = \gamma$ for all $\gamma \in G$. In particular,
>
> $$ge = e \Rightarrow g = e.$$

> Hence, $\varphi : G \to H$ is bijective, and thus an isomorphism. So $G \cong H \leqslant \mathrm{Sym}(X)$ so required.
>
> Automatically, if $|G| < \infty$, then $|X| = |G| < \infty$.

A lot of important results in group theory come from studying group actions.

Definition 4.5 (Orbits and Stabilisers)

Let $G \curvearrowright X$, and let $x \in X$.

1. The **orbit** of x is the set
$$Gx = \{y \in X : \exists g \in G, y = gx\}.$$
2. The **stabiliser** of x is the set
$$\mathrm{Stab}_G(x) = \{g \in G : gx = x\}.$$

Notation. Some sources write G_x for $\mathrm{Stab}_G(x)$, which we will avoid to prevent confusion with subscript notation.

Definition 4.6 (Action transitivity and faithfulness)

If $Gx = X$, we say that the action is **transitive**.

If every element $g \in G$ (except $g = e$) has $x \in X$ such that $gx \neq x$, then $G \curvearrowright X$ is **faithful**.

Lecture 10 · 2025-10-31

Remark. An action $G \curvearrowright X$ is faithful if and only if the corresponding homomorphism $\varphi : G \to \mathrm{Sym}(X)$ is injective.

4.2 Orbit-Stabiliser Theorem

Proposition 4.7

Suppose $G \curvearrowright X$. Then

1. For any $x \in X$, $\mathrm{Stab}_G(x) \leqslant G$.
2. The orbits $\{Gy : y \in X\}$ form a partition of X.

Remark. (2) means that $Gx = X$ iff there is only one orbit. Therefore, transitivity is independent of the choice of x.

Proof.

1. We need to check $\mathrm{Stab}_G(x)$ satisfies the definition of a subgroup.
   - If $g, h \in \mathrm{Stab}_{G(x)}$, then
   $$(g \cdot h)x = g(hx) = gx = x,$$

so $g \cdot h \in \mathrm{Stab}_G(x)$.

- $e_G \in \mathrm{Stab}_G(x)$ since $e_G x = x$.
- If $g \in \mathrm{Stab}_{G(x)}$, then

$$g^{-1}x = g^{-1}(gx) = \left(g^{-1} \cdot g\right)x = e_G x = x,$$

so $g^{-1} \in \mathrm{Stab}_G(x)$.

So all subgroup criteria are satisfied.

2. Similarly to the proof of Lemma 3.3,
   - $x = ex \in Gx$ so orbits cover x.
   - If $Gx_1 \cap Gx_2 \neq \varnothing$, then $\exists y = g_1x_1 = g_2x_2$ for some $g_1 \in G, g_2 \in G$. Hence,

$$\begin{aligned} x_1 &= g_1^{-1}(g_1x_1) \\ &= g_1^{-1}(g_2x_2) \\ &= \left(g_1^{-1}g_2\right)x_2 \\ &\in Gx_2 \end{aligned}$$

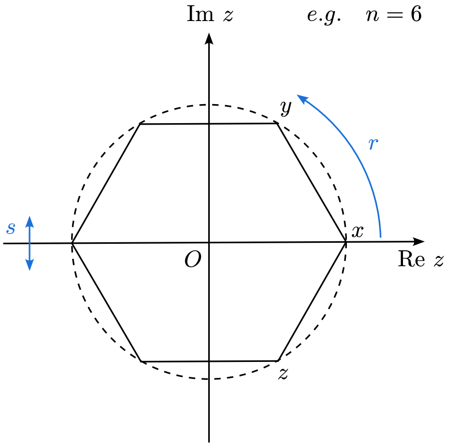
Moreover, any gx_1 can now be written as

$$gx_1 = g\left(g_1^{-1}g_2\right)x_2 \in Gx_2.$$

Hence $Gx_1 \subseteq Gx_2$. By symmetry, we have the reverse inclusion. Thus, the equality holds.

Example 4.8

Consider $D_{2n} \curvearrowright X_n$, where X_n is the set of the regular n-gon.



For any j,

$$r^j s(x) = r^j(x) = e^{\frac{2\pi i j}{n}}.$$

Therefore, $D_{2n}x = \left\{e^{\frac{2\pi i j}{n}} : 0 \leqslant j < n\right\} = \{\text{nth roots of unity}\}$.

The above calculation also shows that $gx = x \Rightarrow g = \{e, s\}$. Hence, $\mathrm{Stab}_{D_{2n}}(x) = \{e, s\}$.

Theorem 4.9 (Orbit-stabiliser theorem)

Suppose G acts on a set X. Then for any $x \in X$, the formula

$$g\,\mathrm{Stab}_G(x) \overset{\Phi}{\mapsto} gx$$

defines a well-defined bijection

$$G/\,\mathrm{Stab}_G(x) \to Gx.$$

Corollary 4.10

If $G \curvearrowright X$ and $x \in X$, then

$$|G| = (|Gx|(\left|\mathrm{Stab}_G(x)\right|)$$

Proof. Theorem 4.9 gives

$$|Gx| = \left|G/\,\mathrm{Stab}_G(x)\right| = \frac{|G|}{\left|\mathrm{Stab}_G(x)\right|}. \quad \text{by Lagrange's theorem}$$

Example 4.11

Consider again $D_{2n} \curvearrowright X_n$ as in the previous example. We saw that, if $x \in X_n$ is a vertex, then

$$\left|D_{2n}x\right| = n \quad \text{and} \quad \left|\mathrm{Stab}_{D_{2n}}(x)\right| = 2.$$

This gives us an easy (but circular for now) proof that

$$\left|D_{2n}\right| = 2n.$$

Proof. [For Theorem 4.9]

For notational convenience, let $S = \mathrm{Stab}_G(x)$, and define

$$\Phi(gS) = gx.$$

We have to check several things about Φ.

- **Φ well-defined.** That is, for any $g_1, g_2 \in G$ such that $g_1S = g_2S$, we have $\Phi(g_1S) = \Phi(g_2S)$, *i.e.* $g_1x = g_2x$.

  Now, $g_1S = g_2S$ means that there is $s \in S$ such that $g_1 = g_2s$. Then,

$$\begin{aligned} g_1x &= (g_2s)x \\ &= g_2(sx) \\ &= g_2x \quad \text{since } sx = x. \end{aligned}$$

Thus, Φ is well-defined.

- **Φ is surjective.** For any $gx \in Gx$, we have

$$\Phi(gS) = gx.$$

Thus, Φ is surjective.

- **Φ is injective.** Suppose $\Phi(g_1 S) = \Phi(g_2 S)$ for some $g_1, g_2 \in G$. By definition, this means that

$$g_1 x = g_2 x.$$

We need to show that $g_1 S = g_2 S$. Let $s = g_2^{-1} g_1$. Now,

$$\begin{aligned} sx &= \left(g_2^{-1} g_1\right) x \\ &= g_2^{-1}(g_1 x) \\ &= g_2^{-1}(g_2 x) \\ &= \left(g_2^{-1} g_2\right) x \\ &= e_G x = x. \end{aligned}$$

Thus, $s \in S$, so

$$g_1 = g_2 g_2^{-1} g_1 = g_2\left(g_2^{-1} g_1\right) = g_2 s \in g_2 S.$$

Since cosets paritition, it follows that $g_1 S = g_2 S$. Hence, Φ is injective.

Example 4.12 (Symmetries of a cube)

Let G be the group of isometries of a cube, and let x be the centre of a face. Then,

$$|Gx| = 6$$

since it is just the number of faces of the cube.

Now, the face is essentially a square, so $\mathrm{Stab}_G(x) \cong D_8$ since the stabiliser must permute the four edges of the face. Thus,

$$\left|\mathrm{Stab}_G(x)\right| = 8.$$

Therefore, by the orbit-stabiliser theorem,

$$|G| = |Gx| \times \left|\mathrm{Stab}_G(x)\right| = 6 \times 8 = 48.$$

Lecture 11 · 2025-11-03

The next theorem is a different kind of application of the orbit-stabiliser theorem.

Theorem 4.13 (Cauchy's Theorem)

If $|G| < \infty$ and p is a prime that divides $|G|$, then there is $g \in G$ such that $o(g) = p$.

Proof. Consider the set X of p-tuples (distinct entries not required)

$$\left\{\left(g_1, \ldots, g_p\right) : g_i \in G \text{ for all } i \text{ and } g_1 \cdot g_2 \cdot \ldots \cdot g_p = e\right\}.$$

Define an action of C_p on X as follows.

If $C_p = \left\{1, t, t^2, \ldots, t^{p-1}\right\}$, let $t^k\left(g_1, \ldots, g_p\right) = \left(g_{k+1}, \ldots, g_p, g_1, \ldots, g_k\right)$, which is just a cyclic rotation of the p-tuple. We need check that this is a well-defined action.

It is easy to see that $t^k t^l\left(g_1, \ldots, g_p\right) = t^{k+l}\left(g_1, \ldots, g_p\right)$.

We also need to check that

$$\left(g_{k+1}, \ldots, g_p, g_1, \ldots, g_k\right) \in X.$$

Suppose, therefore, that

$$\left(g_1, \ldots, g_p\right) \in X.$$

For convenience, let $a = g_1 \cdot \ldots \cdot g_k$ and $b = g_{k+1} \cdot \ldots \cdot g_p$. Then, we know that $a \cdot b = e$. So, $b = a^{-1}$ and therefore $b \cdot a = e$. Hence,

$$g_{k+1} \cdot \ldots \cdot g_p \cdot g_1 \cdot \ldots \cdot g_k = b \cdot a = e.$$

Thus, the action is well-defined.

Now compute $|X|$. For any choices of $g_1, \ldots, g_{p-1}$, there is a unique choice of g_p such that

$$g_1 \cdot g_2 \cdot \ldots \cdot g_p = e$$

as inverses are unique. Thus, there are $|G|^{p-1}$ choices for $\left(g_1, \ldots, g_p\right)$, so

$$|X| = |G|^{p-1}.$$

The C_p action on X partitions X into orbits. So let

$$X = C_p x_1 \cup C_p x_2 \cup \ldots \cup C_p x_k.$$

By orbit-stabiliser, for each j,

$$\left|C_p x_j\right| \mid \left|C_p\right| = p,$$

so either $\left|C_p x_j\right| = 1$ or $\left|C_p x_j\right| = p$. Let l be the number of orbits with size 1. After renumbering, we may assume that

$$\begin{aligned} \left|C_p x_j\right| &= 1 \quad \text{if } (1 \leqslant j \leqslant l) \\ \left|C_p x_j\right| &= p \quad \text{if } (l+1 \leqslant j \leqslant k). \end{aligned}$$

Since the orbits partition X, we have

$$\begin{aligned} |G|^{p-1} &= |X| \\ &= \sum_{j=1}^{k} \left|C_p x_j\right| \\ &= \sum_{j=1}^{l} 1 + \sum_{j=l+1}^{k} p \\ &= l + p(k-l). \end{aligned}$$

Since, by our assumption, p divides $|G|^{p-1}$, it follows that p divides l.

Now, note that $x = \left(g_1, ..., g_p\right)$ has an orbit of size 1 if and only if $g_1 = g_2 = ... = g_p$. In particular, $(e, e, ..., e) \in X$ has an orbit of size 1. Thus, $l \geqslant 1$. Since p divides l and $l \geqslant 1$, we must have

$$l \geqslant p > 1,$$

so there is at least one more orbit $(g, g, ..., g) \in X$ with $g \neq e$.

The definition of X implies that $g^p = e$, so $o(g) \mid p$, whence $o(g) = p$ as required.

4.3 Conjugation

Definition 4.14 (Conjugation)

Let G be a group and $g \in G$. For any $h \in G$, the element $h \cdot g \cdot h^{-1} \in G$ is called the **conjugate** of g by h.

Intuition. One way to think about conjugation is that hgh^{-1} has *the same shape* as g.

Another way is to think about it is that hgh^{-1} corresponds to *changing the coordinates* of g.

Example 4.15

If G is an abelian group, then $hgh^{-1} = g$ for all $g, h \in G$. So the only conjugate of any element is itself.

Definition 4.16 (Conjugacy class)

The **conjugacy class** of an element $g \in G$ is the set

$$\operatorname{ccl}(g) = \left\{hgh^{-1} : h \in G\right\}.$$

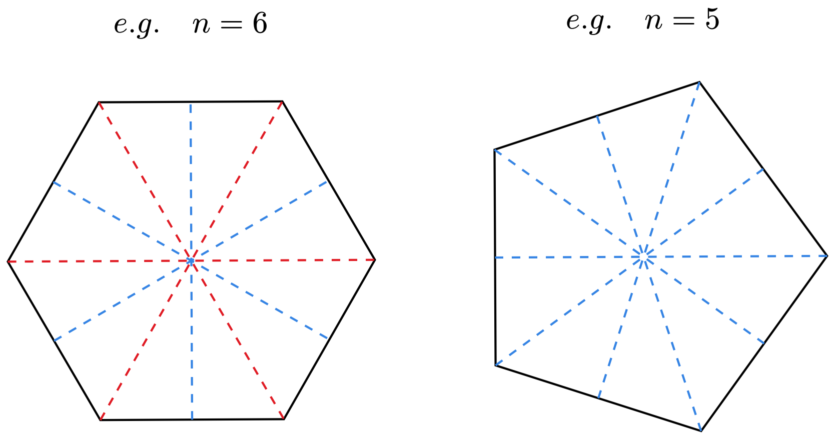
Exercise. G acts on itself by conjugation:

$$g * \gamma = g\gamma g^{-1}$$

defines $G \curvearrowright G$. This is very different from the left regular action. Then $\operatorname{ccl}(g)$ is just the orbit of g under this action.

Example 4.17

In Example Sheet 2 Q6, it is proven that D_{2n} has 1 conjugacy class of reflections if n is odd, and 2 conjugacy classes if n is even.



Note that the red reflections cannot be obtained by conjugating the blue reflections, and vice versa.

Definition 4.18 (Centraliser)

The **centraliser** of g is defined to be

$$C_G(g) = \left\{h \in G : hgh^{-1} = g\right\},$$

which is just the stabiliser of g under the conjugation action.

