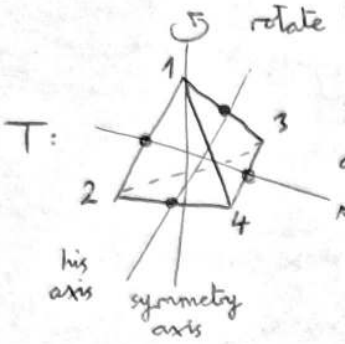
L1.1

Groups

by Oscar Randal-Williams (Notes on his website)

T:



rotate by $0°, \underbrace{120°}_{r}, 240°$

axis through middle of edges

$\circlearrowright 0°, \underbrace{180°}_{s}$

How many rotational symmetries?

1 trivial rotation ($0°$ about ~~any~~ axis)

2×4 symmetry axis rotations

3 blue (midde) rotations

---

12 rotational symmetries

How does r move the vertices?

$1 \to 1$
$2 \to 4$
$3 \to 2$
$4 \to 3$

How does s move the vertices?

$1 \to 3$
$2 \to 4$ (on his drawing)
$3 \to 1$
$4 \to 2$

mine is $1 \leftrightarrow 2$, $3 \leftrightarrow 4$

First r, then s:

$1 \to 1 \to 3$
$2 \to 4 \to 2$
$3 \to 2 \to 4$
$4 \to 3 \to 1$

is a rotation in the axis through the vertex 2

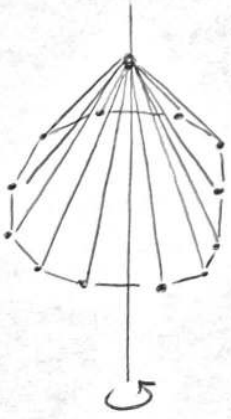
First do s, then r

$1 \to 3 \to 2$
$2 \to 4 \to 3$
$3 \to 1 \to 1$
$4 \to 2 \to 4$

is a rotation in the axis through the vertex 4

Note: $rs \neq sr$

P:



12-sided pyramid

rotate by $0°, 30° = \frac{360°}{12}, 60°, 90°, \ldots, 300°, 330°$

P has 12 rotational symmetries, too

Differences
↓ ↓

L1.2 i) In the symmetries of P, the order we apply the symmetries does not matter:

$$\begin{aligned}(\text{rot. by } a^\circ)\circ(\text{rot. by } b^\circ) &= \text{rot. by } (a+b)^\circ \\ &= \text{rot. by } (b+a)^\circ \\ &= (\text{rot. by } b^\circ)\circ(\text{rot. by } a^\circ)\end{aligned}$$

ii) Symmetries of T repeated 2 or 3 times "do nothing".
Symmetries of C need not (e.g. rot. by 30°).

Groups A set X is a collection of things.
Write $x \in X$ to mean "x is one of the things in X".

$2 \in \mathbb{N}$ $\sqrt{2} \in \mathbb{R}$ $i \notin \mathbb{R}$

A function f from a set X to a set Y is a thing which to each element (x) of X gives us an element ($f(x)$) of Y.
Write $f: X \to Y$.

If X and Y are sets, $X \times Y$ is the set consisting of pairs (x, y) with $x \in X$ and $y \in Y$.

Def^n a binary operation on a set X is a function

$$\cdot : X \times X \to X.$$

Def^n a group is a triple $(G, \cdot, e)$ of a set G, a binary operation $\cdot$, and an element $e \in G$ such that

(G1) $\forall\, a,b,c \in G$, $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ ASSOCIATIVITY

(G2) $\forall\, a \in G$, $a\cdot e = a = e\cdot a$ IDENTITY

(G3) $\forall\, a \in G$, $\exists\, b \in G$ s.t. $a\cdot b = e$ INVERSE

Observations: axiom (G1) says that we do not need to worry about bracketing when multiplying many elements together

$$(a\cdot(b\cdot c))\cdot d = ((a\cdot b)\cdot c)\cdot d = (a\cdot b)\cdot(c\cdot d) = a\cdot(b\cdot(c\cdot d)) = a\cdot b\cdot c\cdot d$$

this can be proved by induction

$(((\cdots)))\cdot(((\cdots)))$

do this ↑ w/ induction

then use associativity to get $((((\cdots))))$

Theorem: Let $(G, \cdot, e)$ be a group

i) if $a, b \in G$ satisfy $a \cdot b = e$, then $b \cdot a = e$.

ii) if $a \in G$ then $e \cdot a = a$.

iii) if $b, b' \in G$ s.t. $a \cdot b = e$ and $a \cdot b' = e$ then $b' = b$.

iv) if $e' \in G$ is s.t. $a \cdot e' = a$ for some $a \in G$, then $e' = e$.

Proof: i) $baba = bea = ba$ using $ab = e$

$\Rightarrow baba(ba)^{-1} = ba(ba)^{-1}$

$\Rightarrow bae = e$

$\Rightarrow ba = e$. □

ii) $ea = (aa^{-1})a = a(a^{-1}a)$

$= ae = a$. □

iii) $b' = b'e = b'ab = eb = b$. □

iv) $ae' = a = ae$

$\Rightarrow a^{-1}ae' = a^{-1}ae$

$\Rightarrow ee' = ee$

$\Rightarrow e' = e$. □

L2.1

Proof i) Preliminary calculation $b = b \cdot e$ by G2

$= b \cdot (a \cdot b)$ by assumption

$= (b \cdot a) \cdot b$ by G1

Now: apply G3 to b, gives $c \in G$ s.t. $e = b \cdot c$

$= ((b \cdot a) \cdot b) \cdot c$ by the above

$= (b \cdot a) \cdot (b \cdot c)$ by G1

$= (b \cdot a) \cdot e$ as $b \cdot c = e$

$= b \cdot a$ by G2

ii) Let $a \in G$. By (G3) there is a $b \in G$ s.t. $a \cdot b = e$

but then by part i), we also have $b \cdot a = e$.

$e \cdot a = (a \cdot b) \cdot a$ as $a \cdot b = e$

$= (a) \cdot (b \cdot a)$ by G1

$= a \cdot e$ by assumption

$= a$ by G2

iii) Suppose $a \cdot b = e$ and $a \cdot b' = e$, so by part i)

also have $b \cdot a = e$. So

$b' = e \cdot b'$ by part ii)

$= (b \cdot a) \cdot b'$ by assumption

$= b \cdot (a \cdot b')$ by G1

$= b \cdot e$ by assumption

$= b$ by G2

iv) for $a \in G$ by G3 have a $b \in G$ s.t. $a \cdot b = e$

and by part i) also $b \cdot a = e$, so

$e = b \cdot a$ by assumption

$= b \cdot (a \cdot e')$ by assumption

$= (b \cdot a) \cdot e'$ by G1

$= e \cdot e'$ by assumption

$= e'$ by part ii) in $(G, \cdot, e)$ □

By part iii), in axiom G3 there is a unique b s.t. $a \cdot b = e$.
We call it a^{-1}. Then G3 and part (i) say

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

This implies $(a^{-1})^{-1} = a$, and $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Extend this notation to $a^1 = a$, $a^0 = e$ and for $n \in \mathbb{Z}^+$
lets define $a^n = a \cdot a^{n-1}$, and similarly for $-n \in \mathbb{Z}^+$
let $a^n = (a^{-1})^{-n}$.

This gives sense to a^n for any integer n.

Def^n a group $(G, \cdot, e)$ is called abelian iff

$$a \cdot b = b \cdot a \quad \forall \ a, b \in G$$

Def^n a group $(G, \cdot, e)$ is called finite if the set G has finitely many elements. Write $|G|$ for the number of elements, called the order of G.

Examples (i) Trivial group: $\{e\}$, $\cdot : \{e\} \times \{e\} \longrightarrow \{e\}$ is $e \cdot e = e$.
Then $(\{e\}, \cdot, e)$ is a group.

(ii) $(\mathbb{Z} = \{\text{integers}\}, +, 0)$ is a group

$(\mathbb{Q} = \{\text{rationals}\}, +, 0)$ "

$(\mathbb{R} = \{\text{reals}\}, +, 0)$ "

$(\mathbb{C}, +, 0)$ "

These are all abelian

(iii) $\{\mathbb{Z}_0^+, +, 0\}$ is not a group (no inverses)

(iv) $\{\mathbb{Z}, -, 0\}$ fails G1 as $1 - (1-1) \neq (1-1) - 1$

(v) $\{\mathbb{Q}, \times, 1\}$ is not a group as $0 \in \mathbb{Q}$ fails G3

$\{\mathbb{Q} \setminus \{0\}, \times, 1\}$ is a group. Similarly

$\{\mathbb{C} \setminus \{0\}, \times, 1\}$ is a group.

L2.3

(vi) If $X \subset \mathbb{R}^3$ is a solid in 3D space, then

$(\{$ rotational symmetries of $X\}$, $\circ$, "do nothing") is a group.

($\circ$: composition; "do nothing": identity function)

Not typically an abelian group.

(vii) $(\mathbb{Q}^+, \times, 1)$ is a group

(viii) $(\{z \in \mathbb{C} \text{ s.t. } |z| = 1\}, \times, 1)$ is a group

(ix) For $n \in \mathbb{N}$,

$$C_n = (\{z \in \mathbb{C} \text{ s.t. } z^n = 1\}, \times, 1)$$

is a group. Its elements are

$$1, e^{2\pi i/n}, e^{(2\pi i/n)\cdot 2}, \dots, e^{(2\pi i/n)\cdot(n-1)}$$

so the group C_n has order n.

(x) Let $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$. Define a binary operation $+_n$ on this set by $a +_n b$ = remainder when $a+b$ divided by n

Then $\{\mathbb{Z}_n, +_n, 0\}$ is a group.

(xi) Let $\mathrm{Isom}(\mathbb{R})$ be the set of functions $f: \mathbb{R} \to \mathbb{R}$ s.t.

$$|f(a) - f(b)| = |a - b| \quad \forall\, a, b \in \mathbb{R},$$

i.e. f is "an isometry" and preserves distances. Then

$(\mathrm{Isom}(\mathbb{R}), \circ, \mathrm{Id})$ is a group.

($\circ$: composition; Id: the function $\mathrm{Id}(x) = x$)

for example $f(x) = x + 1$, $g(x) = -x$ are isometries

$f \circ g(x) = -x + 1$

$g \circ f(x) = -x - 1$

are not the same, so $f \circ g \neq g \circ f$

is not abelian

L3.1

xii) Let $GL_2(\mathbb{R})$ be the set of all 2×2 matrices with entries in $\mathbb{R}$ which are invertible.

$(GL_2(\mathbb{R}), \cdot, \begin{pmatrix}1&0\\0&1\end{pmatrix})$ is a group.

Similarly with $\mathbb{C}$ instead of $\mathbb{R}$.

