Groups

January 26, 2022

Contents

0 Introduction

Book recommendations:

- Algebra & Geometry, Alan Beardon

Notation. $\forall$ denotes "for all"; $\exists$ denotes "there exists"; $\implies$ denotes "implies"; $\therefore$ denotes "therefore"; ⨳ denotes "contradiction"; and $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ denote the integers, naturals, rationals, reals and complex numbers respectively.

1 Basic Definitions and Examples

Definition 1 (Binary Operation)**.** A binary operation $*$ on a set X is a way of combining 2 elements of X to unambiguously give another element of X, i.e. $*: X \times X \to X$.

Definition 2 (Group)**.** If G is a set and $*$ is a binary operation on G, then $(G, *)$ is a *group* if the following 4 axioms hold:

(i) $x, y \in G \implies x * y \in G$ (closure)

(ii) $\exists$ an element $e \in G$ satisfying

$$x * e = x = e * x \qquad \forall x \in G$$

(existence of an identity)

(iii) for every $x \in G$ there is a $y \in G$ such that

$$x * y = e = y * x$$

(existence of inverses)

(iv) for every $x, y, z \in G$ we have:

$$x * (y * z) = (x * y) * z$$

(associative law)

Remark. We can prove that G has only one identity.

Remark. As a result, we can also prove that every element has only one inverse.

Both of these claims are proved in Lemma 1.

1.1 Examples of Groups

(1) $(\mathbb{Z}, +)$, $e = 0$, $x^{-1} = -x$.

(2) $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$

(3) $(\mathbb{Z}, -)$ is *not* a group because associativity fails.

(4) $(\mathbb{Z}, \times)$ is *not* a group because no inverses.

(5) $(\mathbb{Q}, \times)$ is *not* a group because 0^{-1} does not exist.

(6) $(Q \setminus \{0\}, \times)$

(7) $(\{\pm 1\}, \times)$
We can write a multiplication table:

x	1	-1
1	1	-1
-1	-1	1

note that closure holds, $e = 1$ and $(-1)^{-1} = -1$.

(8) $(\{0, 1, 2\}, +_3)$

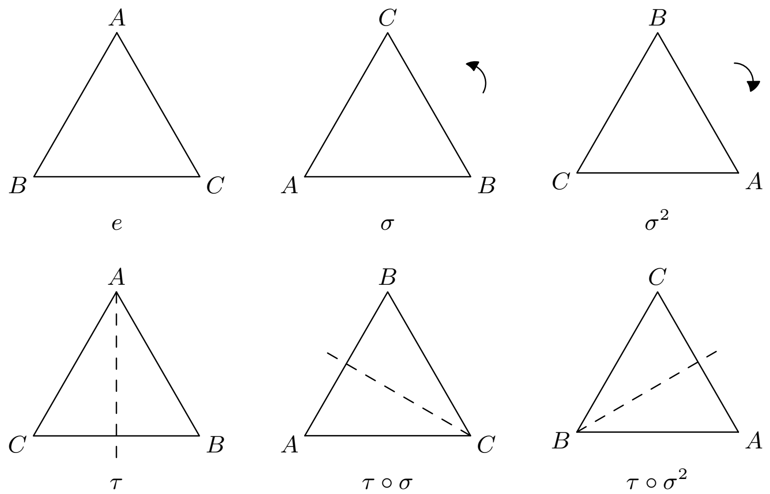
$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

and we have $e = 0$ and $1^{-1} = 2$.

(9) $(\{e, a, b, c\}, *)$

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

(10) "groups are abstractions of symmetries": rotations and reflections of an equilateral triangle are another example of a group.



This forms a group where the binary operator is "do one then the next"

(11) $M_2(\mathbb{R}) = \{2 \times 2 \text{ matrices with entries in } \mathbb{R}\}$

$$= \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \right]$$

under addition is a group:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a+\alpha & b+\beta \\ c+\gamma & d+\delta \end{pmatrix}$$

(12) $GL_2(\mathbb{R}) = \{\text{invertible } 2 \times 2 \text{ matrices with entries in } \mathbb{R}\}$ under multiplication is a group.

Lemma 1. Let $(G, *)$ be a group. Then

1. The identity element is unique.
2. Inverses are unique.

Proof. (i): Suppose e and e' are both identities, so

$$a * e = a = e * a \qquad \text{and} \qquad a * e' = a = e' * a \qquad \forall a \in G.$$

In particular

$$e = e * e' = e'$$

so $e = e'$, so the identity must be unique. □

Proof. (ii): Suppose both y and z are inverses for x, so

$$x * y = e = y * x, \qquad \text{and} \qquad x * z = e = z * x \qquad x \in G.$$

Then

$$\begin{aligned} y &= y * e \\ &= y * (x * z) \\ &= (y * x) * z \\ &= e * z \\ &= z \end{aligned}$$

so $y = z$. □

Remark (Unnesessary brackets)**.** Since the definition of a group involves associativity, we can omit brackets, i.e. $x * y * z$ is unambiguous.

Remark (Omitting $*$)**.** We often omit "$*$" and write $xy := x * y$ and also write $G = (G, *)$. (This is only done when the binary operator can be easily inferred).

Remark (Inverse of product)**.** $(xy)^{-1} = y^{-1}x^{-1}$. This follows immediately by the uniqueness, as it is easy to verify that this is a possible inverse:

$$(xy)y^{-1}x^{-1} = x(yy^{-1})x^{-1} = xx^{-1} = e.$$

Remark (Inverse of inverse)**.** $(x^{-1})^{-1} = x$.

Remark (Coset stuff)**.** If $xy = xz$ then $y = z$; this easily follows from the existence of inverses.

Definition 3 (Abelian Groups)**.** A group G is *abelian* (or commutative) if $xy = yx$ for all $x, y \in G$.

Remark. Note all our examples above are abelian except (10) and (12). (Symmetries of the triangle, and the general linear group).

Definition 4 (Order of a group)**.** Let G be a group. If the number of elements in the set G is finite, then G is called a *finite group*. Otherwise G is called an *infinite group*. If G is a finite group, denote the number of elements in the set G by $|G|$ and we call this the *order* of the group.

Definition 5 (Subgroups)**.** Let $(G, *)$ be a group and H a subset of G ($H \subseteq G$ i.e. $h \in H \implies h \in G$). Then $(H, *)$ is a *subgroup* of $(G, *)$ if $(H, *)$ is a group (with the same operation) i.e. if

(a) $h, k \in H \implies h * k \in H$.

(b) $e_G \in H$

(c) $h \in H \implies h^{-1} \in H$.

(Note associativity is inherited).
i.e. "restricting operation to H still gives a group". We write $H \leq G$.

Examples

- $(\mathbb{Z},+) \leq (\mathbb{Q},+) \leq (\mathbb{R},+)$
- $(\{\pm 1\}, \times) \leq (\mathbb{Q} \setminus \{0\}, \times)$.
- In example (10) (symmetries of a triangle), the rotational symmetries form a subgroup (elements $\{e, \sigma, \sigma^2\}$).
- In example (12) (general linear group), we have that

  $$\begin{aligned} \mathrm{SL}_2(\mathbb{R}) &= \{A \in \mathrm{GL}_2(\mathbb{R}) : \det A = 1\} \\ &\leq \mathrm{GL}_2(\mathbb{R}) \end{aligned}$$

  (SL_2 and GL_2 denote the special linear and general linear groups respectively).
- G a group then $\{e\} \leq G$ is the trivial subgroup. $G \leq G$ is the improper subgroup.
- The subgroups of $(\mathbb{Z},+)$ are exactly

  $$n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}, \qquad n \in \mathbb{Z}_{\geq 0}.$$

  Proof. First note $n\mathbb{Z}$ is a sub group of $\mathbb{Z}$.
  - $0 \in n\mathbb{Z}$
  - If $a, b \in n\mathbb{Z}$, then let $a = na'$, $b = nb'$. Then we have

    $$a + b = na' + nb' = n(a' + b') \in n\mathbb{Z}.$$
  - $-a = n(-a') \in n\mathbb{Z}$
  - Associativity is inherited.

  Conversely assume that $H \leq \mathbb{Z}$. If $H = \{0\} = 0\mathbb{Z}$ which is of the form we claimed. Otherwise choose $0 < n \in H$ with n minimal. (Such an n must exist because H must contain either a negative or positive integer, but since inverses exist this implies that there must be a positive element). Then $n\mathbb{Z} \leq H$ by closure and inverses. Now we show that $H = n\mathbb{Z}$. Suppose $\exists h \in H \setminus n\mathbb{Z}$, then we can write $h = nk + h'$ with $h' \in \{1, 2, \dots, n-1\}$. But $h' = h - nk \in H$, contradicting minimality of n. Thus $H = n\mathbb{Z}$. □

Definitions for Functions

Definition 6 (Functions)**.** F is a *function* between sets A and B if it assigns each element of A a unique element of B

$$f : A \to B \qquad\qquad a \mapsto f(a)$$

For example: $f : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto x + 1$ and $g\mathbb{Z} \to \mathbb{Z}$, $x \mapsto 2x$.

Definition 7 (Composition of functions)**.** Suppose $g : A \to B$ and $f : B \to C$. Define $f \circ g : A \to C$ by
$$a \mapsto (f \circ g)(a) = f(g(a)).$$
For example $(f \circ g)(x) = 2x + 1$ and $(g \circ f)(x) = 2x + 2$ using the example functions above.

Suppose $f_1 : A \to B$, $f_2 : A \to B$. Then $f_1 = f_2$ if and only if $f_1(a) = f_2(a) \forall a \in A$.

Definition 8 (Bijection)**.** $f : A \to B$ is a *bijection* if it defines a pairing between elements of A and elements of B. That is, given $b \in B$ there exists a unique $a \in A$ such that $f(a) = b$. For example $f : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto x + 1$. Given a bijective function f, we can define
$$f^{-1} : B \to A \qquad b \mapsto a \qquad \text{where } f(a) = b.$$
Then $f \circ f^{-1} = \mathrm{id}_B$ and $f^{-1} \circ f = \mathrm{id}_A$. ($\mathrm{id}_B(b) = b$, $\mathrm{id}_A(a) = a$)

Lemma 2 (Composition of bijections)**.** If $g : A \to B$ and $f : B \to C$ are bijections then so is $f \circ g : A \to C$.

Proof. In Numbers & Sets. □

Definition 9 (Homomorphism)**.** Let $(G, *_G)$ and $(H, *_H)$ be groups. Then the function
$$\theta : G \to H$$
is a *homomorphism* if
$$\theta(x *_G y) = \theta(x) *_H \theta(y) \qquad \forall x, y \in G$$
"a map which respects the group operation".

Example. Let $G = (\{0, 1, 2, 3\}, +_4)$ and $H = (\{1, e^{\pi i/2}, e^{\pi i}, e^{3\pi i/2}\}, \times)$. Then the function

$$\theta : G \to H \qquad n \mapsto e^{n\pi i/2}$$

is a homomorphism. This is because

$$\begin{aligned} \theta(n +_4 m) &= e^{(n+_4 m)\pi i/2} \\ &= e^{(n+m)\pi i/2} \qquad \text{since } n + m = n +_4 m + 4n \\ &= e^{n\pi i/2} \times e^{m\pi i/2} \\ &= \theta(n) \times \theta(m) \end{aligned}$$

Lemma 3. Let G and H be groups and $\theta : G \to H$ be a homomorphism. Then

$$\theta(G) = \{\theta(g) : g \in G\},$$

the *image* of θ is a subgroup of H, written $\theta(G) \leq H$.

Proof. We need to prove closure, ...

- To prove closure, let x, y be elements of $\theta(G)$. Then $x = \theta(g)$ and $y = \theta(h)$ for some $h, g \in G$. Then:

$$\begin{aligned} x *_H y &= \theta(g) *_H \theta(h) \\ &= \theta(g *_g h) \\ &\in \theta(G) \end{aligned}$$

- To show that we have an identity, note that

$$\begin{aligned} \theta(e_G) &= \theta(e_G *_G e_G) \\ &= \theta(e_G) *_H \theta(e_G) \end{aligned}$$

  and if we premultiply by $\theta(e_G)^{-1} \in H$ then we get

$$e_H = \theta(e_G) \in \theta(G)$$

- To get inverses, let $x = \theta(g) \in \theta(G)$. Then

$$\begin{aligned} e_H = \theta(e_G) &= \theta(g *_G g^{-1}) \\ &= \theta(g) *_H \theta(g^{-1}) \\ &= x *_H \theta(g^{-1}) \\ &= \theta(g^{-1} *_G g) \\ &= \theta(g^{-1}) *_H x \end{aligned}$$

And since inverses are unique we get

$$\theta(g)^{-1} = \theta(g^{-1}) \in \theta(G)$$

- And finally associativity is just inherited.

□

Definition 10 (Isomorphism)**.** A bijective homomorphism is called an *isomorphism* if G and H are groups and $\theta : G \to H$ is a homomorphism. We say G and H are isomorphic and write $G \cong H$.

Example. Let $G = (\{0, 1, 2, 3\}, +_4)$ and $H = (\{1, e^{i\pi/2}, e^{i\pi}, e^{3i\pi/2}, \times)$. Then $G \cong H$, which can be shown by considering

$$\begin{aligned} \theta : G &\to H \\ n &\mapsto e^{i\pi n/2} \end{aligned}$$

(θ is an isomorphism.)

Isomorphism means roughly "They are essentially the same"

Lemma 4.

(i) The composition of two homomorphisms is a homomorphism. Similarly for isomorphisms, thus if $G_1 \cong G_2$ and $G_2 \cong G_3$, then $G_1 \cong G_3$.

(ii) If $\theta : G_1 \to G_2$ then so is its inverse $\theta^{-1} : G_2 \to G_1$. So $G_1 \cong G_2 \implies G_2 \cong G_1$.

Proof.

(i) Suppose

$$\theta_1 : (G_1, *_1) \to (G_2, *_2)$$
$$\theta_2 : (G_2, *_2) \to (G_3, *_3)$$

are homomorphisms. Then $\theta_2 \circ \theta_1$ is a function from G_1 to G_3, we need to check its a homomorphism. Let $x, y \in G_1$. Then

$$\begin{aligned} \theta_2 \circ \theta_1(x *_1 y) &= \theta_2(\theta_1(x) *_2 \theta_1(y)) \\ &= \theta_2(\theta_1(x)) *_3 \theta_2(\theta_1(y)) \\ &= (\theta_2 \circ \theta_1)(x) *_3 (\theta_2 \circ \theta_1)(y) \end{aligned}$$

(ii) θ is a bijection so θ^{-1} exists. We need to show it is a homomorphsim. Let $y, z \in G_2$. Then $\exists x, k \in G_1$ such that

$$\theta^{-1}(y) = x, \qquad \theta^{-1}(z) = k.$$

Note

$$\begin{aligned} \theta(x *_1 k) &= \theta(x) *_2 \theta(k) \\ &= y *_2 z \implies \theta^{-1}(y *_2 z) \qquad\qquad = x *_1 k \\ &= \theta^{-1}(y) *_1 \theta^{-1}(z) \end{aligned}$$

□

Notation. If $x \in (G, *)$, $n \in \mathbb{Z}$ then

$$x^n = \begin{cases} \overbrace{x * x * \cdots * x}^{n} & n > 0 \\ e & n = 0 \\ \underbrace{x^{-1} * x^{-1} * \cdots * x^{-1}}_{(-n)} & n < 0 \end{cases}$$

Definition 11 (Cyclic Groups)**.** A group H is *cyclic* if $\exists h \in H$ such that each element of H is a power of h, i.e. for each $x \in H \exists n \in \mathbb{Z}$ such that $x = h^n$. Then h is called a *generator* of H and we write $H = \langle h \rangle$.

Example.

- $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$ is the infinite cyclic group. We showed all subgroups of $(\mathbb{Z}, +)$ are cyclic.
- $(\{\pm 1\}, \times) = \langle -1 \rangle$
- $(\{0, 1, 2, 3\}, +_4) = \langle 1 \rangle = \langle 3 \rangle$

Note that a cyclic group is always abelian.

Definition 12 (Orders)**.** Let G be a group and $g \in G$. The order of g written $o(g)$, is the least positive integer n such that $g^n = e$, if it exists. Otherwise g has infinite order.

Lemma 5. Suppose G is a group, $g \in G$ and $o(g) = m$. Let $n \in \mathbb{N}_{>0}$. Then

$$g^n = e \iff m \mid n.$$

Proof. ($\Leftarrow$) Suppose $m \mid n$, then $n = qm$ for some $q \in \mathbb{N}$. This implies that

$$g^n = g^{qm} = (g^m)^q = e^q = e.$$

($\implies$) Suppose $g^n = e$. Then we can write $n = qm + r$ with $0 \leq r < m$, with $q \in \mathbb{N}$. Then

$$\begin{aligned} e = g^n &= g^{qm+r} \\ &= (g^m)^q g^r \\ &= e^q g^r \\ &= e g^r \\ &= g^r \end{aligned}$$

This implies $r = 0$ by minimality of m, hence $n = qm$ as required. □

Remarks

(1) Suppose $g \in G$¿ Then $\{g^n : n \in \mathbb{Z}\}$ is a subgroup of G, in fact it is the smallest subgroup of G containing g. We call it the subgroup of G generated by g and write

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

Also $|\langle g \rangle| = o(g)$ if finite, since if $o(g) = m$ then

$$\langle g \rangle = \{e, g, g^2, \dots, \underbrace{g^{m-1}}_{=g^{-1}}\}$$

Otherwise both are infinite.

(2) We can define the abstract cyclic group of order n

$$C_n = \langle x \rangle \qquad o(x) = n$$

Then

$$(\{0, 1, \dots, n-1\}, +_n) \qquad \text{and} \qquad (\{n^{th} \text{ roots of unity}\}, \times)$$

are realisations of this group, and they are all isomorphic.

(3) Let G be a group and $g_1, \dots, gk \in G$. Then the subgroup of G generated by $g_1, \dots, gk$ denoted by $\langle g_1, \dots, g_k \rangle$ is the smallest subgroup of G containing all the g_i. It is the intersection of all the subgroups of G containing all the g_i.

2 The Dihedral and Symmetric Groups

First note composition of functions is associative:

$$f, g, h : X \to X, \qquad x \in X$$

Then

$$\begin{aligned}(f \circ (g \circ h))(x) &= f((g \circ h)(x)) \\ &= f(g(h(x))) \\ &= (f \circ g)(h(x)) \\ &= ((f(\circ g) \circ h)(x) \implies f \circ (g \circ h) \qquad\qquad = (f \circ g) \circ h\end{aligned}$$

2.1 Dihedral Groups

Let P be a regular polygon with n sides and V its set of vertices. We can assume

$$V = \{e^{2\pi ik/n} : 0 \leq k < n\}$$

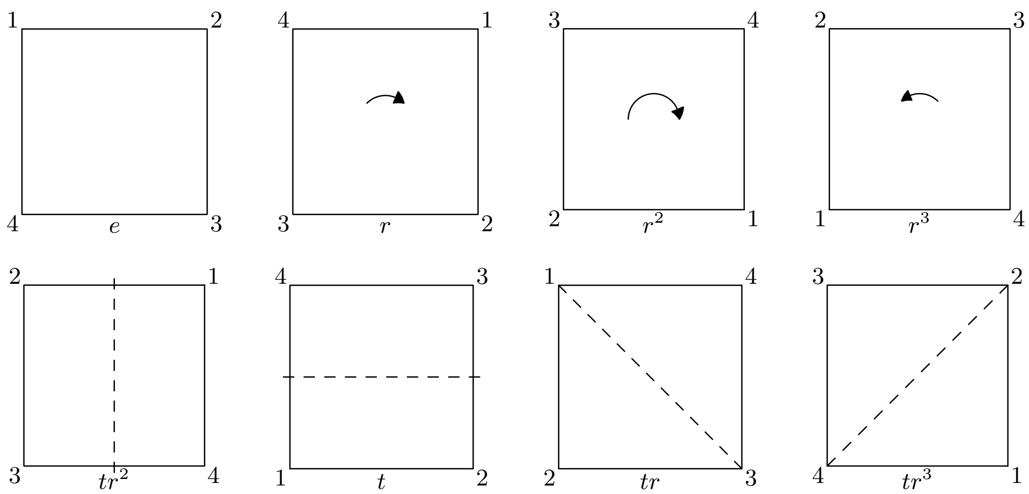
n-th roots of unity in $\mathbb{C}$. Then the symmetries of P are the isometries (i.e. distance preserving maps of $\mathbb{C}$ that map V to V.