Remark. Note that

$$hgh^{-1} = g \Leftrightarrow hg = gh$$

so $C_G(g)$ is the set of elements that commutes with g.

Definition 4.19 (Centre)

The **centre** of G is defined to be

$$Z(G) = \left\{g \in G : hgh^{-1} = g \ \forall h \in G\right\} = \bigcap_{g \in G} C_G(g).$$

This is exactly the set of elements that commutes with every element of G.

Lecture 12 · 2025-11-05

5 The Möbius Group

This chapter is about an interesting group. It is almost a group of bijections of $\mathbb{C}$, but we need to add a formal point at ∞.

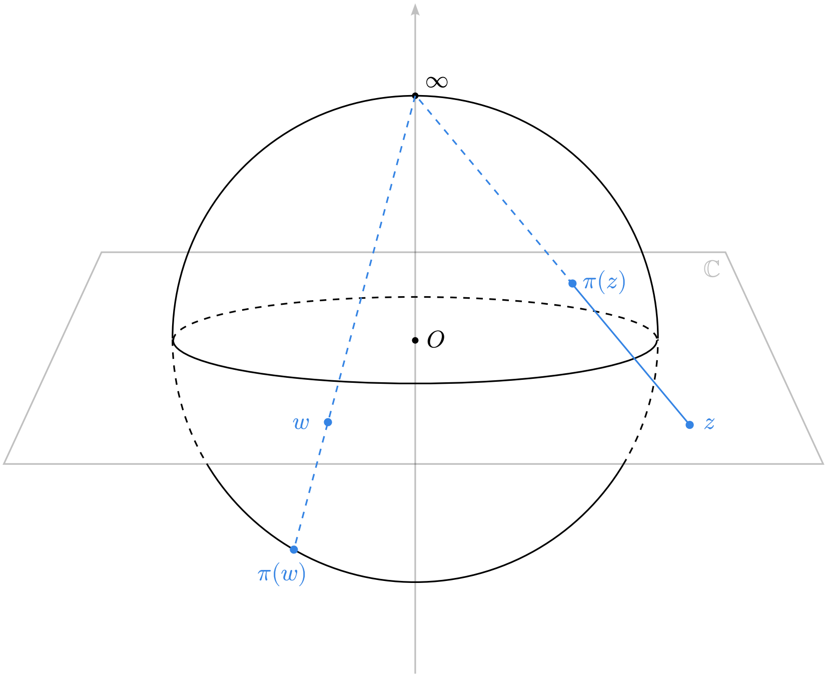
5.1 Riemann Sphere and Möbius Transformations

Definition 5.1 (Riemann Sphere)

The **Riemann sphere** is the set

$$\mathbb{C}_\infty := \mathbb{C} \cup \{\infty\}.$$

This set is called a sphere because we can visualize it as follows.



We can define a map $\pi : \mathbb{C} \to S^2$ called the **stereographic projection**. It identifies $\mathbb{C}$ with all the points on the sphere except the north pole at ∞.

Definition 5.2 (Möbius Transformation)

Let a, b, c, d be complex numbers with $ad - bc \neq 0$. If $c \neq 0$, then the corresponding **Möbius transformation** is the map $\mu : \mathbb{C}_\infty \to \mathbb{C}_\infty$ defined by, if $c \neq 0$,

$$z \mapsto \begin{cases} \frac{az+b}{cz+d} & \text{if } z \in \mathbb{C} \setminus \left\{-\frac{d}{c}\right\} \\ \infty & \text{if } z = -\frac{d}{c} \\ \frac{a}{c} & \text{if } z = \infty \end{cases}$$

If $c = 0$, then μ is defined by

$$z \mapsto \begin{cases} \frac{az+b}{d} & \text{if } z \in \mathbb{C} \\ \infty & \text{if } z = \infty \end{cases}$$

We usually just write $\mu(z) = \frac{az+b}{cz+d}$ and interpreting the cases of 0 and ∞ appropriately.

Then

$$\mathcal{M} = \{f : C_\infty \to C_\infty : f \text{ is a Möbius transformation}\}$$

together with composition of functions forms a group, called the **Möbius group**.

Proposition 5.3

If

$$\mu_1(z) = \frac{a_1 z + b_1}{c_1 z + d_1}, \quad \mu_2(z) = \frac{a_2 z + b_2}{c_2 z + d_2}$$

then

$$\mu_1 \circ \mu_2(z) = \frac{(a_1 a_2 + b_1 c_2)z + (a_1 b_2 + b_1 d_2)}{(c_1 a_2 + d_1 c_2)z + (c_1 b_2 + d_1 d_2)}.$$

Remark. Compare this with matrix multiplication:

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{pmatrix}.$$

5.2 The Möbius Group

Theorem 5.4 (Möbius Group)

$(\mathcal{M}, \circ, \mathrm{id})$ is a group.

Proof.

- Composition of functions is associative.
- The identity map $\mathrm{id}(z) = \frac{1z+0}{0z+1} = z$ is a Möbius transformation with $a = d = 1$ and $b = c = 0$.
- For $\mu : z \mapsto \frac{az+b}{cz+d}$, let $\nu : z \mapsto \frac{dz-b}{-cz+a}$.
  Then ν is also a Möbius transformation and $\mu \circ \nu = \mathrm{id}$ and $\nu \circ \mu = \mathrm{id}$. Hence ν is the inverse of μ.

One important way to study Möbius transformations is via their fixed points.

Definition 5.5

Suppose $f : X \to X$ is a permutation. Any $x \in X$ such that $f(x) = x$ is called a **fixed point** of f.

Lemma 5.6 (Three-point lemma for $\mathcal{M}$)

If $\mu \in \mathcal{M}$ fixes three distinct points w_1, w_2, w_3 of $\mathbb{C}_\infty$, then $\mu = \mathrm{id}$.

Proof. Let $\mu(z) = \frac{az+b}{cz+d}$. A fixed point w_i satisfies

$$w_i = \frac{aw_i + b}{cw_i + d}.$$

Case 1. If there is a fixed point ∞, WLOG let $w_1 = \infty$, then $c = 0$. So w_2 and w_3 satisfy

$$\begin{aligned} w_i &= \frac{aw_i + b}{d} \\ (a-d)w_i + b &= 0. \end{aligned}$$

This is a linear equation with at least 2 roots, so we cannot have two distinct fixed points w_2 and w_3 unless $a = d$ and $b = 0$. Then $\mu = \mathrm{id}$.

Case 2. If none of the fixed points is ∞, then we have three distinct complex numbers w_1, w_2, w_3 satisfying

$$\begin{aligned} (a - cw_i)w_i + b - dw_i &= 0 \\ cw_i^2 + (d-a)w_i - b &= 0. \end{aligned}$$

This is a quadratic equation with at least 3 roots, so we cannot have three distinct fixed points w_1, w_2, w_3 unless $a = d$, $b = 0$, and $c = 0$. Then $\mu = \mathrm{id}$.

Exercise. Show that every $\mu \in \mathcal{M}$ has at least one fixed point in $\mathbb{C}_\infty$.

Example 5.7

1. Consider $\mu(z) = z + 1$. Then $\mathrm{Fix}(\mu) = \{\infty\}$.
2. Consider $\mu(z) = 2z$. Then $\mathrm{Fix}(\mu) = \{0, \infty\}$.

Lemma 5.8 (Triple transitivity)

For any triples of distinct points $z_1, z_2, z_3 \in \mathbb{C}_\infty$ and $w_1, w_2, w_3 \in \mathbb{C}_\infty$, there exists a $\mu \in \mathcal{M}$ such that $\mu(z_i) = w_i$ for $i = 1, 2, 3$.

Proof. Instead of constructing μ directly, we construct two auxiliary Möbius transformations α and β such that $\alpha(z_i) = 0, 1, \infty$ and $\beta(w_i) = 0, 1, \infty$. Then we can let $\mu = \beta^{-1} \circ \alpha$.

Let $\alpha(z)$ be defined by

$$\alpha(z) = \left(\frac{z_2 - z_3}{z_2 - z_1}\right)\frac{z - z_1}{z - z_3}.$$

[Modify appropriately if any of z_1, z_2, z_3 is ∞.]

Then $\alpha(z_1) = 0$, $\alpha(z_2) = 1$, and $\alpha(z_3) = \infty$.

Similarly, let $\beta(z)$ be defined by

$$\beta(z) = \left(\frac{w_2 - w_3}{w_2 - w_1}\right)\frac{z - w_1}{z - w_3}.$$

[Modify appropriately if any of w_1, w_2, w_3 is ∞.]

Then $\beta(w_1) = 0$, $\beta(w_2) = 1$, and $\beta(w_3) = \infty$.

Note that α and β are both in $\mathcal{M}$. Then let

$$\mu = \beta^{-1} \circ \alpha.$$

Then $\mu(z_i) = w_i$ for $i = 1, 2, 3$.

Remark. The three-point lemma implies that μ in Lemma 5.8 is unique. We say that $\mathcal{M} \curvearrowright \mathbb{C}_\infty$ is sharply triply transitive.

Definition 5.9 (Cross Ratio)

Let $z_1, z_2, z_3, z_4 \in \mathbb{C}_\infty$ be distinct points. Because $\mathcal{M} \curvearrowright \mathbb{C}_\infty$ sharply triply transitively, there exists a unique $\alpha \in \mathcal{M}$ such that

$$\alpha(z_1) = 0, \quad \alpha(z_2) = 1, \quad \alpha(z_3) = \infty.$$

The **cross-ratio** is defined as

$$[z_1, z_2, z_3, z_4] \coloneqq \alpha(z_4).$$

Note that we saw that $[z_1, z_2, z_3, z_4]$ can be computed by

$$[z_1, z_2, z_3, z_4] = \frac{(z_4 - z_1)(z_2 - z_3)}{(z_4 - z_3)(z_2 - z_1)}$$

by the proof of Lemma 5.8.

Lecture 13 · 2025-11-07

Just like for dihedral groups, we can use the 3-point lemma to find a generating set for $\mathcal{M}$.

Proposition 5.10

$\mathcal{M}$ is generated by the set of elements of the following 3 forms:
1. $\alpha_a : z \mapsto az$, where $a \neq 0$
2. $\beta_b : z \mapsto z + b$, where $b \in \mathbb{C}$
3. $\gamma : z \mapsto \frac{1}{z}$

Proof. Let $\mu \in \mathcal{M}$ be arbitrary, and let $z_1 = \mu(0)$, $z_2 = \mu(1)$, $z_3 = \mu(\infty)$.

Step 1. Construct μ_1 such that $\mu_1(z_3) = \infty$.

Either $z_3 = \infty$ and $\mu_1 = \text{id}$ or

$$\mu_1 = \frac{1}{z+b}$$

where $b = -z_3$. Then $\mu_1 = \gamma \circ \beta_b$

Let $z_1' = \mu_1(z_1)$ and $z_2' = \mu_1(z_2)$.

Step 2. Let $b' = -z_1'$, and let $\mu_2 = \beta_{b'}$, *i.e.*

$$\mu_2(z) = z + b'.$$

Note that $\mu_2(\infty) = \infty$ and $\mu_2(z_1') = 0$. By construction,

$$\mu_2 \circ \mu_1(z_3) = \infty, \quad \mu_2 \circ \mu_1(z_1) = 0.$$

Let

$$z_2'' = \mu_2 \circ \mu_1(z_2) \neq 0 \text{ or } \infty.$$

Step 3. Let $a = \frac{1}{z_2''}$ and

$$\mu_3(z) \coloneqq \alpha_a(z).$$

By construction,

$$\begin{aligned} \mu_3 \circ \mu_2 \circ \mu_1(z_1) &= 0, \\ \mu_3 \circ \mu_2 \circ \mu_1(z_2) &= 1, \\ \mu_3 \circ \mu_2 \circ \mu_1(z_3) &= \infty. \end{aligned}$$

By the three-point lemma, $\mu_3 \circ \mu_2 \circ \mu_1 = \mu^{-1}$, so

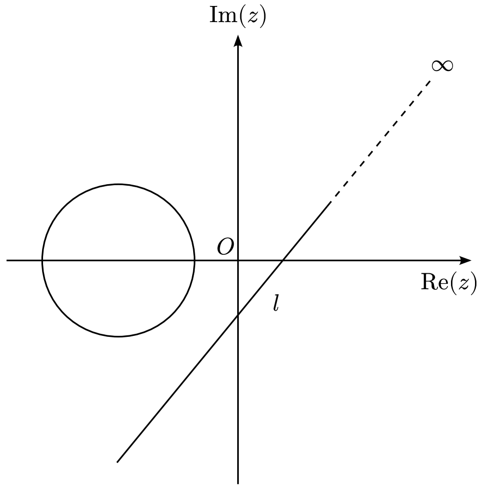
$$\mu = \mu_1^{-1} \circ \mu_2^{-1} \circ \mu_3^{-1}.$$

5.3 Circles

Definition 5.11 (Circle in $\mathbb{C}_\infty$)

A **circle** in C_∞ is either

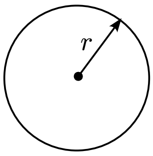
- a Euclidean circle in $\mathbb{C}$, or
- $l \cup \{\infty\}$ where l is a Euclidean straight line in $\mathbb{C}$.



Euclidean circles are described by the equation

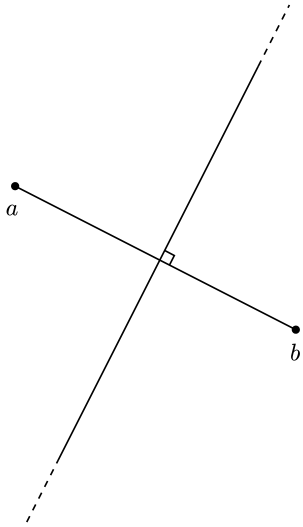
$$|z - a| = r$$

for some $a \in \mathbb{C}$ and $r > 0$,



while lines are described by

$$|z - a| = |z - b| \text{ for } a, b \in \mathbb{C}.$$



Theorem 5.12 (Circles and Möbius Transformations)

Möbius transformations map circles to circles. Formally, if $C \subseteq \mathbb{C}_\infty$ is a circle, then $\mu \in \mathcal{M}$ then $\mu(C)$ is also a circle.