Def^n A group $(H, \cdot_H, e_H)$ is a subgroup of $(G, \cdot_G, e_G)$ if

i) $H \subseteq G$

ii) $e_H = e_G$ ← do we really need it?

iii) $\forall a, b \in H$, $a \cdot_G b = a \cdot_H b$

write as $(H, \cdot_H, e_H) \leq (G, \cdot_G, e_H)$

Proposition: if $(G, \cdot_G, e_G)$ and $H \subseteq G$ is a non-empty subset s.t. $\forall a, b \in H$, $a \cdot_G b^{-1} \in H$, then there is a unique $\cdot_H$ and e_H s.t. $(H, \cdot_H, e_H)$ is a subgroup of $(G, \cdot_G, e_G)$.

by def^n of subgroup

Proof: As H is non-empty, choose an $x \in H$. Then $x \cdot_G x^{-1} = e_G \in H$.

For any $a \in H$, $e_G \cdot_G a^{-1} = a^{-1} \in H$.

For $a, b \in H$, by the above $b^{-1} \in H$ so $a \cdot_G (b^{-1})^{-1} = a \cdot_G b \in H$.

Using this, define $\cdot_H : H \times H \to H$

$(a, b) \to a \cdot_G b$

And define $e_H := e_G$. Then $(H, \cdot_H, e_H)$ is easily seen to be a group, satisfying the properties of a subgroup. □

Examples:

i) $(\mathbb{Z}, +, 0) \leq (\mathbb{Q}, +, 0) \leq (\mathbb{R}, +, 0) \leq (\mathbb{C}, +, 0)$

ii) $(G, \cdot_G, e_H) \leq (G, \cdot_G, e_G)$

iii) $(\{e\}, \cdot, e) \leq (G, \cdot, e)$ for any group G

iv) $(\{\pm 1\}, \times, 1) \leq (\mathbb{Q}\setminus\{0\}, \times, 1)$

v) if $n|m$ then $C_n \leq C_m$

vi) $SL_2(\mathbb{R})$ is the real 2×2 matrices with det. $= 1$. Then

$$(SL_2(\mathbb{R}), \cdot \begin{pmatrix}1&0\\0&1\end{pmatrix}) \leq (GL_2(\mathbb{R}), \cdot, \begin{pmatrix}1&0\\0&1\end{pmatrix})$$

Proposition: the subgroups of $(\mathbb{Z}, +, 0)$ are precisely the subsets

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

Proof: Lets show $n\mathbb{Z}$ is a subgroup. If $a, b \in n\mathbb{Z}$ then

$a = na'$, $b = nb'$ and $a + (-b) = n(a' - b') \in n\mathbb{Z}$,

so by proposition 5 this is a subgroup.

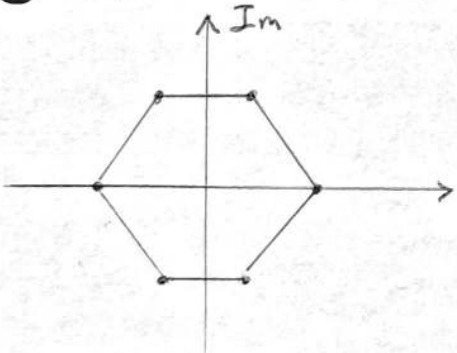
Let $S \subseteq \mathbb{Z}$ be a subgroup. If $S = \{0\} = 0\mathbb{Z}$ then it's already counted. If $S \neq \{0\}$, let $n \in S$ be the smallest positive integer in S. I claim that $S = n\mathbb{Z}$.

As $n \in S$, $k \cdot n \in S$ for all integers k, so $n\mathbb{Z} \subseteq S$.

If $x \in S \setminus n\mathbb{Z}$, then $kn < x < (k+1)n$ for some $k \in \mathbb{Z}$, and hence $0 < x - kn < n$ but $x - kn \in S$. This is impossible, as n is the smallest positive integer in S. Therefore such an x cannot exist, so $S = n\mathbb{Z}$.

For now on, write "G" for a group $(G, \cdot_G, e_G)$ except when we really need to emphasize $\cdot_G$ or e_G.

Symmetries of regular polygons



"regular 6-gon"

The regular n-gon $\subseteq \mathbb{C}$ has vertices at

$$1, e^{\frac{2\pi i}{n}}, e^{\frac{2\pi i}{n} \cdot 2}, \ldots, e^{\frac{2\pi i}{n} \cdot (n-1)}$$

i.e. those $z \in \mathbb{C}$ s.t. $z^n = 1$

Let D_{2n} be the set of isometries of $\mathbb{C}$ which preserve the regular n-gon.

($f : \mathbb{C} \to \mathbb{C}$ s.t. $|f(z) - f(w)| = |z - w|$)

The composition of isometries preserving the n-gon is another one, call it $\circ$.

The identity $Id : \mathbb{C} \to \mathbb{C}$ is in D_{2n}.

L3.3 **Theorem** $(D_{2n}, \circ, Id)$ is a group, with $2n$ elements. It is called the n^{th} dihedral group.

Proof: First verify group axioms: (G1) holds as composition is associative.

For (G2) $f \circ Id(z) = f(Id(z)) = f(z) \Rightarrow f \circ Id = f$.

Let $r: \mathbb{C} \to \mathbb{C}$ be $r(z) = z \cdot e^{\frac{2\pi i}{n}}$. This preserves the n-gon, and

$$\begin{aligned} |r(z) - r(w)| &= |z \cdot e^{2\pi i/n} - w \cdot e^{2\pi i/n}| \\ &= |(z-w)e^{2\pi i/n}| \\ &= |z-w|\,|e^{2\pi i/n}| \quad > 1 \\ &= |z-w| \text{ is an isometry.} \end{aligned}$$

Let $s: \mathbb{C} \to \mathbb{C}$ be $s(z) = \overline{z}$. This is an isometry, and preserves the n-gon.

Note $r^n = r \circ (r^{n-1}) = Id$, so r has an inverse. Also $s^2 = Id$.

To show (G3) and that there are $2n$ elements, I'll show that

$$D_{2n} = \{Id, r, r^2, \cdots, r^{n-1}, s, rs, \cdots, r^{n-1}s\}.$$

Let $f: \mathbb{C} \to \mathbb{C}$ be in D_{2n}. If $f(1) = e^{\frac{2\pi i}{n}k}$ for some k, then $(r^{-k} \circ f)(1) = 1$ giving an isometry fixing 1.

Now $r^{-1} \circ f$ sends ω to ω or ω^{n-1} $(\omega = e^{\frac{2\pi i}{n}})$.

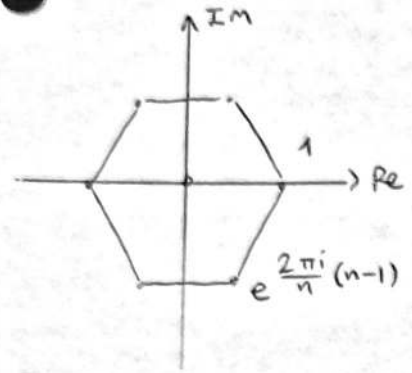
So $r^{-k} \circ f$ or $s \circ r^{-k} \circ f$ fixes 1 and ω.

But then $r^{-k} \circ f$ or $s \circ r^{-k} \circ f$ is Id, so

$$f = r^k \text{ or } r^k \circ s. \qquad \square$$

What is sr?

$$sr(1) = s\left(e^{\frac{2\pi i}{n}}\right) = e^{-\frac{2\pi i}{n}} = e^{\frac{2\pi i}{n}(n-1)}$$



Also $r^{-1}(1) = e^{\frac{2\pi i}{n}(n-1)}$,

so $r^{+1} sr(1) = 1$.

$$rsr\left(e^{\frac{2\pi i}{n}}\right) = rs\left(e^{\frac{2\pi i}{n}\cdot 2}\right)$$

$$= r\left(e^{\frac{2\pi i}{n}(n-2)}\right) = e^{\frac{2\pi i}{n}(n-1)}$$

So $srsr$ fixes 1 and $e^{\frac{2\pi i}{n}}$, so $srsr = Id$

$\therefore rsr = s^{-1} = s$

$\therefore sr = r^{-1}s = r^{(n-1)}s$

This lets us write any string of rs and ss into the from r^i or $r^i s$.

Permutations

For a set X, a permutation of X is an invertible function $f: X \to X$ i.e. such that $\exists\, g: X \to X$ and $f \circ g = Id$ and $g \circ f = Id$.

If f and f' are permutations of X, they have inverses g and g', so that

$$(f \circ f') \circ (g' \circ g) = f \circ (f' \circ g') \circ g = f \circ Id \circ g = f \circ g = Id$$

and

$$(g' \circ g) \circ (f \circ f') = g' \circ (g \circ f) \circ f' = g' \circ Id \circ f' = g' \circ f' = Id$$

$\Rightarrow$ composition of functions $\circ$ is a binary operation on the set

$$Sym(X) = \{ f: X \to X \text{ s.t. } f \text{ is a permutation} \}$$

Note $f \circ Id = f$, and by def^n any permutation has an inverse.

Then, Theorem: $(Sym(X), \circ, Id)$ is a group $\forall\, X$.

When $X = \{1, 2, \ldots, n\}$ we denote this group by S_n, called the symmetric group on n elements.

There are $n!$ permutations of $\{1,2,\dots,n\}$, so $|S_n| = n!$.

Homomorphisms

Def^n: If G and H are groups, a function $\phi: H \to G$ is called a group homomorphism if $\phi(a \cdot_H b) = \phi(a) \cdot_G \phi(b) \quad \forall\ a, b \in H$.

If ϕ is invertible, then it's called a group isomorphism, and then $\phi^{-1}: G \to H$ is so too. We then say H and G are isomorphic, and write $H \cong G$.

Examples:

i) the function $\phi: H \to G$ given by $\phi(h) = e_G \ \forall\ h \in H$ is a homomorphism.

ii) if $H \leq G$, then $\text{inc}: H \to G$, $h \to h$ is a homomorphism.

iii) if $n|m$, then $\phi: C_m \to C_n$, $z \to z^{m/n}$ is a homomorphism.

iv) The function $x \to e^x : \mathbb{R} \to \mathbb{R}^+$ is a homomorphism

$$\exp: (\mathbb{R}, +, 0) \to (\mathbb{R}^+, \times, 1)$$

In fact it is an isomorphism.

Lemma: if $\phi: H \to G$ is a homomorphism then

i) $\phi(e_H) = e_G$

ii) $\phi(a^{-1}) = \phi(a)^{-1} \ \forall\ a \in H$.

Proof: for (i), consider $e_H \cdot_H e_H = e_H$, so $\phi(e_H) = \phi(e_H \cdot_H e_H) = \phi(e_H) \cdot_G \phi(e_H)$

$\Rightarrow \phi(e_H) = e_G$ since $\phi(e_H) \cdot_G \phi(e_H)^{-1} = e_G$.

for (ii) consider

$\phi(a) \cdot_G \phi(a^{-1}) = \phi(a \cdot_H a^{-1}) = \phi(e_H) = e_G$ (by (i))

by uniqueness of inverses, $\phi(a^{-1}) = \phi(a)^{-1}$. □

L4.3

Def^n: if $\phi: H \to G$ is a homomorphism, then

i) the image of ϕ is

$$Im(\phi) = \{ g \in G : \exists h \in H \text{ s.t. } \phi(h) = g \}$$

ii) the kernel of ϕ is

$$Ker(\phi) = \{ h \in H : \phi(h) = e_G \}$$

Proposition: if $\phi: H \to G$ is a homomorphism, then

$Im(\phi) \leq G$ and $Ker(\phi) \leq H$.