We will show that for $n \geq 3$ the set of symmetries of P, under composition form a nonabelian group of order $2n$. This group is called the *dihedral group* of order $2n$ and denoted by D_{2n}.

Notation. Sometimes D_{2n} is denoted D_n.

We have already met D_6 in example 10.

Consider D_8



Let $r : P \to P$

$$z \mapsto e^{2\pi i/n} z$$

$$t : p \to P$$

$$z \mapsto \overline{z}$$

These are both isometries.

$$\begin{aligned} |r(z) - r(w)| &= |e^{2\pi i/n} z - e^{2\pi i/n} w| \\ &= |e^{2\pi i/n}||z - w| \\ &= |z - w| \end{aligned}$$

$$\begin{aligned} |t(z) - t(w)|^2 &= |\overline{z} - \overline{w}|^2 \\ &= (\overline{z} - \overline{w})(z - w) \\ &= |z - w|^2 \\ \implies |t(z) - t(w)| &= |z - w| \end{aligned}$$

Note, $r^n = \text{id} = \text{identity}$

$$\implies r^{-1} = r^{n-1}$$

and also

$$t^2 = \text{id} \implies t = t^{-1}$$

$$tr(z) = e^{-2\pi i/n} \overline{z} = r^{-1} t(z)$$

$$\implies tr = r^{-1} t$$

We show that the symmetries of P is

$$\{\underbrace{e = \text{id}, r, r^2, \ldots, r^{n-1}}_{\text{rotations}}, \underbrace{t, rt, \ldots, r^{n-1} t}_{\text{reflections}}\}$$

Then this set under composition of functions gives the group D_{2n}.

Let f be a symmetry of P. Then $f(1) = e^{2\pi i k/n}$ for some k.

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

So, $g(e^{2\pi i/n}) = e^{2\pi i/n}$ or $e^{-2\pi i/n}$. If $g(e^{2\pi i/n} = e^{2\pi i/n}$ then g fixes 1 and $e^{2\pi i/n}$, Also g interchanges vertices of P so fixes P's centre of mass

$$\frac{1}{n} = \sum_{k=0}^{n-1} e^{2\pi i k/n} = 0.$$

So g fixes 0, 1 and $e^{2\pi i/n}$

$$g = \text{id} \implies f = r^k.$$

If $g(e^{2\pi i/n}) = e^{-2\pi i/n}$ then

$$\begin{aligned} t \circ g(e^{2\pi i/n} &= e^{2\pi i/n} \\ t \circ g(1) &= 1 \\ t \circ g(0) &= 0 \\ \implies t \circ g &= \text{id} \\ t \circ r^{-k} \circ f &= \text{id} \\ \implies f &= r^k \circ t^{-1} \\ &= r^k \circ t \end{aligned}$$

Algebraically we write,

$$D_{2n} = \langle \underbrace{r, t}_{\text{generators}} \mid \underbrace{r^n = e, t^2 = e, trt = r^{-1}}_{\text{relations}} \rangle$$

Finally, $D_2 \cong C_2$ and $D_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ are the only abelian dihedral groups. Also note that D_∞ exists.

2.2 Symmetric Groups

Let X be a set. A bijection

$$f : X \to X$$

is called a *permutation* of X. Let $\text{Sym}(X)$ denote the set of all permutations of X.

Proposition 1. $\text{Sym}(X)$ is a group under composition of functions. It is called the symmetric group on X.

Proof.

- Closure - follows from a lemma in Numbers & Sets
- identity, define $c(x) = x \quad \forall x \in X$
- Let $f \in \text{Sym}(X)$. As f is a bijection, f^{-1} exists and is a bijection and satisfies

$$f \circ f^{-1} = c = f^{-1} \circ f$$

- composition of functions is associative as shown earlier

□

Notation (Symmetric Groups)**.** Suppose X is finite and $X = |n|$. Then we often take X to be the set $\{1, 2, \dots, n\}$ and we write S_n for $\mathrm{Sym}(X)$. We call S_n the symmetric group of degree n.

We'll use double row notation (for now).

If $\sigma \in S_n$ write

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

For example

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in S_3$$

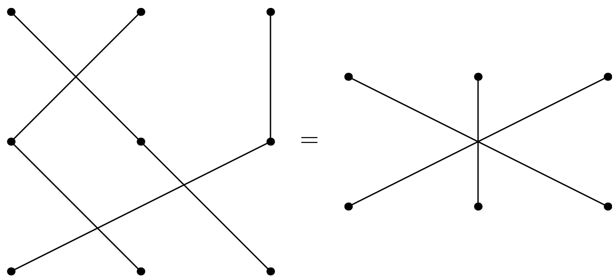
and

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \in S_5$$

Composition:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \text{“} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \\ 3 & 2 & 1 \end{pmatrix} \text{”} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

or



Small n

$$S_1 = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \{c\} \right\} \qquad \text{trivial group}$$

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \cong (\{\pm 1\}, \times) \cong C_2 \right\}.$$

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} \cong D_6$$

Remarks

(i) $|S_n| = n!$ because number of choices for $\sigma(1)$ is n, number of choices for $\sigma(2)$ is $n-1\ldots$

(ii) For $n \geq 3$, S_n is not abelian. Consider

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 3 & 1 & 4 & \cdots n \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 3 & 2 & 4 & \cdots & n \end{pmatrix}$$

(iii) D_{2n} naturally embeds in S_n. For example $D_8 \lesssim S_4$

$$r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \qquad t = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

"Double row notation is cumbersome and hides what's going on. We introduce cycle notation."

New Notation

Definition 13. Let $a_1, \ldots, a_k$ be distinct integers in $\{1, \ldots, n\}$. Suppose $\sigma \in S_n$ and

$$\sigma(a) = \begin{cases} a_{i+1} & \text{if there exists } i \text{ such that } a_i = a \text{ (taken modulo } k\text{).} \\ a & \text{otherwise} \end{cases}$$

Then σ is a k-*angle* and we write $\sigma = (a_1, a_2, \ldots, a_k)$. For example

$$\sigma = (1, 2, 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Remarks

(i)

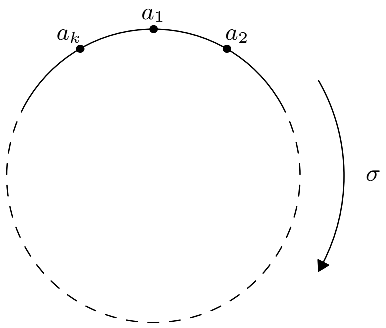
$$(a_1, a_2, \ldots, a_k) = (a_k, a_1, a_2, \ldots, a_{k-1}) = \cdots$$

We usually write the smallest a_i first.

(ii)

$$(a_1, a_2, \ldots, a_k)^{-1} = (a_1, a_k, a_{k-1}, \ldots, a_2$$

(iii) $o(\sigma) = k$, σ is like rotations of k points



(iv) a 2-cycle is called a *transposition*.

Definition 14. Two cycles $\sigma(a_1, \dots, a_k)$ and $\tau = (b_1, \dots, b_l)$ are *disjoint* if $\{a_1, \dots, a_k\} \cap \{b_1, \dots, b_l\} = \emptyset$.

Lemma 6. If $\sigma, \tau \in S_n$ are disjoint then

$$\sigma\tau = \tau\sigma \qquad (\sigma \circ \tau = \tau \circ \sigma).$$

Proof. If $x \in \{1, \dots, n\} \setminus \{a_1, \dots, a_k\} \cup \{b_1, \dots, b_l\}$, then

$$(\sigma \circ \tau)(x) = \sigma(\tau(x)) = x = (\tau \circ \sigma)(x).$$

For $1 \leq i \leq k-1$ we have

$$\begin{aligned}(\sigma \circ \tau)(a_i) &= \sigma(\tau(a_i)) \\ &= \sigma(a_i) \\ &= a_{i+1}\end{aligned}$$

$$\begin{aligned}(\tau \circ \sigma)(a_i) &= \tau(\sigma(a_i)) \\ &= \tau(a_{i+1}) = a_{i+1}\end{aligned}$$

And $\sigma \circ \tau(a_k) = a_1$ and $a\tau \circ \sigma(a_k) = a_1$. The same argument works for the b_i. Thus $\sigma \circ \tau$ and $\tau \circ \sigma$ agree everywhere which implies that $\sigma \circ \tau = \tau \circ \sigma$. □

Example.

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

However this is not necessarily true if two cycles are disjoint.

Example. Consider $\sigma = (1\ 2\ 3)$ and $\tau = (2\ 4)$. Then we have

$$\begin{aligned}\sigma \circ \tau(1) &= \sigma(1) = 2\\ \sigma \circ \tau(2) &= \sigma(4) = 4\\ \sigma \circ \tau(3) &= \sigma(2) = 1\\ \sigma \circ \tau(4) &= \sigma(3) = 3\end{aligned}$$

Hence $\sigma \circ \tau = (1\ 2\ 4\ 3)$ but $\tau \circ \sigma = (1\ 4\ 2\ 3)$.

Example.
$$(1\ 2\ 3)(2\ 3) = (1\ 2)(3) = (1\ 2)$$
but
$$(2\ 3)(1\ 2\ 3) = (1\ 3)$$

Notation. When using cycle notation, we often suppress 1-cycles.

Theorem 1. Every permutation can be written as a product of disjoint cycles (in an essentially unique way).

Example.

$$\begin{aligned}\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 5 & 7 & 6 & 3 & 1 & 9 & 8 \end{pmatrix}\\ &= (1\ 2\ 4\ 7)(3\ 5\ 6)(8\ 9)\end{aligned}$$

Proof. Let $a_1 \in \{1, 2, \dots, n\} = X$. Consider a_1, $\sigma(a_1)$, $\sigma^2(a_1)$, $\dots$. Since X is finite there exists a minimal j such that $\sigma^j(a_1) \in \{a_1, \sigma(a_1), \dots, \sigma^{j-1}(a_1)\}$. We claim: $\sigma^j(a_1) = a_1$ since if not we can assume
$$\sigma^j(a_1) = \sigma^i(a_i)$$
where $j > i \geq 1$. Then this implies
$$\sigma^{j-i}(a_1) = a_1$$
which contradicts the minimality of j. So, $(a_1, \sigma(a_1), \dots, \sigma^{j-1}(a_1))$ is a cycle in σ. If there exists $b \in X \setminus \{a_1, \sigma(a_1), \dots, \sigma^{j-1}(a_1)\}$ consider $b, \sigma(b), \dots$. Now we can note that $(b, \sigma(b), \dots, \sigma^{k-1}(b))$ is disjoint from $(a_1, \sigma(a_1), \dots, \sigma^{j-1}(a_1))$ since σ is a bijection. Continue in this way until all elements of X are reached. □

Lemma 7. Let σ, τ be disjoint cycles in S_n. Then

$$o(\sigma\tau) = \text{lcm}\{o(\sigma), o(\tau)\}.$$

Proof. Let lcm$\{o(\sigma), o(\tau)\}$ so $o(\sigma) \mid k$ and $o(\tau) \mid k$. Then

$$\begin{aligned} (\sigma\tau)^k &= \sigma\tau\sigma\tau\cdots\sigma\tau \\ &= \sigma^k\tau^k \\ &= ee \\ &= e \\ \implies o(\sigma\tau) \mid k \end{aligned}$$

Now suppose $o(\sigma\tau) = n$. Then

$$\begin{aligned} (\sigma\tau)^n &= e \\ \implies \sigma^n\tau^n \\ &= e \end{aligned}$$

But σ, τ move different elements of X which implies that we must have $\sigma^n = e$ and $\sigma^n = e$, which implies that $o(\sigma) \mid n$ and $o(\tau) \mid n$ which implies that $k \mid n$, and hence

$$o(\sigma\tau) = \text{lcm}\{o(\sigma), o(\tau)\}$$

as desired. □

Proposition 2. Any $\sigma \in S_n$ (with $n \geq 2$) can be written as a product of transpositions.

Proof. By the previous theorem it is sufficient to show that a k-cycle can be written as a product of transpositions. We can do this directly:

$$(a_1,\ a_2,\ \ldots,\ a_k) = (a_1,\ a_2)(a_2,\ a_3)\cdots(a_{k-2},\ a_{k-1})(a_{k-1},\ a_1)$$

□

Example.

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

Note that the representation as a product of transpositions is not unique.

Definition 15. Let $\sigma \in S_n$ with $(n \geq 2)$. Then the *sign* of σ, written sgn(σ) is $(-1)^k$ where k is the number of transpositions in some expression of σ as a product of transpositions.

Lemma 8. The function sgn : $S_n \to \{\pm 1\}$ defined by $\sigma \mapsto \text{sgn}(\sigma)$ is well-defined. i.e. if

$$\begin{aligned} \sigma &= \tau_1 \cdots \tau_a \\ &= \tau_1' \cdots \tau_b' \end{aligned}$$

with τ_i and τ_i' transpositions then

$$(-1)^a = (-1)^b.$$

Proof. Let $c(\sigma)$ denote the number of cycles in a disjoint cycle decomposition of σ including 1-cycles, so $c(\text{id}) = n$. Let τ be a transposition.

Claim.

$$c(\sigma\tau) = c(\sigma) \pm 1 \equiv c(\sigma) + 1 \pmod 2$$

Let $\tau = (k,\ l)$. 2 cases:

(i) k, l in different cycles of σ:

$$(k, a_1, \dots, a_r)(l, b_1, \dots, b_s)(k, l) = (k, b_1, b_2, \dots, b_s, l, a_1, \dots, a_r)$$

and hence $c(\sigma\tau) = c(\sigma) - 1$.

(ii) when k, l in same cycle in σ we have

$$(k, a_1, \dots, a_r, l, b_1, \dots, b_s)(k, l) = (k, b_1, \dots, b_s)(l, a_1, \dots, a_r)$$

$$\implies c(\sigma\tau) = c(\sigma) + 1.$$

Now assume

$$\begin{aligned} \sigma &= \text{id} \cdot \tau_1 \cdots \tau_a \\ &= \text{id} \cdot \tau_1' \cdots \tau_a' \end{aligned}$$

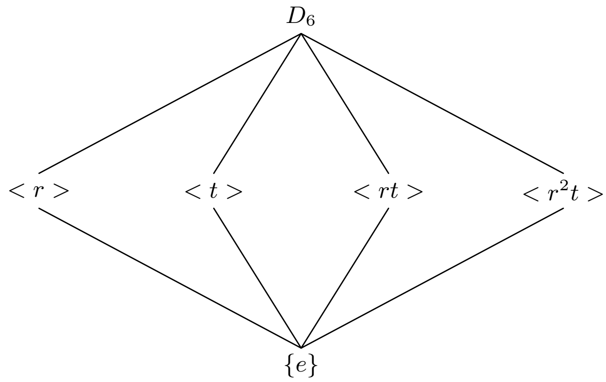
Then

$$\begin{aligned} c(\sigma) &\equiv n + a \pmod 2 \\ &\equiv n + b \pmod 2 \\ \implies a &\equiv b \pmod 2 \\ \implies (-1)^a &= (-1)^b \end{aligned}$$

□

Aside

Subgroup lattice of $D_6 = \{e, r, r^2, t, rt, r^2t\}$:



So we just connect subgroups with a line if one is a subgroup of another.

Theorem 2. Let $n \geq 2$. The map

$$\text{sgn} : (S_n, \circ) \to (\{\pm 1\}, \times) \qquad \sigma \mapsto \text{sgn}(\sigma)$$

is a well-defined non-trivial homomorphism.

Proof.

- Well-defined as proven earlier.
- $\text{sgn}\left((1\ 2)\right) = -1$, so non-trivial.
- Now we prove that it is a homomorphism:
  Let $\alpha, \beta \in S_n$ with $\text{sgn}(\alpha) = (-1)^k$, $\text{sgn}(\beta) = (-1)^k$, so there exists transpositions τ_i and τ_i' such that

$$\alpha = \tau_1 \cdots \tau_k \qquad \beta = \tau_1' \cdots \tau_l'$$
$$\implies \alpha\beta = \tau_1 \cdots \tau_k \tau_1' \cdots \tau_l'$$

$$\begin{aligned} \implies \text{sgn}(\alpha\beta) &= (-1)^{k+l} \\ &= (-1)^k(-1)^l \\ &= \text{sgn}(\alpha)\text{sgn}(\beta) \end{aligned}$$

□

Definition 16. σ is an *even* permutation if $\text{sgn}(\sigma) = 1$ and an odd permutation if $\text{sgn}(\sigma) = -1$.

Corollary 1. The even permutations of S_n $(n \geq 2)$ form a subgroup called the *alternating group* and denoted A_n.

Proof.

- Identity: $\mathrm{id} = (1\ 2)(1\ 2) \in A_n$.
- $$\begin{aligned} &\mathrm{sgn}(\sigma) = 1 = \mathrm{sgn}(\rho) \\ \implies &\mathrm{sgn}(\sigma\rho) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\rho) = 1 \end{aligned}$$

  by the previous theorem
- If
  $$\sigma = \tau_1 \cdots \tau_k$$
  then
  $$\begin{aligned} \sigma^{-1} &= \tau_k \cdots \tau_1 \\ \implies \mathrm{sgn}(\sigma) &= \mathrm{sgn}(\sigma^{-1}) \end{aligned}$$
- Associativity is inherited.

□

Example.
$$\begin{aligned} A_4 = \{&e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), \\ &(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), \\ &(2\ 3\ 4), (2\ 4\ 3), (1\ 3\ 4), (1\ 4\ 3)\} \end{aligned}$$

Remarks

(i) $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$ (exercise - see later)

(ii) cycles of even length are odd, and cycles of odd length are even.

(iii) $A_n = \mathrm{Ker}(\mathrm{sgn})$, hence a subgroup. (question 9, sheet 1)

3 Cosets and Lagrange

Definition 17 (Cosets)**.** Let $H \leq G$ and $g \in G$. The *left coset* gH is defined to be

$$\{gh : h \in H\}.$$

Similarly the right coset is given by

$$Hg = \{hg : h \in H\}.$$

Example.

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

$$H = \{\text{id}, (1\ 2\ 3), (1\ 3\ 2)\} = A_3.$$

$$(1\ 2)H = \{(1\ 2), (1\ 2)(1\ 2\ 3), (1\ 2)(1\ 3\ 2)\} = \{(1\ 2), (2\ 3), (1\ 3)\}$$

$$(1\ 2\ 3)H = H$$

Note, $H \dot{\cup} (1\ 2)H = S_3$.

Notation. We sometimes use $\dot{\cup}$ instead of $\cup$ if we wish to emphasise that we have a disjoint union.

Lemma 9. Let $H \leq G$ and $g \in G$. Then there is a bijection between H and gH. In particular if H is finite then

$$|H| = |gH|.$$

Proof. Define

$$\theta_g : H \to gH \qquad h \mapsto gh$$

We show θ_g is a bijection.

surj: If $gh \in gH$ then $\theta_g(h) = gh$.