Proof. Recall that $\mathcal{M}$ is generated by

$$\begin{aligned}\alpha_a(z) &= az\\ \beta_b(z) &= z+b\\ \gamma(z) &= \frac{1}{z}.\end{aligned}$$

So it suffices to show that each of these generators maps circles to circles.

It is clear that α_a and β_b map circles to circles. So we just need to show that γ maps circles to circles.

If C is a Euclidean circle in $\mathbb{C}$, then $\gamma(C)$ has equation

$$\begin{aligned}\left|\frac{1}{z}-c\right| = r \Leftrightarrow \left|\frac{1}{z}-c\right|^2 &= r^2\\ \Leftrightarrow \left(\frac{1}{z}-c\right)\left(\frac{1}{\overline{z}}-\overline{c}\right) &= r^2\\ \Leftrightarrow \frac{1}{|z|^2}-\frac{c}{\overline{z}}-\frac{\overline{c}}{z}+|c|^2-r^2 &= 0\\ \Leftrightarrow \left(|c|^2-r^2\right)\left|z^2\right|-cz-\overline{c}\,\overline{z}+1 &= 0.\end{aligned}$$

If $|c|^2 = r^2$, then we have

$$\begin{aligned}cz+\overline{c}\,\overline{z} = 1 \Leftrightarrow \frac{z}{\overline{c}}+\frac{\overline{z}}{c} &= \frac{1}{|c|^2}\\ \Leftrightarrow |z|^2 = |z|^2-\frac{z}{\overline{c}}-\frac{\overline{z}}{c}+\frac{1}{|c|^2} &= \left|z-\frac{1}{c}\right|^2\\ \Leftrightarrow |z| &= \left|z-\frac{1}{c}\right|.\end{aligned}$$

This is the equation of a line. Otherwise, $|c|^2 \neq r^2$, and the equation becomes

$$\begin{aligned}|z|^2-\left(\frac{c}{|c|^2-r^2}\right)z-\left(\frac{\overline{c}}{|c|^2-r^2}\right)\overline{z}+\frac{1}{|c|^2-r^2} &= 0\\ \Leftrightarrow \left|z-\frac{\overline{c}}{|c|^2-r^2}\right|^2 = \frac{|c|^2}{(|c^2|-r^2)^2}-\frac{1}{|c^2|-r^2} &= \frac{r^2}{(|c|^2-r^2)^2}\end{aligned}$$

which is the equation of a circle.

We are left with the case where C is a line, which follows a very similar calculation to the above and is left as an exercise.

Corollary 5.13

Four points $z_1, z_2, z_3, z_4 \in \mathbb{C}_\infty$ lie on a circle if and only if their cross-ratio $[z_1, z_2, z_3, z_4] \in \mathbb{R}_\infty$.

Proof. Let $\alpha \in \mathcal{M}$ such that $\alpha(z_1) = 0$, $\alpha(z_2) = 1$, $\alpha(z_3) = \infty$, and so $\alpha(z_4) = [z_1, z_2, z_3, z_4]$

$[\Rightarrow]$ If $z_1, \ldots, z_4 \in \mathbb{C}$ lie on a circle C, then by the previous theorem, $\alpha(C)$ is also a circle containing $0, 1, \infty$. The only such circle is the real line $\mathbb{R}_\infty$, so $[z_1, z_2, z_3, z_4] \in \mathbb{R}_\infty$.

> [⇐] If $\alpha(z_4) \in \mathbb{R}_\infty$, then $0, 1, \infty, [z_1, z_2, z_3, z_4]$ lie on the circle $\mathbb{R}_\infty$. So by the previous theorem, their preimages z_1, z_2, z_3, z_4 also lie on a circle.

6 Finite Groups

We have already seen some nice theorems about finite groups, including Lagrange's, orbit-stabilizer, Cayley's, and Cauchy's theorems.

Lecture 14 · 2025-11-10

We will now develop some small examples of finite groups. We shall proceed naively, trying to list examples by order.

$$\begin{aligned} |G| = 1 \quad &\Rightarrow \quad G \cong 1 \\ |G| = 2 \quad &\Rightarrow \quad G \cong C_2 \text{ since 2 is prime} \\ |G| = 3 \quad &\Rightarrow \quad G \cong C_3 \text{ since 3 is prime} \end{aligned}$$

Now, if $|G| = 4$, we know that C_4 is always an option. But is there another?

Definition 6.1 (Direct Product)

If G, H are groups, the **direct product** is

$$G \times H = \{(g, h) : g \in G, h \in H\}$$

with operation

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot g_2, h_1 \cdot h_2).$$

Note that (e_G, e_H) is a identity, and $(g, h)^{-1} = \left(g^{-1}, h^{-1}\right)$.

Example 6.2 (Klien 4-group)

The **Klein 4-group** is $K_4 := C_2 \times C_2$. It can also be thought of as D_4. Note that, for every $(a, b) \in K_4$, we have $(a, b)^2 = (e, e)$. So every element has order at most 2. In particular, $K_4 \ncong C_4$.

Theorem 6.3 (Direct Product Theorem)

If $H_1, H_2 \leqslant G$ and

1. $H_1 \cap H_2 = \{e\}$,
2. $\forall h_1 \in H_1, h_2 \in H_2, h_1 h_2 = h_2 h_1$,
3. $G = H_1 H_2$, *i.e.* for every $g \in G$, there exist $h_1 \in H_1, h_2 \in H_2$ such that $g = h_1 h_2$,

then $G \cong H_1 \times H_2$.

Proof. Define $\Phi : H_1 \times H_2 \to G$ with $(h_1, h_2) \mapsto h_1 h_2$. We need to show that Φ is an isomorphism.

Φ IS A HOMOMORPHISM

For any $h_1, h_1' \in H$, $h_2, h_2' \in H$, by definition,

$$\begin{aligned}\Phi(h_1,h_2)\Phi(h_1',h_2') &= (h_1h_2)(h_1'h_2')\\ &= h_1h_1'h_2h_2' \quad \text{by (2)}\\ &= \Phi(h_1h_1',h_2h_2')\\ &= \Phi((h_1,h_2)(h_1',h_2')) \quad \text{as required.}\end{aligned}$$

Φ IS SURJECTIVE

This is immediate from (3).

Φ IS INJECTIVE

Recall that we need to show that $\ker(\Phi) = \{(e,e)\}$. Suppose that $\Phi(h_1,h_2) = e$. Then $h_1h_2 = e$, so $h_2 = h_1^{-1} \in H_1$. But $h_2 \in H_2$ also, so by (1), we must have $h_2 = e$ and $h_1 = e$. Thus $(h_1,h_2) = (e,e)$, as required.

Remark. If $H_1 \cap H_2 = \{e\}$, then $|H_1H_2| = |H_1||H_2|$. In particular, if $|H_1||H_2| = |G|$, we can conclude that (1) implies (3).

Lemma 6.4 (Groups of order 4)

If $|G| = 4$, then $G \cong C_4$ or $G \cong K_4$.

Proof. By Lagrange's theorem, every non-trivial element of G has order 2 or 4. If there is a $g \in G$ such that $o(g) = 4$, then $G \cong C_4$.

Otherwise, every non-trivial element has order 2. Let $a, b \in G$ be distinct elements such that $o(a) = o(g) = 2$. Let $H_1 = \langle a\rangle$ and $H_2 = \langle b\rangle$. It is immediate that $H_1 \cap H_2 = \{e\}$ [this can be seen by writing out the elements explicitly], which gives us (1). Following the remark, (3) holds.

Finally, since $o(ab) = 2$, we have $abab = e$, so $ab = ba$, giving us (2) [this was mentioned in Example Sheet 1, Q11]. Thus by the direct product theorem, $G \cong H_1 \times H_2 \cong C_2 \times C_2 \cong K_4$, as required.

Another application of the direct product theorem 6.3 is to find out when a product of two cyclic groups is cyclic.

Theorem 6.5 (Chinese Remainder Theorem)

If $\gcd(m,n) = 1$, then $C_m \times C_n \cong C_{mn}$.

Proof. Let $C_{mn} = \langle g\rangle$. Set

$$H_1 = \langle g^n\rangle, \quad H_2 = \langle g^m\rangle.$$

We will check against DPT 6.3.

1. Note that

$$\begin{aligned} g^k \in H_1 &\Leftrightarrow k = np + mnq \quad \text{for some } p, q \in \mathbb{Z} \\ &\Leftrightarrow n \mid k. \end{aligned}$$

Similarly,

$$g^k \in H_2 \Leftrightarrow m \mid k.$$

Therefore, $g^k \in H_1 \cap H_2$ iff mn divides k. Since $o(g) = mn$, this happens iff $g^k = e$. Thus, $H_1 \cap H_2 = \{e\}$ as required.

2. Since C_{mn} is abelian, this is immediate.
3. This follows from (1) and the remark after DPT.

We shall now move on to groups of order 5 and above.

$$|G| = 5 \quad \Rightarrow \quad G \cong C_5 \text{ since 5 is prime}$$

Lemma 6.6 (Groups of order 6)

If $|G| = 6$, then $G \cong C_6$ or $G \cong D_6$.

Proof. By Cauchy's theorem 4.13, there exist $r, s \in G$ such that $o(r) = 3$ and $o(s) = 2$. Since $|\langle r\rangle| = 3$, $[G : \langle r\rangle] = 2$, and $s \notin \langle r\rangle$. Therefore,

$$s\langle r\rangle = G \setminus \langle r\rangle = \langle r\rangle s$$

since the other coset must be $\langle r\rangle$. So $sr = r^i s$ for some $i \in \{0, 1, 2\}$.

- If $i = 0$, then $sr = r^0 s = s$, so $r = e$, a contradiction.
- If $i = 1$, then $sr = rs$. Then $\langle s\rangle$ and $\langle r\rangle$ satisfy the conditions of DPT 6.3, so
$$G \cong \langle r\rangle \times \langle s\rangle \cong C_3 \times C_2 \cong C_6.$$
- If $i = 2$, then $sr = r^2 s$. In this case, $G = \langle r, s\rangle$ with relations $r^3 = s^2 = e$, $sr = r^{-1}s$, which is satisfies the dihedral relation 1.33. Thus, $G \cong D_6$.

Remark. S_3 is a non-abelian group of order 6, so by the above lemma, $S_3 \cong D_6$.

Continuing on,

$$|G| = 7 \quad \Rightarrow \quad G \cong C_7 \text{ since 7 is prime}$$

Lecture 15 · 2025-11-12

Consider $|G| = 8$.

We have C_8 and $C_2 \times C_4$ and $C_2 \times C_2 \times C_2$ as abelian groups of order 8.

We also have D_8 as a non-abelian group of order 8.

Exercise. None of the groups D_8, C_8, $C_2 \times C_4$, and $C_2 \times C_2 \times C_2$ are isomorphic to each other.

Definition 6.7 (Quaternion Group)

Let

$$Q_8 = \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \begin{pmatrix} \pm \mathrm{i} & 0 \\ 0 & \mp \mathrm{i} \end{pmatrix}, \begin{pmatrix} 0 & \pm 1 \\ \mp 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \pm \mathrm{i} \\ \pm \mathrm{i} & 0 \end{pmatrix} \right\}.$$

It is easy to check that these form a group. We usually use Hamilton's notation:

$$\begin{aligned} 1 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, & -1 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \\ i &= \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix}, & -i &= \begin{pmatrix} -\mathrm{i} & 0 \\ 0 & \mathrm{i} \end{pmatrix}, \\ j &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, & -j &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \\ k &= \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, & -k &= \begin{pmatrix} 0 & -\mathrm{i} \\ -\mathrm{i} & 0 \end{pmatrix}. \end{aligned}$$

So the elements of Q_8 are $\{\pm 1, \pm i, \pm j, \pm k\}$, with relations

- $i^2 = j^2 = k^2 = -1$,
- $(-1)i = -i$, *etc.*
- $ij = k$, $jk = i$, $ki = j$,
- -1 commutes with everything.

We call this group the **quaternion group**.

Since $ji = -k \neq k = ij$, Q_8 is non-abelian and so $Q_8 \ncong C_2 \times C_2 \times C_2, C_4 \times C_2, C_8$.

By considering the orders of elements, we can also see that $Q_8 \ncong D_8$. D_8 has 5 elements of order 2 (one 180° rotation and the 4 reflections), whereas Q_8 has only one (the element -1).

It can be shown that these are all the groups of order 8.

Lemma 6.8 (Groups of order 8)

If $|G| = 8$, then G is isomorphic to one of C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_8, or Q_8.

Proof. By Lagrange's theorem, the possible orders of elements in G are 1, 2, 4, or 8. We have the following cases:

- If there is an element of order 8, then $G \cong C_8$.
- If every non-trivial element has order 2, then $G \cong C_2 \times C_2 \times C_2$ by a similar argument as in Lemma 6.4. We will start by choosing non-trivial elements $a, b, c \in G$ with $a \neq b$ and $c \neq a, b, ab$. We can see that

  $$G \cong \langle a \rangle \times \langle b \rangle \times \langle c \rangle \cong C_2 \times C_2 \times C_2$$

  by using Theorem 6.3 twice. [Check Example Sheet 1, Q11 for related details.]

- If there is an element of order 4, but no element of order 8, let $a \in G$ with $o(a) = 4$. Let $b \in G \setminus \langle a \rangle$. By Lagrange's theorem,

  $$[G : \langle a \rangle = 2]$$

  so

  $$b\langle a \rangle = G \setminus \langle a \rangle = \langle a \rangle b.$$

  In particular, $ba = a^i b$ for some $i \in \{0, 1, 2, 3\}$.