Proof: note that $\phi(e_H) = e_G$, so $e_G \in Im(\phi)$ and $e_H \in Ker(\phi)$.

We now apply subgroup criteria:

$a, b \in Im(\phi)$, let $a = \phi(x)$ and $b = \phi(y)$

so, $a \cdot_G b^{-1} = \phi(x) \cdot_G \phi(y)^{-1} = \phi(x) \cdot_G \phi(y^{-1}) = \phi(x \cdot_H y^{-1})$ and so

$a \cdot_G b^{-1} \in Im(\phi)$ and $Im(\phi) \leq G$.

$a, b \in Ker(\phi)$, $\phi(a \cdot_H b^{-1}) = \phi(a) \cdot_G \phi(b^{-1})$

$= \phi(a) \cdot_G \phi(b)^{-1}$

$= e_G \cdot_G e_G^{-1}$

$= e_G$

here $a \cdot_H b^{-1} \in Ker(\phi)$ and $Ker(\phi) \leq H$. □

Lemma: if $\phi: H \to G$ is a homomorphism then it is an isomorphism iff

$Ker(\phi) = \{e_H\}$ and $Im(\phi) = G$.

Proof: $Im(\phi) = G \iff \phi$ is surjective

To see ϕ is injective, suppose $\phi(a) = \phi(b)$. Then $\phi(a \cdot b^{-1}) = \phi(a) \cdot \phi(b)^{-1} = e_G$

so $a \cdot b^{-1} \in Ker(\phi)$ and hence $a \cdot b^{-1} = e_H$. Then $a = b$. □

$\phi(a) = \phi(a) \cdot e_G = \phi(a) \cdot \phi(k) = \phi(a \cdot k)$ where $k \in Ker(\phi)$

$\Rightarrow a = a \cdot k$ by injectivity $\Rightarrow k = e_H$

Cyclic groups

The group

$$C_n = \left(\{z \in \mathbb{C} : z^n = 1\}, \times, 1\right)$$

writing $\xi = e^{\frac{2\pi i}{n}}$, the elements of this group are

$$1 = \xi^0, \ \xi = \xi^1, \ \xi^2, \ \dots, \ \xi^{n-1}$$

so every element is of the form ξ^k, for some $k \in \mathbb{Z}$.

Def^n: a group G is cyclic if $\exists\, a \in G$ s.t.

$\forall\, g \in G, \ \exists k \in \mathbb{Z}$ s.t. $g = a^k$.

Say that a is a generator of G.

Examples: The C_n are cyclic

The group $(\mathbb{Z}, +, 0)$ is also cyclic, with generator 1, as

$1^k = k \in \mathbb{Z}$.

The group $(\mathbb{Z}_n, +_n, 0)$ is also cyclic, with generator 1.

Consider $\varphi : \mathbb{Z}_n \to C_n$ given by $\varphi(k) = \xi^k$.

This is a homomorphism:

$$\varphi(k +_n \ell) = \xi^r = \xi^r \cdot \xi^{xn} = \xi^k \cdot \xi^\ell = \varphi(k) \cdot \varphi(\ell)$$

r s.t. $k + \ell \equiv_n r$ with $0 \le r < n-1$, i.e. $k + \ell = r + x \cdot n$

Obviously invertible, with $\varphi^{-1}(\xi^k) = k$. So it is an isomorphism.

Theorem: A cyclic group is isomorphic to some $\mathbb{Z}_n / C_n$ (← not quotient!!) or to $\mathbb{Z}$. (← a.k.a C_∞)

Proof: Let G be cyclic and $a \in G$ be a generator.

Consider $S := \{k \in \mathbb{Z}^+ : a^k = e\}$. If $S \neq \emptyset$, let $n = \min(S)$.

Consider $\phi : C_n = \{\xi^0, \xi^1, \dots, \xi^{n-1}\} \to G$

$$\xi^k \longrightarrow a^k.$$

If $0 \leq k, l < n$ and $k + l \geq n$, then $k + l = n + r$ for $0 \leq r < n$. So

$$\phi(\xi^k \cdot \xi^l) = \phi(\xi^{k+l}) = \phi(\xi^n \cdot \xi^r)$$
$$= \phi(\xi^r) = a^r = a^{n+r} \quad \text{since } n \in S$$
$$= a^{k+l} = a^k \cdot a^l$$
$$= \phi(\xi^k) \cdot \phi(\xi^l)$$

If $k+l < n$, same but easier. Thus ϕ is a homomorphism.

As a generates G, ϕ is surjective, i.e. $\mathrm{Im}(\phi) = G$.

If $\phi(\xi^k) = e$, then $a^k = e$ so $k \in S$?

As $0 \leq k < n$ and n is minimal s.t. $a^n = e$, where $n > 0$, we have that $k = 0$. So

$$\mathrm{Ker}(\phi) = \{1\}.$$

The previous lemma shows ϕ is an isomorphism.

If, instead $S = \phi$, let $\phi : \mathbb{Z} \to G$

$$k \longrightarrow a^k.$$

Then $\phi(k+l) = a^{k+l} = a^k \cdot a^l = \phi(k)\phi(l)$, so ϕ is a hom^{sm}.

Again the image of ϕ is G.

If $k \in \mathrm{Ker}(\phi)$ then $a^k = e$, so as $S = \phi$, k cannot be +ve, and hence $k = 0$ since $a^k = e \Rightarrow (a^k) = e$ for -ves.

Thus $\mathrm{Ker}(\phi) = \{0\}$ so it is an isomorphism. □

Convenient for $\mathbb{Z}_\infty^C$ to be $(\mathbb{Z}, +, 0)$.

Defn if G is a group and $g \in G$, the order of g is the smallest $n \in \mathbb{Z}^+$ s.t. $g^n = e$, written $n = \mathrm{ord}(g)$. If no such n exists, we say $\mathrm{ord}(g) = \infty$: infinite order

??

For $g \in G$ can form $\langle g \rangle \subseteq G$ consisting of all elements g^k for $k \in \mathbb{Z}$.

This is a subgroup: $g \in \langle g \rangle$ so $\langle g \rangle \neq \emptyset$.

If $g^k, g^\ell \in \langle g \rangle$ then $g^k \cdot (g^\ell)^{-1} = g^k \cdot g^{-\ell}$

$= g^{k-\ell} \in \langle g \rangle$.

By definition, this is a cyclic group generated by g.

So $\langle g \rangle \cong C_n$ or $\mathbb{Z}$ ($= C_\infty$) for some n.

This number n is precisely $\mathrm{ord}(g)$, and the order of $\langle g \rangle$.

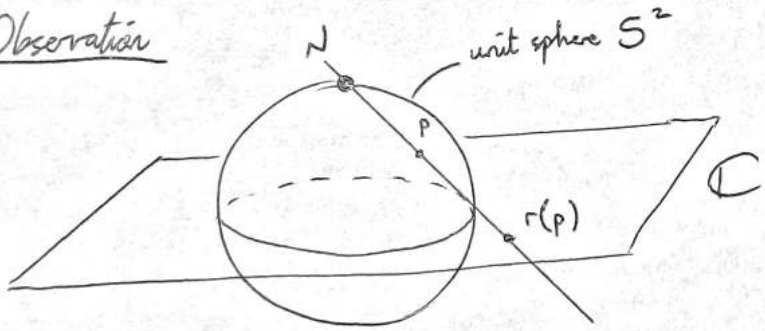
The Möbius group

Want to study maps $f(z) = \frac{cz+b}{cz+d}$, $f: \mathbb{C} \to \mathbb{C}$,

where $a, b, c, d \in \mathbb{C}$. However, our definition fails for $-\frac{d}{c}$.

Define the extended complex numbers: $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$

Observation



let $r: S^2 \to \hat{\mathbb{C}}$ be given by

$$P \to \begin{cases} NP \cap \mathbb{C} & \text{if } P \neq N, \\ \infty & \text{if } P = N. \end{cases}$$

This is a bijection. Given $a, b, c, d \in \mathbb{C}$, define $f: \hat{\mathbb{C}} \to \hat{\mathbb{C}}$

by $f(z) = \begin{cases} \frac{az+b}{cz+d} & \text{for } z \notin \{\infty, -\frac{d}{c}\} \\ \infty & \text{for } z = -\frac{d}{c} \\ \frac{a}{c} & \text{for } z = \infty. \end{cases}$

In practice, continue to write $\frac{az+b}{cz+d}$ using $\frac{1}{0} = \infty$ and $\frac{a\infty}{c\infty} = \frac{a}{c}$.

Note: $\frac{az+b}{cz+d} = \frac{a(cz+d)}{c(cz+d)} - \frac{ad-bc}{c(cz+d)}$ so if $ad-bc=0$, f is not injective.

A Möbius transformation is such a function for $ad-bc \neq 0$

$A^A = A \iff A \neq 2$ lmao

The Möbius group is

$$\mathcal{M} = \{ f : \hat{\mathbb{C}} \to \hat{\mathbb{C}} \mid f \text{ is a Möbius transformation} \}.$$

Setting $a=1, b=0, c=0, d=1$, get $f(z) = \frac{1 \cdot z + 0}{0 \cdot z + 1} = z$

so the identity function is a Möbius transformation.

If f' is the Möbius transformation associated to a', b', c', d' then

$$f'(f(z)) = \frac{a' \frac{az+b}{cz+d} + b'}{c' \frac{az+b}{cz+d} + d'} = \frac{a'(az+b) + b'(cz+d)}{c'(az+b) + d'(cz+d)}$$

$$= \frac{(a'a + b'c)z + (a'b + b'd)}{(c'a + d'c)z + (c'b + d'd)}$$

$$=: \frac{a''z + b''}{c''z + d''}$$

note $\begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

so taking determinants:

$a''d'' - b''c'' = (a'd' - b'c')(ad - bc) \neq 0$ as f and f' are Möbius trans.

$\Rightarrow f' \circ f$ is also a Möbius transformation

may like to check $\infty, -\frac{d}{c}$ cases

Theorem: $(\mathcal{M}, \circ, Id)$ is a group

Proof: (G1) is satisfied as $\circ$ is associative

(G2) is satisfied as $f \circ Id = f$

(G3) is satisfied as $g(z) = \frac{dz - b}{-cz + a}$ is the inverse to $f(z) = \frac{az+b}{cz+d}$. □

Note: for $\lambda \neq 0$, $\lambda a, \lambda b, \lambda c, \lambda d$ determines the same Möbius transformation as a, b, c, d.

Note $f(z) = \frac{1}{z-a}$ sends $a \in \mathbb{C} \subseteq \hat{\mathbb{C}}$ to $\infty \in \hat{\mathbb{C}}$.

Proposition Every Möbius transformation is a composition of:

i) $f(z) = az = \frac{az+0}{0z+1}$ $\quad a \neq 0$ — dilation / rotation

ii) $f(z) = z+b = \frac{1z+b}{0z+1}$ — translation

iii) $f(z) = \frac{1}{z} = \frac{0z+1}{z+0}$ — inversion

Proof: Let $f(z) = \frac{az+b}{cz+d}$ be Möbius.