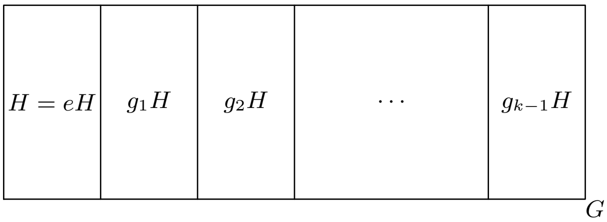
inj: If

$$\begin{aligned} &\theta_g(h_1) = \theta_g(h_2) \\ \implies &gh_1 = gh_2 \\ \implies &h_1 = h_2 \end{aligned}$$

Lemma 10. The left cosets of H in G form a partition called of G i.e.

(i) each $g \in G$ lies in some left coset of H in G.

(ii) if $aH \cap bH \neq \emptyset$ for some $a, b \in G$ then $aH = bH$.



Proof.

(i) $g \in gH$.

(ii) Suppose $c \in aH \cup bH$. Then we claim that $aH = cH = bH$. Now $c \in aH$ so $c = ak$ for some $k \in H$

$$\implies cH = \{ch : h \in H\}$$
$$= \{akh : h \in H\} \subseteq aH$$

Similarly, $a = ck^{-1} \in cH$

$$\implies aH \subseteq cH$$

So $aH = cH$. Similarly $cH = bH$.

For example $S_n = A_n \dot{\cup} (1\ 2)A_n$. □

Lemma 11. Let $H \leq G$, $a, b \in G$. Then

$$aH = bH \iff a^{-1}b \in H.$$

($\Rightarrow$) $b \in bH = aH$

$$\implies b = ah \qquad \text{for some } h \in H$$
$$\implies a^{-1}b = h \in H$$

($\Leftarrow$) Suppose $a^{-1}b = k \in H$.

$$\implies b = ak \in aH$$

also $b \in bH$,

$$\implies aH = bH \qquad \text{by earlier lemma}$$

□

Theorem 3 (Lagrange's Theorem)**.** Let H be a subgroup of the finite group G. Then the order of H divides the order of G (i.e. $|H| \mid |G|$).

Proof. By Lemma 10 G is partitioned into distinct cosets of H, say

$$G = g_1 H \dot{\cup} g_2 H \dot{\cup} \cdots \dot{\cup} g_k H$$

($g_1 = e$ say)
By Lemma 9

$$|g_i H| = |H| \qquad 1 \leq i \leq k$$
$$\implies |G| = |H|k$$

so the order of H divides the order of G. □

Definition 18 (14)**.** Let $H \leq G$. The *index* of H in G is the number of left cosets of H in G, denoted $|G : H|$.

Remark.

(i) If G is finite, $|G : H| = \frac{|G|}{|H|}$. But can have $|G : H|$ finite but G and H both infinite.

(ii) We write $(G : H)$ for the set of left cosets of H in G.

Corollary 2 (Lagrange's Corollary)**.** Let G be a finite group and g an element of G. Then $o(g) \mid |G|$. In particular, $g^{|G|} = e$.

Proof. Note

$$\langle g \rangle = \{e, g, \ldots, g^{n-1}\}$$

where $o(g) = n$. Then

$$o(g) = |\langle g \rangle| \mid |G|$$

by Lagrange's Theorem

$$\implies g^{|G|} = e.$$

□

Corollary 3. If $|G| = p$ for some prime p, then G is cyclic.

Proof. Let $e \neq g$. Then

$$\{e\} \neq \langle g \rangle \leq G$$

BY Lagrange

$$1 \neq |\langle g \rangle| \,\big|\, |G| = p.$$
$$\implies |\langle g \rangle| = p = |G|$$
$$\implies \langle g \rangle = |G|$$

i.e. G is cyclic. □

Definition 19 (Euler Totient Function)**.** Let $n \in \mathbb{N}$ then we define

$$\varphi(n) = |\{1 \leq a \leq n : (a, n) = 1\}|$$

so for example $\varphi(12) = |\{1, 5, 7, 11\}| = 4$.

Theorem 4 (Fermat-Euler Theorem)**.** Let $n \in \mathbb{N}$, $a \in \mathbb{Z}$ with $(a, n) = 1$. Then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Fermat's Little Theorem is a special case:
P prime, $a \in \mathbb{Z}$, $(a, p) = 1$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

We prove Fermat-Euler Theorem by using Lagrange, first we need to set it up. Let $n \in \mathbb{N}$,

$$R_n = \{0, 1, \ldots, n-1\}$$
$$R_n^* = \{a \in R_n : (a, n) = 1\}.$$

Define $\times_n$ to be multiplication modulo n.

Claim. $(R_n^*, \times_n)$ is a group.

Notation, $u \in \mathbb{Z}$ then $\underline{u} \in R_n$ such that $u \equiv \underline{u} \pmod{n}$. Closure:

$$(a, n) = 1 = (b, n) \implies (ab, n) = 1 \implies (\underline{ab}, n) = 1$$

Identity is 1, and clearly associative.
Inverses: Let $a \in R_n^*$ with $(a, n) = 1$.

$$\implies \exists u, v \in \mathbb{Z}$$

such that $au + vn = 1$ (Bezout's Theorem)

$$\implies au \equiv 1 \pmod{n}$$

Then $\underline{u} \in R_n^*$ is a^{-1}.

Now we can prove Fermat Euler Theorem:
Proof. Note $|R_n^*| = \varphi(n)$

$$a \equiv \underline{a} \pmod{n} \qquad \underline{a} \in R_n^*$$

By Corollary 2

$$\underline{a}^{\varphi(n)} = \underline{a}^{|R_n^*|} = 1 \qquad \text{in } R_n^*$$

$$\implies a^{\varphi(n)} \equiv 1 \pmod{n}$$

∎

4 Normal Subgroups, Quotient Groups and Homomorphisms

Given a group G, subgroup H of G and the set of left cosets of H in G, $(G : H)$, we would like to define a group operation on the cosets, $\circ$, so that $((G : H), \circ)$ is a group. We would like

$$(gH) \circ (kH) = gkH.$$

When does this work?

$$gHkH = gkHH = gkH \iff kH = Hk$$

This motivates the following definition:

Definition 20 (15)**.** A subgroup K of G is called *normal* if $gK = Kg$ for all $g \in G$. We write $K \trianglelefteq G$.

Example.

$$K = \{\text{id}, (1\ 2\ 3), (1\ 3\ 2)\} \trianglelefteq S_3.$$

$$(1\ 2)K = \{(1\ 2), (2\ 3), (1\ 3)\} = K(1\ 2)$$

$$(1\ 3)K = K(1\ 3)$$

$$(2\ 3)K = K(2\ 3)$$

And $(1\ 2\ 3)K = K = K(1\ 2\ 3)$ etc. But $H = \{1, (1\ 2)\}$ is not normal in S_3:

$$(1\ 3)H = \{(1\ 3), (1\ 2\ 3)\}$$

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

Proposition 3 (4)**.** Let $K \leq G$. TFAE (the following are equivalent):

(i) $gK = Kg\ \forall g \in G$

(ii) $gKg^{-1} = K\ \forall g \in G$

(iii) $gkg^{-1} \in K\ \forall k \in K, g \in G$.

Proof. (i) $\implies$ (ii):

$$\begin{aligned} gKg^{-1} &= \{gkg^{-1} : k \in K\} \\ &= (gK)g^{-1} \\ &= (Kg)g^{-1} \\ &= K \end{aligned}$$

(ii) $\implies$ (iii): trivial.
(iii) $\implies$ (i): For any $k \in K$, $g \in G$, there exists $k' \in K$ such that

$$gkg^{-1} = k'$$
$$\implies gk = k'g \in Kg$$
$$\implies gK \subseteq Kg$$

Similarly $g^{-1}kg = k''$ for some $k'' \in K$

$$\implies kg = gk''$$
$$\implies Kg \subseteq gK$$
$$\implies gK = Kg.$$

□

Examples

- $\{e\} \trianglelefteq G$, $G \trianglelefteq G$.
- If G is abelian then all subgroups are normal. Since if $k \in K$, $g \in G$, $K \trianglelefteq G$ follows from
$$gkg^{-1} = gg^{-1}k = k \in K.$$
- Kernels of homomorphisms are normal subgroups (Sheet 1, question 9).
$$\implies A_n \trianglelefteq S_n$$
since $A_n = Ker(\text{sgn})$.
- $D_{2n} = \langle r, y : r^n = 1 = t^2, trt = r^{-1} \rangle$ Then $\langle r \rangle \trianglelefteq D_{2n}$. Clearly $r^i r^j r^{-i} = r^j \in \langle r \rangle$. Also
$$\begin{aligned}(r^i t)r^j(r^i t)^{-1} &= r^i t r^j t r^{-1} \\ &= r^i - j - i = r^{-j} \in \langle r \rangle\end{aligned}$$
Or we can use the following lemma.

Lemma 12. If $K \leq G$ and the index of K in G is 2, then $K \trianglelefteq G$.

Proof.

$$\begin{aligned}G &= K \dot{\cup} gK \\ &= K \dot{\cup} Kg \\ \implies gK &= Kg \ \forall g \in G\end{aligned}$$

□

Theorem 5. If $K \trianglelefteq G$, the set $(G : K)$ of left cosets of K in G is a group under coset multiplication, i.e.

$$gK \cdot hK = ghK$$

This group is called the *quotient group* (or factor group of G by K and denoted G/K.

Proof. We need to check that cost multiplication is well-defined, i.e. if

$$gK = \hat{g}K$$

and

$$hK = \hat{h}K$$

then

$$ghK = \hat{g}\hat{h}K.$$

By Lemma 11,

$$gK = \hat{g}K \implies \hat{g}^{-1}g \in K$$
$$hK = \hat{h}K \implies \hat{h}^{-1}h \in K$$

Now $\hat{g}^{-1}g \in K$

$$\implies h^{-1}\hat{g}^{-1}gh \in K$$

since $K \trianglelefteq G$.

$$\implies \hat{h}^{-1}hh^{-1}\hat{g}^{-1}gh \in K$$
$$\implies \hat{h}^{-1}\hat{g}^{-1}gh \in K$$
$$\implies ghK = \hat{g}\hat{h}K$$

by Lemma 11. So coset multiplication is well-defined. Group axioms now follow easily:

- By construction coset multiplication is closed as $ghK \in (G : H)$ $g_1h \in G$.
- identity given by $eK = K$
- $(gK)^{-1} = g^{-1}K$.
- associativity holds since it does in G, to check:

$$\begin{aligned}(gKhK)lK &= (gh)lK \\ &= g(hl)K \\ &= gk(HklK)\end{aligned}$$

□

Examples

(i) $S_n/A_n = (\{A_n, (1\ 2)A_n\}, \circ) \cong C_2$.

(ii) $D_8 = \langle a, b : a^4 = 1 = b^2, bab = a^{-1} \langle$ Let $K = \{1, a^2\}$.

Claim. $K \trianglelefteq D_8$.

$$\begin{aligned}(a^i b)a^2(a^i b)^{-1} &= a^i b a^2 b a^{-i} \\ &= a^{-2} = a^2 \in K \\ a^i a^2 a^{-1} &= a^2 \in K\end{aligned}$$

$$\frac{|D_8|}{|K|} = 4 = |(D_8 : K)|$$

4 distinct left cosets:

$$\begin{aligned}K &= \{1, a^2\} \\ aK &= \{a, a^3\} \\ bK &= \{b, ba^2\} = \{b, a^2 b\} \\ abK &= \{ab, aba^2\} = \{ab, a^3 b\}\end{aligned}$$

$\circ$	K	aK	bK	abK
K	K	aK	bK	abK
aK	aK	K	abK	bK
bK	bK	abK	K	aK
abK	abK	bK	aK	K

Note: $aKaK = a^2K = K \cong$ example 9.

(iii) Recall the subgroups of $(\mathbb{Z}, +)$ are precisely the groups $(n\mathbb{Z}, +)$ where $n \in \mathbb{N}$,

$$n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}.$$

Since $(\mathbb{Z}, +)$ abelian, all subgroups are normal, $n\mathbb{Z} \trianglelefteq \mathbb{Z}$. Suppose $n = 5$, cosets given by,

$$\begin{aligned}5\mathbb{Z} &= \{5k : k \in \mathbb{Z}\} \\ 1 + 5\mathbb{Z} &= \{1 + 5k : k \in \mathbb{Z}\} \\ 2 + 5\mathbb{Z} &= \{2 + 5k : k \in \mathbb{Z}\} \\ 3 + 5\mathbb{Z} &= \{3 + 5k : k \in \mathbb{Z}\} \\ 4 + 5\mathbb{Z} &= \{4 + 5k : k \in \mathbb{Z}\}\end{aligned}$$

$$(1+5\mathbb{Z})+(2+5\mathbb{Z})=3+5\mathbb{Z}.$$

$$(3+5\mathbb{Z})+(4+5\mathbb{Z})=7+5\mathbb{Z}=2+5\mathbb{Z}.$$

$$(\mathbb{Z}/5\mathbb{Z},\circ)\cong(\{0,1,2,3,4\},+_5)$$

$$n+5\mathbb{Z}\to\underline{n}\qquad\text{such that}\qquad n\equiv\overline{n}\pmod 5$$

$\overline{n}\in\{0,1,2,3,4\}$. Well-defined map:
if $n+5\mathbb{Z}=m+5\mathbb{Z}$ then

$$\begin{aligned}&-m+n\in 5\mathbb{Z}\\ \implies &-m+n\equiv 0\pmod 5\\ &\implies n\equiv m\pmod 5\\ &\implies \overline{n}=\overline{m}\end{aligned}$$

homomorphism:

$$\begin{aligned}\theta((n+5\mathbb{Z})+(m+5\mathbb{Z}))&=\theta(n+m+5\mathbb{Z})\\ &=\overline{n+m}\\ &=\overline{n}+_5\overline{m}\\ &=\theta(n+5\mathbb{Z})+\theta(m+5\mathbb{Z})\end{aligned}$$

In general

$$(\mathbb{Z}/n\mathbb{Z},\circ)\cong(\{0,1,2,3,4\},+_n).$$

Recall $\theta:G\to H$ is a homomorphism if

$$\theta(xy)=\theta(x)\theta(y)$$

$$\mathrm{Im}(\theta)=\{\theta(g):g\in G\}\leq H$$

$$\mathrm{Ker}(\theta)=\{g\in G:\theta g=e_H\}\trianglelefteq G$$

Theorem 6 (First Isomorphism Theorem)**.** Let G, H be groups and $\theta:G\to H$ be a group homomorphism. Then $\mathrm{Im}(\theta)\leq H$ and $\mathrm{Ker}(\theta)\trianglelefteq G$ and $G/\mathrm{Ker}(\theta)\cong\mathrm{Im}(\theta)$.

Definition 21 (16)**.** A group is called *simple* if its only normal subgroups are $\{e\}$ and G. For example C_p for some prime p.

Definition (Injection)**.** Suppose $f:A\to B$. Then f is *injective* if for any $a_1,a_2\in A$, if $f(a_1)=f(a_2)$ then $a_1=a_2$. (each element of A maps to a different element of B).

Definition (Surjection)**.** Suppose $f : A \to B$. Then f is *surjective* if given $b \in B$, $\exists a \in A$ such that $f(a) = b$. (every element in B is 'hit').

Definition 22 (Bijection)**.** A function is *bijective* if it is both injective and surjective.

Now we can prove the first isomorphism theorem.

Proof. Need to construct an isomorphism $\theta : G/\text{Ker}\theta \to \text{Im}\theta$ where $gK \mapsto \theta(g)$. Let $K = \text{Ker}\theta$; need θ well-defined:
Suppose $gK = hK$, then

$$\begin{aligned} h^{-1}g &\in K \\ \implies \theta(h^{-1}g) &= e_H \\ \implies \theta(h)^{-1}\theta(g) &= e_H \qquad \text{since } \theta \text{ is a homomorphism} \\ \implies \theta(g) &= \theta(h) \\ \implies \theta(gK) &= \theta(hK) \end{aligned}$$

Need θ a homomorphism:

$$\begin{aligned} \theta(gKhK) &= \theta(ghK) \\ &= \theta(gh) \\ &= \theta(g)\theta(h) \qquad \text{since } \theta \text{ is a homomorpism} \\ &= \theta(gK)\theta(hK) \end{aligned}$$

θ surjective:

$$\theta(g) \in \text{Im}\theta \implies \theta(gK) = \theta(g)$$

θ injective:
Suppose $\theta(gK) = \theta(hK)$ then

$$\begin{aligned} \theta(g) &= \theta(h) \\ \implies \theta(h)^{-1}\theta(g) &= e_H \\ \theta(h^{-1}g) &= e_H \\ \implies h^{-1}g &\in K \\ \implies gK &= hK \end{aligned}$$

□

Examples

(i) sgn : $S_n \to (\{\pm 1\}, \times)$ with $\sigma \mapsto \text{sgn}(\sigma)$. Then

$$\begin{aligned} \text{Im(sgn)} &= (\{\pm 1\}, \times) \\ \text{Ker(sgn)} &= A_n \\ \implies S_n/A_n &\cong (\{\pm 1\}, \times) \cong C_2 \\ \implies |A_n| &= |S_n|/2 \end{aligned}$$

(ii) $\theta : (\mathbb{R}, +) \to (\mathbb{C} \setminus \{0\}, \times)$ defined by $r \mapsto e^{2\pi i r}$. Note, $\theta(r+s) = \theta(r)\theta(s)$. Also,

$$\text{Im}(\theta) = S' = \{z \in \mathbb{Z} : |z| = 1\} \qquad \text{unit circle}$$

$$\text{Ker}(\theta) = (\mathbb{Z}, +) \trianglelefteq (\mathbb{R}, +)$$

$$(\mathbb{R}, +)/(\mathbb{Z}, +) \cong S'$$

(iii) Recall

$$\text{GL}_2(\mathbb{R}) = \{2 \times 2 \text{ matrices, entries in } \mathbb{R}, \det \neq 0\}$$

Then we observe that $\det : \text{GL}_2(\mathbb{R}) \to (\mathbb{R} \setminus \{0\}, \times)$, $M \mapsto \det(M)$ is a homomorphism since

$$\det(AB) = \det(A)\det(B).$$

$$\text{Im}(\det) = (\mathbb{R} \setminus \{0\}, \times)$$

since

$$\det \begin{pmatrix} \alpha & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} = \alpha \in \mathbb{R} \setminus \{0\}.$$

$$\begin{aligned} \text{Ker}(\det) &= \text{SL}_2(\mathbb{R}) \\ &= \{2 \times 2 \text{ matrices, entries in } \mathbb{R}, \det = 1.\} \\ \implies \text{SL}_2(\mathbb{R}) &\trianglelefteq \text{GL}_2(\mathbb{R}) \end{aligned}$$

and $\text{GL}_2(\mathbb{R})/\text{SL}_2(\mathbb{R}) \cong (\mathbb{R} \setminus \{0\}, \times)$.

(iv) $\theta : (\mathbb{Z}, +) \to (\{0, 1, \ldots, n-1\}, +_n)$ with $n \mapsto \underline{n}$.

$$\text{Ker}\theta = n\mathbb{Z}$$

Remark. Let $K \trianglelefteq G$. Then K is the kernel of the natural surjective homomorphism

$$\begin{aligned} \theta : G &\to G/K \\ g &\mapsto gK \end{aligned}$$

Thus homomorphic images of G are equivalent to quotients of G.

Lemma 13. A homomorphism $\theta : G \to H$ is injective if and only if $\text{Ker}\theta = \{e_G\}$.

Proof.

($\Rightarrow$) Suppose $\theta(g) = e_H = \theta(e_G)$. Injective implies that $g = e_G$.