  - If $i = 0$, then $ba = a^0 b = b$, so $a = e$. ※
  - If $i = 1$, then $ba = ab$, so $ba^j = a^j b$ for all j, then G is abelian. **[Case A.]**
  - If $i = 2$, then $ba = a^2 b$, so $bab^{-1} = a^2$. But $o\left(bab^{-1}\right) = o(a) = 4$ by Example Sheet 2, Q1. However, $o\left(a^2\right) = 2$. ※
  - If $i = 3$, then $ba = a^3 b = a^{-1} b$, which looks similar to the dihedral relation. **[Case B.]**

  Next, note that if $b^2 = ba^i$, then $b = a^j$ and so $b \in \langle a \rangle$. ※

  Thus $b^2 \in \langle a \rangle$. We have several more cases:

  - $b^2 = e$, which we will handle later. **[Case I.]**
  - If $b^2 = a$, then $o(b) = 8$, so $G \cong C_8$. ※
  - $b^2 = a^2$, which we will handle later. **[Case II.]**
  - If $b^2 = a^3 = a^{-1}$, then $o(b) = 8$, so $G \cong C_8$. ※

  There are now four subcases to consider:

  - **[Case A, I.]** If G is abelian and $\langle b \rangle \cong C_2$, then $\langle a \rangle \cap \langle b \rangle = \{e\}$, so by Theorem 6.3,

    $$G \cong \langle a \rangle \times \langle b \rangle \cong C_4 \times C_2.$$

  - **[Case A, II.]** If G is abelian, $b^2 = a^2$, so

    $$\left(ab^{-1}\right)^2 = e \Rightarrow o\left(ab^{-1}\right) = 2.$$

    Again, $G \equiv C_2 \times C_2$ by Theorem 6.3.

  - **[Case B, I.]** We have $o(a) = 4$ and $o(b) = 2$ with relation $ba = a^{-1}b$. These are exactly the relations for D_8 (using Proposition 2.16), so $G \cong D_8$.

  - **[Case B, II.]** We have $b^2 = a^2$ and $o(a) = 4$ with $ba = a^{-1}b$.

    Let $i = a$, $j = b$, $k = ab$, $-1 = a^2 = b^2$.

    Then, the elements of G are $\left\{e, a, a^2, a^3, b, ab, a^2 b, a^3 b\right\}$ which are $\{\pm 1, \pm i, \pm j, \pm k\}$ in Hamilton's notation.

    It is easy to check that the relations in G match those in Q_8. This defines an isomorphism between G and Q_8.

    Therefore $G \cong Q_8$, as required.

In summary, the groups of order up to 8 are as follows:

1. 1
2. C_2
3. C_3
4. C_4, $C_2 \times C_2$
5. C_5
6. C_6, D_6
7. C_7
8. C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_8, Q_8

7 Quotient Groups

7.1 Normal Subgroups

Let $\varphi : G \to H$ be a group homomorphism.

$$\ker\varphi \leqslant G$$

is always a special kind of subgroup.

Definition 7.1 (Normal subgroup)

$H \leqslant G$ is called a **normal subgroup** if for all $h \in H, g \in G$, we have $ghg^{-1} \in H$. If so, we write $H \lhd G$.

Example 7.2

1. $1 \lhd G$, $G \lhd G$ for any group G.
2. If G is abelian and $H \leqslant G$, then $H \lhd G$.
3. $\langle r\rangle \lhd D_{2n}$ since

   $$sr^k s^{-1} = r^{-k} \in \langle r\rangle$$

   by the dihedral relation [we don't have to check r since it is in $\langle r\rangle$]. But $\langle s\rangle$ is not normal since

   $$rsr^{-1} = sr^{-2} \neq s.$$

4. Suppose $\varphi : G \to G'$ is a homomorphism. If $h \in \ker\varphi$ and $g \in G$ then

   $$\varphi\left(ghg^{-1}\right) = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = e,$$

   so $ghg^{-1} \in \ker\varphi$. Thus $\ker\varphi \lhd G$.

Lecture 16 · 2025-11-14

Lemma 7.3

Suppose $H \leqslant G$. Then $H \lhd G$ iff

$$gH = Hg$$

for all $g \in G$.

Proof.

[$\Rightarrow$] Let $h \in H$ and $g \in G$. Since $H \lhd G$, we have $ghg^{-1} \in H$. Therefore

$$gh = \left(ghg^{-1}\right)g \in Hg.$$

Therefore $gH \subseteq Hg$. Similarly, for any $h' \in H$, we have $g^{-1}h'g \in H$ so

$$h'g = g\left(g^{-1}h'g\right) \in gH.$$

Thus $Hg \subseteq gH$, and so $gH = Hg$.

[⇐] Suppose $gH = Hg$ for all $g \in G$. Let $h \in H$. Then

$$gh \in gH = Hg$$

so there exists $h' \in H$ such that $gh = h'g$.

$$ghg^{-1} = h' \in H.$$

Thus $H \lhd G$.

7.2 Quotient Groups

Theorem 7.4 (Quotient group is a group)

If $H \lhd G$, the set of (left) cosets G/H is a group with operation

$$(g_1H)(g_2H) = (g_1g_2)H.$$

Proof. We need to check that the operation is well-defined and satisfies the group axioms.

WELL-DEFINEDNESS

Suppose $g_1H = g_1'H$ and $g_2H = g_2'H \Leftrightarrow Hg_2 = Hg'2$ since $H \lhd G$.

That is, there are $h_1, h_2 \in H$ such that

$$g_1 = g_1'h_1, \quad g_2 = h_2g_2'.$$

Therefore,

$$g_1g_2 = (g_1'h_1)(h_2g_2') = g_1'\underbrace{(h_1h_2)g_2'}_{\in Hg_2'} = g_1'g_2'h_3$$

by Lemma 7.3, for some $h_3 \in H$. Thus,

$$(g_1g_2)H = (g_1'g_2')H$$

so

$$(g_1g_2)H = (g_1'g_2')H$$

since cosets partition.

GROUP AXIOMS

- **Associativity.** Immediate from associativity in G.
- **Identity.** The identity is $eH = H$.

- **Inverses.** The inverse of gH is $g^{-1}H$ since

$$(gH)\left(g^{-1}H\right) = \left(gg^{-1}\right)H = eH.$$

- **Closure.** Immediate from the definition of the operation.

Therefore G/H is a group.

Definition 7.5 (Quotient group)

If $H \lhd G$, the group G/H provided by Theorem 7.4 is called the **quotient** of G by H.

Example 7.6

1. $G/1 \cong G$, $G/G \cong 1$.
2. Since $\mathbb{Z}$ is abelian, $n\mathbb{Z} \lhd \mathbb{Z}$ for any n. Thus, for any $n \in \mathbb{Z}^*$, we have the quotient group

$$\mathbb{Z}/n\mathbb{Z} \cong C_n$$

   with generator $1 + n\mathbb{Z}$ of order n.
3. Let G be a group, $H \leqslant G$, and suppose $[G : H] = 2$. Then, for any $g \notin H$,

$$gH = G \setminus H = Hg.$$

   and $eH = He$. So by Lemma 7.3, $H \lhd G$. Furthermore, $G/H \cong C_2$ since its order is 2.
4. An example of (3) is

$$C_n \cong \langle r \rangle \lhd D_{2n}$$

   and hence $D_{2n}/C_n \cong C_2$.

Important. It is a common error that one might think we can *multiply* groups using direct products and get back to the original group.

5. Note that

$$C_4/C_2 \cong C_2, \quad \text{and} \quad K_4/C_2 \cong C_2.$$

   But $C_4 \not\cong K_4$ since C_4 is cyclic but K_4 is not. This shows that quotient groups do not *undo* direct products. In particular, for groups A, B, C,

$$A/B \equiv C \not\Rightarrow A \equiv B \times C.$$

7.3 The Isomorphism Theorem

Theorem 7.7 (Isomorphism theorem)

If $\varphi : G \to H$ is a homomorphism, then

$$G/\ker\varphi \cong \operatorname{im}\varphi.$$

Proof. Since $\ker\varphi \lhd G$, the quotient $G/\ker\varphi$ is a group. Let us define

$$\begin{aligned}\overline{\varphi} : G/\ker\varphi &\to \operatorname{im}\varphi\\ g\ker\varphi &\mapsto \varphi(g).\end{aligned}$$

We first check that $\overline{\varphi}$ is a well-defined isomorphism.

WELL-DEFINEDNESS

Suppose $g_1\ker\varphi = g_2\ker\varphi$. We need to show that $\varphi(g_1) = \varphi(g_2)$.

We have

$$g_1 = g_2k$$

for some $k \in \ker\varphi$ since $g_1\ker\varphi = g_2\ker\varphi$. Then,

$$\overline{\varphi}(g_1\ker\varphi) = \varphi(g_1) = \varphi(g_2k) = \varphi(g_2)\varphi(k) = \varphi(g_2)e = \varphi(g_2) = \overline{\varphi}(g_2\ker\varphi).$$

HOMOMORPHISM

For $g_1, g_2 \in G$,

$$\overline{\varphi}((g_1\ker\varphi)(g_2\ker\varphi)) = \overline{\varphi}((g_1g_2)\ker\varphi) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \overline{\varphi}(g_1\ker\varphi)\overline{\varphi}(g_2\ker\varphi).$$

INJECTIVITY

Recall that a homomorphism is injective iff its kernel is trivial.

If $\overline{\varphi}(g\ker\varphi) = e$, then

$$\varphi(g) = \overline{\varphi}(g\ker\varphi) = e,$$

so $g \in \ker\varphi$, and hence $g\ker\varphi = \ker\varphi$.

That is, $\ker\overline{\varphi} = \{\ker\varphi\}$, so $\overline{\varphi}$ is injective.

SURJECTIVITY

A typical element of $\operatorname{im}\varphi$ is $\varphi(g)$ for some $g \in G$. But

$$\overline{\varphi}(g\ker\varphi) = \varphi(g),$$

so $\overline{\varphi}$ is surjective.

Example 7.8

1. Because $\varphi : \mathbb{Z} \to \mathbb{C}^*_\times$ defined by $\varphi(k) = \mathrm{e}^{\frac{2\pi i k}{n}}$ is a homomorphism with image C_n and kernel $n\mathbb{Z}$, by isomorphism theorem 7.7, we have

$$\mathbb{Z}/n\mathbb{Z} \cong \operatorname{im}\varphi \cong C_n.$$

2. Similarly, $\varphi : \mathbb{R} \to \mathbb{C}^*_\times$ defined by $\varphi(t) = \mathrm{e}^{2\pi i t}$ is a homomorphism with

$$\begin{aligned} \operatorname{im}\varphi &= \{z \in \mathbb{C} : |z| = 1\} = U(1) \\ \ker\varphi &= \mathbb{Z} \end{aligned}$$

so by isomorphism theorem 7.7, we have

$$\mathbb{R}/\mathbb{Z} \cong U(1).$$

Lecture 17 · 2025-11-17

Definition 7.9 (Simple group)

A group G is **simple** if the only normal subgroups are 1 and G itself. Thus every homomorphism $\varphi : G \to H$ is either trivial or injective. [Since $\ker\varphi \lhd G$, so either $\ker\varphi = 1$ or $\ker\varphi = G$.]

Example 7.10

C_p is simple whenever p is a prime.

An important question in group theory is to find and understand examples of non-abelian simple groups.

8 Permutations

8.1 Permutations and Cycle Notation

Recall from Definition 1.13 that a **permutation** of a set X is a bijection $X \to X$, and from Definition 1.14 that $\mathrm{Sym}(X)$ is the set of all permutations of X.

Example 8.1

If $X = \{1, 2, 3\}$, then $\mathrm{Sym}(X) \cong S_3$. So examples of permutations include

$$\sigma : \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \tau : \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

We can compute by representing permutations as lists.

Example 8.2

$$\underbrace{\begin{array}{c} 1 \xmapsto{\sigma} 3 \xmapsto{\tau} 3 \\ 2 \xmapsto{\sigma} 1 \xmapsto{\tau} 2 \\ 3 \xmapsto{\sigma} 2 \xmapsto{\tau} 1 \end{array}}_{\tau\sigma}$$

This is nonetheless a bit cumbersome. A more compact notation is to write permutations in **cycle notation**.

Definition 8.3 (Cycle)

Any list of distinct elements

$$a_1, a_2, \ldots, a_k \in \{1, 2, \ldots, n\}$$

defines a ***k*-cycle**:

$$\sigma = (a_1 \;\; a_2 \;\; \ldots \;\; a_k)$$

which sends

$$a_1 \mapsto a_2, a_2 \mapsto a_3, \ldots, a_{k-1} \mapsto a_k, a_k \mapsto a_1,$$

and leaves all other elements fixed.

Example 8.4

For Example 8.1, we have

$$\begin{aligned} \sigma &= (1 \;\; 3 \;\; 2) = (2 \;\; 3 \;\; 1) = (3 \;\; 2 \;\; 1), \\ \tau &= (1 \;\; 2) = (2 \;\; 1). \end{aligned}$$

The important rule about cycle multiplication is that the rightmost cycle acts first.

Example 8.5

For Example 8.1, we have

$$\tau\sigma = (1\ \ 2)(1\ \ 3\ \ 2) = (1\ \ 3).$$

Another example is

$$(1\ \ 4\ \ 3\ \ 2)(2\ \ 4\ \ 3) = (1\ \ 4\ \ 2\ \ 3).$$

Remark. $(a_1\ \dots\ a_k) = (a_2\ \dots\ a_k\ \ a_1)$.

Definition 8.6 (Disjoint Cycles)

Cycles $(a_1\ \dots\ a_k)$ and $(b_1\ \dots\ b_m)$ are **disjoint** if the sets $\{a_1, \dots, a_k\}$ and $\{b_1, \dots, b_m\}$ are disjoint. Note that disjoint cycles commute.

Theorem 8.7 (Disjoint cycles)

Every $\sigma \in S_n$ can be written as a product of disjoint cycles. This expression is unique up to

1. shifting the elements within each cycle, and
2. reordering the cycles.

Proof. The action of $\langle\sigma\rangle$ on $X = \{1, 2, \dots, n\}$ partitions X into orbits. Let

$$X = \langle\sigma\rangle i_1 \cup \langle\sigma\rangle i_2 \cup \dots \cup \langle\sigma\rangle i_k.$$

Let $n_j = \left|\langle\sigma\rangle i_j\right|$. We see that

$$\sigma = \left(i_1\ \ \sigma(i_1)\ \ \dots\ \ \sigma^{n_1-1}(i_1)\right)\dots\left(i_k\ \ \sigma(i_k)\ \ \dots\ \ \sigma^{n_k-1}(i_k)\right)$$

which proves existence of the decomposition.

The choices we have made are on the representatives of each orbit, and the order of the orbits, which proves uniqueness up to the stated conditions.