If $c \neq 0$, then $\frac{az+b}{cz+d} = \frac{a}{c} + \frac{bc-ad}{c(cz+d)}$. Thus

$$z \xrightarrow{(i)} cz \xrightarrow{(ii)} cz+d \xrightarrow{(i)} c(cz+d) \xrightarrow{(iii)} \frac{1}{c(cz+d)} \xrightarrow{(i)} \frac{bc-ad}{c(cz+d)}$$

$$\xrightarrow{(ii)} \frac{a}{c} + \frac{bc-ad}{c(cz+d)} = \frac{az+b}{cz+d}.$$

If $c=0$, then $\frac{az+b}{cz+d} = \frac{a}{d}\cdot z + \frac{b}{d}$. $\quad z \xrightarrow{(i)} \frac{a}{d}z \xrightarrow{(ii)} \frac{a}{d}z + \frac{b}{d}$. ($\frac{a}{d} \neq 0$) □

Def: A **fixed point** of a Möbius transformation $f: \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ is a $z_0 \in \hat{\mathbb{C}}$ such that

- $f(z_0) = z_0$.

Theorem: A Möbius transformation with at least 3 fixed points is Id.

Proof: $f(z) = \frac{az+b}{cz+d}$. If ∞ is a fixed point, $\infty = f(\infty) = \frac{a}{c}$ if $c \neq 0$ or ∞ if $c=0$

Hence $c=0$. If z_0 is another fixed point, then $z_0 = f(z_0) = \frac{az_0}{d} + \frac{b}{d}$ so rearranging, $(d-a)z_0 - b = 0$. If $d-a \neq 0$, this has exactly 1 solution. As f has 2 fixed points apart from ∞, we must have $d-a=0$. But then b must be 0 to give solutions. So $f(z) = \frac{cz+0}{0z+a} = z$ so $f = Id$.

L6.3

If ∞ is not a fixed point, then all 3 fixed points lie in $\mathbb{C} \subseteq \hat{\mathbb{C}}$, and satisfy $z_0 = f(z_0) = \frac{az_0+b}{cz_0+d}$, so $cz_0^2 + (d-a)z_0 - b = 0$.

This is quadratic (a priori), so it has ≤ 2 solutions, unless we have $c=0$, $a-d=0$, $b=0$ at which point $f = Id$. □

Theorem if $z_1, z_2, z_3 \in \hat{\mathbb{C}}$ and $w_1, w_2, w_3 \in \hat{\mathbb{C}}$ are two triples of distinct points, then there is a unique $f \in M$ s.t. $f(z_i) = w_i$ for $i = 1, 2, 3$.

Proof Suppose first $(w_1, w_2, w_3) = (0, 1, \infty)$. If $z_i \neq 0$ for $i=1,2,3$,

$$f(z) = \frac{(z_2 - z_3)(z - z_1)}{(z_2 - z_1)(z - z_3)}$$ is a Möbius transformation s.t.

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

If $z_3 = \infty$ then use $f(z) = \frac{z - z_1}{z_2 - z_1}$ $\Rightarrow f(z_1) = 0$, $f(z_2) = 1$, $f(z_3) = \infty$.

Similar for $z_1, z_2 = \infty$. Thus we are done for $(w_1, w_2, w_3) = (0, 1, \infty)$.

In general, given w_1, w_2, w_3 choose g such that $g(w_1) = 0$, $g(w_2) = 1$, $g(w_3) = 0$ so that $g^{-1} \circ f$ sends z_i to w_i for $i = 1, 2, 3$. ⊠

If $h, k \in M$ s.t. $\begin{matrix} h(z_i) = w_i \\ k(z_i) = w_i \end{matrix}$. Then $h^{-1} \circ k(z_i) = z_i$ for $i = 1, 2, 3$ so

$h^{-1} \circ k = Id \Rightarrow k = h$. □

---

worried about groups ES

$f(z) = \frac{z+b}{cz+d}$ compose with $\frac{1}{?}$

$f(z) = \frac{cz+d}{z+b} = \frac{z + \frac{d}{c}}{\frac{1}{c}z + \frac{b}{c}}$ goes to $\frac{1}{c^2}$ oof

Def^n in a group G, elements a, b are called conjugate if there is a $g \in G$ such that $b = gag^{-1}$.

Note: also $a = g^{-1}bg$

If $c = hbh^{-1}$ then $c = hga(hg)^{-1}$.

If $f \in M$ satisfies $f(x) = x$ then $(gfg^{-1})(g(x)) = g(x)$ and vice versa.

So f and gfg^{-1} have the same no. of fixed points.

Theorem: Every Möbius transformation other than Id has 1 or 2 fixed points.

If f has 1 fixed point, then it is conjugate to $z \to z+1$. If f has 2 fixed points then it's conjugate to $z \to az$ for some $a \in \mathbb{C} \setminus \{0\}$.

Proof: Already know f has at most 2 fixed points.

Need to show it can't have no fixed points.

Let $f : z \to \frac{az+b}{cz+d}$. If $c = 0$, ∞ is a fixed point.

If $c \neq 0$, then fixed points are solutions to $cz^2 + (d-a)z - b = 0$.

For $c \neq 0$, this has a solution.

If f has exactly 1 fixed point, z_0, choose $z_1 \neq z_0$. Then $(z_1, f(z_1), z_0)$ are distinct points, so we can find $g \in M$ sending these to $(0, 1, \infty)$. Then gfg^{-1} fixes ∞ and sends 0 to 1, so must be $z \to z+1$. * since it has only one fixed point

If f has exactly 2 fixed points, z_0 and z_1, then we can find a Möbius transformation sending (z_0, z_1) to $(0, \infty)$, let it be g, such that gfg^{-1} fixes 0 and ∞. So if $gfg^{-1} : z \to \frac{az+b}{cz+d}$, then $b = 0$, $c = 0$. So $gfg^{-1} = \frac{a}{d}z$. □

Circles Def^n a circle in $\hat{\mathbb{C}}$ is the set of $z \in \hat{\mathbb{C}}$ satisfying

$Az\bar{z} + \bar{B}z + B\bar{z} + C = 0$ for $A, C \in \mathbb{R}$ and $|B|^2 > AC$.

∞ is a sol^n iff $A = 0$.

e.g. if $|z-b| = r$ describes the circle centre b radius r, can write as $(z-b)\overline{(z-b)} = r^2 \Leftrightarrow z\bar{z} - \bar{b}z - b\bar{z} + (b\bar{b} - r^2) = 0$.

e.g. if we consider the set

$$\{ z \in \mathbb{C} \mid a \cdot \mathrm{Re}(z) + b\,\mathrm{Im}(z) = c \} \cup \{\infty\},$$

which is a straight line + ∞, we can see it as the solutions to

$$\frac{\overline{a+ib}}{2} z + \frac{a+ib}{\#2} \bar{z} - c = 0$$

Theorem: Möbius transformations send circles in $\hat{\mathbb{C}}$ to circles.

Proof: Enough to show $z \to az$, $z \to z+b$, $z \to \frac{1}{z}$ preserve circles.

Writing $S_{A,B,C}$ for the circle given by A, B, C as before.

Under $z \to az$, $S_{A,B,C}$ goes to $S_{A/a\bar{a}, B/\bar{a}, C}$. (dividir)

Under $z \to z+b$, $S_{A,B,C}$ goes to $S_{A, B-\bar{A}b, C + Ab\bar{b} - \bar{B}b - B\bar{b}}$.

useless

Under $z \to \frac{1}{z}$, $S_{A,B,C}$ goes to $S_{C, \bar{B}, A}$. □

The cross-ratio

Def^n: if $z_1, z_2, z_3, z_4 \in \hat{\mathbb{C}}$ are pairwise distinct, their cross-ratio is

$[z_1, z_2, z_3, z_4] := f(z_4)$ where $f \in \mathcal{M}$ is the unique Möbius map sending (z_1, z_2, z_3) to $(0, 1, \infty)$.

Note: $[z_1, z_2, z_3, z_4] = \dfrac{(z_4 - z_1)(z_2 - z_3)}{(z_4 - z_3)(z_2 - z_1)}$ where if one is ∞ we cross out its two terms.

The claim is that

$z \to \dfrac{(z - z_1)(z_2 - z_3)}{(z_2 - z_1)(z - z_3)}$ sends (z_1, z_2, z_3) to $(0, 1, \infty)$, which is true

L7.3

Theorem: if $z_1, z_2, z_3, z_4 \in \hat{\mathbb{C}}$ are pairwise distinct and if $g \in M$, then

$$[z_1, z_2, z_3, z_4] = [g(z_1), g(z_2), g(z_3), g(z_4)].$$

Proof: if f sends (z_1, z_2, z_3) ~~ser~~ to $(0, 1, \infty)$, then fg^{-1} sends $(g(z_1), g(z_2), g(z_3))$ to $(0, 1, \infty)$. Then

$$[g(z_1), g(z_2), g(z_3), g(z_4)] = fg^{-1}(g(z_4)) = f(z_4)$$
$$= [z_1, z_2, z_3, z_4]. \qquad \square$$

Corollary: points $z_1, z_2, z_3, z_4 \in \hat{\mathbb{C}}$ are concyclic iff

$$[z_1, z_2, z_3, z_4] \in \mathbb{R}.$$

Proof: let $g \in M$ be the unique Möbius transformation sending z_1, z_2, z_3 to $(0, 1, \infty)$, so that $[z_1, z_2, z_3, z_4] = g(z_4)$. If S if the circle through z_1, z_2, z_3, then $g(S)$ is the unique circle through $0, 1, \infty$ which is $\mathbb{R} \cup \{\infty\}$. Then $g(z_4) \in S$ iff $g(z_4) \in g(S) = \mathbb{R} \cup \{\infty\}$

$$\Leftrightarrow [z_1, z_2, z_3, z_4] = \mathbb{R}.$$

f sends $(0, 1, \infty)$ to $(f(0), f(1), f(\infty))$ is invertible preserves cross ratio

$$[0, 1, \infty, z] = z = [f(0), f(1), f(\infty), f(z)]$$

Let $g \in M$ send $f(0)$ to 0, $f(1)$ to 1, $f(\infty)$ to ∞.

Then $g(f(z)) = z \ \forall z$ and g^{-1} is Möbius

A. Epelde

Group actions

Def^n: an action of a group $(G, \cdot, e)$ on a set X is a function $* : G \times X \longrightarrow X$ satisfying

(A1) $e * x = x \quad \forall x \in X$

(A2) $a * (b * x) = (a \cdot b) * x \quad \forall a, b \in G, x \in X$

Examples

i) Any group G acts on any set X via $g * x = x$.

ii) Any group G acts on the set G via $g * g' = g \cdot g'$.

iii) The symmetric group $Sym(X)$ acts on X via $f * x = f(x)$

iv) The group of symmetries of a solid $X \subset \mathbb{R}^3$ acts on X, on vertices of X, on edges of X...

v) The dihedral group D_{2n} acts on the set of vertices of the regular n-gon.

vi) The Möbius group acts on $\hat{\mathbb{C}}$.