($\Leftarrow$)

$$\begin{aligned} &\theta(g) = \theta(h) \\ \implies &\theta(h)^{-1}\theta(g) = e_H \\ \implies &\theta(h^{-1}g) = e_H \\ \implies &h^{-1}g \in \text{Ker } \theta = \{e_G\} \\ \implies &h^{-1}g = e_G \\ \implies &h = g \end{aligned}$$

Recall, $N \trianglelefteq G$, $g \in G$, $n \in N$ implies

$$\begin{aligned} gng^{-1} &\in N \\ gng^{-1} &= \hat{n} \qquad \text{for some } \hat{n} \in N \\ &= gn = \hat{n}g \end{aligned}$$

□

Lemma 14. (i) Let $N \trianglelefteq G$ and $H \leq G$. Then $NH = \{nh : n \in N, h \in H\} \leq G$.

(ii) Let $N \trianglelefteq G$, $M \trianglelefteq G$, then

$$NM \trianglelefteq G.$$

Proof.

(i) closure, nh, $\underline{nh} \in NH$, then

$$n\,\underbrace{h\underline{n}}_{\hat{n}h}\,\underline{h} = n\hat{n}h\underline{h} \in NH$$

identity: $\text{id} = e = ee \in NH$
inverse:

$$\begin{aligned} (nh)^{-1} &= h^{-1}n^{-1} \\ &= \hat{n}h^{-1} \qquad \text{for some } \hat{n} \in N. \\ &\in NH \end{aligned}$$

(ii) check normality

$$g(nm)g^{-1} = \underbrace{gng^{-1}}_{\in N}\underbrace{gmg^{-1}}_{\in M} \in NM$$

□

5 Direct products and Small Groups

5.1 Direct Products

Let H and K be groups. We construct the (external) *direct product*, $H \times K$, to be the set

$$\{(h,k) : h \in H, k \in K\}$$

with operation

$$(h_1,k_1) * (h_2,k_2) = (h_1 *_H h_2, k_1 *_K k_2) = (h_1h_2, k_1k_2)$$

i.e. componentwise multiplication.

Then $(H \times K, *)$ is a group, which can verify easily as follows:

closure H group implies $h_1h_2 \in H$ and K group implies $k_1k_2 \in K$.

identity (e_H, e_K)

inverse $(h,k)^{-1} = (h^{-1}, k^{-1})$

associativity since group operations in both H and K are associative.

Remarks

(i) If H, K both finite, then $|H \times K| = |H||K|$.

(ii) $H \times K$ abelian if and only if

$$\begin{aligned} &(h_1,k_1)*(h_2,k_2) = (h_2,k_2)*(h_1,k_1) \quad \forall h_1,h_2 \in H, k_1,k_2 \in K \\ \iff &(h_1h_2, k_1k_2) = (h_2h_1, k_2k_1) \\ \iff &h_1h_2 = h_2h_2 \qquad \text{and} \qquad k_1k_2 = k_2k_1 \\ \iff &H \text{ abelian and } K \text{ abelian} \end{aligned}$$

(iii) $H \cong \{(h, e_K) : h \in H\} \leq H \times k$ and $K \cong \{(e_H, k) : k \in K\} \leq H \times K$.

Examples

(i)

$$\begin{aligned} C_2 \times C_2 &= \langle x \rangle \times \langle y \rangle \\ &= \{e,x\} \times \{e,y\} \end{aligned}$$

elements $(e,e), (x,e), (e,y), (x,y)$.

$\circ$	(e,e)	(x,e)	(e,y)	(x,y)
(e,e)	(e,e)	(x,e)	(e,y)	(x,y)
(x,e)	(x,e)	(e,e)	(x,y)	(e,y)
(e,y)	(e,y)	(x,y)	(e,e)	(x,e)
(x,y)	(x,y)	(e,y)	(x,e)	(e,e)

Klein 4-group $\cong$ example 9. Note $o((x, e)) = o(e, y)) = o(x, y)) = 2$. So $C_2 \times C_2 \not\cong C_4$.

(ii) However, $C_2 \times C_3 \cong C_6$. (sheet 2, question 10)

Lemma 15. Let $(h, k) \in H \times K$ where H, K groups. Then

$$o((h, k)) = \text{lcm}(o(h), o(k))$$

Proof. Let $n = o((h, k))$ and $m = \text{lcm}(o(h), o(k))$. Then $h^m = e_H$, $k^m = e_K$. So $(h, k)^m = (h^m, k^m) = (e_H, e_K)$ and hence $n \mid m$ by Lemma 5. Also,

$$\begin{aligned} (e_H, e_K) &= (h, k)^n \\ &+ (h^n, k^n) \\ \implies o(h) &\mid n, o(k) \mid n \\ \implies m &\mid n \end{aligned}$$

Thus we know when $C_m \times C_n \cong C_{mn}$ (Sheet 2, q10). □

Recognising when a group can be written as a direct product of subgroups is trickier.

Proposition 4 (5)**.** Let G be a group with subgroups H and K, then if

(i) each element of G can be written as hk for $h \in H$ and $k \in K$;

(ii) $H \cap K = \{e\}$;

(iii) $hk = kh \ \forall h \in H, k \in K$,

Then $G \cong H \times K$ and we call G the (internal) direct product of H and K.

Proof. Let $\theta : H \times K \to G$ defined by $(h, k) \mapsto hk$. First we check that θ is a homomorphism:

$$\begin{aligned} \theta((h_1, k_1)(h_2, k_2)) &= \theta((h_1 h_2, k_1 k_2)) \\ &= h_1 h_2 k_1 k_2 \\ &= h_1 k_1 h_2 k_2 \\ &= \theta((h_1, k_1))\theta((h_1, k_2)) \end{aligned}$$

To check that θ is injective,

$$\begin{aligned} \theta((h_1, k_1)) &= \theta((h_2, k_2)) \\ \implies h_1 k_2 &= h_2 k_2 \\ \implies h^{-1} h_1 &= k_2 k_1^{-1} \in H \cap K = \{e\} \\ \implies h_1 = h_2 \quad &\text{and} \quad k_1 = k_2 \end{aligned}$$

so $(h_1, k_1) = (h_2, k_2)$. θ is surjective by (i), so θ is an isomorphism as required. $\square$

Remark. There are alternative equivalent definitions of internal direct product. G is the internal direct product of subgroups H and K if

(i)' $H \trianglelefteq G$, $K \trianglelefteq G$;

(ii)' $H \cap K = \{e\}$;

(iii)' $HK = G$.

Need to show (i), (ii), (iii) are equivalent to (i)', (ii)', (iii)'.

($\Rightarrow$) we show $K \trianglelefteq G$. Let $k \in K$, $g = h_1 k_1 \in G$ by (i). Then

$$gkg^{-1} = h_1 k_1 k k_1^{-1} h^{-1} = h_1 \underline{k} h^{-1} = \underline{k} \in K$$

Similarly $H \trianglelefteq G$.

($\Leftarrow$) Need to show (iii). Let $h \in H$, $k \in K$ and consider

$$h^{-1} \underbrace{k^{-1} h k}_{\in H} \in H \qquad \text{since } H \trianglelefteq G.$$

Similarly, this expression is in K, so

$$\begin{aligned} & h^{-1}k^{-1}hk \in H \cap K = \{e\} \\ \implies & hk = kh \end{aligned}$$

Example. $G = \langle a \rangle \cong C_{15}$. Then

$$\begin{aligned} C_5 \cong \langle a^3 \rangle &= H \trianglelefteq G \\ C_3 \cong \langle a^5 \rangle &= K \trianglelefteq G \\ H \cap K = \langle a^3 \rangle \cap \langle a^5 \rangle &= \{e\} \\ a^k &= (a^3)^{2k}(a^5)^{-k} \in HK \\ \implies C_{15} &\cong C_3 \times C_5 \cong K \times H \end{aligned}$$

5.2 Small Groups

Recall D_{2n}, the symmetries of a regular n-gon, generated by

$$r : z \mapsto e^{2i\pi/n} z$$

$$t : z \mapsto \underline{z}$$

Then the elements of D_{2n} are

$$\{e, \underbrace{r, \dots, r^{n-1}}_{\text{rotations}}, \underbrace{t, rt, \dots, rt^{n-1}}_{\text{reflection}}\}$$

Now suppose G a group, $n \geq 3$ with $|G| = 2n$, and $\exists b \in G$ with $o(b) = n$ and $a \in G$, $o(a) = 2$ and $aba = b^{-1}$. Then $G \cong D_{2n}$. Note $\langle b \rangle \trianglelefteq G$ since of index 2. Also $a \notin \langle b \rangle$, since $ab \neq ba$. So $G = \langle b \rangle \cup \langle b \rangle a = \{e, b, \dots, b^{n-1}, a, ba, \dots, b^{n-1}a\}$. Furthermore

$$\begin{aligned} ab &= b^{-1}a \\ \implies ab^k &= (ab)b^{k-1} \\ &= b^{-1}ab^{k-1} \\ &= b^{-2}ab^{k-2} \\ &= \cdots \\ &= b^{-k}a \end{aligned}$$

So, $(b^k a)(b^k a) = b^k b^{-k} aa = e$. We can check that

$$\begin{aligned} \theta : D_{2n} &\to G \\ r &\mapsto b \\ t &\mapsto a \end{aligned}$$

is an isomorphism.

- $|G| = 1$, $G = \{e\}$.
- $|G| = 2 \implies G \cong C_2$ (by Lagrange's Theorem)
- $|G| = 3 \implies G \cong C_3$
- $|G| = 4$, by Lagrange's Theorem, $1 \neq g \in G$ then $o(g) \mid 4$. If $\exists g \in G$ with $o(g) = 4$ then this implies $G \cong C_4$. Suppose not. Let $1 \neq a \in G \implies o(a) = 2$. Then by sheet 1 q7, G is abelian, so $C_2 \cong \langle a \rangle \trianglelefteq G$. Now let $b \in G \setminus \langle a \rangle$, then $C_2 \cong \langle b \rangle \trianglelefteq G$. Also, $\langle a \rangle \cap \langle b \rangle = \{e\}$. Now consider ab:
  - if $ab = e \implies a = b^{-1} = b$ ⨳
  - if $ab = a \implies b = e$ ⨳
  - if $ab = b \implies a = e$ ⨳

  So,

$$\begin{aligned} G &= \{e, a, b, ab\} \\ &= \langle a \rangle \langle b \rangle \\ &\cong \langle a \rangle \times \langle b \rangle \\ &\cong C_2 \times C_2 \end{aligned}$$

  Two groups of order 4: C_4 and $C_2 \times C_2$, both of which are abelian.

- $|G| = 5 \implies G \cong C_5$ by Lagrange's Theorem.

- $|G| = 6$ then $1 \neq g \in G \implies o(g) \in \{2,3,6\}$ by Lagrange. If all non-identity elements have order 2 then $|G|$ is a 2-power, ※. So there exists $b \in G$ such that $o(b) = 3$ (Note if $o(g) = 6$ then $o(g^2) = 3$). Therefore $C_3 \cong \langle b \rangle \trianglelefteq G$ since of index 2. Let $a \in G \setminus \langle b \rangle$. Hence $a^2 \in \langle b \rangle$. (Consider $a\langle b \rangle \in G/\langle b \rangle$). If $a^2 = b$ or b^2 then $o(a) = 6 \implies G \cong C_6$. Now suppose $a^2 = e$. Also $aba^{-1} \in \langle b \rangle$. If $aba^{-1} = e$ then $b = e$ which is a contradiction. If $aba^{-1} = b$ then $ab = ba \implies o(ab) = 6 \implies G \cong C_2$. If $aba^{-1} = b^2$, then in other words we have $aba^{-1} = b^{-1}$, so $G = \langle a, b : a^2 = b^3 = e, aba^{-1} = b^{-1} \rangle \cong D_6$. So there are two groups of order 6, they are C_6 and $D_6 \cong S_3$. Note $C_6 \not\cong D_6$ as C_6 is abelian and D_6 is not.

- $|G| = 7 \implies G \cong C_7$.

- $|G| = 8$. By Lagrange, if $1 \neq g \in G$ then $o(g) \in \{2,4,8\}$. If all non-identity elements have order 2 and hence G is abelian. Let $1 \neq a \in G$, $C_2 \cong \langle a \rangle \trianglelefteq G$. Choose $b \notin \langle a \rangle$,

$$\begin{aligned} \langle a, b \rangle &= \{1, a, b, ab\} \\ &= \langle a \rangle \langle b \rangle \qquad \cong \langle a \rangle \times \langle b \rangle \end{aligned}$$

Choose $c \in G \setminus \langle a, b \rangle$. Then

$$\begin{aligned} G &= \langle a, b \rangle \cup \langle a, b \rangle c \\ &= \langle a, b \rangle \langle c \rangle \\ &\cong \langle a, b \rangle \times \langle c \rangle \\ &\cong \langle a \rangle \times \langle b \rangle \times \langle c \rangle \\ &\cong C_2 \times C_2 \times C_2 \end{aligned}$$

Now suppose $\exists g \in G$ such that $o(g) > 2 \implies \exists a \in G, o(a) = 4 \implies C_4 \cong \langle a \rangle \trianglelefteq G$. Let $b \in G \setminus \langle c \rangle \implies b^2 \in \langle a \rangle$. If $b^2 \in \{a, a^3\} \implies o(b) = 8 \implies G \cong C_8$. Now, $bab^{-1} \in \langle a \rangle$ (since $\langle a \rangle G$), so $bab^{-1} = a^i$ for some i. This implies

$$\begin{aligned} b^2ab^{-2} &= ba^ib^{-1} \\ &= (bab^{-1})^i \\ &= a^{i^2} \end{aligned}$$

But $b^2 \in \langle a \rangle \implies b^2ab^{-2} = a$. Hence $i^2 \equiv 1 \pmod 4 \implies i \equiv \pm 1 \pmod 4$. If $bab^{-1} = a \implies ba = ab$ so G is abelian. If $b^2 = e$ then

$$\begin{aligned} G &= \langle a \rangle \cup \langle a \rangle b \\ &= \langle a \rangle \langle b \rangle \\ &\cong \langle a \rangle \times \langle b \rangle \\ &\cong C_4 \times C_2 \end{aligned}$$

if $b^2 = a^2$ then $(ba^{-1})^2 = e$ then

$$\begin{aligned} G &\cong \langle a \rangle \times \langle ba^{-1} \rangle \\ &\cong C_4 \times C_2 \end{aligned}$$

Suppose $bab^{-1} = a^{-1}$. Then if $b^2 = e$ then $G \cong D_8$. However if $b^2 = a^2$; we have a new group Q_8, the quaternion group.

Definition (Quaternion Group). $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ with $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$, $ik = ij$ and $i^2 = j^2 = k^2 = -1$. So $o(i) = o(j) = o(k) = 4$ and $o(-1) = 2$. Another way to define the group is:

$$\{\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\} \le \mathrm{SL}_2(\mathbb{C}).$$

alternatively,

$$Q_8 = \langle a, b \mid a^4 = e, b^2 = a^2, bab^{-1} = a^{-1} \rangle.$$

So 5 isomorphism classes of groups of order 8:

$$\underbrace{C_8, \quad C_4 \times C_2, \quad C_2 \times C_2 \times C_2}_{\text{abelian}}$$

all different, because

- C_8 has an element of order 8;
- $C_4 \times C_2$ does not have an element of order 4;
- $C_2 \times C_2 \times C_2$ has all elements order 2.

and D_8 and Q_8 are non-abelian so must be different to these 3. Q_8 has 6 elements of order 4, but D_8 only has 2, so these are non-isomorphic.

- $|G| = 9$. We will show later that groups of order p^2 with p prime are abelian. Either $G \cong C_9$ or all non-identity elements have order 3. Choose $e \neq a \in G$, $b \in G \setminus \langle a \rangle$, then

$$\begin{aligned} G &= \langle a \rangle \cup \langle a \rangle b \cup \langle a \rangle b^2 \\ &= \langle a \rangle \langle b \rangle \\ &\cong \langle a \rangle \times \langle b \rangle \\ &\cong C_3 \times C_3 \end{aligned}$$

- $|G| = 10$, must be either C_{10} or D_{10} (question 12, sheet 2)

Remark. There are lots and lots of groups of order 2^k; there are about 10 of order 16, and about 5×10^{10} of order 2^{10}.

6 Group Actions

It's often easier to understand a group if it's doing something, permuting elements, rotating a square etc.

Definition 23 (16)**.** Let G be a group and X a non-empty set. We say that G *acts* on X if there is a mapping

$$\rho : G \times X \to X \qquad (g, x) \mapsto \rho(g, x) = g(x)$$

such that

(0) if $g \in G$, $x \in X$, then $\rho(g, x) = g(x) \in X$ (implied by notation $\rho : G \times X \to X$)

(i) $\rho(gh, x) = \rho(g, \rho(h, x))$ (in shorthand, $gh(x) = g(h(x))$)

(ii) $\rho(e, x) = x$ (in shorthand, $e(x) = x$)

Examples

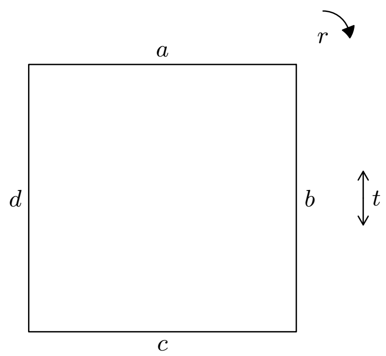
(i) trivial action $\rho(g, x) = x \forall x \in X, g \in G$.

(ii) S_n acts on the set $\{1, 2, \dots, n\} = X$ by permuting the elements of X. For example, S_3 acts on $\{1, 2, 3\}$:

$$\begin{aligned} \sigma &= (1\ 2) \in S_3 : \qquad \sigma(1) = 2, \quad \sigma(2) = 1, \quad \sigma(3) = 3 \\ \tau &= (1\ 3) \in S_3 \\ \tau\sigma &= (1\ 3)(1\ 2) = (1\ 2\ 3) \\ (\tau\sigma)(1) &= 2 = \tau(2) = \tau(\sigma(1)) \end{aligned}$$

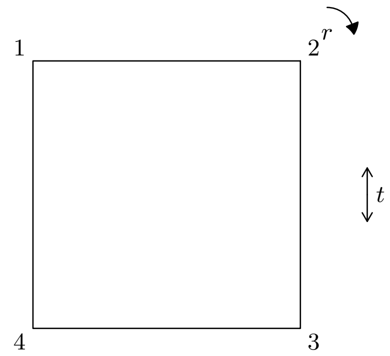
Similarly subgroups of S_n act on X.

(iii) $D_8 = \{e, r, r^2, r^3, t, rt, r^2t, r^3t\}$ acts on edges of a square



$$t(a) = c, t(c) = a, t(b) = b, t(d) = d, s(a) = b, \ldots$$

Also acts on the vertices of a square



$$t(1) = 3, t(4) = 1, t(2) = 3, t(3) = 2$$

(iv) G acts on itself by left multiplication. This is called the *left regular action.*

$$G\times \to G \qquad (g, k) \mapsto gk$$

Check:

(0) $gk \in G$ by closure

(i) $\rho(gh, k) = ghk$, $\rho(g, \rho(h, k)) = \rho(g, hk) = ghk$. Or, in shorthand $(gh)k = ghk$, $g(h(k)) = g(hk) = ghk$.

(ii) $\rho(e, k) = ek = k$.

We also have the *right regular action*

$$G \times G \to G \qquad (g, k) \mapsto kg^{-1}$$

(v) G acts on itself by *conjugation*

$$G \times G \to G$$

Check:

(0) $gkg^{-1} \in G$

(i) $\rho(gh, k) = (gh)k(gh)^{-1} = ghkh^{-1}g{-}1$ and $\rho(g, \rho(h, k)) = \rho(g, hkh{-}1) = g(hkh^{-1})g^{-1}$

(ii) $\rho(e, k) = eke^{-1} = k$.