Example 8.8

Consider

$$(1\ \ 2)(3\ \ 4)(5\ \ 6)(1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6) = (1)(2\ \ 4\ \ 6)(3)(5) = (2\ \ 4\ \ 6).$$

Definition 8.9 (Cycle type)

If

$$\sigma = \left(a_1^1\ \ \dots\ \ a_{k_1}^1\right)\dots\left(a_1^l\ \ \dots\ \ a_{k_l}^l\right)$$

then σ is called a $(k_1, \ldots, k_l)$-cycle.

The (multi)set of numbers $\{k_1, \ldots, k_l\}$ is called the **cycle type** of σ. We often omit singletons from the cycle type.

Remark. If σ is a k-cycle, then $o(\sigma) = k$. More generally, if σ is a $(k_1, \ldots, k_l)$-cycle, then $o(\sigma) = \operatorname{lcm}(k_1, \ldots, k_l)$.

8.2 Transpositions and the Sign Homomorphism

Definition 8.10 (Transposition)

A **transposition** is a 2-cycle.

Theorem 8.11 (Transpositions generate)

The set of transpositions generates S_n for any finite n.

Proof. We shall prove by induction on n.

Base case. Consider $n = 2$. Then $S_2 = \{\mathrm{id}, (1\ \ 2)\}$ is generated by the transposition $(1\ \ 2)$.

Inductive step. Assume that S_{n-1} is generated by transpositions. Consider S_n. Let $\sigma \in S_n$.

- If $\sigma(n) = n$, then $\sigma \in S_{n-1} \leqslant S_n$, so by the inductive hypothesis σ is generated by transpositions.
- Otherwise, let $\tau = (n, \sigma(n))$. Then

  $$\tau\sigma(n) = \tau(\sigma(n)) = n.$$

  So $\tau\sigma \in S_{n-1} \leqslant S_n$, so by the inductive hypothesis $\tau\sigma$ is generated by transpositions. Since

  $$\sigma = \tau(\tau\sigma),$$

  we see that σ is also generated by transpositions.

Lecture 18 · 2025-11-19

Definition 8.12 (Adjacent transpositions)

A transposition of the form $(i\ \ i{+}1)$ is called **adjacent**.

Lemma 8.13

Any transposition $(i\ \ j)$ can be written as a product of an odd number of adjacent transpositions.

Proof. Assume $j > i$. Then the proof is by induction on $j - i$.

Base case. If $j - i = 1$, then $(i \;\; j) = (i \;\; i{+}1)$ is already an adjacent transposition.

Inductive step. Assume that we can write $(i \;\; j{-}1)$ as a product of an odd number of adjacent transpositions. Then

$$(i \;\; j) = (j - 1 \;\; j)(i \;\; j - 1)(j - 1 \;\; j)$$

and since $(i, j - 1)$ can be written as a product of an odd number of adjacent transpositions by the inductive hypothesis, so can (i, j).

In particular, S_n is generated by adjacent transpositions.

This discussion leads to a notion of parity for permutations.

Lemma 8.14

If $\tau_1, ..., \tau_k$ are all transpositions and

$$\sigma = \tau_1 ... \tau_k = e,$$

then k is even.

Proof. By Lemma 8.13, we may assume that all τ_i are adjacent transpositions.

We say that a pair $\{i, j\} \subseteq \{1, 2, ..., n\}$ is called an inversion of a permutation σ if $i < j$ but $\sigma(i) > \sigma(j)$.

Claim. For any $\sigma = \tau_1 ... \tau_k$, the number of inversions of σ has the same parity as k.

Proof. We prove this by induction on k.

Base case. If $k = 0$, then $\sigma = e$ has 0 inversions, which is even.

Inductive step. Let

$$\sigma = \underbrace{\tau_1}_{\tau} \underbrace{\tau_2 ... \tau_k}_{\sigma'} = \tau\sigma'.$$

Since τ_i are all adjacent transpositions, we have $\tau = (l \;\; l{+}1)$ for some l. Consider which pairs $\{i, j\}$ would be inversions of σ' but not σ, or vice versa.

The only such pair is $\{i, j\}$ such that $\sigma'(i) = l$ and $\sigma'(j) = l + 1$. This is because τ only swaps l and $l + 1$, so any other pair would remain an inversion or non-inversion in both σ' and σ.

For this pair, we have

$$\sigma'(i) = l < l + 1 = \sigma'(j)$$

but

$$\sigma(i) = l + 1 > l = \sigma(j).$$

Therefore, if $i < j$ and $\{i, j\}$ is an inversion for σ but not for σ', while if $j < i$ and $\{i, j\}$ is an inversion for σ' but not for σ.

In either case,

> > $$\#\text{ inversions of } \sigma = \#\text{ inversions of } \sigma' \pm 1$$
> >
> > as required.
>
> By the claim, since $\sigma = e$ has 0 inversions, we see that k must be even.

This enables us to define the sign homomorphism.

Theorem 8.15 (Sign homomorphism)

The map

$$\begin{aligned} \operatorname{sign} : S_n &\to C_2 = \{\pm 1\} \\ \tau_1 \dots \tau_k &\mapsto (-1)^k \end{aligned}$$

is a well-defined homomorphism.

Proof. To see that this is well-defined, suppose τ_i, τ_j' are all transpositions such that

$$\tau_1 \dots \tau_k = \tau_1' \dots \tau_l'$$

Then

$$\tau_1 \dots \tau_k (\tau_l' \dots \tau_1') = e,$$

so by the previous lemma, $k + l$ is even. Therefore, $k \equiv l \bmod 2$, so $(-1)^k = (-1)^l$.

To see that this is a homomorphism, note that

$$\operatorname{sign}(\tau_1 \dots \tau_k \tau_1' \dots \tau_l') = (-1)^{k+l} = (-1)^k (-1)^l = \operatorname{sign}(\tau_1 \dots \tau_k) \operatorname{sign}(\tau_1' \dots \tau_l').$$

Definition 8.16 (Parity of a permutation)

If $\operatorname{sign}(\sigma) = 1$, then σ is called an **even permutation**. Otherwise, it is called an **odd permutation**.

Definition 8.17 (Alternating group)

The subgroup

$$A_n = \ker(\operatorname{sign}) \lhd S_n$$

is called the **alternating group** on n elements. *i.e.* it is the set of all even permutations in S_n.

Example 8.18

In S_3, the permutations are

$$S_3 = \{e, (1\ \ 2), (1\ \ 3), (2\ \ 3), (1\ \ 2\ \ 3), (1\ \ 3\ \ 2)\}.$$

We have $(1 \;\; 2 \;\; 3) = (1 \;\; 2)(2 \;\; 3)$ and $(1 \;\; 3 \;\; 2) = (2 \;\; 3)(1 \;\; 2)$, so the even permutations are

$$A_3 = \{e, (1 \;\; 2 \;\; 3), (1 \;\; 3 \;\; 2)\} \cong C_3.$$

Remark. The cycle type makes it easy to determine the sign of a permutation.

Indeed,

$$(a_1 \;\; \dots \;\; a_k) = (a_1 \;\; a_k), (a_1, a_{k-}1), \dots, (a_1 \;\; a_3)(a_1 \;\; a_2)$$

so $(a_1 \;\; \dots \;\; a_k)$ is even iff k is odd.

More generally, a $(k_1, \dots, k_l)$-cycle is even iff $|\{\text{even } k_i\}|$ is even.

Example 8.19

- $(1 \;\; 2)(3 \;\; 4)$ is even
- $(1 \;\; 2)(3 \;\; 4)(5 \;\; 6)$ is odd

8.3 Conjugacy in S_n and A_n

We shall apply what we have obtained so far to study conjugacy in S_n in A_n. Recall that since A_n is a normal subgroup of S_n, the conjugacy class of any element $\alpha \in A_n$ in S_n is contained in A_n.

Theorem 8.20 (Conjugacy in S_n)

Two permutations $\sigma_1, \sigma_2 \in S_n$ are conjugate iff they have the same cycle type.

Proof.

[⇐] Suppose

$$\sigma_1 = \left(a_1^1 \;\; \dots \;\; a_{l_1}^1\right) \dots \left(a_1^k \;\; \dots \;\; a_{l_k}^k\right)$$

is a product of disjoint cycles. We have

$$\sigma_1\left(a_j^i\right) = a_{j+1 \bmod l_i}^i.$$

Since the cycle types are the same, σ_2 can be written as

$$\sigma_2 = \left(b_1^1 \;\; \dots \;\; b_{l_1}^1\right) \dots \left(b_1^k \;\; \dots \;\; b_{l_k}^k\right).$$

Now

$$\tau\left(a_j^i\right) = b_j^i$$

defines a permutation of $\{1, 2, \dots, n\} = \left\{a_j^i\right\} = \left\{b_j^i\right\}$. We can compute

$$\tau\sigma_1\tau^{-1}\left(b_j^i\right) = \tau\sigma_1\left(a_j^i\right) = \tau\left(a_{j+1 \bmod l_i}^i\right) = b_{j+1 \bmod l_i}^i = \sigma_2\left(b_j^i\right).$$

Therefore, $\sigma_2 = \tau\sigma_1\tau^{-1}$.

Lecture 19 · 2025-11-21

[⇒] Suppose $\sigma_2 = \tau\sigma_1\tau^{-1}$. The above argument shows that, if

$$\sigma_1 = \left(a_1^1 \ \dots \ a_{l_1}^1\right) \dots \left(a_1^k \ \dots \ a_{l_k}^k\right),$$

then we can define $b_j^i = \tau\left(a_j^i\right)$ so that

$$\sigma_2 = \left(b_1^1 \ \dots \ b_{l_1}^1\right) \dots \left(b_1^k \ \dots \ b_{l_k}^k\right)$$

for all $1 \leqslant i \leqslant k$ and $1 \leqslant j \leqslant l_i$. Therefore, σ_1 and σ_2 have the same cycle type.

This makes it easy to count conjugacy classes in S_n.

Example 8.21

Consider

$$S_3 = \{e, (1 \ \ 2), (1 \ \ 2 \ \ 3)\}.$$

Then we have

$$\left|\mathrm{ccl}_{S_3}(1 \ \ 2)\right| = \binom{3}{2} = 3,$$
$$\left|\mathrm{ccl}_{S_3}(1 \ \ 2 \ \ 3)\right| = 2 \times 1 = 2.$$

Example 8.22

Consdier S_4 without knowing its exact elements. Then we have

$$\left|\mathrm{ccl}_{S_4}((1 \ \ 2)(3 \ \ 4))\right| = \binom{4}{2} \times \frac{1}{2} = 3.$$

Recall that Conjugation Classes 4.16 are essentially orbits under the conjugation action of S_n on itself, and the Centraliser 4.18 of an element is its stabiliser under this action.

Then, Orbit-Stabiliser Theorem 4.9 implies that

$$\left|C_{S_n}(\gamma)\right| = \frac{|S_n|}{\left|\mathrm{ccl}_{S_n}(\gamma)\right|}$$

Therefore, it is also easy to cound the sizes of centralisers.

Example 8.23

In S_4, we have

$$C_{S_4}((1\ \ 2)(3\ \ 4)) = \frac{|S_4|}{\left|\mathrm{ccl}_{S_4}((1\ \ 2)(3\ \ 4))\right|} = \frac{24}{3} = 8.$$

Indeed, we can make a list:

$$C_{S_4}((1\ \ 2)(3\ \ 4)) = \{e, (1\ \ 2)(3\ \ 4), (1\ \ 2), (3\ \ 4), (1\ \ 3)(2\ \ 4), (1\ \ 4)(2\ \ 3), (1\ \ 4\ \ 2\ \ 3), (1\ \ 3\ \ 2\ \ 4)\}.$$

Example 8.24 (Conjugacy at S_4)

We can list all the conjugacy classes in S_4.

We can write out a table:

Typical element γ	$\left\lvert\mathrm{ccl}_{S_4}(\gamma)\right\rvert$	$\left\lvert C_{S_4}(\gamma)\right\rvert$
e	1	24
$(1\ \ 2)$	$\binom{4}{2} = 6$	4
$(1\ \ 2)(3\ \ 4)$	$\frac{1}{2}\binom{4}{2} = 3$	8
$(1\ \ 2\ \ 3)$	$\binom{4}{3} \times 2 = 8$	3
$(1\ \ 2\ \ 3\ \ 4)$	$3! = 6$	4

We should verify that the sizes of the conjugacy classes add up to 24.

Indeed, $1 + 6 + 3 + 8 + 6 = 24$ as expected.

Now, counting conjugacy classes in A_n is slightly more subtle. Recall that $C_G(g)$ is the set of elements of G that commute with g.

Lemma 8.25 (Conjugacy classes in A_n)

Let $\gamma \in A_n \lhd S_n$.

1. If some odd element of S_n commutes with γ, then
$$\mathrm{ccl}_{A_n}(\gamma) = \mathrm{ccl}_{S_n}(\gamma).$$
2. Otherwise, if every element of S_n that commutes with γ is even, then $\mathrm{ccl}_{S_n}(\gamma)$ splits into two:
$$\mathrm{ccl}_{A_n}(\gamma) \cup \mathrm{ccl}_{A_n}\left(\tau\gamma\tau^{-1}\right) = \mathrm{ccl}_{S_n}(\gamma)$$
where τ is any transposition (or any odd permutation).