Theorem: An action $*$ of a group G on the set X is the same as a homomorphism $\rho : G \longrightarrow Sym(X)$

Proof: Given an action $*$, for each $g \in G$ we can form

$$t_g : X \longrightarrow X, \quad x \longrightarrow g * x$$

Notice there is a similar function $t_{g^{-1}}$ and

$$t_{g^{-1}}(t_g(x)) = t_{g^{-1}}(g * x) = g^{-1} * (g * x) \overset{(A2)}{=} (g^{-1} \cdot g) * x = e * x \overset{(A1)}{=} x.$$

Similarly $t_g(t_{g^{-1}}(x)) = x$. So $t_{g^{-1}} = (t_g)^{-1}$, so t_g is an invertible function, so an element of $Sym(X)$.

Define $\rho(g) = t_g$. Then $\rho(g \cdot g')(x) = t_{g \cdot g'}(x) = (g \cdot g') * x$

$$= g * (g' * x) = t_g(t_{g'}(x)) = (\rho(g) \circ \rho(g'))(x).$$

So $\rho(g \cdot g') = \rho(g) \circ \rho(g')$ and ρ is a homomorphism.

L 8.2 On the other hand, given such a ρ, define

$$g * x := \rho(g)(x).$$

($\rho(e) = Id$ since it's homomorphism)

- This satisfies (A1) as $e * x = \rho(e)(x) = Id(x) = x$

It satisfies (A2) as

$$g * (g' * x) = g * (\rho(g')(x)) = \rho(g)(\rho(g')(x))$$
$$= (\rho(g) \circ \rho(g'))(x) = \rho(g \cdot g')(x) \quad \text{as } \rho \text{ is homomorphism}$$
$$= (g \cdot g') * x. \qquad \square$$

Cayley's Theorem: Any group is isomorphic to a subgroup of some symmetric group.

- Proof: As in example (ii), G acts on the set G via $g * g' = g \cdot g'$. By the theorem, this corresponds to a homomorphism $\rho : G \to Sym(G)$. We can consider this is a homomorphism $\bar{\rho} : G \to Im(\rho)$ which is surjective. If $g \in Ker(\bar{\rho})$, then $t_g = Id$ so $g * g' = g' \ \forall g' \in G$. This means $g = e$, so $Ker(\bar{\rho}) = \{e\}$. As $Im(\bar{\rho}) = Im(\rho)$ (codomain of $\bar{\rho}$), $\bar{\rho}$ satisfies the conditions of the "isomorphism theorem" so $\bar{\rho}$ is an isomorphism. Then $G \cong Im(\rho) \leq Sym(G)$. $\square$

Def^n: Let G act on X.

- i) The orbit of $x \in X$ is $Gx := \{ y \in X \text{ s.t. } y = g * x \text{ for some } g \in G \}$

The action is called transitive if $Gx = X$. (for some x $\Leftrightarrow$ for all x as will be shown by orbits partitioning)

ii) The stabiliser of $x \in X$ is $G_x = \{ g \in G \text{ s.t. } g * x = x \}$

iii) The kernel of the action is $\{ g \in G \text{ s.t. } \forall x \in X, g * x = x \}$. (i.e. the kernel of ρ)

The action is called faithful if its kernel is $\{e\}$.

Theorem: Let G act on X.

- i) $\forall x \in X$, G_x is a subgroup of G
- ii) The set of orbits $\{Gx\}$ partition X.

Note $e \in G_x$!

Proof: For (i), let $g, h \in G_x$. Then

$h * x = x$

so $h^{-1} * (h * x) = h^{-1} * x$

$\overset{A2}{=} (h^{-1} \cdot h) * x$

$= e * x$

$\overset{A1}{=} x$

and hence $h^{-1} \in G_x$.

So $(g \cdot h^{-1}) * x \overset{A2}{=} g * (h^{-1} * x)$

$= g * x$

$= x$

so $g \cdot h^{-1} \in G_x$.

For (ii), first note $x \in Gx$ since $x = e * x$, so any element of X lies in some orbit. Need to show orbits are disjoint or equal. Suppose $(Gx) \cap (Gy) \neq \emptyset$, and let $z \in (Gx) \cap (Gy)$. As $z \in Gx$, there is some $g \in G$ s.t. $g * x = z$. As $z \in Gy$, $\exists\, h \in G$ s.t. $h * y = z$. So $x = g^{-1} * (h * y)$ $= (g^{-1} \cdot h) * y$, i.e. $x \in Gy$.

If $k * x$ is any element of Gx, we have

$k * x = k * ((g^{-1} \cdot h) * y)$

$\overset{A2}{=} (k \cdot g^{-1} \cdot h) * y \in Gy$

$\Rightarrow Gx \subset Gy$. Same argument shows $Gy \subset Gx$, so $Gy = Gx$. □

What we have discussed so far is a left action of G on X. A right action of G on X is a $\bullet : X \times G \to X$ s.t. $x \bullet e = x$ and $(x \bullet g) \bullet h = x \bullet (g \cdot h)$. All the results we have discussed also hold for right actions.

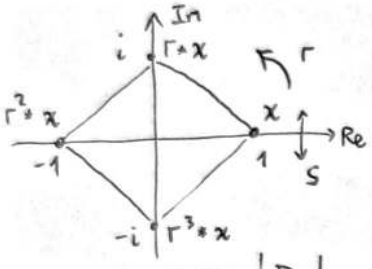
Def^n if G acts on the left of a set X, then the set of orbits $G\backslash X$ is

$$G\backslash X = \{\mathcal{O} \subset X : \mathcal{O} = Gx \text{ for some } x \in X\}.$$

If G acts on the right of a set X then X/G is

$$X/G = \{\mathcal{O} \subset X : \mathcal{O} = xG \text{ for some } x \in X\}.$$

Example Consider the group D_8 of symmetries of the regular 4-gon



$$D_8 x = \{1, i, -1, -i\}$$

$$(D_8)_x = \{e, s\}$$

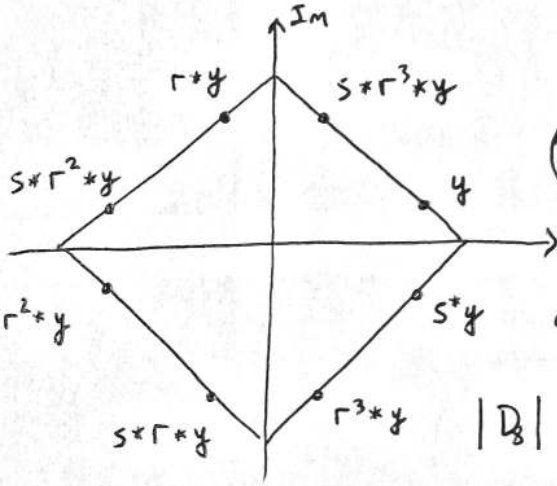
$$|D_8| = 8 \qquad |D_8 x| = 4 \qquad |(D_8)_x| = 2$$

so $|D_8| = |D_8 x||(D_8)_x|$.

Easily extend this to

$$|D_{2n}| = |D_{2n} x||(D_{2n})_x|.$$

$2n$ n 2



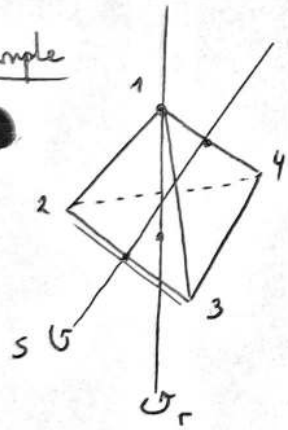
$D_8 y = \{\text{all } 8\}$

$(D_8)_y = \{e\}$

again

$$|D_8| = |D_8 y||(D_8)_y|.$$

Example



$G = \{\text{symmetries of tetrahedron}\}$ act on the set $V = \{1, 2, 3, 4\}$ of vertices.

Then $G1 = V$.

$G_1 = \{e, r, r^2\}$.

$$12 = |G| = |G1||G_1|$$

Act on the set E of edges. Let $e \in E$ be the edge from 2 to 3.

Again $Ge = E$. $G_e = \{Id, s\}$. So $|G| = |Ge||G_e|$.

The regular action

Any group G acts on G on the left via $g * g' = g \cdot g'$.

● This is the left regular action.

G also acts on G on the right, via $g' \bullet g = g' \cdot g$.

Similarly, if $H \leq G$ then H acts on G via $h * g = h \cdot g$ or $g \bullet h = g \cdot h$.

Def^n: a left coset of H in G is an orbit of the right regular action of H on G, i.e. $gH = \{g' \in G : g' = gh \text{ for some } h \in H\}$.

A right coset of H in G is an orbit of the left regular action of H on G, i.e.

● $Hg = \{g' \in G : g' = hg \text{ for some } h \in H\}$.

Note $Hg = Hg' \iff g'g^{-1} \in H$.

$gH = g'H \iff g^{-1}g' \in H$.

As with actions in general, let

$$G/H = \{\mathcal{O} \subset G : \mathcal{O} = gH \text{ for some } g \in G\}$$

and

$$H\backslash G = \{\mathcal{O} \subset G : \mathcal{O} = Hg \text{ for some } g \in G\}.$$

● These are the sets of left and right cosets respectively.

Examples:

i) Consider $2\mathbb{Z} \leq \mathbb{Z}$. Note $a, b \in \mathbb{Z}$ are in the same $2\mathbb{Z}$ orbit (for the left action) $\iff a - b \in 2\mathbb{Z}$. So there are 2 orbits: the even numbers and the odd numbers: $2\mathbb{Z}$ and $2\mathbb{Z} + 1$.

ii) Symmetries of the regular 3-gon, $D_6 = \{Id, r, r^2, s, rs, r^2s\}$.

Here $r^3 = Id$, $s^2 = Id$, $sr = r^2s$.

● Let $R = \{Id, r, r^2\}$ $S = \{Id, s\}$. Both subgroups of D_6.

The ~~right~~ right cosets of R are $RId = \{Id, r, r^2\}$ and $Rs = \{s, rs, r^2s\}$.

~~Left~~

The left cosets of R are $\mathrm{Id}\,R = \{\mathrm{Id}, r, r^2\}$ and $sR = \{s, sr, sr^2\}$

$= \{s, r^2s, rs\}$.

The right cosets of S are

$S\,\mathrm{Id} = \{\mathrm{Id}, s\}$ $\quad Sr = \{r, sr\} = \{r^4, r^2s\}$

$Sr^2 = \{\cancel{\mathrm{Id}}, sr^2\} = \{r^2, rs\}$. ← no match

r^2

The left cosets of S are

$\mathrm{Id}S = \{\mathrm{Id}, s\}$ $\quad rS = \{r, rs\}$ $\quad r^2S = \{r^2, r^2s\}$

iv) M acts on $\hat{\mathbb{C}}$ (on the left). Let M_0 be the stabiliser of 0,

$M_0 = \{g \in M : g(0) = 0\}$.

$fM_0 = f'M_0 \iff f^{-1}f' \in M_0 \iff f^{-1}f'(0) = 0 \iff f'(0) = f(0)$.

You can look at what it means for $M_0f = M_0f'$. It is not very natural.