(vi) Let $N \trianglelefteq G$, then G acts on N by conjugation

$$G \times N \to N \qquad (g, n) \mapsto gng^{-1}$$

(0) $gng^{-1} \in N$ since $N \trianglelefteq G$.

(i) as above

(ii) as above

(vii) Let $H \leq G$, then G acts on the set of left cosets, $(G : H)$, of H in G. Called the *left coset action*

$$G \times (G : H) \to (G : H) \qquad (g, kH) \mapsto (gkH)$$

(0) $gkH \in (G : H)$

(i) $\rho(gh, kH) = (gh)kH = ghkH$ and $\rho(g, \rho(h, kH)) = \rho(g, hkH) = ghkH$

(ii) $\rho(e, kH) = ekH = kH$.

Remark. Recall a permutation of a set X is a bijection of X. We have commented that a bijection $f : X \to X$ has a 2-sided inverse, i.e. there exists $g : X \to X$ such that

$$f \circ g(x) = x = g \circ f(x) \quad \forall x \in X$$

Conversely, if $f : X \to X$ is a map with a 2-sided inverse, then f is a bijection:

$$f \circ g(x) = x \quad \forall x \in X \implies \text{surjective}$$

$$g \circ f(x) = x \quad \forall x \in X \implies \text{injective}$$

Note. 2-sided is necessary, because we can consider $\phi : \mathbb{Z} \to \mathbb{Z}$ defined by $x \mapsto 2x$ and $\psi\mathbb{Z} \to \mathbb{Z}$ defined by $2x \mapsto x$ and $2x + 1 \mapsto 0$. Then $\psi\phi = \text{id}$ but $\phi\psi \neq \text{id}$.

Lemma 16. Suppose the group G acts on the non-empty set X. Fix $g \in G$, then $\theta_g : X \to X$ defined by $x \mapsto \rho(g, x) = g(x)$ is a permutation of X, i.e. $\theta_g \in \text{Sym}(X)$.

Proof. Clearly θ_g is a map from X to X. We need to show θ_g is a bijection, enough to show it has a 2-sided inverse.

$$\begin{aligned}
\theta_{g-1} \circ \theta_g(x) &= \theta_{g-1}(\rho(g, x)) \\
&= \rho(g^{-1}(\rho(g, x))) \\
&= \rho(g^{-1}g, x) && \text{since } \rho \text{ group action} \\
&= \rho(e, x) \\
&= x && \forall x \in X
\end{aligned}$$

Similarly,

$$\theta_g \circ \theta_{g-1}(c) = x \qquad \forall x \in X$$

□

Proposition 5 (6)**.** Suppose G acts on the set X. Then the map

$$\theta : G \to \text{Sym}(X) \qquad g \mapsto \theta_g$$

as in Lemma 16, is a homomorphism.

Proof. We need to show θ is a homomorphism, i.e. we need

$$\theta(gh) = \theta(g) \circ \theta(h)$$

i.e.

$$\theta_{gh} = \theta_g \circ \theta_h.$$

Let $x \in X$, then

$$\begin{aligned} \theta_{gh}(x) &= \rho(gh, x) \\ &= \rho(g, \rho(h, x)) \\ &= \theta_g \circ \theta_h(x) \end{aligned}$$

True $\forall x \in X$, so done. □

Remark. Proposition 6 gives us an equivalent definition of a group action. If G is a group and X a set such that $\theta : g \to \text{Sym}(X)$ is a group homomorphism, then $\rho : G \times X \to X$ defined by $(g, x) \mapsto \theta_g(x)$ where $\theta(g) = \theta_g$, is a group action.

Remark. Using notation of proposition 6, by first Isomorphism Theorem,

$$G/\text{Ker } \theta \cong \text{Im } \theta \leq \text{Sym}(X)$$

Note

$$\begin{aligned} \text{Ker } \theta &= \{g \in G : \theta(g) = \text{id}_X \in \text{Sym}(X)\} \\ &= \{g \in G : \theta_g(x) = \rho(g, x) = x \forall x\} \\ &\trianglelefteq G \end{aligned}$$

i.e. all those elements that fix every element of X, that act 'trivially'. We say the action is *faithful* if Ker $\theta = \{e\}$.

Examples of Kernels

(i) Trivial action - Ker $\theta = G$.

(ii) S_n acts on $\{1, \ldots, n\}$ - faithful

(iii) D_8 acts on edges - faithful

(iv) Left regular action - faithful

(v) Conjugation

$$\begin{aligned}\text{Ker }\theta &= \{g \in G : gkg^{-1} = k \forall k \in G\} \\ &= z(G)\end{aligned}$$

where $z(G)$ is the *centre of* G. 'the elements that commute with everything'

(vi) conjugation on $N \trianglelefteq G$

$$\begin{aligned}\text{Ker }\theta &= \{g \in G : gng^{-1} = n \forall n \in N\} \\ &= C_G(N)\end{aligned}$$

where $C_G(N)$ is the *centraliser of* N *in* G.

(vii) Left coset action

$$\begin{aligned}\text{Ker }\theta &= \{g \in G : gkH = kH \forall k \in G\} \\ &= \{g \in G : k^{-1}gk \in H \forall k \in G\} \\ &= \{g \in G : g \in kHk^{-1} \forall k \in G\} \\ &= \bigcap_{k \in G} kHk^{-1} \\ &= \text{Core}_G(H) \\ &\trianglelefteq G \\ &\leq H\end{aligned}$$

Note. If Ker $\theta = \{e\}$ then G is isomorphic to a subgroup of $\text{Sym}(X)$, we write $G \lesssim \text{Sym}(X)$. So if $|G|$ does not divide $|\text{Sym}(X)|$ then Ker $\theta \neq \{e\}$.

Theorem 7 (Cayley's Theorem)**.** Any group G is isomorphic to a subgroup of $\text{Sym}(X)$ for some non-empty set X.

Proof. We take X to be G and consider the left regular action $G \times G \to G$ defined by $(g, h) \mapsto gh$. This is a faithful action as $gh = h \ \forall h \in G \implies g = e$. Thus we have an injective homomorphism

$$\theta : G \mapsto \text{Sym}(G)$$

and $G \lesssim \text{Sym}(G)$ as required. □

Definition 24 (17)**.** Let G act on a set X and $x \in X$. The *orbit* of $x \in X$ is given by

$$\mathrm{Orb}_G(x) = \{g(x) : g \in G\} \subseteq X$$

i.e. the set of points in X which x can be mapped to.

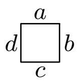
Examples

(i) trivial action, $\mathrm{Orb}_G(x) = \{x\}$.

(ii) S_n acts on $\{1, 2, \ldots, n\} = X$, $\mathrm{Orb}_G(1) = X$. If $H = \langle(1\ 2)(3\ 4\ 5)\rangle$ acting on $X = \{1, 2, 3, 4, 5\}$ then

$$\mathrm{Orb}_G(1) = \{1, 2\}$$

$$\mathrm{Orb}_G(3) = \{3, 4, 5\}.$$

(iii) D_8 on 

:

$$\mathrm{Orb}_{D_8}(a) = \{a, b, c, d\}.$$

(iv) left regular action

$$\mathrm{Orb}_G(k) = G$$

since $g = g(k^{-1}k) = (gk^{-1})k$ for any $g \in G$.

(v) conjugation

$$\begin{aligned}\mathrm{Orb}_G(k) &= \{g(k) : g \in G\} \\ &= \{gkg^{-1} : g \in G\} \\ &= \mathrm{ccl}_G(k)\end{aligned}$$

conjugacy class of k in G. If $h \in \mathrm{ccl}_G(k)$ we say h and k are *conjugate.*

Definition 25 (18)**.** We say G acts *transitively* on X if for any $x \in X$, $\mathrm{Orb}_G(x) = X$. Equivalently, if given any pair $x_1, x_2 \in X$ $\exists g \in G$ such that $g(x_1) = x_2$.

So, the left regular action is a transitive action.

Lemma 17. The distinct G-orbits form a partition of X.

Proof. Let $x \in X$, then $x \in \mathrm{Orb}_G(x)$ since $x = ex$. Suppose $z \in \mathrm{Orb}_G(x) \cap \mathrm{Orb}_G(y)$, we show

$$\mathrm{Orb}_G(x) = \mathrm{Orb}_G(z) = \mathrm{Orb}_G(y).$$

$z \in \mathrm{Orb}_G(x) \implies \exists g \in G$ such that $g(x) = z$. Suppose $t \in \mathrm{Orb}_G(x)$, then $\exists h \in G$ such that $h(z) = t$ and hence $t = h(g(x)) = (hg)(x)$. Therefore $t \in \mathrm{Orb}_G(x)$ and hence $\mathrm{Orb}_G(z) \subseteq \mathrm{Orb}_G(x)$. Similarly $g(x) = z$

$$x = e(x) = (g^{-1}g)(x) = g^{-1}(z)$$

and hence $\mathrm{Orb}_G(x) \subseteq \mathrm{Orb}_G(z)$. Thus $\mathrm{Orb}_G(x) = \mathrm{Orb}_G(z)$. Similarly $\mathrm{Orb}_G(z) = \mathrm{Orb}_G(y)$. □

Remarks

(i) We could have proved Lemma 17 by noting that $x_1 \sim x_2$ if $\exists g \in G$ such that $g(x_1) = x_2$ is an equivalence relation.

(ii) $\mathrm{Orb}_G(x)$ is G invariant, i.e.

$$g(\mathrm{Orb}_G(x)) \subseteq \mathrm{Orb}_G(x).$$

Since if $y \in \mathrm{Orb}_G(x)$, then $y = hx$ for some $h \in G$.

$$\begin{aligned} \implies g(y) &= g(h(x)) \\ &= (gh)(x) \in \mathrm{Orb}_G(x) \end{aligned}$$

(iii) G is transitive on $\mathrm{Orb}_G(x)$. Let $y, z \in \mathrm{Orb}_G(x)$, so $y = g(x)$, $z = h(x)$ for some $g, h \in G$. Then

$$z = h(g^{-1}(y))$$

Definition (19)**.** Let G act on X and $x \in X$. The *stabiliser* of x in G is given by

$$\mathrm{Stab}_G(x) = \{g \in G : g(x) = x\} \subseteq G.$$

i.e. all those elements in G that fix x.

Examples

(i) trivial action,

$$\mathrm{Stab}_G(x) = G.$$

(ii) S_n on $X = \{1, 2, \ldots, n\}$

$$\mathrm{Stab}_G(1) \cong S_{n-1}$$

$H = \langle (12)(345) \rangle$ on X

$$\begin{aligned} \mathrm{Stab}_H(1) &= \langle (345) \rangle \\ &= \{e, (345), (354)\} \end{aligned}$$

(iii) D_8 on edges of a square,

$$\text{Stab}_{D_8}(e) = \{e, t\}$$

(iv) left regular action

$$\text{Stab}_G(k) = \{e\}$$
$$gk = k \implies g = e$$

(v) conjugation

$$\begin{aligned}\text{Stab}_G(k) &= \{g \in G : g(k) = k\} \\ &= \{g \in G : gkg^{-1} = k\} \\ &= \{g \in G : gk = kg\} \\ &= C_G(k)\end{aligned}$$

centraliser of k in G i.e. all elements of G that commute with k.

Lemma 18. $\text{Stab}_G(x)$ is a subgroup of G.

Proof.

- $e(x) = x \implies e \in \text{Stab}_G(x)$
- if $g, h \in \text{Stab}_G(x)$ then

$$\begin{aligned}(gh)(x) &= g(h(x)) \\ &= g(x) \\ &= x \\ \implies gh &\in \text{Stab}_G(x)\end{aligned}$$

- $g \in \text{Stab}_G(x)$

$$g(x) = x$$
$$x = e(x) = (g^{-1}g(X) = g^{-1}(gx) = g^{-1}(x)$$
$$\implies g^{-1} \in \text{Stab}_G(x)$$

- associativity inherited from G.

□

Remark. Recall $\phi : G \to \text{Sym}(x)$

$$\begin{aligned}\text{Ker } \theta &= \{g \in G : g(x) = x \ \forall x \in X\} \\ &= \cap \text{Stab}_G(x)\end{aligned}$$

Theorem 8 (Orbit-Stabiliser Theorem)**.** Let G be a finite group acting on a non-empty set X. Then $\mathrm{Stab}_g(x) \leq G$ and

$$|G| = |\mathrm{Stab}_G(x)||\mathrm{Orb}(x)|.$$

Remark. We actually prove that $|G : \mathrm{Stab}_G(x)|$, the number of left cosets of $\mathrm{Stab}_G(x)$ in G, is equal to $|\mathrm{Orb}_G(x)|$, a more general statement.

Proof. $(G : \mathrm{Stab}_G(x))$ set of left cosets of $\mathrm{Stab}_G(x)$ in G. Consider the map

$$\theta : \mathrm{Orb}_G(x) \to (G : \mathrm{Stab}_G(x) \qquad g(x) \mapsto g\mathrm{Stab}_G(x)$$

θ well-defined because:

$$\begin{aligned} g(x) = h(x) \implies h^{-1}g(x) & = x \\ \implies h^{-1}g \in \mathrm{Stab}_G(x) \\ \implies g\mathrm{Stab}_G(x) = h\mathrm{Stab}_G(x) \\ \implies \theta(g(x)) = \theta(h(x)) \end{aligned}$$

θ injective:

$$\begin{aligned} \theta(g(x)) &= \theta(h(x)) \\ \implies g\mathrm{Stab}_G(x) &= h\mathrm{Stab}_G(x) \\ \implies h^{-1}g &\in \mathrm{Stab}_G(x) \\ \implies h^{-1}g(x) &= x \\ \implies g(x) &= h(x) \end{aligned}$$

θ surjective:
Given $g\mathrm{Stab}_G(x) \in (G : \mathrm{Stab}_G(x))$ then $g(x) \in \mathrm{Orb}_G(x)$ and

$$\theta(g(x)) = g\mathrm{Stab}_G(x).$$

Thus θ a well-defined bijection as required. □

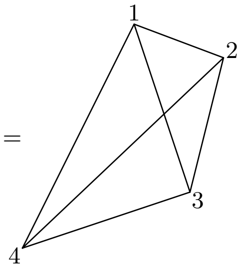
6.1 Applications to Symmetry Groups of Regular Solids

Let S be a regular solid and V its vertices. Then the symmetries of S are the isometries (distance preserving maps) of $\mathbb{R}^2$ or $\mathbb{R}^3$ that maps S to itself.

Examples of Symmetries

Example. (Tetrahedron)
This is self-duel. Let G be group of symmetries of T, and $X = \{\text{vertices of } T\} = \{1, 2, 3, 4\}$.

$T =$

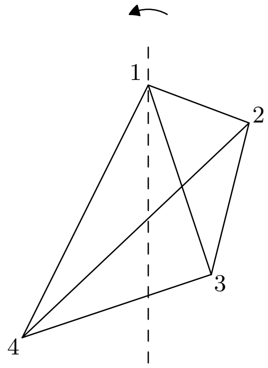


faces are 4
equilateral triangles

Then $\exists$ group homomorphism

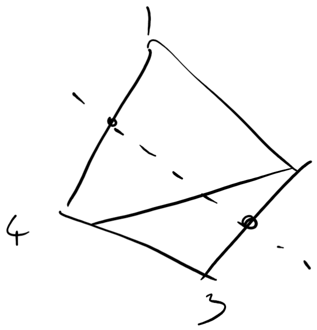
$$\phi : G \to \text{Sym}(X) \cong S_4$$

(Proposition 6). Note Ker $\phi = \{e\}$, if all vertices fixed, then T fixed.
Consider $G' \leq G$ subgroup of rotations.



rotation of $\frac{2\pi}{3}$
3-cycle (2 3 4)
and $\frac{4\pi}{3}$ (2 4 3)

4 such axes implies 8 rotations of order 3 (3-cycles).



rotation of π
double transp
(1 4)(2 3)

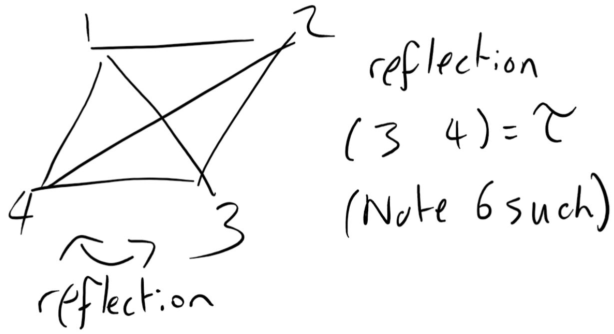
3 such axes and identity

$$\implies G^+ \cong A_4$$

Now consider G (all symmetries). Clearly

$$\begin{aligned}\mathrm{Orb}_G(1) &= \{1,2,3,4\} \\ &= \mathrm{Orb}_{G^+}\end{aligned}$$

Consider $\mathrm{Stab}_G(1)$. Note if 3 vertices are fixed then T fixed. Consider $\mathrm{Stab}_G(1)$. Note if 3 Suppose vertices 1 and 2 are fixed.

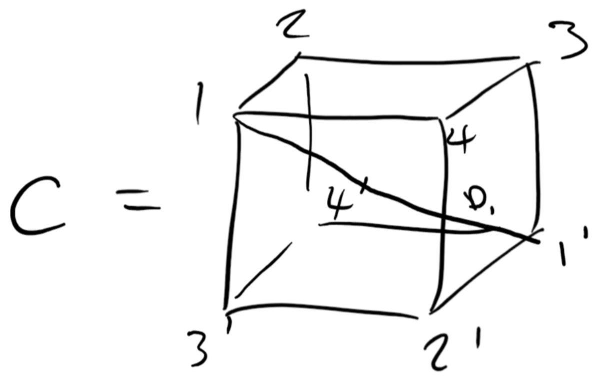


If just 1 fixed have order 3 rotation from before $= \sigma$. This is everything

$$\begin{aligned}\mathrm{Stab}_G(1) &= \langle \sigma, \tau \rangle \\ &\cong D_6 \\ \implies |G| &= |\mathrm{Orb}_G(1)||\mathrm{Stab}_G(1)| \\ &= 4 \times 6 \\ &= 24 \\ \implies G &\cong S_4\end{aligned}$$

Note $\mathrm{Stab}_{G^+}(1) = \langle G \rangle$. Also $(1234) = (12)(234)$.

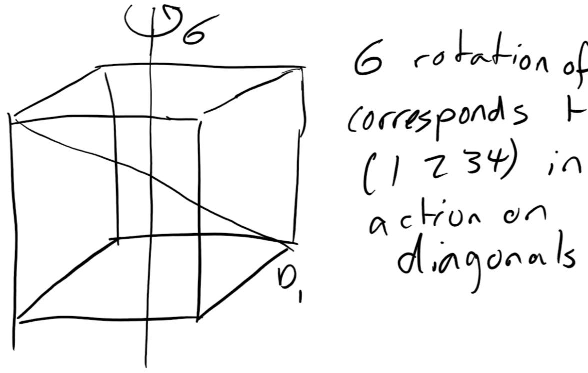
Example. (Cube)
Dual to octahedron.