Proof. Orbit-Stabiliser Theorem 4.9 gives

$$\left|S_n\right| = \left|\mathrm{ccl}_{S_n}(\gamma)\right| \cdot \left|C_{S_n}(\gamma)\right|$$
$$\left|A_n\right| = \left|\mathrm{ccl}_{A_n}(\gamma)\right| \cdot \left|C_{A_n}(\gamma)\right|$$

Since $|S_n| = 2|A_n|$, this gives

$$\left|\mathrm{ccl}_{S_n}(\gamma)\right| = 2\frac{\left|C_{A_n}(\gamma)\right|}{\left|C_{S_n}(\gamma)\right|} \cdot \left|\mathrm{ccl}_{A_n}(\gamma)\right|. \qquad (*)$$

$C_{A_n}(\gamma)$ is the even permutations that commute with γ, and $C_{S_n}(\gamma)$ is all permutations that commute with γ. [So $C_{A_n}(\gamma)$ is the even *bits* of $C_{S_n}(\gamma)$.] Therefore, we can write $C_{A_n}(\gamma)$ as the kernel of the sign homomorphism restricted to $C_{S_n}(\gamma)$:

$$C_{A_n}(\gamma) = \ker\left(\mathrm{sign}|_{C_{S_n}(\gamma)} : C_{S_n}(\gamma) \to C_2\right).$$

The image of $\mathrm{sign}|_{C_{S_n}(\gamma)}$ has size 1 or 2 [since it is a subgroup of C_2], so by the Isomorphism Theorem 7.7, we have

$$\left[C_{S_n}(\gamma) : C_{A_n}(\gamma)\right] = 1 \text{ or } 2.$$

1. If there is an odd element of S_n that commutes with γ[, then this element is in $C_{S_n}(\gamma)$ but not in $C_{A_n}(\gamma)$], so

   $$\left[C_{S_{n(\gamma)}} : C_{A_n}(\gamma)\right] = 2.$$

   Using Lagrange's theorem 3.6, [we have $\left|C_{S_n}(\gamma)\right| = 2\left|C_{A_n}(\gamma)\right|$, and] Equation * then becomes

   $$\left|\mathrm{ccl}_{S_n}(\gamma)\right| = \frac{2\cancel{\left|C_{A_n}(\gamma)\right|}}{2\cancel{\left|C_{A_n}(\gamma)\right|}} \cdot \left|\mathrm{ccl}_{A_n}(\gamma)\right| = \left|\mathrm{ccl}_{A_n}(\gamma)\right|.$$

   Since $\mathrm{ccl}_{A_n}(\gamma) \subseteq \mathrm{ccl}_{S_n}(\gamma)$, $\mathrm{ccl}_{A_n}(\gamma) = \mathrm{ccl}_{S_n}(\gamma)$ as required.
2. The hypothesis means that

   $$C_{S_n}(\gamma) = C_{A_n}(\gamma)$$

   so Equation * becomes

   $$\left|\mathrm{ccl}_{S_n}(\gamma)\right| = 2\left|\mathrm{ccl}_{A_n}(\gamma)\right|.$$

   So $\mathrm{ccl}_{A_n}(\gamma)$ is half as big as $\mathrm{ccl}_{S_n}(\gamma)$.

   Now consider a transposition $\tau \in S_n$. Note that $\tau\gamma\tau^{-1} \in \mathrm{ccl}_{S_n}(\gamma)$.

   For the sake of contradiction, suppose $\tau\gamma\tau^{-1} \in \mathrm{ccl}_{A_n}(\gamma)$. Then there exists $\alpha \in A_n$ such that

   $$\tau\gamma\tau^{-1} = \alpha\gamma\alpha^{-1}.$$

   But then, by rearranging, we have

   $$(\tau\alpha)\gamma(\tau\alpha)^{-1} = \gamma,$$

   which means that $\tau\alpha$ commutes with γ. So $\tau\alpha \in C_{S_n}(\gamma)$. But $\tau\alpha$ is odd[, so some odd permutation now commutes with γ]. ※

   Therefore, $\tau\gamma\tau^{-1} \notin \mathrm{ccl}_{A_n}(\gamma)$, as required.

This makes it possible to determine the conjugacy classes in A_n.

Example 8.26 (Conjugacy in A_4)

Consider $A_4 \lhd S_4$. The even elements of S_4 are e, $(2,2)$-cycles and 3-cycles. Note that e commutes with every element, so its conjugacy class in A_4 is the same as in S_4.

Since there is an odd number of $(2,2)$-cycles in S_4, the conjugacy class of $(1\ \ 2)(3\ \ 4)$ remains intact in A_4 [we cannot split it into two equal parts].

Finally, consider a 3-cycle, say $\sigma = (1\ \ 2\ \ 3)$. We have

$$\left|C_{S_4}(1\ \ 2\ \ 3)\right| = 3$$

and since we know that the cyclic group generated by σ definitely commutes with σ, we have

$$C_{S_4}(1\ \ 2\ \ 3) = \langle(1\ \ 2\ \ 3)\rangle \leqslant A_4$$

and the conjugacy class of σ splits into two in A_4. In summary,

Typical element γ	$\left\lvert \mathrm{ccl}_{A_4}(\gamma)\right\rvert$
e	1
$(1\ \ 2)(3\ \ 4)$	3
$(1\ \ 2\ \ 3)$	4
$(3\ \ 2\ \ 1)$	4

Lecture 20 · 2025-11-24

Finally, let us look at conjugacy in S_5 and A_5.

Example 8.27 (Conjugacy in S_5)

We can write out the conjugacy classes in S_5 as follows:

Even	**Typical element** γ	$\left\lvert \mathrm{ccl}_{S_5}(\gamma)\right\rvert$	$\left\lvert C_{S_5}(\gamma)\right\rvert$
✓	e	1	120
×	$(1\ \ 2)$	$\binom{5}{2} = 10$	12
✓	$(1\ \ 2\ \ 3)$	$\binom{5}{3} \times 2 = 20$	6
✓	$(1\ \ 2)(3\ \ 4)$	$\frac{1}{2}\binom{5}{2}\binom{3}{2} = 15$	8
×	$(1\ \ 2\ \ 3)(4\ \ 5)$	$\binom{5}{3} \times 2 = 20$	6
×	$(1\ \ 2\ \ 3\ \ 4)$	$\binom{5}{4} \times 3! = 30$	4
✓	$(1\ \ 2\ \ 3\ \ 4\ \ 5)$	$4! = 24$	5

The sizes of the conjugacy classes add up to 120 as expected.

Example 8.28 (Conjugacy in A_5)

Consider $A_5 \lhd S_5$. The even elements of S_5 are e, (3)-cycles, $(2,2)$-cycles and (5)-cycles.

Note that

- e commutes with every element, so its conjugacy class in A_5 is the same as in S_5.
- $(4\ 5) \leqslant C_{S_5}(1\ 2\ 3)$, so the conjugacy class of $(1\ 2\ 3)$ remains intact in A_5.
- Since 15 is odd, the conjugacy class of $(1\ 2)(3\ 4)$ remains intact in A_5.
- $\left|C_{S_5}(1\ 2\ 3\ 4\ 5)\right| = 5$, so $C_{S_5}(1\ 2\ 3\ 4\ 5) = \langle(1\ 2\ 3\ 4\ 5)\rangle \leqslant A_5$. Therefore, the conjugacy class of $(1\ 2\ 3\ 4\ 5)$ splits into two in A_5.

Typical element γ	$\left\lvert \mathrm{ccl}_{A_5}(\gamma) \right\rvert$
e	1
$(1\ 2\ 3)$	20
$(1\ 2)(3\ 4)$	15
$(1\ 2\ 3\ 4\ 5)$	12
$(5\ 4\ 3\ 2\ 1)$	12

The sizes of the conjugacy classes add up to 60 as expected.

Theorem 8.29

A_5 is simple.

Proof. Suppose $N \lhd A_5$. By Example Sheet 3 Q5, N is a union of conjugacy classes in A_5. At this point, we can list the possible union sizes of conjugacy classes in A_5 and see if they divide 60 (by Lagrange's Theorem 3.6).

The possible union sizes are [note that e must be included]:

$$\begin{aligned}
1 &= 1 & \checkmark \\
1 + 20 &= 21 & \times \\
1 + 20 + 15 &= 36 & \times \\
1 + 20 + 12 &= 33 & \times \\
1 + 20 + 15 + 12 &= 48 & \times \\
1 + 20 + 15 + 12 + 12 &= 60 & \checkmark \\
1 + 20 + 12 + 12 &= 45 & \times \\
1 + 15 &= 16 & \times \\
1 + 15 + 12 &= 28 & \times \\
1 + 15 + 12 + 12 &= 40 & \times \\
1 + 12 &= 13 & \times \\
1 + 12 + 12 &= 25 & \times
\end{aligned}$$

Therefore, the only possible sizes for N are 1 and 60, so $N = \{e\}$ or $N = A_5$. Hence, A_5 is simple.

9 Matrix Groups

Let $M_n(\mathbb{R})$ be the set of all $n \times n$ matrices with real entries.

From IA Vectors and Matrices, we know that matrix multiplication is associative and has an identity element, the identity matrix $\mathbf{I}_n$, though not all matrices have inverses under multiplication.

Lemma 9.1

$\mathbf{A} \in M_n(\mathbb{R})$ has an inverse iff $\det \mathbf{A} \neq 0$.

Definition 9.2 (General linear group)

Let $\mathrm{GL}_n(\mathbb{R}) = \{\mathbf{A} \in M_n(\mathbb{R}) : \det \mathbf{A} \neq 0\}$. This is a group under matrix multiplication.

Here is another result from IA Vectors and Matrices.

Lemma 9.3

For $\mathbf{A}, \mathbf{B} \in M_n(\mathbb{R})$, $\det(\mathbf{AB}) = \det \mathbf{A} \cdot \det \mathbf{B}$.

This implies that det is a homomorphism

$$\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times \quad \text{with} \quad \mathbf{A} \mapsto \det \mathbf{A}.$$

Definition 9.4 (Special linear group)

Let $\mathrm{SL}_n(\mathbb{R}) = \ker \det = \{\mathbf{A} \in M_n(\mathbb{R}) : \det \mathbf{A} = 1\}$. This is a subgroup of $\mathrm{GL}_n(\mathbb{R})$ called the special linear group.

By the Isomorphism Theorem 7.7,

$$\mathrm{SL}_n(\mathbb{R}) \lhd \mathrm{GL}_n(\mathbb{R})$$
$$\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong \operatorname{im} \det .$$

For any $x \in \mathbb{R}$,

$$\det \begin{pmatrix} x & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} = x.$$

Hence $\operatorname{im} \det = \mathbb{R}^\times$ and so

$$\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R}^\times.$$

Remark. We can replace $\mathbb{R}$ with $\mathbb{C}$ in the above and get similar results. Therefore we have

$$\mathrm{GL}_n(\mathbb{C})/\mathrm{SL}_n(\mathbb{C}) \cong \mathbb{C}^\times.$$

9.1 Change of Basis

This is a familiar concept from IA Vectors and Matrices. There is a natural action by conjugation:

$$\mathrm{GL}_n(\mathbb{R}) \curvearrowright M_n(\mathbb{R})$$
$$\mathbf{P}(\mathbf{A}) := \mathbf{P}\mathbf{A}\mathbf{P}^{-1}.$$

Proposition 9.5

Let V be an n-dimensional vector space over $\mathbb{R}$, and $\alpha : V \to V$ a linear map. If $\mathbf{A} \in M_n(\mathbb{R})$ that represents α in some basis, then the orbit

$$\mathrm{GL}_n(\mathbb{R})\mathbf{A} = \left\{\mathbf{P}\mathbf{A}\mathbf{P}^{-1} : \mathbf{P} \in \mathrm{GL}_n(\mathbb{R})\right\}$$

consists of all matrices that represent α in any basis.

Proof. A basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ for V defines an isomorphism of vector spaces

$$\varphi : \mathbb{R}^n \to V \quad \text{with} \quad \begin{pmatrix} \lambda_1 \\ \ldots \\ \lambda_n \end{pmatrix} \mapsto \sum_{i=1}^{n} \lambda_i \mathbf{v}_i.$$

The claim that $\mathbf{A}$ represents α in this basis means that

$$\begin{tikzcd} \mathbb{R}^n \arrow[r, "\overset{\varphi}{\cong}"] \arrow[d, "\mathbf{A}"'] & V \arrow[d, "\alpha"] \\ \mathbb{R}^n \arrow[r, "\overset{\varphi}{\cong}"] & V \end{tikzcd}$$

and so $\alpha = \varphi\mathbf{A}\varphi^{-1}$.

Lecture 21 · 2025-11-26

Likewise, another basis $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ for V corresponds to another isomorphism

$$\psi : \mathbb{R}^n \to V,$$

and a matrix $\mathbf{B}$ represents α in these coordinates if

$$\alpha = \psi\mathbf{B}\psi^{-1}.$$

Therefore,

$$\begin{aligned} \mathbf{B} &= \psi^{-1}\alpha\psi = \psi^{-1}\varphi\mathbf{A}\varphi^{-1}\psi \\ &= \left(\psi^{-1}\varphi\right)\mathbf{A}\left(\psi^{-1}\varphi\right)^{-1} \\ &= \mathbf{P}\mathbf{A}\mathbf{P}^{-1}. \end{aligned}$$

where $\mathbf{P} \in \mathrm{GL}_n(\mathbb{R})$ [because its inverse exists, namely the matrix representing $\varphi^{-1}\psi$] represents the isomorphism $\psi^{-1}\varphi : \mathbb{R}^n \to \mathbb{R}^n$ in the standard basis. Thus, the set of all matrices representing α in any basis is contained in the orbit $\mathrm{GL}_n(\mathbb{R})\mathbf{A}$.

Conversely, if

$$\mathbf{B} = \mathbf{P}\mathbf{A}\mathbf{P}^{-1}$$

for some $\mathbf{P} \in \mathrm{GL}_n(\mathbb{R})$, then setting

$$\psi = \varphi\mathbf{P}^{-1} : \mathbb{R}^n \to V$$

we get a basis

$$\{\mathbf{u}_1 = \psi(\boldsymbol{e}_i)\}$$

for V. In this basis, $\mathbf{B}$ represents α.

9.2 Möbius Transformations, Revisited

Recall that multiplication in $\mathcal{M}$ looked similar to multiplication of 2×2 matrices.

Proposition 9.6

Identify

$$\mathbb{C}^\times = \left\{\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C}) : \lambda \in \mathbb{C}^\times\right\}$$

then

$$\mathbb{C}^\times \lhd \mathrm{GL}_2(\mathbb{C})$$

and

$$\mathrm{GL}_2(\mathbb{C})/\mathbb{C}^\times \cong \mathcal{M}.$$

Proof. We can prove both statements by constructing a surjective homomorphism from $\mathrm{GL}_2(\mathbb{C})$ onto $\mathcal{M}$ with kernel $\mathbb{C}^\times$, by the Isomorphism Theorem 7.7. Consider the map

$$\Phi : \mathrm{GL}_2(\mathbb{C}) \to \mathcal{M} \quad \text{with} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \left(z \mapsto \frac{az+b}{cz+d}\right).$$

By our previous computation of multiplication in $\mathcal{M}$, we see that Φ is a homomorphism. Also, Φ is surjective since for any Möbius transformation $f(z) = \frac{az+b}{cz+d}$ with $ad - bc \neq 0$, the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is in $\mathrm{GL}_2(\mathbb{C})$.

A matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \ker\Phi$ iff its image fixes 0, 1 and ∞ by the Three Point Lemma for $\mathcal{M}$ 5.6. Hence

$$b = 0, c = 0, a = d.$$

Thus, $\ker\Phi = \left\{\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda \end{smallmatrix}\right) : \lambda \in \mathbb{C}^\times\right\}$ which we have identified with $\mathbb{C}^\times$.

Therefore, by the Isomorphism Theorem 7.7

$$\mathrm{GL}_2(\mathbb{C})/\mathbb{C}^\times \cong \mathcal{M}.$$

9.3 Orthogonal Groups

Let us write $\|\cdot\|$ for the normal notion of length on $\mathbb{R}^n$, *i.e.*

$$\|\boldsymbol{u}\| = \sqrt{\sum_{i=1}^{n} u_i^2}.$$

Definition 9.7 (Orthogonal Group)

The ***n*-dimensional orthogonal group** is the subgroup of $\mathrm{GL}_n(\mathbb{R})$ that preserves distance in $\mathbb{R}^n$:

$$O(n) = \{\mathbf{A} \in \mathrm{GL}_n(\mathbb{R}) : \forall \mathbf{v} \in \mathbb{R}^n, \|\mathbf{A}\mathbf{v}\| = \|\mathbf{v}\|\}.$$

In fact, the **dot product**

$$\boldsymbol{u} \cdot \boldsymbol{v} = \sum_{i=1}^{n} u_i v_i$$

is often more convenient to work with.

Lemma 9.8 (Polarisation Identity)

For any $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{R}^n$,

$$2\boldsymbol{u} \cdot \boldsymbol{v} = \|\boldsymbol{u}\|^2 + \|\boldsymbol{v}\|^2 - \|\boldsymbol{u} - \boldsymbol{v}\|^2.$$

Proof.

$$\begin{aligned} \|\boldsymbol{u} - \boldsymbol{v}\|^2 &= (\boldsymbol{u} - \boldsymbol{v}) \cdot (\boldsymbol{u} - \boldsymbol{v}) \\ &= \boldsymbol{u} \cdot \boldsymbol{u} - 2\boldsymbol{u} \cdot \boldsymbol{v} + \boldsymbol{v} \cdot \boldsymbol{v} \\ &= \|\boldsymbol{u}\|^2 - 2\boldsymbol{u} \cdot \boldsymbol{v} + \|\boldsymbol{v}\|^2. \end{aligned}$$

It follows that we can characterise $O(n)$ using the dot product.

Lemma 9.9 ($O(n)$ and the Dot Product)

$$O(n) = \{\mathbf{A} \in \mathrm{GL}_n(\mathbb{R}) : \forall \boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n, (\mathbf{A}\boldsymbol{x}) \cdot (\mathbf{A}\boldsymbol{y}) = \boldsymbol{x} \cdot \boldsymbol{y}\}.$$

Proof. If $(\mathbf{A}\boldsymbol{x}) \cdot (\mathbf{A}\boldsymbol{y}) = \boldsymbol{x} \cdot \boldsymbol{y}$ for all $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$, then for any $\boldsymbol{v} \in \mathbb{R}^n$,

$$\begin{aligned} \|\mathbf{A}\boldsymbol{v}\|^2 &= (\mathbf{A}\boldsymbol{v}) \cdot (\mathbf{A}\boldsymbol{v}) \\ &= \boldsymbol{v} \cdot \boldsymbol{v} \\ &= \|\boldsymbol{v}\|^2. \end{aligned}$$

$$\|\mathbf{A}\boldsymbol{v}\| = \|\boldsymbol{v}\|.$$

Therefore $\mathbf{A} \in O(n)$.

Conversely, if $\mathbf{A} \in O(n)$, then $\forall \boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$,

$$\begin{aligned}2(\mathbf{A}\boldsymbol{x})\cdot(\mathbf{A}\boldsymbol{y}) &= \|\mathbf{A}\mathbf{x}\|^2+\|\mathbf{A}\mathbf{y}\|^2-\|\mathbf{A}\mathbf{x}-\mathbf{A}\mathbf{y}\|^2\\ &= \|\mathbf{A}\mathbf{x}\|^2+\|\mathbf{A}\mathbf{y}\|^2-\|\mathbf{A}(\boldsymbol{x}-\boldsymbol{y})\|^2\\ &= \|\mathbf{x}\|^2+\|\mathbf{y}\|^2-\|\mathbf{x}-\mathbf{y}\|^2\\ &= 2\boldsymbol{x}\cdot\boldsymbol{y}.\end{aligned}$$

Hence $(\mathbf{A}\boldsymbol{x})\cdot(\mathbf{A}\boldsymbol{y})=\boldsymbol{x}\cdot\boldsymbol{y}$ for all $\boldsymbol{x},\boldsymbol{y}\in\mathbb{R}^n$ as required.

This quickly leads to a nice characterisations of matrices in $O(n)$.

Lemma 9.10 (Matrices in $O(n)$)

Let $\mathbf{A}\in M_n(\mathbb{R})$. The following are equivalent:

1. $\mathbf{A}\in O(n)$.
2. The columns of $\mathbf{A}$ form an orthonormal basis of $\mathbb{R}^n$.
3. $\mathbf{A}^\mathsf{T}\mathbf{A}=\mathbf{I}_n$.

Proof. Let $\mathbf{A}=\left(a_{ij}\right)$.

[(1) ⇒ (2).] Let $\{\boldsymbol{e}_1,\ldots,\boldsymbol{e}_n\}$ be the standard basis for $\mathbb{R}^n$. The ith column of $\mathbf{A}$ is $\mathbf{A}\boldsymbol{e}_i$. since

$$\begin{aligned}(\mathbf{A}\boldsymbol{e}_i)\cdot\left(\mathbf{A}\boldsymbol{e}_j\right) &= \boldsymbol{e}_i\cdot\boldsymbol{e}_j\\ &= \delta_{ij},\end{aligned}$$

The columns of $\mathbf{A}$ form an orthonormal basis.

[(2) ⇒ (3).] As explained above, (2) means that

$$\mathbf{A}\boldsymbol{e}_i\cdot\mathbf{A}\boldsymbol{e}_j=\delta_{ij}.$$

Since $\boldsymbol{u}\cdot\boldsymbol{v}=\boldsymbol{u}^\mathsf{T}\boldsymbol{v}$, this means that

$$\begin{aligned}(\mathbf{A}\boldsymbol{e}_i)^\mathsf{T}\left(\mathbf{A}\boldsymbol{e}_j\right) &= \delta_{ij}\\ \boldsymbol{e}_i^\mathsf{T}\mathbf{A}^\mathsf{T}\mathbf{A}\boldsymbol{e}_j &= \delta_{ij}.\end{aligned}$$

But $\boldsymbol{e}_i^\mathsf{T}\mathbf{M}\boldsymbol{e}_j$ is the (i,j)th entry of the matrix $\mathbf{M}$, so this shows that the (i,j)th entry of $\mathbf{A}^\mathsf{T}\mathbf{A}$ is δ_{ij} for all i,j. Therefore $\mathbf{A}^\mathsf{T}\mathbf{A}=\mathbf{I}_\mathbf{n}$.

[(3) ⇒ (1).]

Suppose $\boldsymbol{u},\boldsymbol{v}\in\mathbb{R}^n$. then

$$\begin{aligned}(\mathbf{A}\boldsymbol{u})\cdot(\mathbf{A}\boldsymbol{v}) &= (\mathbf{A}\boldsymbol{u})^\mathsf{T}(\mathbf{A}\boldsymbol{v})\\ &= \boldsymbol{u}^\mathsf{T}\mathbf{A}^\mathsf{T}\mathbf{A}\mathbf{v}\\ &= \boldsymbol{u}^\mathsf{T}\mathbf{I}_\mathbf{n}\boldsymbol{v}\\ &= \boldsymbol{u}\cdot\boldsymbol{v}.\end{aligned}$$

Hence $\mathbf{A}\in O(n)$ as required.

Recall that $\det\mathbf{A}^\mathsf{T}=\det\mathbf{A}$. Therefore,

$$1 = \det(\mathbf{I_n}) = \det(\mathbf{A}^\top\mathbf{A}) = \det(\mathbf{A}^\top) \cdot \det(\mathbf{A}) = (\det \mathbf{A})^2.$$

So $\det \mathbf{A} = \pm 1$ for any $\mathbf{A} \in O(n)$.

Lecture 22 · 2025-11-28

Definition 9.11 (Special Orthogonal Group)

The **special orthogonal group** is the subgroup

$$\mathrm{SO}(n) := O(n) \cap \mathrm{SL}_n(\mathbb{R}) = \{\mathbf{A} \in O(n) : \det \mathbf{A} = 1\}.$$

Note that

$$\mathrm{SO}(n) = \ker(\det : O(n) \to \{\pm 1\}).$$

Thus,

$$[O(n) : \mathrm{SO}(n)] = 2.$$

Examples of elements of $O(n) \setminus \mathrm{SO}(n)$ are provided by reflections.

Definition 9.12 (Reflection)

Any $\mathbf{v} \in \mathbb{R}^n \setminus \{0\}$ defines an orthogonal plane $\mathbf{v}^\perp = P_\mathbf{v} = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{x} \cdot \mathbf{v} = 0\}$.

The **reflection** in $P_\mathbf{v}$ is defined to be

$$S_\mathbf{v}(\mathbf{x}) = \mathbf{x} - \frac{2(\mathbf{x} \cdot \mathbf{v})}{\|\mathbf{v}\|^2}\mathbf{v}.$$

Remark.

1. We will sometimes write S_P for the reflection in the plane P.
2. We may replace $\mathbf{v}$ by $\frac{\mathbf{v}}{\|\mathbf{v}\|}$ and assume that $\|\mathbf{v}\| = 1$. then

$$S_\mathbf{v}(\mathbf{x}) = \mathbf{x} - 2(\mathbf{x} \cdot \mathbf{v})\mathbf{v}.$$

Lemma 9.13

1. $S_\mathbf{v}^2 = \mathrm{id}$
2. $S_\mathbf{v} \in O(n)$

Proof. We may assume that $\|\mathbf{v}\| = 1$. From the definition, $S_\mathbf{v}$ is linear in $\mathbf{x}$. So we can think of $S_\mathbf{v}$ as a matrix $\mathbf{S_v} \in M_n(\mathbb{R})$. Now,

$$\begin{aligned}(S_\mathbf{v}(\mathbf{x}) \cdot \mathbf{v}) &= (\mathbf{x} \cdot \mathbf{v}) - 2(\mathbf{x} \cdot \mathbf{v})(\mathbf{v} \cdot \mathbf{v}) \\ &= (\mathbf{x} \cdot \mathbf{v}) - 2(\mathbf{x} \cdot \mathbf{v}) \\ &= -(\mathbf{x} \cdot \mathbf{v}).\end{aligned}$$

So,

$$\begin{aligned} S_v^2(\mathbf{x}) &= S_v(\mathbf{x}) - 2(S_v(\mathbf{x})\cdot\mathbf{v})\mathbf{v} \\ &= \mathbf{x} - 2(\mathbf{x}\cdot\mathbf{v})\mathbf{v} - 2(-(\mathbf{x}\cdot\mathbf{v}))\mathbf{v} \\ &= \mathbf{x}. \end{aligned}$$

So indeed $S_v^2 = \mathrm{id}$. In particular, S_v is invertible with inverse S_v, So

$$\mathbf{S}_v \in \mathrm{GL}_n(\mathbb{R}).$$

Finally, for any $\mathbf{x} \in \mathbb{R}^n$,

$$\begin{aligned} \|S_v(\mathbf{x})\|^2 &= (S_v(\mathbf{x}))\cdot(S_v(\mathbf{x})) \\ &= (\mathbf{x} - 2(\mathbf{x}\cdot\mathbf{v})\mathbf{v})\cdot(\mathbf{x} - 2(\mathbf{x}\cdot\mathbf{v})\mathbf{v}) \\ &= \mathbf{x}\cdot\mathbf{x} - 4(\mathbf{x}\cdot\mathbf{v})(\mathbf{x}\cdot\mathbf{v}) + 4(\mathbf{x}\cdot\mathbf{v})^2(\mathbf{v}\cdot\mathbf{v}) \\ &= \|\mathbf{x}\|^2. \end{aligned}$$

Hence $S_v \in O(n)$ as required.

Remark. Let $\|\mathbf{v}\| = 1$, and pick an orthonormal basis $\{\mathbf{v}_1, \dots, \mathbf{v}_{n-1}\}$ for P_v. In the basis $\{\mathbf{v}_1, \dots, \mathbf{v}_{n-1}, \mathbf{v}\}$ for $\mathbb{R}^n$, S_v has matrix

$$\mathbf{S}_v = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & -1 \end{pmatrix}$$

so $\det \mathbf{S}_v = -1$ and hence $S_v \in O(n) \setminus \mathrm{SO}(n)$.

Theorem 9.14 (Reflections Generate $O(n)$)

Every $\mathbf{A} \in O(n)$ is a product of at most n reflections.

Proof. We will prove this by induction on n.

Base case. When $n = 1$, $O(1) = \{\pm 1\} = \langle S_1 \rangle \cong C_2$. The matrix (-1) is the reflection in the origin, so the result holds.

Inductive step. Let $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ be the standard basis for $\mathbb{R}^n$. Let $\mathbf{v} = \mathbf{e}_n - \mathbf{A}\mathbf{e}_n$.

Then $\mathbf{S}_v(\mathbf{A}\mathbf{e}_n) = \mathbf{e}_n$, [and since $\mathbf{S}_v\mathbf{A}$ is an orthogonal transformation, by Lemma 9.9, dot products are preserved, and hence vectors that are orthogonal to $\mathbf{e}_n$ are sent to some vector that is still orthogonal to $\mathbf{e}_n$,] so $\mathbf{S}_v\mathbf{A}$ preserves $P_{\mathbf{e}_n} = \mathbb{R}^{n-1} \times \{0\}$.