$\Updownarrow$

$f'f^{-1}(0) = 0 \iff f^{-1}(0) = f'^{-1}(0)$

not so unnatural

Lagrange's Theorem

- If $H \leq G$, then $f: H \to gH$ and $g: gH \to H$ are inverse functions. So
  $h \to gh$ $\quad$ $x \to g^{-1}x$

if H is finite, then $|gH| = |H|$.

Lagrange's Theorem: if G is a finite group and $H \leq G$ then $|G| = |H| \cdot |G/H|$. In particular $|H|$ divides $|G|$.

Proof: G is disjoint union of left cosets gH. They each have size $|gH| = |H|$. There are $|G/H|$ many cosets, so $|G| = |H| \cdot |G/H|$. □

- Can repeat with right cosets: $|G| = |H| \cdot |H \backslash G| \Rightarrow |G/H| = |H \backslash G|$.

Def^n: if $H \leq G$ then $|G/H|$ is called the index of H in G (might be ∞)

Lagrange is: $|G/H| = \dfrac{|G|}{|H|}$

Corollary: if G is finite and $g \in G$ then $\text{ord}(g)$ divides $|G|$.

Proof: consider $\langle g \rangle$ the cyclic subgroup of G generated by g. We already
- know $\text{ord}(g) = |\langle g \rangle|$. As $\langle g \rangle \leq G$, by Lagrange, $|\langle g \rangle|$ divides $|G|$. □

Corollary: if G is finite and $g \in G$, then $g^{|G|} = e$.

Proof: we know $\text{ord}(g)$ divides $|G|$, so $|G| = \text{ord}(g) \cdot n$ for some n.

So $g^{|G|} = g^{\text{ord}(g) \cdot n} = (g^{\text{ord}(g)})^n = e^n = e$. □

Corollary: if G is a group and $|G|$ is prime, then G is cyclic and generated by any non-identity element.

- Proof: Let $g \in G$ not be e. Then $\text{ord}(g)$ divides $|G|$. So as $|G|$ is prime, $\text{ord}(g) = 1$ or $\text{ord}(g) = |G|$. Can't have $\text{ord}(g) = 1$, as this would mean $g = e$. So $\langle g \rangle \leq G$ is a cyclic subgroup with $\text{ord}(g) = |G|$ many

elements. So must have $\langle g \rangle = G$. □

Recall $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ and $+_n$ meaning "take the sum and find the remainder upon division by n".

Similarly $a \cdot_n b$ = the remainder when ab is divided by n.

This is not a group as $0 \cdot_n a = 0$ so 0 doesn't have an inverse.

Let $U_n \subset \{0, 1, \ldots, n-1\}$ be those elements a such that there is a b with $a \cdot_n b = 1$. Then $(U_n, \cdot_n, 1)$ is a group.

Claim: $U_n = \{a \in \mathbb{Z}_n : a \text{ is coprime to } n\}$

If $(a, n) = 1$, then there exist $b, m \in \mathbb{Z}$ such that $ab + nm = 1$

$\Rightarrow a \cdot_n b = 1$. Conversely, if $a \in U_n$ there is a b s.t. $a \cdot_n b = 1$, i.e. $ab = 1 + nq$. So if a prime p divided a and n then it would divide $ab - nq = 1$, a contradiction. Hence $(a, n) = 1$.

Define: Euler's totient function is $\phi(n) = |U_n|$. This is the number of numbers which are coprime to n below n.

Theorem (Euler-Fermat): if a is coprime to n, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof: can write $a = x + nm$ for some $x \in \{0, 1, \ldots, n-1\}$. As a is coprime to n, so is x. So $x \in U_n$. Hence $x^{|U_n|} = 1$ in U_n. So $x^{\phi(n)} = 1$ in U_n.

$$a^N = (x + nm)^N = x^N + \binom{N}{1} x^{N-1} nm + \cdots + \binom{N}{N} (nm)^N \equiv x^N \pmod{n}.$$

Taking $N = \phi(n)$, get $a^{\phi(n)} \equiv x^{\phi(n)} \equiv 1 \pmod{n}$. □

The Orbit-Stabilises Theorem

Theorem: if a group G acts on a set X (on the left) and $x \in X$ then the functions

$$\phi : G/G_x \longrightarrow Gx \qquad \text{and} \qquad \psi : Gx \longrightarrow G/G_x$$
$$gG_x \longrightarrow g*x \qquad\qquad g*x \longrightarrow gG_x$$

are well-defined and inverse to each other.

Proof: for ϕ, suppose $gG_x = g'G_x$. Then $g' = gh$ for some $h \in G_x$. So

$$g'*x = (gh)*x \overset{A2}{=} g*(h*x) = g*x \text{ as } h \in G_x.$$ Hence ϕ is well-defined.

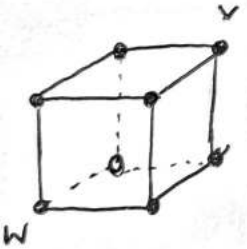
For ψ, if $g*x = g'*x$, then $x = g^{-1}*(g'*x) = (g^{-1}g')*x$. So $g^{-1}g' \in G_x$, hence $gG_x = g'G_x$. Hence ϕ and ψ are well defined and inverses. □

Corollary (Counting version of OST)

If a finite group G acts on a set X then $|G/G_x| = |Gx|$.

Hence $|G| = |G_x||Gx|$, using Lagrange.

Example



Let G be the group of rot. sym. of the cube.
Let X be the vertices of the cube, so $|X| = 8$.
So the action is transitive, i.e. $Gv = X$ for $v \in V$.
We see that G_x is the 3 rotations about the axis through v, w.

$$|G| = |Gv| * |G_v| = 8 \cdot 3 = 24$$

Theorem (Cauchy): Let G be a finite group and p be a prime number dividing $|G|$. Then G has an element of order p.

Proof: Let $Y := G^p = \overbrace{G \times G \times \cdots \times G}^{p \text{ times}}$, and

$X := \{(g_1, \cdots, g_p) \in Y \text{ s.t. } g_1 \cdots g_p = e\}$. Note $|Y| = |G|^p$. If $(g_1, \cdots, g_p) \in X$, then $g_p = (g_1 \cdots g_{p-1})^{-1}$. So $(g_1, \cdots, g_{p-1})$ uniquely determines $(g_1, \cdots, g_p) \in X$. So $|X| = |G|^{p-1}$. Let $H = C_p$, the cyclic group of order p. We have $H = \{Id, \xi, \xi^2, \cdots, \xi^{p-1}\}$, where $\xi = e^{\frac{2\pi i}{p}}$. Let H act on X by

- rotation: $\xi^i * (g_1, \cdots, g_p) = (g_{i+1}, g_{i+2}, \cdots, g_p, g_1, \cdots, g_i)$.

Note: $g_{i+1} \cdots g_p g_1 \cdots g_i = (g_{i+1} \cdots g_p) \underbrace{(g_1 \cdots g_p)}_{= e \text{ as } (g_1, \cdots, g_p) \in X} \underbrace{(g_{i+1} \cdots g_p)^{-1}}_{g_p^{-1} \cdots g_{i+1}^{-1}}$

$$= (g_{i+1} \cdots g_p)(g_{i+1} \cdots g_p)^{-1} = e$$

so $(g_{i+1}, \cdots, g_p, g_1, \cdots, g_i) \in X$. This is an action.

- For any $x \in X$, $H_x \leq H$ is a subgroup, so by Lagrange, since $|H|$ is prime, then $|H_x| = 1$ or p. By OST: $|H| = |H_x||Hx|$ so $|Hx| = p$ or 1.

Hence $|X| = 1 \cdot$ # orbits of size $1 + p \cdot$ # orbits of size p.

If $x = (g_1, \cdots, g_p)$ is an orbit of size 1, then $(g_1, \cdots, g_p) = (g_2, \cdots, g_p, g_1)$

so $g_1 = g_2 = \cdots = g_p$. So orbits of size 1 are elements $(g, \cdots, g) \in X$.

So $\underbrace{g \cdots g}_{p \text{ times}} = g^p = e$. If $g^p = e$, then $\text{ord}(g) | p$ so is 1 or p.

- So # orbits of size 1 = 1 + # elements of order p

Have p divides $|G|$, so divides $|X|$. So # orbits of size $1 \equiv 0 \pmod p$.

elements of order $p \equiv -1 \pmod p$. $\therefore$ # elements of order $p \geq p - 1$ □

The conjugation action

Def^n: For G a group, the conjugation action of G on the set G is

$$g * h := g \cdot h \cdot g^{-1}.$$

Note: $e * h = e \cdot h \cdot e^{-1} = h$ (A1✓)

$$g * (k * h) = g * (k \cdot h \cdot k^{-1}) = g \cdot k \cdot h \cdot k^{-1} \cdot g^{-1} = (g \cdot k) \cdot h \cdot (g \cdot k)^{-1}$$
$$= (g \cdot k) * h \quad \text{(A2✓)}$$

Def^n: The conjugacy classes of G are the orbits of the conjugation action

- The conjugacy class of $h \in G$ is

$$ccl(h) = \{ k \in G \text{ s.t. } k = g \cdot h \cdot g^{-1} \text{ for some } g \in G \}.$$

The centraliser of $h \in G$ is the stabiliser of h for the conjugation action:

$$C_G(h) = \{ g \in G \text{ s.t. } g \cdot h \cdot g^{-1} = h \} = \{ g \in G \text{ s.t. } g \cdot h = h \cdot g \}.$$

The centre of G is the kernel of the conjugation action.

$$Z(G) = \{ g \in G \text{ s.t. } g \cdot h \cdot g^{-1} = h \ \forall \ h \in G \}$$
$$= \{ g \in G \text{ s.t. } g \cdot h = h \cdot g \ \forall \ h \in G \}.$$

-

Example

i) For $G = D_{2n} = \{ Id, r, r^2, \dots, r^{n-1}, s, rs, \dots, r^{n-1}s \}$ with $r^n = Id$, $s^2 = Id$, $sr = r^{-1}s = r^{n-1}s$. Then $s * r^i = s \cdot r^i \cdot s^{-1} = r^{-i} \cdot s \cdot s^{-1} = r^{-i}$.

Also $r * r^i = r \cdot r^i \cdot r^{-1} = r^i$. Can deduce $g * r^i$ for any g.

Similarly $s * (r^i s) = s \cdot r^i \cdot s \cdot s^{-1} = r^{-i}s = r^{n-i}s$, and

$$r * (r^i s) = r \cdot r^i \cdot s \cdot r^{-1} = r^{i+2}s.$$

-

ii) In the Möbius group $\mathcal{M}$, all non-identity elements are conjugate to $z \to z+1$ or $z \to a \cdot z$ for some $a \in \mathbb{C} \setminus \{0\}$.

Def^n: If $H \leq G$ and $g \in G$, then the conjugate of H by g is

$$gHg^{-1} = \{k \in G \text{ s.t. } k = ghg^{-1} \text{ for some } h \in H\}.$$

Lemma: $gHg^{-1} \leq G$

Proof: Note $e = g \cdot e \cdot g^{-1} \in gHg^{-1}$ so gHg^{-1} is non-empty.

Let $a, b \in gHg^{-1}$, so $a = ghg^{-1}$ and $b = gkg^{-1}$ for some $h, k \in H$.