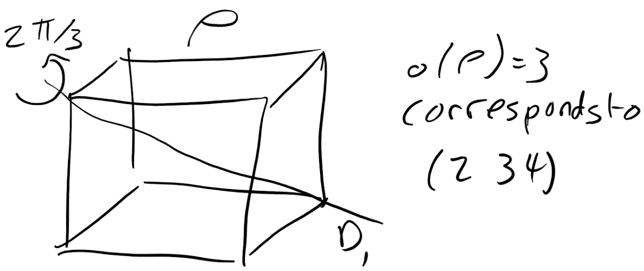
Let G^+ be group of rotations of C. Then G^+ acts on set of diagonals $X = \{D_1, D_2, D_3, D_4\}$. If a rotation σ fixes all diagonals, then $\sigma = \text{id}$. So we have an injective homomorphism

$$\phi : G^+ \to \text{Sym}(C) \cong S_4$$

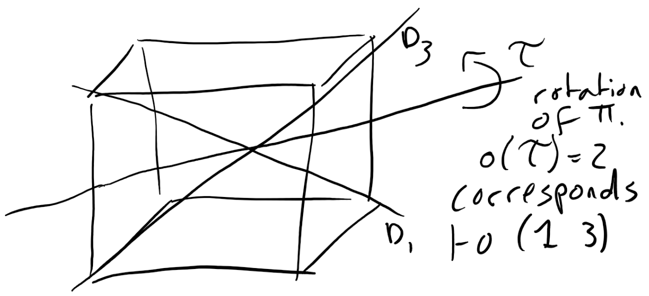
roatations: $-$id



3 such axes, hence 6 elements of order 4, 3 elements of order 2.



4 such axes, hence 8 elements of order 3.



6 such axes, i.e. $G^+ \cong S_4$.
Note $\text{Orb}_{G^+}(D_1) = \{D_1, D_2, D_3, D_4\}$

$$\text{Stab}_{G^+}(D_1) = \langle \sigma, \tau' \rangle$$

or consider G^+ acting on vertex 1

$$|\mathrm{Orb}_{G^+}(1)| = 8$$

$$|\mathrm{Stab}_G(1)| = |\langle\rho\rangle| = 3$$

$$\implies |G^+| = 24$$

Now consider full symmetry group of C, call it G. Consider action on faces $F_1, \dots, F_6$. Yields an injective homomorphism (faithful)

$$\phi : G \to \mathrm{Sym}\{F_i\} \cong S_6$$

$$|\mathrm{Orb}(F_1)| = 6$$

$$\mathrm{Stab}(F_1) \cong D_8$$

$$\implies |G| = 6 \times 8 = 48.$$

So, action on diagonals is not faithful;

$$\exists g \in G \quad g(D_i) = D)i) \qquad i \leq i \leq 4$$

but $g \neq \mathrm{id}$. Label vertices of C as $\{(\pm 1, \pm 1, \pm 1)\}$

$$g : (x, y, z) \mapsto (-x, -y, -z)$$

if label faces of cube as a dice; 1 opposite 6, 2 opposite 5, 3 opposite 4 then

$$g = (16)(25)(34)$$

Then $G \cong F^+ \times \langle g\rangle$. Then $G^+ \trianglelefteq G$ (index 2) and $\langle g\rangle \trianglelefteq G$ (commutes with all rotations) and

$$G^+ \cap \langle g\rangle = \{e\}$$

$$|G^+\langle g\rangle| = 48 = |G|.$$

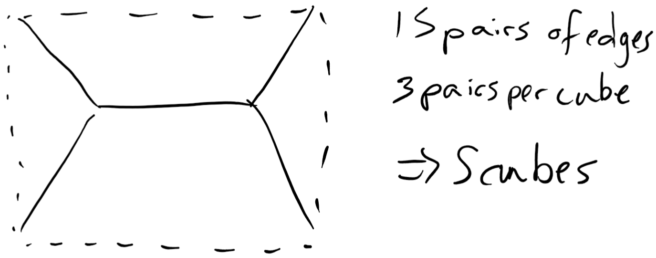
Example. (Dodecahedron)
Dual to icosahedron. We denote by D. 12 regular pentagonal faces, 30 edges, 20 vertices. Let G^+ be the grou pof rotations of D. Let F be a face of D.

$$|\mathrm{Orb}_{G^+}(F)| = 12$$

$$|\mathrm{Stab}_{G^+}(F)| = 5$$

$$\implies |G^+| = 5 \times 12 = 60$$

There are five cubes embedded in D:



G^+ acts faithfully on cubes

$$\implies \phi : G^+ \to S_5$$

injective and $|G^+| = 60$ hence $G^+ \cong A_5$ (there is some work in the "hence" here but one can do it with some determination). Can find elements of A_5:

- rotations through opposite faces - 5 cycles. (6 axes, 4 elements per axis)
- rotation through opposite vertices - 3 cycles.
- rotation through opposite edges - double transpositions (15 such).

Another application of the Orbit Stabiliser Theorem:

Theorem 8 (Cauchy's Theorem)**.** Let G be a finite group and p a prime that divides $|G|$. Then there exists an element in G of order p.

Proof. Let

$$X = \{(x_1, x_2, \dots, x_p) : x_1, x_2, \dots, x_p = e, x_i \in G\}.$$

Let $H = \langle h : h^p = e \rangle \cong C_p$ act on X as follows:

$$H \times X \to X \qquad (h, (x_1, \dots, x_p)) \mapsto (x_2, x_3, \dots, x_p, x_1)$$

in general,

$$(h^i, (x_1, \dots, x_p)) \mapsto (x_{1+i}, x_{2+i}, \dots, x_{p+i})$$

where suffices are taken modulo p.
Check this is a group action:

(0) Since $x_1 x_2 \cdots x_p = e$, we have

$$\begin{aligned} x_1 x_2 \cdots x_p &= (x_1 x_2 \cdots x_i)^{-1} x_1 x_2 \cdots x_p (x_1 x_2 \cdots x_i) \\ &= (x_1 x_2 \cdots x_i)^{-1} e (x_1 x_2 \cdots x_i) \\ &= e \end{aligned}$$

(i) We simply check that

$$\begin{aligned} h^{i+j} &= (x_{1+i+j}, \dots, x_{p+i+j}) \\ &= h^i(h^j(x_1, \dots, x_p)) \end{aligned}$$

(ii) For identity, we heck that

$$\begin{aligned} e(x_1, \dots, x_p) &= h^p(x_1, \dots, x_p) \\ &= (x_1, \dots, x_p) \end{aligned}$$

Let

$$\overline{x} = (x_1, x_2, \dots, x_p) \in X.$$

As distinct orbits partition X (Lemma 17)

$$\implies \sum_{\substack{\text{distinct} \\ \text{orbits}}} |\mathrm{Orb}_H(\overline{x})| = |X|$$

Note $|X| = |G|^{p-1}$ (choose $x_1, \dots, x_{p-1}$ then x_p determined)

$$\implies p \,\big|\, |X|$$

$$\implies p \,\big|\, LHS$$

But by Orbit Stabiliser Theorem:

$$\begin{aligned} &|\mathrm{Orb}_H(\overline{x})| \,\big|\, |H| = p \\ \implies &|\mathrm{Orb}_H(\overline{x})| = 1 \text{ or } p \end{aligned}$$

Now,

$$\overline{e} = (e, e, \dots, e) \in X \qquad |\mathrm{Orb}_H(\overline{e})| = 1.$$

So there exists at least $p - 1$ other orbits of length 1. So there exists $\overline{x} \in X$ with $\mathrm{Orb}_H(\overline{x}) = 1$

$$\implies \overline{X} = (x, x, \dots, x)$$

so $x \neq e$ and $x^p = e$. □

6.2 Conjugacy Action

Reminder of the definition of conjugation:

$$G \times G \to G \qquad (g, h) \mapsto ghg^{-1}.$$

orbits are called conjugacy classes:

$$\mathrm{ccl}_G(h) = \{ghg^{-1} : g \in G\}.$$

Stabilisers are called centralisers:

$$C_G(h) = \{g \in G : ghg^{-1} = h\}.$$

Remarks

(i) By Lemma 17 the conjugacy classes partition G.

(ii) By Orbit Stabiliser Theorem, $h \in G$

$$|G| = |C_G(h)||\text{ccl}_G(h)|.$$

In particular,

$$|\text{ccl}_G| \mid |G|.$$

(iii) If $k \in \text{ccl}_G(h)$ then $o(k) = o(h)$. Since $k = ghg^{-1}$ for some $g \in G$,

$$\begin{aligned} k^{o(h)} &= (ghg^{-1})^{o(h)} \\ &= gh^{o(h)}g^{-1} \\ &= e \\ \implies o(k) &\mid o(h) \end{aligned}$$

Similarly, $h = g^{-1}kg$ hence $o(h) \mid o(k)$, so $o(h) = o(k)$ as desired.

(iv) Recall

$$\begin{aligned} Z(G) &= \{g \in G : gh = hg \ \forall h \in G\} \\ &\trianglelefteq G \end{aligned}$$

And,

$$Z(G) = \bigcap_{h \in G} C_G(h)$$

Note, $z \in Z(G)$ if and only if $|\text{ccl}_G(z)| = 1$. If $z \in Z(G)$

$$\implies \text{ccl}_G(z) = \{gzg^{-1} : g \in G\} = \{z : g \in G\} = \{z\}.$$

If $|\text{ccl}_G(z)| = 1$ then note

$$z = eze^{-1} \in \text{ccl}_G(z).$$

So $gzg^{-1} = z \ \forall g \in G$.

(v) Let $H \leq G$, then H is normal if and only if it is a union of conjugacy classes. (Sheet 3 question 3)

(vi) G abelian if and only if $G = Z(G)$.

Proposition 7. Let p a prime and G a group of order p^n. Then $Z(G)$ is nontrivial, i.e. $Z(G) \gneq \{e\}$.

Proof. Let G act on G by conjugation. Then the conjugacy classes of G partition it by Lemma 17:

$$G = \bigcup_{\substack{\text{distinct} \\ \text{conjugacy} \\ \text{classes}}} \text{ccl}_G(x)$$

By Orbit Stabiliser Theorem

$$|\text{ccl}_G(x)| \,\big|\, |G| = p^n.$$

Either $|\text{ccl}_G(x) = 1$ or $p \,\big|\, \text{ccl}_G(x)$. So by (iv) above

$$|G| = \sum_{x \in Z(G)} |\text{ccl}_G(x)| + \sum_{\substack{\text{distinct} \\ \text{conjugacy} \\ \text{classes} \\ \text{with} \\ p \,|\, \text{ccl}_G(x)}} |\text{ccl}_G(x)|$$

Now $p \mid LHS$ so $p \mid RHS$

$$\implies p \left| \sum_{z \in Z(G)} |\text{ccl}_G(x)| = |Z(G)|. \right.$$

But $e \in Z(G)$, hence we must have $|Z(G)| \geq p > 1$, as desired. □

Lemma 19. Let G be a finite group and $Z(G)$ the centre of G. If $G/Z(G)$ is cyclic then G is abelian.

Proof. Let $Z = Z(G)$. Since G/Z is cyclic, $G/Z = \langle yZ \rangle$ for some $y \in G$. Let $g, h \in G$. Then $gZ = y^i Z$ for some i, so $g = z^i z_1$ for some $z_1 \in Z$. Similarly, $hZ = y^j Z$ for some j, so $g = z^j z_2$ for some $z_2 \in Z$. Now,

$$\begin{aligned} gh &= y^i z_1 y^j z_2 \\ &= y^i y^j z_1 z_2 && z_1 \in Z \\ &= y^j y^i z_2 z_1 \\ &= y^j z_2 y^i z_1 \\ &= hg \end{aligned}$$

so G is abelian as required. □

Corollary 5. Suppose $|G| = p^2$ for some prime p. Then G is abelian and there are, up to isomorphism, just two groups of order p^2, namely $C_p \times C_p$ and C_{p^2}.

Proof. (Sheet 3 Question 10) □

Remark

(i) A group of order p^n for a prime p is called a finite p-group.

(ii) If all elements have p-power order G is called a p-group. For example C_{p^∞} (Prüfer group).

Conjugation in S_n

Definition 20. Let $\sigma \in S_n$ and write σ as a product of disjoint cycles including 1-cycles. Then the *cycle-type* of σ is $(n_1, n_2, \ldots, n_k)$ where $n_1 \geq n_2 \geq \cdots \geq n_k \geq 1$ and the cycles in σ have length n_i. Note $n = n_1 + n_2 + \cdots + n_k$. For example

$$(1234)(567) = (1234)(567(8) \in S_8$$

has cycle type $(4, 3, 1)$, and $e \in S_5$ has cycle type $(1, 1, 1, 1, 1)$.

Theorem 9. The permutations π and σ in S_n are conjugate *in* S_n if and only if they have the same cycle type.

Proof. Suppose σ has cycle type $(n_1, n_2, \ldots, n_k)$. Write

$$\sigma = (a_{11}a_{12}\ldots a_{1n_1})(a_{21}a_{22}\ldots a_{2n_2})\cdots(a_{k1}a_{k2}\ldots a_{kn_k}).$$

Let $\tau \in S_n$. Then

$$\begin{aligned}\tau\sigma\tau^{-1}(\tau(a_{ij})) &= \tau\sigma(a_{ij}) \\ &= \begin{cases}\tau(a_{ij}) & j < n_i \\ \tau(a_{ii}) & j = n_i\end{cases}\end{aligned}$$

Thus 2 permutations of the same cycle type are conjugate. □

For example,

$$(14)(123)(14)^{-1} = (423)$$

$$(1l)(1k)(1l) = (lk).$$

Consider S_4: let $x \in S_4$. Recall $24 = |S_4| = |\mathrm{ccl}_{S_4}(x)||C_{S_4}(x)|$ by Orbit-Stabiliser Theorem.

example member x	cycle type	size	sign	$\lvert C_{S_4}(x)\rvert$	$C_{S_4}(x)$
e	$(1,1,1,1)$	1	1	24	S_4
$(12)(3)(4)$	$(2,1,1)$	6	-1	4	$\langle(12),(34)\rangle \cong C_2 \times C_2$
$(123)(4)$	$(3,1)$	8	1	3	$\langle(123)\rangle \cong C_3$
$(12)(34)$	$(2,2)$	3	1	8	$\langle(1234),(12)\rangle \cong D_8$
(1234)	(4)	6	-1	4	$\langle(1234)\rangle \cong C_4$

Corollary 6. The number of distinct conjugacy classes of S_n is given by $p(n)$, the number of partitions of n into positive integers, i.e. $n = n_1 + \cdots + n_k$ with $n_1 \geq n_2 \geq \cdots \geq n_k \geq 1$.

However in A_n conjugation is less clear. Certainly

$$\mathrm{ccl}_{A_n}(x) = \{gxg^{-1} : g \in A_n\} \subseteq \{gxg^{-1} : g \in S_n\} = \mathrm{ccl}_{S_n}(x)$$

since $A_n \leq S_n$.
So if two elements are conjugate in A_n they have the same cycle type. But having the same cycle type in A_n does not guarantee being conjugate. For example (123) not conjugate to (132) in A_4. If $\tau(123)\tau^{-1} = (132)$ then $\tau = (12)$, or (32) or (13), none of which are in A_4.

Or consider $C_{A_4}((123)) = C_{S_4}((123)) \cap A_4$. For example

$$C_{S_4}((123)) = \langle (123) \rangle \leq A_4$$

So, $C_{A_4}((123)) = C_{S_4}((123))$

$$\implies |\mathrm{ccl}((123))| = \frac{|A_4|}{|C_{A_4}((123))|} = \frac{|S_4|/2}{|C_{S_4}((123))|} = \frac{|\mathrm{ccl}_{S_4}((123))|}{2}$$

So the conjugacy of 8 3-cycles in S_4 splits into 2 conjugacy classes in A_4.

Key point: let $x \in A_n$. If $C_{A_n}(x) = C_{5_n}(x)$

$$\implies |\mathrm{ccl}_{A_n}(x)| = \frac{|\mathrm{ccl}_{S_n}(x)|}{2}.$$

If $C_{A_n}(x) \leq C_{S_n}(x)$, then $C_{S_n}(x)$ contains an odd permutation and

$$|C_{A_n}(x)| = |C_{S_n}(x) \cap A_n| = \frac{|C_{S_n}(x)|}{2}$$

(Sheet 2, Q4)

$$\implies |\mathrm{ccl}_{A_n}(x)| = |\mathrm{ccl}_{S_n}(x)|.$$

example member x	cycle type	$C_{A_4}(x)$	size of conj class
e	$(1,1,1,1)$	A_4	1
(123)	$(3,1)$	$\langle (123) \rangle$	4
(132)	$(3,1)$	$\langle (132) \rangle$	4
(12)(34)	$(2,2)$	$\{e, (12)(34), (13)(24), (14)(23)\} \cong C_2 \times C_2$	3

Remark. The number of elements in S_n with k_l cycles of length l is given by

$$\frac{n!}{\prod_l k_l! l^{k_l}}$$

Think of cycles as trays, put in elements of $X = \{1, 2, \dots, n\}$. This gives $n!$ options, but we've overcounted. Each cycle of length l can be written l ways, this gives l^{k_l} factor. Also k_l cycles of length l can be permuted $k_l!$ ways.

Let us consider S_5 (note $|S_5| = 120$).

Example member x	Cycle type	#	sgn	$\lvert C_{S_5}(x)\rvert$	$C_{S_5}(x)$
e	$(1,1,1,1,1)$	1	1	120	S_5
(12)	$(2,1,1,1)$	10	-1	12	$\langle(12)\rangle \times \mathrm{Sym}\{3,4,5\} \cong C_2 \times S_3$
(12)(34)	$(2,2,1)$	15	1	8	$\langle(1324),(12)\rangle \cong D_8$
(123)	$(3,1,1)$	20	1	6	$\langle(123),(45)\rangle \cong C_6$
(123)(45)	(32)	20	-1	6	$\langle(123),(45)\rangle \cong C_6$
(1234)	$(4,1)$	30	-1	4	$\langle(1234)\rangle \cong C_4$
(12345)	(5)	24	1	5	$\langle(12345)\rangle \cong C_5$

Now consider A_5 (note $|A_5| = 60$).

Example member x	Cycle type	$C_{A_5}(x)$	$\lvert \mathrm{ccl}_{A_5}(x)\rvert$
e	$(1,1,1,1,1)$	A_5	1
(12)(34)	$(2,2,1)$	$\langle(12)(34),(13)(24)\rangle$	15
(123)	$(3,1,1)$	$\langle(123)\rangle$	20
(12345)	(5)	$\langle(12345)\rangle$	12
(21345)	(5)	$\langle(21345)\rangle$	12

Recall a group is *simple* if it has no non-trivial proper normal subgroups, i.e. if only normal subgroups are $\{e\}$ and G.

Theorem 10. A_5 is a simple group.

Proof. Suppose $N \trianglelefteq A_5$. Then N is a union of conjugacy classes (Sheet 3, question 3(a)). Hence

$$|N| = 1 + 15a + 20b + 12c$$

where $b, a \in \{0,1\}$ and $c \in \{0,1,2\}$. But by Lagrange's Theorem, $|N| \mid |A_5| = 60$. Only possibility is $|N| = 1$ or $|N| = 60$. □

Comments

(i) A_5 is the smallest non-abelian simple group.

(ii) A_n simple $\forall n \geq 5$ (GRM). But A_4 is not simple.

(iii) Classification of finite simple groups exists, includes infinite families.