By induction, there are $\mathbf{v}_1, \dots, \mathbf{v}_n \in \mathbb{R}^{n-1}$ such that

$$\mathbf{S}_v\mathbf{A} = \mathbf{S}_{v_1} \dots \mathbf{S}_{v_{n-1}} \quad \text{on } \mathbb{R}^{n-1}.$$

Since both sides also fix $\mathbf{e}_n$, they also agree on $\mathbb{R}^n$. Therefore,

$$\mathbf{A} = \mathbf{S}_v\mathbf{S}_{v_1} \dots \mathbf{S}_{v_{n-1}}.$$

Orthogonal transformations are especially easy to analyse in low dimensions.

Lemma 9.15 (Elements of $O(2)$)

Let $\mathbf{A} \in O(2)$.

1. If $\mathbf{A} \notin \mathrm{SO}(2)$ then $\mathbf{A}$ is a reflection.
2. If $\mathbf{A} \in \mathrm{SO}(2)$ then $\mathbf{A}$ is a rotation about O.

Proof. Recall that $\det \mathbf{S}_{\boldsymbol{v}} = -1$, so $\det\left(\mathbf{S}_{\boldsymbol{v}_1}\mathbf{S}_{\boldsymbol{v}_2}...\mathbf{S}_{\boldsymbol{v}_k}\right) = (-1)^k$. By Theorem 9.14, we may take $k \leqslant 2$.

1. If $\mathbf{A} \notin \mathrm{SO}(2)$, then k is odd and hence $k = 1$. So $\mathbf{A} = \mathbf{S}_{\boldsymbol{v}_1}$ is a reflection.
2. If $\mathbf{A} \in \mathrm{SO}(2)$, then k is even, so unless $\mathbf{A} = \mathbf{I}$, we can write $\mathbf{A} = \mathbf{S}_{\boldsymbol{u}}\mathbf{S}_{\boldsymbol{v}}$ for some $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{R}^2$ that are not parallel.

   We claim that $\mathbf{A} = \mathbf{S}_{\boldsymbol{u}}\mathbf{S}_{\boldsymbol{v}}$ only fixes the origin. [Here, we define a rotation to be an orthogonal transformation that only fixes the origin.] Indeed, for $\boldsymbol{x} \neq 0$, suppose

   $$\mathbf{S}_{\boldsymbol{u}}\mathbf{S}_{\boldsymbol{v}}(\boldsymbol{x}) = \boldsymbol{x} \Leftrightarrow \mathbf{S}_{\boldsymbol{v}}\boldsymbol{x} = \mathbf{S}_{\boldsymbol{u}}\boldsymbol{x}.$$

   But $\boldsymbol{v}$ is parallel to $\boldsymbol{x} - \mathbf{S}_{\boldsymbol{v}}\boldsymbol{x}$ and $\boldsymbol{u}$ is parallel to $\boldsymbol{x} - \mathbf{S}_{\boldsymbol{u}}\boldsymbol{x}$, so this implies that $\boldsymbol{u}$ is parallel to $\boldsymbol{v}$. ※

   Hence $\mathbf{A}$ only fixes the origin, and is therefore a rotation about O.

Remark. Let $\mathbf{A} \in \mathrm{SO}(2)$. We have seen that the columns form an orthonormal basis of $\mathbb{R}^2$, so we may write

$$\mathbf{A} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

with $a^2 + b^2 = 1$. Thus, there exists $\theta \in \mathbb{R}$ such that $a = \cos\theta$ and $b = \sin\theta$, so

$$\mathbf{A} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}.$$

Lemma 9.16 (Elements of $\mathrm{SO}(3)$)

If $\mathbf{A} \in \mathrm{SO}(3)$, the $\mathbf{A}$ is a rotation.

Proof. By Theorem 9.14, $\mathbf{A}$ is a product of at most 3 reflections. Since $\det \mathbf{A} = 1$, either $\mathbf{A} = \mathbf{I}$ or $\mathbf{A} = \mathbf{S}_{\boldsymbol{u}}\mathbf{S}_{\boldsymbol{v}}$ for some $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{R}^3$ that are not parallel. Since $n = 3$,

$$P_{\boldsymbol{u}} \cap P_{\boldsymbol{v}} = l$$

where l is a line through the origin. Since $P_{\boldsymbol{u}}$ fixes l pointwise and $P_{\boldsymbol{v}}$ also fixes l pointwise, their composition $\mathbf{A}$ also fixes l pointwise. [We shall define a rotation in $\mathbb{R}^3$ to be an orthogonal transformation that fixes a line pointwise.]

Also $\mathbf{S}_{\boldsymbol{u}}\mathbf{S}_{\boldsymbol{v}}\boldsymbol{x} = \boldsymbol{x} \Rightarrow \mathbf{S}_{\boldsymbol{u}}\boldsymbol{x} = \mathbf{S}_{\boldsymbol{v}}\boldsymbol{x}$, similar to Lemma 9.15, either

1. $\boldsymbol{x} \in l$, in which case $\boldsymbol{x}$ is fixed by $\mathbf{A}$, or
2. $\boldsymbol{u}$ is parallel to $\boldsymbol{v}$. ※

Thus, $\mathbf{A}$ only fixes the line l pointwise, and is therefore a rotation.

Lecture 23 · 2025-12-01

10 Platonic Solids

While there are infinitely many regular 2-dimensional polygons, in three dimensions there are only five regular solids, known as the **Platonic solids**.

Definition 10.1

A convex polyhedron $X \subseteq \mathbb{R}^3$ is a **Platonic solid** if

- every face of X is a regular n-gon for some n,
- $G = \mathrm{Isom}(X)$ acts transitively on the faces.
- if $x \in X$ is the midpoint of a face, then

$$\mathrm{Stab}_G(x) \cong D_{2n}.$$

Proposition 10.2

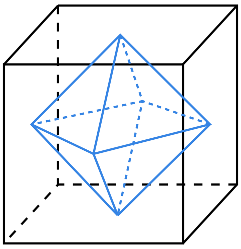
There are, up to similarity, exactly five Platonic solids:

- the tetrahedron, with 4 triangular faces and 4 vertices,
- the cube, with 6 square faces and 8 vertices,
- the octahedron, with 8 triangular faces and 6 vertices,
- the dodecahedron, with 12 pentagonal faces and 20 vertices,
- the icosahedron, with 20 triangular faces and 12 vertices.

Two solids X, Y are **dual** if Y can be constructed from X by putting vertices in the centers of each face, and then joining vertices in adjacent faces by edges.

Example 10.3

The cube and the octahedron are dual.



Example 10.4

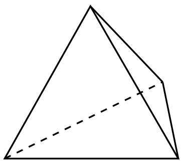
The tetrahedron is dual to itself.

Example 10.5

> The dodecahedron and the icosahedron are dual.

In particular, if X and Y are dual, then $\mathrm{Isom}(X) \cong \mathrm{Isom}(Y)$, so we only have three distinct isometry groups of Platonic solids to consider.

Example 10.6 (Tetrahedron)



Let $G = \mathrm{Isom}(\text{tetrahedron})$. By definition, G acts transitively on the four faces, and the $\mathrm{Stab}_G(x) \cong D_6$ so by the orbit-stabilizer theorem,

$$|G| = 4 \cdot 6 = 24,$$

where x is the center of a face.

Furthermore, the action of G on the four vertices defines a homomorphism

$$\theta : G \to S_4.$$

We shall prove that θ is injective. Suppose $\theta(g) = e$. Then g fixes each vertex of the tetrahedron, which are not coplanar. So $g = \mathrm{id}$ by the 4-point lemma. Therefore θ is injective, and we may identify G with a subgroup of S_4.

But $|S_4| = 24$ and $|G| = 24$, so in fact $G \cong S_4$.

Let us also identify the group of rotational symmetries [which are the ones we can actually realize by rotating the solid in space]:

$$G_0 = G \cap SO(3)$$

where the tetrahedron is centered at the origin.

Lemma 10.7 (Uniqueness of A_n)

If $H \leqslant S_n$ and $[S_n : H] = 2$, then $H \cong A_n$.

Proof. Because $[S_n : H] = 2$, $H \lhd S_n$, and $S_n/H \cong C_2$. We therefore have surjective homomorphism $\theta : S_n \to C_2 = \{\pm 1\}$ with $\ker(\varphi) = H$.

Since transpositions generate S_n, there is a transposition $\tau_0 \in S_n$ with $\theta(\tau_0) = -1$. Because all transpositions are conjugate [they have the same cycle type], so $\tau = \sigma\tau_0\sigma^{-1}$ for any other transposition τ and some $\sigma \in S_n$. Thus

$$\theta(\tau) = \theta(\sigma)\theta(\tau_0)\theta(\sigma)^{-1} = -1. \quad \text{(since } C_2 \text{ is abelian)}$$

Therefore $\theta = \mathrm{sign}$, so

$$H = \ker\theta = \ker \mathrm{sign} = A_n.$$

Therefore, since $[S_4 : G_0] = 2$, we have $G_0 \cong A_4$.

Example 10.8 (Cube and Octahedron)

Let $G = \mathrm{Isom}(\text{cube})$. By definition, G acts transitively on the six faces, and the $\mathrm{Stab}_G(x) \cong D_8$ so by the orbit-stabilizer theorem,

$$|G| = 6 \cdot 8 = 48,$$

where x is the center of a face.

In particular, the index-two rotational subgroup G_0 has order 24.

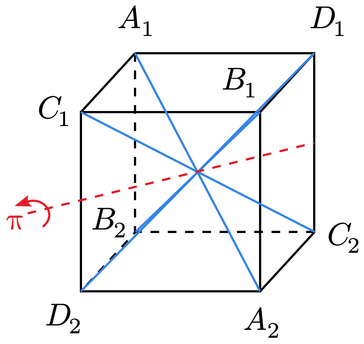
In Example Sheet 2 Q7, we saw that G acts on the set of the four long diagonals of the cube, giving a homomorphism

$$\theta : G_0 \to S_4.$$

Since both G_0 and S_4 have order 24, to show that θ is injective it suffices to show that it is surjective.

Claim. θ is surjective.

Proof. Since Transpositions Generate 8.11, it suffices to show that all transpositions are contained in $\operatorname{im}\theta$. Indeed,



rotation about the axis through the midpoints of an edge maps to a transposition under θ.

We get $\frac{12}{2} = 6$ different transpositions this way, which is all of them [because it happens that $\binom{4}{2} = 6$]. Therefore $\operatorname{im}\theta = S_4$.

Hence comparing orders, we have $G_0 \cong S_4$.

Now, since $-\mathbf{I} \notin G_0$ commutes with everything in G_0, by Direct Product Theorem 6.3 we have

$$G \cong G_0 \times C_2 \cong S_4 \times C_2.$$

Lecture 24 · 2025-12-03

Remark. We have $G \leqslant O(3)$ and $G_0 = G \cap SO(3) = \ker(\det|_G : G \to C_2)$, so

$$[G : G_0] = |\operatorname{im}(\det|_G)| \leqslant 2$$

> Since cubes have reflectional symmetries, we have $[G : G_0] = 2$ in that case. The same applies to the other Platonic solids as well.

Now, for the final two Platonic solids.

Example 10.9 (Dodecahedron and Icosahedron [Non-Examinable])

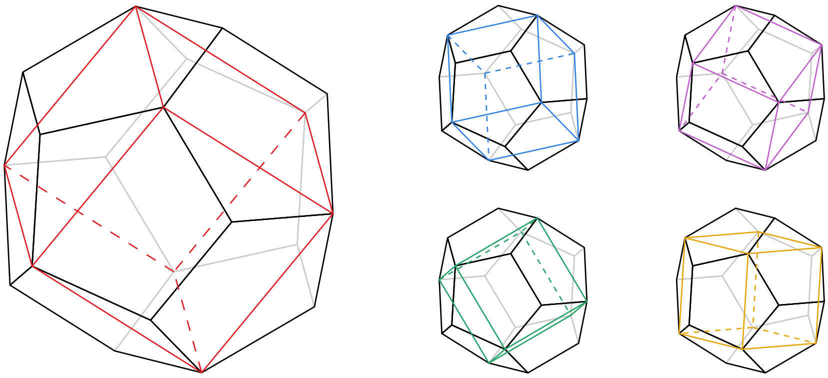
Let $G = \mathrm{Isom}(\text{dodecahedron})$ and G_0 the rotational subgourp of index two.

By definition, G acts transitively on the twelve faces, and the $\mathrm{Stab}_G(x) \cong D_{10}$ so by the orbit-stabilizer theorem,

$$|G| = 12 \cdot 10 = 120,$$

where x is the center of a face. And so $|G_0| = 60$.

By drawing diagonals on faces, we may inscribe 5 cubes into the dodecahedron.



Since the 5 cubes are built symmetrically from the geometry of the dodecahedron, G_0 acts on the set of these 5 cubes, giving a homomorphism

$$\theta : G_0 \to S_5.$$

Rotation around the axes through an opposite pair of vertices leads to a 3-cycle. There are 10 diagonals between opposite pairs of vertices, so we get 10 inverse pairs of 3-cycles. So, we get all 10 3-cycles in S_5.

> ***Claim.*** Let $X \subseteq A_5$ be the set of 3-cycles. Then
>
> $$\langle X \rangle = A_5.$$

> ***Proof.*** By Example Sheet 4 Q2,
>
> $$\langle X \rangle \lhd A_5.$$
>
> Since A_5 is simple, either $\langle X \rangle = \{e\}$ or $\langle X \rangle = A_5$. Since $X \neq \{e\}$, we must have $\langle X \rangle = A_5$.

In summary, if X is the set of 3-cycles, we have seen that

$$X \subseteq \operatorname{im}\theta \quad \text{and} \quad \langle X \rangle = A_5 \leqslant \operatorname{im}\theta.$$

Therefore we have

$$60 = |G_0| \geqslant \operatorname{im}\theta \geqslant |A_5| = 60,$$

so θ is surjective and hence an isomorphism. Therefore $G_0 \cong A_5$.

Finally, since $-\mathbf{I} \notin G_0$ commutes with everything in G_0, by Direct Product Theorem 6.3 we have

$$G \cong G_0 \times C_2 \cong A_5 \times C_2.$$

END OF DOCUMENT ■