So $ab^{-1} = (ghg^{-1})(gkg^{-1})^{-1} = ghg^{-1}gk^{-1}g^{-1} = g\underbrace{(hk^{-1})}_{\in H}g^{-1} \in gHg^{-1}$,

and we are done. □

The quaternions

- Consider the complex matrices

$$\underline{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \underline{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

$$\underline{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad \underline{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Then $(\{\pm\underline{1}, \pm\underline{i}, \pm\underline{j}, \pm\underline{k}\}, \cdot, \underline{1})$ is a group of order 8.

Have $(-\underline{1})^2 = \underline{1}$, $\quad -\underline{1} = \underline{i}^2 = \underline{j}^2 = \underline{k}^2$ so $\underline{i}, \underline{j}, \underline{k}$ have order 4.

- $\underline{i}\underline{j} = \underline{k}$, $\underline{j}\underline{k} = \underline{i}$, $\underline{k}\underline{i} = \underline{j}$ $\qquad \underline{i}\underline{j}\underline{k} = -\underline{1}$
- $\underline{j}\underline{i} = -\underline{k}$, $\underline{k}\underline{j} = -\underline{i}$, $\underline{i}\underline{k} = -\underline{j}$

Direct product

Def^n: if $(G, \cdot_G, e_G)$ and $(H, \cdot_H, e_H)$ are groups then define a binary operation $\cdot_{G\times H}$ on the set $G \times H$, via

$$(g_1, h_1) \cdot_{G\times H} (g_2, h_2) = (g_1 \cdot_G g_2, h_1 \cdot_H h_2)$$

Lemma: the data $(G\times H, \cdot_{G\times H}, (e_G, e_H))$ is a group, called the direct product of G and H.

Write as $G \times H$. You should check $\quad G\times H \cong H \times G$

and $\quad (G\times H)\times K \cong G \times (H \times K)$.

Theorem: (Chinese remainder theorem) If $n, m \in \mathbb{N}$ are coprime, then the homomorphism

$$\phi : (\mathbb{Z}_{nm}, +_{nm}, 0) \to (\mathbb{Z}_n, +_n, 0) \times (\mathbb{Z}_m, +_m, 0)$$
$$a \longrightarrow (a \bmod n,\ a \bmod m)$$

is an isomorphism.

Proof: ϕ is a homomorphism as: if $a +_{nm} b = r$ then $a + b = r + knm$ for some $k \in \mathbb{Z}$. So $a +_n b = r \pmod n$ and $a +_m b = r \pmod m$.

So $\phi(a +_{nm} b) = \phi(r) = (r \bmod n, r \bmod m)$

$= (a +_n b, a +_m b)$

$= \phi(a) \cdot \phi(b)$.

Both $\mathbb{Z}_{nm}$ and $\mathbb{Z}_n \times \mathbb{Z}_m$ have nm elements, so if ϕ is injective, then it is an isomorphism. Suppose $\phi(a) = (0,0)$. Then $a \equiv 0 \pmod n$, $a \equiv 0 \pmod m$. So n divides a and so does m. As $(n,m) = 1$, it follows that $nm \mid a$, i.e. $a \equiv 0 \pmod{nm}$. Thus $a = 0 \in \mathbb{Z}_{nm}$, hence ϕ is injective. □

Theorem (Direct product theorem) Let $H_1, H_2 \leq G$. If:

i) $H_1 \cap H_2 = \{e\}$,

ii) $\forall\, h_1 \in H_1, h_2 \in H_2$, $h_1 h_2 = h_2 h_1$, and

iii) $\forall\, g \in G$, $\exists\, h_1 \in H_1, h_2 \in H_2$, $g = h_1 h_2$,

then $G \cong H_1 \times H_2$.

Proof: consider $\phi : H_1 \times H_2 \longrightarrow G$, $(h_1, h_2) \longrightarrow h_1 h_2$. Then

$\phi((h_1,h_2)\cdot(h_1',h_2')) = \phi(h_1 h_1', h_2 h_2')$

$= h_1 h_1' h_2 h_2'$

$= h_1 h_2 h_1' h_2'$ by ii)

$= \phi(h_1,h_2)\cdot\phi(h_1',h_2')$

so ϕ is a homomorphism.

ϕ is surjective by (iii)

If $\phi(h_1,h_2) = e_G$, then $h_1 h_2 = e_G$

so $h_1 = h_2^{-1} \in H_1 \cap H_2$.

By i), $h_1 = h_2 = e$, so ϕ is injective. □

Groups of small order

Proposition: Let G be a finite group where every non-trivial element has order 2. Then $G \cong C_2 \times C_2 \times \cdots \times C_2$.

Proof: First we show G is abelian. If $a, b \in G$ then $a^2 = e$, $b^2 = e$, $(ab)^2 = e$

$abab = e$ so $ab = b^{-1}a^{-1} = ba$, as $a = a^{-1}$, $b = b^{-1}$.

Let $a_1 \in G$ be a non-identity element and consider $G_1 = H_1 = \langle a_1 \rangle \leq G$.

Then $G_1 \cong C_2$. If $G_1 = G$ (i.e. if $|G| = 2$) then $G \cong C_2$ so done.

Otherwise, choose $a_2 \in G \setminus G_1$ and let $H_2 = \langle a_2 \rangle$. Let $G_2 = \langle a_1, a_2 \rangle$ be the subgroup generated by a_1 and a_2. Apply the direct product theorem to $H_1, H_2 \leq G_2$. Then i) is satisfied, as $a_2 \notin G_1$, ii) is satisfied as G is abelian and iii) is satisfied as G_2 is generated by a_1 and a_2 by definition.

$\Rightarrow G_2 \cong H_1 \times H_2 \cong C_{n_2} \times C_2$.

If $|G| = 4$, then $G = G_2 \cong C_2 \times C_2$. If not, choose an $a_3 \in G \setminus G_2$ and continue as above. This terminates as G is finite. □

Begin the classification (order ≤ 8)

1. Prime order: If $|G| = p$ is prime, then choose a $g \in G \setminus \{e\}$: it then has order p, so $\langle g \rangle \cong C_p$. As $|\langle g \rangle| = p$, $G = \langle g \rangle$. So $G \cong C_p$.

2. Order 4: Claim that C_4, $C_2 \times C_2$ are all the groups of order 4.

- These are not isomorphic, as C_4 contains an element of order 4, but $C_2 \times C_2$ does not.

If G is some group of order 4, by Lagrange's theorem, the elements of G can have order 1, 2 or 4.

If $g \in G$ has order 4, then $\langle g \rangle \leq G$ but these have the same order, so $G = \langle g \rangle \cong C_4$.

If no element of G has order 4, then all non-identity elements have order 2. By the previous proposition, we must have $G \cong C_2 \times C_2$.

- 3. Order 6: Claim that C_6, $S_3 \ (\cong D_6)$ are all such groups.

Not isomorphic as C_6 has an element of order 6 and S_3 does not.

If $g \in G$, where $|G| = 6$, then $\text{ord}(g) = 1, 2, 3$, or 6. If there is an element of order 6, then $\langle g \rangle = G$, so $G \cong C_6$.

Otherwise, all elements have order 1, 2, or 3. By Cauchy's Theorem, there is an element $s \in G$ of order 2. Then $\langle s \rangle \cong C_2$ has order 2, so $G/\langle s \rangle$ has $3 = \frac{|G|}{|\langle s \rangle|} = \frac{6}{2}$ elements by Lagrange's Theorem.

- The set $G/\langle s \rangle$ has a left G-action via $g * (g'\langle s \rangle) = gg'\langle s \rangle$.

This gives a homomorphism $\rho : G \longrightarrow \text{Sym}(G/\langle s \rangle) \cong S_3$,

↑ pick a bijection from $G/\langle s \rangle$ to $\{1, 2, 3\}$

and $|S_3| = 3! = 6$.

If $g \in \ker(\rho)$ then $g'\langle s \rangle = g * (g'\langle s \rangle) = gg'\langle s \rangle$ for any $g' \in G$.

In particular, $e\langle s \rangle = ge\langle s \rangle$ so $g \in \langle s \rangle$, so $g = e$ or $g = s$.

If $g = s$, then $sg'\langle s \rangle = g'\langle s \rangle$ for all g'.

- $\Rightarrow (g')^{-1} s g' \in \langle s \rangle$ for all g'.

$\Rightarrow (g')^{-1} s g' = e$ or s $\Rightarrow (g')^{-1} s g' = s$ for all $g' \Rightarrow sg' = g's$ for all g' $(*)$

impossible as if $(g')^{-1} s g' = e \Rightarrow s = e!$: $e(e-1)\ldots$

Again by Cauchy, there is an $r \in G$ of order 3. Consider rs. What is its order?

- 1? $rs = e$ then $r = s^{-1} = s$ has order 2 and 3 ✗

2? $(rs)^2 = rsrs = rrss$ by $(*)$

$= r^2 \neq e$ as $\text{ord}(r) = 3$

3? $(rs)^3 = rsrsrs = r^3 s^3$ by $(*)$

$= s^3 = s \neq e$.

So rs has order 6, this is a contradiction, as we supposed G has no elements of order 6. This shows that $s \notin \ker(\rho)$, so $\ker(\rho) = \{e\}$, and hence ρ is injective.

- As $|G| = |S_3| = 6$, ρ is an isomorphism. □

4. Order 8: Claim that $\overbrace{C_8, C_4 \times C_2, C_2 \times C_2 \times C_2}^{\text{abelian}}, \overbrace{D_8, \text{ and } Q_8}^{\text{non-abelian}}$ are all the groups of order 8 up to isomorphism.

The first three are distinguished by the maximal order of an element they contain. Q_8 only has -1 as an element of order 2. D_8 contains s, r^2 of order 2, so $D_8 \not\cong Q_8$.

- An element $g \in G$ has order 1, 2, 4, or 8, by Lagrange's Theorem. If there is an element of order 8, then $G = \langle g \rangle \cong C_8$. If all elements have order 1 or 2, then by our proposition, $G \cong C_2 \times C_2 \times C_2$.

This leaves the case where G has no elements of order 8, but does have an element $f \in G$ of order 4.

The subgroup $\langle f \rangle$ has order 4, so it has index 2 by Lagrange. So call the cosets $e\langle f \rangle$ and $g\langle f \rangle$ for some $g \in G \setminus \langle f \rangle$. Then

- $G = \{e, f, f^2, f^3, g, gf, gf^2, gf^3\}$.

In which coset is g^2? If $g^2 \in g\langle f \rangle$, then $g \in \langle f \rangle$, contradiction.

So $g^2 \in \langle f \rangle$.

L13.3

If $g^2 = f$ or f^3, then $g^4 = f^2 \Rightarrow \text{ord}(g) = 8$, contradiction.

So the remaining possibilities are $g^2 = e$ or $g^2 = f^2$.

Suppose $g^2 = e$. The element fg lies in $e\langle f\rangle$ or in $g\langle f\rangle$. The first case is impossible as $fg \in \langle f\rangle \Rightarrow g \in \langle f\rangle$, a contradiction. Then

- $fg \in g\langle f\rangle = \{gf, gf^2, gf^3, g\}$

so $g^{-1}fg \in \{e, f, f^2, f^3\}$. As f has order 4, so does $g^{-1}fg$. So

$g^{-1}fg \in \{f, f^3\}$. If $g^{-1}fg = f$, then $fg = gf$, and G is abelian.