- C_p for p prime (only abelian simple groups).
- A_n with $n \geq 5$.
- groups of 'Lie type' (matrix groups)
- 26 sporadic groups (including the monster and baby monster)

Aside

For example, number of cycles in S_5 of type $(\bullet\ \bullet)(\bullet\ \bullet)$ so $k_2 = 2$, $k_1 = 1$.

$$\# = \frac{q5!}{2!w^2 \cdot 1! \cdot 1} = 15$$

For $(\bullet\ \bullet\ \bullet)(\bullet\ \bullet)$ we have $k_3 = 1$, $k_2 = 1$

$$\# = \frac{5!}{1!3^1 1!2^1} = 20.$$

7 Matrix Groups

Let $M_n(\mathbb{R})$ denote the set of all $n \times n$ matrices with entries in $\mathbb{R}$. Define

$$\mathrm{GL}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det A \neq 0\}$$

Proposition 8. $\mathrm{GL}_n(\mathbb{R})$ is a group under matrix multiplication. It is called the *general linear group.*

Proof. Closure: $A, B \in \mathrm{GL}_n(\mathbb{R})$ clearly $AB \in M_n(\mathbb{R})$ and $\det(AB) = \det A \det B \neq 0$ so $AB \in \mathrm{GL}_n(\mathbb{R})$.
Identity:

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix} \in \mathrm{GL}_n(\mathbb{R})$$

Inverse: $\det A \neq 0$ implies A^{-1} exists and $\det(A^{-1}) = \frac{1}{\det A} \neq 0$.
Associative:

$$\begin{aligned} (A(BC))_{ij} &= A_{ix}(BC)_{xj} \\ &= A_{ix}B_{xt}C_{tj} \\ ((AB)C)_{ij} &= (AB)_{ix}C_{xj} \\ &= A_{it}B_{tx}C_{xj} \end{aligned}$$

□

Example. We have that

$$\mathrm{GL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}$$

and we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Proposition 9.

$$\det : \mathrm{GL}_n(\mathbb{R}) \to (\mathbb{R} \setminus \{0\}, \times) \qquad A \mapsto \det A$$

is a surjective group homomorphism.

Proof. Note $(\mathbb{R} \setminus \{0\}, \times)$ is a group. Determinant is clearly a map to $(\mathbb{R} \setminus \{0\}, \times)$. Need to check it's a group homomorphism

$$\det(AB) = \det A \cdot \det B$$

And we need to show that it is surjective, which follows because given $r \in (\mathbb{R} \setminus \{0\}, \times)$, let

$$A = \begin{pmatrix} r & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots 0 & 1 & \end{pmatrix} \in \mathrm{GL}_n(\mathbb{R})$$

and notice that $\det A = r$. □

By First Isomorphism Theorem

$$\mathrm{Ker}(\det) \trianglelefteq \mathrm{GL}_n(\mathbb{R})$$

and we can find that

$$\begin{aligned} \mathrm{Ker}(\det) &= \{A \in \mathrm{GL}_n(\mathbb{R}) : \det A = 1\} \\ &= \mathrm{SL}_n(\mathbb{R}) \end{aligned}$$

This is known as the *special linear group*. Furthermore, by First Isomorphism Theorem

$$\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong (\mathbb{R} \setminus \{0\}, \times).$$

Remark. More generally we can define the general linear group and special linear group over any field. Examples of fields: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{F}_p$ where

$$\mathbb{F}_p = (\{0, 1, 2, \dots, p-1\}, +_p, \times_p)$$

for some prime p. Note that $\mathrm{GL}_n(\mathbb{F}_p)$ and $\mathrm{SL}_n(\mathbb{F}_p)$ are finite groups.

What is $|\mathrm{GL}_3(\mathbb{F}_p)|$? Non-zero determinant means we need linearly independent columns. So the number of choices for first column is $p^3 - 1$ (any choice is fine except $(0, 0, 0)$). Second column is not a multiple of first, so number of choices for second column is $p^3 - p$. (Note that the zero vector is a multiple of the first column). Third column not in space spanned by first two columns, this space has size p^2 (consider $\alpha c_1 + \beta c_2$, $\alpha, \beta \in \mathbb{F}_p$). So number of choices for third column is $p^3 - p^2$. So

$$|\mathrm{GL}_3(\mathbb{F}_p)| = (p^3 - 1)(p^2 - p)(p^3 - p^2)$$

We can still consider

$$\det : \mathrm{GL}_3(\mathbb{F}_p) \to (\mathbb{F}_p \setminus \{0\}, \times) \qquad A \mapsto \det A$$

Note $(\mathbb{F}_p \setminus \{0\}, \times)$ is a group.

Proof. Closure, identity and associativity can all easily be verified. Let $a \in \mathbb{F}_p \setminus \{0\}$, by Bezout's Theorem, there exists x, y such that $ax + py = 1$. Then we have $ax \equiv 1 \pmod p$. Choose $\overline{x} \equiv x \pmod p$ with $1 \leq \overline{x} \leq p - 1$. So $a^{-1} \equiv x$. □

Determinant is a surjective homomorphism to $(\mathbb{F}_p \setminus \{0\}, \times)$ so by First Isomorphism Theorem:

$$|\mathrm{GL}_3(\mathbb{F}_p)|/|\mathrm{SL}_2(\mathbb{F}_p)| = p - 1$$

$$\implies |\mathrm{SL}_3(\mathbb{F}_p)| = \frac{(p^3-1)(p^2-p)(p^3-p^2)}{p-1}$$

Actions of $\mathrm{GL}_n(\mathbb{C})$

(i) Let $\mathbb{C}^n$ denote vectors of length n with entries in $\mathbb{C}$:

$$\mathrm{GL}_n(\mathbb{C}) \times \mathbb{C}^n \to \mathbb{C}^n \qquad (A, \mathbf{v}) \mapsto A\mathbf{v}$$

Note $I\mathbf{v} = \mathbf{v}$, $(AB)\mathbf{v} = A(B(\mathbf{v}))$. This action is faithful:

$$A\mathbf{v} = \mathbf{v}\ \forall \mathbf{v} \in \mathbb{C}^n \implies A = I_n$$

(consider multiplying A by $(1, 0, \ldots, 0)$, $(0, 1, \ldots, 0)$ etc) The action has two orbits:

$$\mathrm{Orb}_{\mathrm{GL}_n(\mathbb{C})}(\mathbf{0}) = \{\mathbf{0}\} \qquad \mathbf{0} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

and for $\mathbf{v} \neq 0$ we have:

$$\mathrm{Orb}_{\mathrm{GL}_n(\mathbb{C})}(\mathbf{v}) = \mathbb{C}^n \setminus \{\mathbf{0}\}$$

because given $\mathbf{w} \neq \mathbf{0}$ there exists $A \in \mathrm{GL}_n(\mathbb{C})$ such that $A\mathbf{v} = \mathbf{w}$.

(ii) Conjugation action of $\mathrm{GL}_n(\mathbb{C})$ on $M_n(\mathbb{C})$

$$\mathrm{GL}_n(\mathbb{C}) \times M_n(\mathbb{C}) \to M_n(\mathbb{C}) \qquad (P, A) \mapsto PAP^{-1}$$

Note:

$$\begin{aligned} PQ(A) &= PQA(PQ)^{-1} \\ &= PQAQ^{-1}P^{-1} \\ &= P(Q(A)) \end{aligned}$$

Remark. Matrices A and B are conjugate if they represent the same linear map. If $PAP^{-1} = B$, then P represents a change of basis matrix (see linear algebra next year). For example

$$e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$A : e_1 \mapsto 2e_1 \qquad e_2 \mapsto 3e_2$$

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$$

Let

$$P : e_1 \mapsto e_2, \quad e_2 \mapsto e_1$$

change of basis

$$P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = p^{-1}$$

Then

$$\begin{aligned} PAP^{-1} &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 3 \\ 2 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix} \end{aligned}$$

i.e. $e_2 \mapsto 3e_2$ and $e_1 \mapsto 2e_1$. We will use the following result from Vectors and Matrices when investigating Möbius groups.

Result. Let $A \in M_2(\mathbb{C})$ and consider conjugation action of $\mathrm{GL}_2(\mathbb{C})$ on $M_2(\mathbb{C})$. Then precisely one of the following occurs:

(i) the orbit of A contains a diagonal matrix

$$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$$

with $\lambda \neq \mu$.

(ii) the orbit of A is

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} = \lambda I$$

for some λ.

(iii) the orbit of A contains a matrix

$$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$$

for some λ.

Proof. See Vectors and Matrices but essentially

(i) In this case A has 2 distinct eigenvalues $\lambda \neq \mu$, take a basis consisting of an eigenvector for λ and an eigenvector for μ. Distinct pairs give distinct orbits.

(ii) $A = \lambda I$, eigenvalues λ, λ, 2 linearly independent eigenvectors.

(iii) In this case A has a repeated eigenvalue, but just one linearly independent eigenvector.

□

Recall if $A \in M_(\mathbb{R})$, $A^\top$ is defined by $(A^\top)_{ij} = A_{ji}$, i.e. the ij-th entry of $A^\top$ is ji-th entry of A:

$$A = \begin{pmatrix} 2 & 4 \\ 3 & 5 \end{pmatrix} \qquad A^\top = \begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix}$$

Note. (i) We have $(AB)^\top = B^\top A^\top$ because

$$[(AB)^\top]_{ij} = (AB)_{ji} = AjkB_{ki}$$

$$[B^\top A^\top]_{ij} = B^\top_{ik} A^\top_{kj} = B_{ki} A_{jk}$$

(ii) $AA^\top = I \iff A^\top A = I$ and hence

$$A^\top A = A^{-1} A A^\top A = A^{-1} A = I$$

(iii) $(A^\top)^{-1} = (A^{-1})^\top$ since

$$\begin{aligned} I_n &= (AA^{-1})^\top \\ &= (A^{-1})^\top A^\top \end{aligned}$$

(iv) $\det(A^\top) = \det A$.

$$\mathrm{O}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : A^\top A = I\}$$

(So columns of A form an orthonormal basis for $\mathbb{R}^n$).

Proposition 10. $\mathrm{O}_n(\mathbb{R})$ is a subgroup of $\mathrm{GL}_n(\mathbb{R})$ called the *orthogonal group.*

Proof.

$$\begin{aligned} 1 &= \det(A^\top A) \\ &= \det(A^\top)\det(A) \\ &= (\det A)^2 \\ \implies \det A & \\ &\neq 0 \end{aligned}$$

Hence $\mathrm{O}_n(\mathbb{R})$ is a subset of $\mathrm{GL}_n(\mathbb{R})$; associativity is inherited.

- $I_n = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix} \in \mathrm{O}_n(\mathbb{R})$
- closure: $A, B \in \mathrm{O}_n(\mathbb{R})$,

$$\begin{aligned} (AB)^\top (AB) &= B^\top A^\top AB \\ &= B^\top B \\ &= I \\ \implies B &\in \mathrm{O}_n(\mathbb{R}) \end{aligned}$$

- inverse: $A^\top A = I_n \implies A^\top = A^{-1}$ and $A^\top \in \mathrm{O}_n(\mathbb{R})$ since $(A^\top)^\top = A$ and $AA^\top = I$.

□

Note $1 = (\det A)^2 \implies \det A = \pm 1$ if $A \in \mathrm{O}_n(\mathbb{R})$. So, $\mathrm{Det} : \mathrm{O}_n(\mathbb{R}) \to (\{\pm 1\}, \times)$, $A \mapsto \det A$ is a surjective homomorphism, as

$$\begin{pmatrix} -1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \in \mathrm{O}_n(\mathbb{R})$$

So

$$\mathrm{Ker}(\mathrm{Det}) = \{A \in \mathrm{O}_n(\mathbb{R}) : \det A = 1\} = \mathrm{SO}_n(\mathbb{R}) \trianglelefteq \mathrm{O}_n(\mathbb{R})$$

By First Isomorphism Theorem:

$$\mathrm{O}_n(\mathbb{R})/\mathrm{SO}_n(\mathbb{R}) \cong C_2$$

Lemma 20. Let $A \in \mathrm{O}_n(\mathbb{R})$ and $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$. Then

(i) $A\mathbf{x} \cdot A\mathbf{y} = \mathbf{x} \cdot \mathbf{y}$

(ii) $|A\mathbf{x}| = |\mathbf{x}|$

So A is an isometry (distance preserving map) of Euclidean space $\mathbb{R}^n$.

Proof.

(i)
$$\begin{aligned} A\mathbf{x} \cdot A\mathbf{y} &= (A\mathbf{x})^\top (A\mathbf{y}) \\ &= \mathbf{x}^\top A^\top A\mathbf{y} \\ &= \mathbf{x}^\top \mathbf{y} \\ &= \mathbf{x} \cdot \mathbf{y} \end{aligned}$$

(ii)
$$|A\mathbf{x}|^2 = A\mathbf{x} \cdot A\mathbf{x} = \mathbf{x} \cdot \mathbf{x} = |\mathbf{x}|^2$$

□

Note by (ii) if λ an eigenvalue of A, then $A\mathbf{x} = \lambda\mathbf{x}$

$$\implies |\lambda\mathbf{x}| = |\mathbf{x}|$$

i.e. $|\lambda| = 1$.

In 2 dimensions

Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$$

$$I = AA^\top = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

$$\implies 1 = a^2 + b^2 = c^2 + d^2$$

$$0 = ac + bd.$$

$$I = A^\top A = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$\implies 1 = a^2 + c^2 = b^2 + d^2$$

$$0 = ab + cd$$

For $0 \leq \theta < 2\pi$ let

$$\begin{pmatrix} a \\ c \end{pmatrix} = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix} \qquad \text{so} \qquad \begin{pmatrix} b \\ d \end{pmatrix} = \pm \begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix}$$

<u>First case</u>:

$$A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

$\det A = 1$

$$A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cos\theta x & -\sin\theta y \\ \sin\theta x & \cos\theta y \end{pmatrix}$$

A represents a rotation.
Let $z = x + iy$ then

$$e^{i\theta} z = (\cos\theta x - \sin\theta y) + i(\sin\theta x + \cos\theta y)$$

All elements of $\mathrm{SO}_2(\mathbb{R})$ are of this form.

<u>Second case</u>

$$A = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$$

$\det A = -1$

$$A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cos\theta x & \sin\theta y \\ \sin\theta x & -\cos\theta y \end{pmatrix}$$

$$e^{i\theta} \overline{z} = (\cos\theta x + \sin\theta y) + i(\sin\theta x - \cos\theta y)$$

What are the fixed points?

$$\begin{aligned} z = e^{i\theta}\overline{z} &\iff e^{-\theta/2}z = e^{i\theta/2}\overline{z} \\ &\iff e^{-i\theta/2}z = t \in \mathbb{R} \\ &\iff z = e^{i\theta/2}t \end{aligned}$$

hence a reflection in line $te^{i\theta/2}$.
All elements of $\mathrm{O}_2(\mathbb{R}) \setminus \mathrm{SO}_2(\mathbb{R})$ are of this form.

So,

$$\mathrm{O}_2(\mathbb{R}) = \mathrm{SO}_2(\mathbb{R}) \cup \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \mathrm{SO}_2(\mathbb{R})$$

Note any element of $\mathrm{O}_2(\mathbb{R})$ is a product of at most two reflections. Since if $A \in \mathrm{SO}_2(\mathbb{R})$ then

$$A = \left(A \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

3 dimensions

Proposition 11. Let $A \in \mathrm{SO}_3(\mathbb{R})$. Then A has an eigenvector with eigenvalue 1.

Proof.

$$\begin{aligned} \det(A - I) &= \det(A - AA^\top) \\ &= \det A \det(I - A^\top) \\ &= \det((I - A)^\top) \\ &= \det(I - A) \\ &= (-1)^3 \det(A - I) \\ &= -\det(A - I) \end{aligned}$$

hence $\det(A - I) = 0$ and A has eigenvalue 1. □
Alternatively consider $\chi_A(x)$ the characteristic polynomial of A, it is a cubic in $\mathbb{R}$. Thus has a real root, $\lambda = 1$ or $\lambda = -1$. But the other eigenvalues are either a complex conjugate pair, then $\lambda = 1$ or all are real either $1, -1, -1$ or $1, 1, 1$.

Theorem 11. Let $A \in \mathrm{SO}_3(\mathbb{R})$ then A Is conjugate to a matrix of the form

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

for some $\theta \in [0, 2\pi]$. In particular, A is a rotation round an axis through the origin.

Proof. By proposition 11, there is a $\mathbf{v} \in \mathbb{R}^3$ with $A\mathbf{v} = \mathbf{v}$, and we can assume $|\mathbf{v}| = 1$. Let $\{e_1, e_2, e_3\}$ be the standard orthonormal basis for $\mathbb{R}^3$. There exists $P \in \mathrm{SO}_3(\mathbb{R})$ such that $P\mathbf{v} = e_3$. So $PAP^{-1}(e_3) = e_3$ and for π plane perpendicular to e_3 then $PAP^{-1}(\pi)$ perpendicular to e_3. So,

$$PAP^{-1} = \left(\begin{array}{cc|c} \multicolumn{2}{c|}{\text{action on } \pi} & \begin{matrix} 0 \\ 0 \end{matrix} \\ \hline 0 & 0 & 1 \end{array}\right) = \left(\begin{array}{cc|c} \multicolumn{2}{c|}{Q} & \begin{matrix} 0 \\ 0 \end{matrix} \\ \hline 0 & 0 & 1 \end{array}\right)$$

$\det PAP^{-1} = \det A = 1$, so $\det Q = 1$, $Q^\top Q = I$. So

$$Q = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

for some θ as required. □

Suppose $\mathbf{r}$ is a reflection in a plane π through 0. Let $\mathbf{n}$ be unit vector perpendicular to π. Then

$$r(\mathbf{x}) = \mathbf{x} - 2(\mathbf{x} \cdot \mathbf{n})\mathbf{n}$$

$$\mathbf{n} \mapsto -\mathbf{n}$$

π fixed. So $\mathbf{r}$ is conjugate to

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{O}_3(\mathbb{R})$$

$$\mathrm{O}_3(\mathbb{R}) = \mathrm{SO}_3(\mathbb{R}) \cup \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mathrm{SO}_3(\mathbb{R})$$

Theorem 13. Any element of $\mathrm{O}_3(\mathbb{R})$ is a product of at most 3 reflections.

Proof. Let $\{e_1, e_2, e_3\}$ be standard orthonormal basis for $\mathbb{R}^3$. Let $A \in \mathrm{O}_3(\mathbb{R})$. Then

$$|Ae_3| = |e_3| = 1,$$

since A is an isometry. So there exists a reflection r_1 such that

$$r_1 A(e_3) = e_3.$$

Let $\pi = \langle e_1, e_2 \rangle$ (the plane perpendicular to e_3). Then $r_1 A(\pi) = \pi$. There exists a reflection r_2 such that

$$r_2(e_3) = e_3, \qquad r_2(r_1 A(e_2)) = e_2.$$

So $r_2 r_1 A$ fixes e_2 and e_3. So $r_2 r_1 A(e_1) = \pm e_1$. If $e_1 = e_1$, set $r_3 = \text{id}$. If $e_1 = -e_1$, let r_3 be reflection in plane perpendicular to e_1. So $r_3 r_2 r_1 A$ fixes e_1, e_2, e_3, so

$$r_3 r_2 r_1 A = \text{id}$$
$$\implies A = r_1^{-1} r_2^{-1} r_3^{-1} = r_1 r_2 r_3.$$

□

Alternatively, any element in $\mathrm{S0}_2(\mathbb{R})$ is a product of at most 2 reflections, via 2-dimensional case. Thus any element of

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mathrm{SO}_3(\mathbb{R})$$

is a product of at most 3 reflections. Note we do need 3, for example consider

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

8 Möbius Groups

A Möbius transformation (or map) is a function of a complex variable z that can be written in the form

$$f(z) = \frac{az+b}{cz+d}$$

for some $a, b, c, d \in \mathbb{C}$ with $ad - bc \neq 0$. Why $ad - bc \neq 0$?

$$f(z) - f(w) = \frac{(ad-bc)(z-w)}{(cz+d)(cw+d)}.$$

So, $ad - bc = 0$ implies f constant (not interesting), and $ad - bc \neq 0$ implies f injective.
When does $f(z) = g(z)$?
Suppose there exists at least 3 values of z in $\mathbb{C}$ such that

$$\frac{az+b}{cz+d} = \frac{\alpha z+\beta}{\gamma z+\delta}$$

$ad - bc \neq 0$, $\alpha\delta - \beta\gamma \neq 0$. Then there exists $\lambda \neq 0$, $\lambda \in \mathbb{C}$ such that

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \lambda \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Since, we have 3 distinct values of z for which

$$(az+b)(\gamma z+\delta) = (\alpha z+\beta)(cz+d)$$

so these quadratics are identical. Hence

$$a\gamma = \alpha c, \qquad b\delta = \beta d$$

$$a\delta + b\gamma = \alpha d + \beta c$$

Let $\mu = a\delta - \beta c = \alpha d - b\gamma$ (so $\mu^2 = (ad-bc)(\alpha\delta - \beta\gamma) \neq 0$). Then

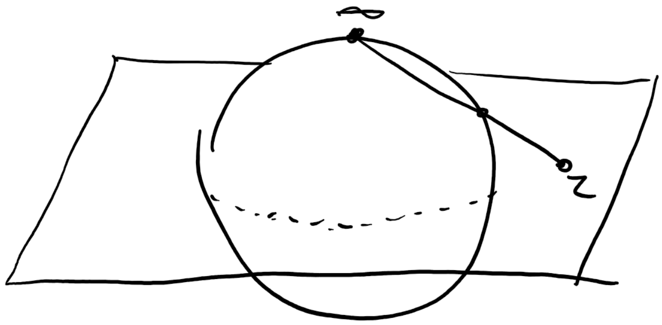
$$\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \mu & 0 \\ 0 & \mu \end{pmatrix}$$

$$\implies \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \frac{\mu}{ad-bc} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Problem: f is not defined at $z = -\frac{d}{c}$. We would like $f\left(-\frac{d}{c}\right) = \infty$. We consider f defined on $\mathbb{C} \cup \{\infty\} = \mathbb{C}_\infty$, the extended complex plane. So if

$$f(z) = \frac{az+b}{cz+d},$$

domain is now $\mathbb{C}_\infty$; $c \neq 0$; $f(\infty) = \frac{a}{c}$, $f\left(-\frac{d}{c}\right) = \infty$. For $c = 0$; $f(\infty) = \infty$.



(Riemann Sphere and stereographic projection.)

Theorem 14. The set $\mathcal{M}$ of all Möbius maps on $\mathbb{C}_\infty$ is a group under composition. It is a subgroup of $\mathrm{Sym}(\mathbb{C}_\infty)$.

Proof.

- composition of maps is associative
- $I(z) = z \in \mathcal{M}$.
- closure: Let
$$f(z) = \frac{az+b}{cz+d}, \qquad g(z) = \frac{\alpha z+\beta}{\gamma z+\delta}$$
Suppose $c \neq 0$, $\delta \neq 0$. First suppose $z \in \mathbb{C} \setminus \{-\delta/\gamma\}$. Then
$$\begin{aligned} f(g(z)) &= \frac{a\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right)+b}{c\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right)+d} \\ &= \frac{(a\alpha+b\gamma)z+(a\beta+b\delta)}{(c\alpha+d\gamma)+(c\beta+\delta d)} \in \mathcal{M} \end{aligned}$$
since
$$(a\alpha+b\gamma)(c\beta+\delta d)-(a\beta+b\delta)(c\alpha+d\gamma) = (ad-bc)(\alpha\delta-\beta\gamma) \neq 0.$$
Also, $f\left(g\left(-\frac{\delta}{\gamma}\right)\right) = f(\infty) = \frac{a}{c}$. And
$$\begin{aligned} \frac{(a\alpha+b\gamma)\left(-\frac{\delta}{\gamma}\right)+(a\beta+b\delta)}{(c\alpha+d\gamma)\left(-\frac{\delta}{\gamma}\right)+(c\beta+\delta d)} &= \frac{a\alpha\left(-\frac{\delta}{\gamma}\right)+\alpha\beta}{c\alpha\left(-\frac{\delta}{\gamma}\right)+c\beta} \\ &= \frac{a}{c} \end{aligned}$$
Need to check $c = 0$ separately.

- inverses: For some a, b, c, d with $ad - bc \neq 0$, let

$$f(z) = \frac{az+b}{cz+d} \qquad \text{and} \qquad f^*(z) = \frac{dz-b}{-cz+a}$$

Then $f(f^*(z)) = z = f^*(f(z))$ for $z \neq -\frac{d}{c}, -\frac{a}{c}, \infty$. These are cases are ok. If $c = 0$ then

$$f(f^*(\infty)) = f(\infty = \infty = f^*(f(\infty)).$$

□

Theorem 15.

$$\frac{\mathrm{GL}_2(\mathbb{C})}{Z} \cong \mathcal{M}$$

where

$$Z = \{\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \lambda \in \mathbb{C} \setminus \{0\}\}.$$

Proof. We construct a surjective homomorphism from $\mathrm{GL}_2(\mathbb{C})$ onto $\mathcal{M}$ with kernel Z. Let $\phi : \mathrm{GL}_2(\mathbb{C}) \to \mathcal{M}$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto f(z) = \frac{az+b}{cz+d}.$$

Note ϕ a homomorphism:

$$f(z) = \frac{az+b}{cz+d}, \qquad g(z) = \frac{\alpha z+\beta}{\gamma z+\delta}.$$

$$\begin{aligned}
\phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)\phi\left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\right)(z) &= f \circ g(z) \\
&= \frac{(a\alpha + b\gamma)z + (a\beta + b\delta)}{(c\alpha + d\gamma)z + (c\beta + \delta d)} \\
&= \phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\right)
\end{aligned}$$

Clearly ϕ surjective.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Ker}\ \phi$$

if and only if $\frac{az+b}{cz+d} = z\ \forall\ z \in \mathbb{C}_\infty$. Note

$$z = \infty \implies c = 0$$

$$z = 0 \implies b = 0$$

$$z = 1 \implies a = d$$

$$\implies \mathrm{Ker}\ \phi = z$$

Finally apply First Isomorphism Theorem. □

Corollary 7.

$$\frac{\mathrm{SL}_2(\mathbb{C})}{\{\pm I\}} \cong \mathcal{M}.$$

Proof. Restrict ϕ to $\mathrm{SL}_2(\mathbb{C})$

$$\phi : \mathrm{SL}_2(\mathbb{C}) \to \mathcal{M}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \frac{az+b}{cz+d}.$$

We require ϕ to be surjective:

$$f(z) = \frac{az+b}{cz+d} = \frac{\left(\frac{a}{(ad-bc)^{1/2}}\right) z + \frac{b}{(ad-bc)^{1/2}}}{\left(\frac{c}{(ad-bc)^{1/2}}\right) z + \frac{d}{(ad-bc)^{1/2}}}.$$

And Ker $\phi = \{\pm I\}$. □

Proposition 13. Every Möbius map can be written as a somposition of maps of the following forms:

(i) $z \mapsto az$, $a \neq 0$; represents a dilation or rotation

(ii) $z \mapsto z + b$; a translation

(iii) $z \mapsto \frac{1}{z}$; inversion.

Proof. Let $f(z) = \frac{az+b}{cz+d}$. If $c = 0$;

$$z \mapsto \left(\frac{a}{d}\right) z \to\mapsto \left(\frac{a}{d}\right) z + \left(\frac{b}{d}\right)$$

f_1 is type (i), f_2 is type (ii). We can write $f = f_2 \circ f_1$. If $c \neq 0$, write

$$\begin{aligned} f(z) &= \frac{az+b}{cz+d} \\ &= \frac{\left(\frac{a}{c}\right) z + \left(\frac{b}{c}\right)}{z + \left(\frac{d}{c}\right)} \\ &= \frac{a}{c} + \frac{\left(\frac{-ad+bc}{c^2}\right)}{\left(z + \frac{d}{c}\right)} \\ &= A + \frac{B}{z + \frac{d}{c}} \end{aligned}$$

$$z \overset{\text{(ii)}}{\mapsto} z + \frac{d}{c} \overset{\text{(iii)}}{\mapsto} \frac{1}{z + \frac{d}{c}} \overset{\text{(i)}}{\mapsto} \frac{B}{z + \frac{d}{c}} \overset{\text{(ii)}}{\mapsto} A + \frac{B}{z + \frac{d}{c}}.$$

Now we can write $f = f_4 \circ f_3 \circ f_2 \circ f_1$. □

Definition 22. A group G acts *triply transitively* on a set X if given $x_1, x_2, x_3 \in X$ all distinct and $y_1, y_2, y_3 \in X$ all distinct, there exists $g \in G$ such that $g(x_i) = y_i$, for $i = 1, 2, 3$.
A group G acts *sharply triply transitively* if such a g is unique.

Theorem 16. The action of $\mathcal{M}$ on $\mathbb{C}_\infty$ is sharply triply transitive.

Proof. Label first triple $\{z_0, z_1, z_\infty\}$ and second triple $\{\omega_0, \omega_1, \omega_\infty\}$. We construct $g \in \mathcal{M}$ such that

$$\begin{aligned} g : z_0 &\mapsto 0 \\ z_1 &\mapsto 1 \\ z_\infty &\mapsto \infty \end{aligned}$$

First suppose $z_0, z_1, z_\infty \neq \infty$

$$g(z) = \frac{(z - z_0)(z_1 - z_\infty)}{(z - z_\infty)(z_1 - z_0)}$$

check: "$ad - bc$" $= (z_0 - z_\infty)(z_1 - z_\infty)(z_1 - z_0) \neq 0$. If $z_\infty = \infty$:

$$g(z) = \frac{(z - z_0)}{(z_1 - z_0)}$$

If $z_1 = \infty$:

$$g(z) = \frac{(z - z_0)}{(z - z_\infty)}$$

If $z_0 = \infty$:

$$g(z) = \frac{(z_1 - z_\infty)}{(z - z_\infty)}.$$

Similarly find h such that

$$\begin{aligned} h : \omega_0 &\mapsto 0 \\ \omega_1 &\mapsto 1 \\ \omega_\infty &\mapsto \infty \end{aligned}$$

Then $f = h^{-1}g : z_i \mapsto \omega_i$ as required. Now to prove uniqueness. Suppose $f' : z_i \mapsto \omega_i$. Then $f^{-1}f' : z_i \mapsto z_i$. Let g be as above, then

$$\begin{aligned} gf^{-1}f'g^{-1} : 0 \mapsto 0 &\implies b = 0 \\ 1 \mapsto 1 &\implies a = d \\ \infty \mapsto \infty &\implies c = 0 \end{aligned}$$

$$
\begin{aligned}
\implies gf^{-1}f'g^{-1} &= \mathrm{id} \\
\implies f^{-1}f' &= \mathrm{id} \\
\implies f &= f'.
\end{aligned}
$$

$\square$

So, the image of just three points determines the map.

Conjugacy classes in $\mathcal{M}$

Recall $\phi : \mathrm{GL}_2(\mathbb{C}) \twoheadrightarrow \mathcal{M}$. Suppose A, B conjugate in $\mathrm{GL}_2(\mathbb{C})$, i.e. there exists $P \in \mathrm{GL}_2(\mathbb{C})$ such that

$$PAP^{-1} = B$$

then

$$
\begin{aligned}
\phi(P)\phi(A)\phi(P)^{-1} &= \phi(PAP^{-1}) \\
&= \phi(B) \in \mathcal{B}
\end{aligned}
$$

i.e. $\phi(A)$ and $\phi(B)$ are conjugate in $\mathcal{M}$. Use knowledge of conjugacy classes in $\mathrm{GL}_2(\mathbb{C})$.

(i) For some $\lambda \neq \mu$, $\lambda \neq 0 \neq \mu$

$$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$$

$$\phi\left(\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}\right) = f$$

$f(z) = \nu z$, $\nu \neq 0, 1$.

(ii) For some $\lambda \neq 0$,

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$$

$$\phi\left(\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}\right) = \mathrm{id}.$$

(iii) For some $\lambda \neq 0$,

$$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$$

$$\phi\left(\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}\right) = f$$

$f(z) = \frac{\lambda z + 1}{\lambda} = z + \frac{1}{\lambda}$, i.e.

$$f = \phi\left(\begin{pmatrix} 1 & \frac{1}{\lambda} \\ 0 & 1 \end{pmatrix}\right)$$

And it's conjugate to

$$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} = \begin{pmatrix}\lambda & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & \frac{1}{\lambda}\\ 0 & 1\end{pmatrix}\begin{pmatrix}\frac{1}{\lambda} & 0\\ 0 & 1\end{pmatrix}$$

So f conjugate to g where $g(z) = z + 1$.

Theorem 17. Any non-identity Möbius map is conjugate to one of

(i) $z \mapsto \nu z$, $\nu \neq 0, 1$

(ii) $z \mapsto z + 1$.

Corollary 8. A non-identity Möbius map f has either

(i) 2 fixed points or

(ii) 1 fixed point.

Proof. Suppose $gfg^{-1} = h$. Then α is a fixed point of f (i.e. $f(\alpha) = \alpha$) if and only if $g(\alpha)$ is a fixed point of h (i.e. $h(g(\alpha)) = g(\alpha)$). So number of fixed points of f is the same as the number of fixed points of h. By Theorem 17 either,

- f conjugate to $z \mapsto \nu z$ which has 2 fixed points: 0, ∞.
- or f conjugate to $z \mapsto z + 1$ which has 1 fixed points; ∞.

□

8.1 Circles in $\mathbb{C}_\infty$

A Euclidean circle is the set of points in $\mathbb{C}$ given by some equation

$$|z - z_0| = r, \qquad r > 0.$$

A Euclidean line is the set of points in $\mathbb{C}$ given by some equation

$$|z - a| = |z - b|$$

A *circle in* $\mathbb{C}_\infty$ is either a Euclidean circle or a set $L \cup \{\infty\}$ where L is a Euclidean line. Its general equation is of the form

$$Az\overline{z} + B\overline{z} + \overline{B}z + C = 0$$

for some $A, C \in \mathbb{R}$, $|B|^2 > AC$. Where $z = \infty$ is a solution if and only if $A = 0$.

- $A = 0$: line
- $C = 0$: goes through origin

There is a unique circle passing through any 3 distinct points in $\mathbb{C}_\infty$.

Theorem. Let $f \in \mathcal{M}$ and C a circle in $\mathbb{C}_\infty$, then $f(C)$ is a circle in $\mathbb{C}_\infty$.

Proof. By proposition 13, just need to consider $f(z) = az$, $z + b$ or $\frac{1}{z}$. Let $S_{A,B,C}$ be circle defined by $(*)$. Then

$$f(z) = az : S_{A,B,C} \mapsto S_{A/a\bar{a},B/\bar{a},C}$$

$$f(z) = z + b : S_{A,B,C} \mapsto S_{A,B-Ab,C+Ab\bar{b}-\overline{B}b-B\bar{b}}$$

$$f(z) = \frac{1}{z} := \omega : S_{A,B,C} \mapsto A + B\omega + B\omega + \overline{B}\overline{\omega} + C\omega\overline{\omega} = 0 = S_{C,\overline{B},A}$$

□

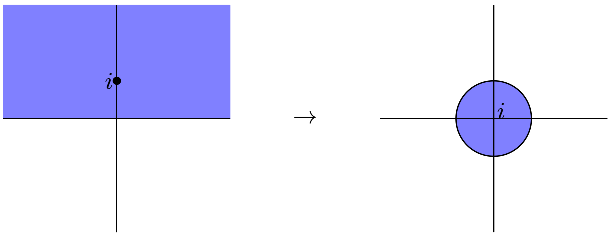
e.g. Consider the image of $\mathbb{R} \cup \{\infty\}$ under

$$f(z) = \frac{z - i}{z + i}.$$

It is a circle in $\mathbb{C}_\infty$ containing

$$f(0) = -1, f(\infty) = 1, f(1) = -i$$

So $f(\mathbb{R} \cup \{\infty\}) =$ unit circle. Furthermore, complimentary components are mapped to complimentary components.



8.2 Cross-Ratios

Definition 23. The cross-ratio of distinct points $z_1, z_2, z_3, z_4 \in \mathbb{C}$ is defined by

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

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

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

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

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

Note $[0, 1, \omega, \infty] = \omega$.

Notation. Different authors use different permutations of 1, 2, 3, 4 as definition.

Theorem. Given $z_1, z_2, z_3, z_4 \in \mathbb{C}_\infty$ distinct and $\omega_1, \omega_2, \omega_3, \omega_4 \in \mathbb{C}_\infty$ distinct then there exists $f \in \mathcal{M}$ such that $f(z_i) = f(\omega_i)$ if and only if

$$[z_1, z_2, z_3, z_4] = [\omega_1, \omega_2, \omega_3, \omega_4].$$

In particular, Möbius maps preserve cross-ratios

$$[z_1, z_2, z_3, z_4] = [f(z_1), f(z_2), f(z_3), f(z_4)].$$

Proof. For the forward direction, suppose $f(z_j) = \omega_j$ and $z_i, \omega_i \neq \infty$ for all i and

$$f(z) = \frac{az + b}{cz + d}$$

then $cz_j + d \neq 0 \forall j$. So

$$\begin{aligned} \omega_j - \omega_k &= f(z_j) - f(z_k) \\ &\quad + \frac{(ad - bc)(z_j - z_k)}{(cz_j + d)(cz_k + d)} \\ \implies [z_1, z_2, z_3, z_4] &= [\omega_1, \omega_2, \omega_3, \omega_4] \\ &= [f(z_1), f(z_2), f(z_3), f(z_4)] \end{aligned}$$

Need to check other cases; $z_i = \infty$, $\omega_i = f(\infty = \frac{a}{c}$ etc.
For the other direction, suppose that

$$[z_1, z_2, z_3, z_4] = [\omega_1, \omega_2, \omega_3, \omega_4]$$

Let $g \in \mathcal{M}$ such that $g(z_1) = 0$, $g(z_2) = 1$ and $g(z_4) = \infty$. Let $h \in \mathcal{M}$ such that $h(\omega_1) = 0$, $h(\omega_2) = 1$, $h(\omega_4) = \infty$. Then

$$\begin{aligned} g(z_3) &= [0, 1, g(z_3), \infty] \\ &= [g(z_1), g(z_2), g(z_3), g(z_4)] \\ &= [z_1, z_2, z_3, z_4] \\ &= [\omega_1, \omega_2, \omega_3, \omega_4] \\ &= [h(\omega_1), h(\omega_2), h(\omega_3), h(\omega_4)] \\ &= [0, 1, h(\omega), \infty] && = h(\omega_3) \end{aligned}$$

So $h^{-1}g$ is the required map. □
So $[z_1, z_2, z_3, z_4] = f(z_3)$ where f is the unique Möbius map that sends $z_1 \mapsto 0$, $z_2 \mapsto 1$, $z_4 \mapsto \infty$.

Corollary. z_1, z_2, z_3, z_4 lie in some circle in $\mathbb{C}_\infty$ if and only if $[z_1, z_2, z_3, z_4] \in \mathbb{R}$.

Proof. C circle through z_1, z_2, z_4, Let $g : C \to \mathbb{R} \cup \{\infty\}$,

$$g(z_1) = 0, g(z_2) = 1, g(z_4) = \infty$$

$$\begin{aligned} g(z_3) &= [0, 1, g(z_3), \infty] \\ &= [g(z_1), g(z_2), g(z_3), g(z_4)] \\ &= [z_1, z_2, z_3, z_4] \end{aligned}$$

By Theorem 19. So

$$[z_1, z_2, z_3, z_4] \in \mathbb{R} \iff g(z_3) \in \mathbb{R} \iff z_3 \in C.$$

□

THE END