Apply Direct Product Theorem to $H_1 = \langle f\rangle$, $H_2 = \langle g\rangle$.

i) $H_1 \cap H_2 = \{e\}$.

ii) G is abelian

iii) f & g generate G

So $G \cong H_1 \times H_2 \cong C_4 \times C_2$.

If $g^{-1}fg = f^3 = f^{-1}$, we recognise the group as D_8.

Suppose $g^2 = f^2$. As above, $g^{-1}fg \in \{f, f^3\}$.

- If $g^{-1}fg = f$, then $fg = gf$ so G is abelian. Then gf^{-1} has order 2, since $(gf^{-1})^2 = gf^{-1}gf^{-1} = g^2f^{-2} = e$. Apply Direct Product Theorem to $H_1 = \langle f\rangle$ and $H_2 = \langle gf^{-1}\rangle$. The properties are satisfied, so $G \cong C_4 \times C_2$.

- $g^{-1}fg = f^3 = f^{-1}$. One checks that $\phi : G \to Q_8$ given by

$e \to \underline{1}$ $\quad g \to \underline{j}$

$f \to \underline{i}$ $\quad gf \to -\underline{k}$

$f^2 \to -\underline{1}$ $\quad gf^2 \to -\underline{j}$

$f^3 \to -\underline{i}$ $\quad gf^3 \to \underline{k}$, is an isomorphism. □

Normal subgroups

Def^n: a subgroup $H \leq G$ is called normal, if, for all $h \in H$ and $g \in G$, $ghg^{-1} \in H$. Write $H \triangleleft G$.

Examples i) For any G, $\{e\} \leq G$ and $G \leq G$ are both normal.

ii) The subgroup generated by the rotations in D_{2n} is normal.

The subgroup $\langle s \rangle \leq D_{2n}$ is not normal for $n \geq 3$.

iii) If G is abelian then all subgroups are normal, as $ghg^{-1} = h \; \forall g, h \in G$.

Lemma: a subgroup $H \leq G$ is normal iff $Hg = gH \; \forall g \in G$.

Proof: Suppose $H \triangleleft G$. Let $h \in H, g \in G$. Then $ghg^{-1} \in H$, so $ghg^{-1} = h'$, so $gh = h'g$. So $gH \subset Hg$. Conversely, $Hg \subset gH$, so $Hg = gH$. (*)

Suppose instead that (*) holds $\forall g \in G$. Then if $h \in H$, $gh \in gH = Hg$, so $gh = h'g$ for some $h' \in H$. But then $ghg^{-1} = h' \in H$. □

Corollary: if $H \leq G$ of index 2, then $H \triangleleft G$.

Proof: H has two left cosets in G, so $G = eH \cup gH$ for some g. But it also has 2 right cosets, so $G = He \cup Hg'$. As $g \notin He$, we must have $g \in Hg'$, so $Hg' = Hg$. So Hg is complement of H in G, as is gH, so $gH = Hg$ and H is normal. □

Proposition: Let $\phi : G \to K$ be a group homomorphism. Then $\ker(\phi)$ is a normal subgroup of G.

Proof: Let $h \in \ker(\phi)$, $g \in G$. Then $\phi(ghg^{-1}) = \phi(g)\underbrace{\phi(h)}_{e}\phi(g)^{-1}$

$= \phi(g)\phi(g)^{-1} = e$, so $ghg^{-1} \in \ker(\phi)$. □

Quotient group Let $H \leq G$, and consider G/H. Try to define a group operation on this set by

$$(g_1H)\cdot(g_2H) =: g_1g_2H.$$

This satisfies G1, G2, G3, so long as it is well-defined.

Let $g_1'H = g_1H$ and $g_2'H = g_2H$, so $g_1' = g_1h_1$, $g_2' = g_2h_2$

$$(g_1'H)(g_2'H) = g_1'g_2'H = g_1h_1g_2h_2H$$

$$= g_1h_1g_2H$$

[If H is normal, $g_2^{-1}h_1g_2 \in H$, so $g_2^{-1}h_1g_2 = h_3$]

$$= g_1g_2(g_2^{-1}h_1g_2)H$$

$$= g_1g_2H \text{ as } g_2^{-1}h_1g_2 \in H.$$

Theorem: If $H \trianglelefteq G$, then $(g_1H)\cdot(g_2H) = g_1g_2H$ is a well defined binary operation on the set G/H, and the data $(G/H, \cdot, eH)$ is a group.

Def: in the above situation, G/H is called the quotient group of G by H.

Examples i) The subgroup $n\mathbb{Z} \leq \mathbb{Z}$ is normal since $\mathbb{Z}$ is abelian. So can form $\mathbb{Z}/n\mathbb{Z}$, the quotient group. Consider

$$\phi : \mathbb{Z}_n \to \mathbb{Z}/n\mathbb{Z}$$
$$k \longrightarrow k + n\mathbb{Z}$$

[If $k + n\mathbb{Z} = k' + n\mathbb{Z}$, $k - k' \in n\mathbb{Z}$, so $k \equiv k' \bmod n$]

ϕ is a bijection. It is clearly a homomorphism.

So $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

ii) $R = \{ id, r, r^2, \dots, r^{n-1} \} \leq D_{2n}$. This is normal, as

- $(r^i s) r^j (r^i s)^{-1} = r^i s r^j s^{-1} r^{-i} = r^i r^{-j} r^{-i}$ as $srs^{-1} = r^{-1}$

$$= r^{-j} \in R$$

$$r^i r^j (r^i)^{-1} = r^i r^j r^{-i} = r^j \in R$$

So have quotient group D_{2n}/R. By Lagrange:

$$|D_{2n}/R| = \frac{|D_{2n}|}{|R|} = \frac{2n}{n} = 2.$$

So $D_{2n}/R \cong C_2$. Its elements are $\{eR, sR\}$.

iii) Consider $K = \{ id, r^2 \} \leq D_8$. By the calculation above this is normal. So can form the quotient group D_8/K. This has size $\frac{|D_8|}{|K|} = 4$.

Its elements are $\{eK, sK, rK, rsK\}$ (these are all distinct).

Note $(rK)\cdot(rK) = r^2K = eK$ as $r^2 \in K$.

$(sK)\cdot(sK) = s^2K = eK$

$(rsK)\cdot(rsK) = rsrsK = r\cdot r^3 \cdot s\cdot s\, K = eK$ using $sr = r^{-1}s = r^3 s$, $r^4 = e$, $s^2 = e$.

- So by our classification $D_8/K \cong C_2 \times C_2 \cong D_4$

iv) Consider $K = \{ 1, -1 \} \leq Q_8$. This is normal (in fact, it is in the centre of Q_8). We can form Q_8/K a group of order 4.

Its elements are $\{ 1K, iK, jK, kK \}$, and

$(iK)\cdot(iK) = i^2K = -1K = 1K$ similarly $(jK)^2 = (kK)^2 = 1K$,

so again $Q_8/K \cong C_2 \times C_2$.

v) Both D_8 and Q_8 contain normal subgroups iso. to C_2, and the quotient groups are iso. to $C_2 \times C_2$. But $D_8 \not\cong Q_8$.

The isomorphism theorem: Let $\phi: G \to H$ be a homomorphism.

Then the function $\bar{\phi}: G/\mathrm{Ker}(\phi) \longrightarrow \mathrm{Im}(\phi)$

$$g\,\mathrm{Ker}(\phi) \longrightarrow \phi(g)$$

is well-defined, and is a group isomorphism.

Proof: We know $\mathrm{Ker}(\phi) \trianglelefteq G$, so we have a quotient group $G/\mathrm{Ker}(\phi)$.

If $g\,\mathrm{Ker}(\phi) = g'\,\mathrm{Ker}(\phi)$, then $g' = gh$ for some $h \in \mathrm{Ker}(\phi)$. So

$\phi(g') = \phi(gh) = \phi(g)\underbrace{\phi(h)}_{e \text{ as } h \in \mathrm{Ker}(\phi)} = \phi(g)$. Thus $\bar{\phi}(g\,\mathrm{Ker}(\phi)) = \bar{\phi}(g'\,\mathrm{Ker}(\phi))$

and $\bar{\phi}$ is well-defined.

Consider $\bar{\phi}(a\,\mathrm{Ker}(\phi)\cdot b\,\mathrm{Ker}(\phi)) = \bar{\phi}(ab\,\mathrm{Ker}(\phi))$

$= \phi(ab)$

$= \phi(a)\,\phi(b)$ as ϕ is a hom.

$= \bar{\phi}(a\,\mathrm{Ker}(\phi))\,\bar{\phi}(b\,\mathrm{Ker}(\phi))$,

so $\bar{\phi}$ is a homomorphism.

The map $\bar{\phi}$ is surjective by definition of $\mathrm{Im}(\phi)$.

For injectivity, suppose $\bar{\phi}(g\,\mathrm{Ker}(\phi)) = e_H$.

$\phi(g) =$

so $g \in \mathrm{Ker}(\phi)$. So $g\,\mathrm{Ker}(\phi) = e\,\mathrm{Ker}(\phi) = e_{G/\mathrm{Ker}(\phi)}$. □

Example

i) The function $\phi: (\mathbb{Z}, +, 0) \to (\mathbb{Z}_n, +_n, 0)$ given $\phi(k) = k \bmod n$

is a hom. as $\phi(k+k') = (k+k') \bmod n = k \bmod n \;+_n\; k' \bmod n$.

ϕ is surjective, so $\mathrm{Im}(\phi) = \mathbb{Z}_n$. $\mathrm{Ker}(\phi) = \{k \in \mathbb{Z} : k \bmod n = 0\} = n\mathbb{Z}$

Isomorphism Theorem $\Rightarrow \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

ii) The function $\phi : (\mathbb{R}, +, 0) \longrightarrow (\mathbb{C}\setminus\{0\}, \times, 1)$

$$t \longrightarrow e^{2\pi i t}$$

is a homomorphism. It has

$$\mathrm{Im}(\phi) = \{ z \in \mathbb{C}\setminus\{0\} : |z| = 1 \} =: S^1$$

the unit complex numbers.

$$\mathrm{Ker}(\phi) = \{ t \in \mathbb{R} : e^{2\pi i t} = 1 \} = \mathbb{Z}$$

Isomorphism Theorem $\Rightarrow \mathbb{R}/\mathbb{Z} \cong S^1$.

iii) If G and H are groups, we have direct product $G \times H$. This has a subgroup $\{e\} \times H$.

Claim: this is normal. Let $(e,h) \in \{e\}\times H$ and $(a,b) \in G \times H$.

$$\begin{aligned}(a,b)(e,h)(a,b)^{-1} &= (a,b)(e,h)(a^{-1}, b^{-1}) \\ &= (aea^{-1}, bhb^{-1}) \\ &= (e, bhb^{-1}) \in \{e\}\times H.\end{aligned}$$

□

What is $\dfrac{G\times H}{\{e\}\times H}$? Consider $\phi : G\times H \longrightarrow G$ This is a homomorphism

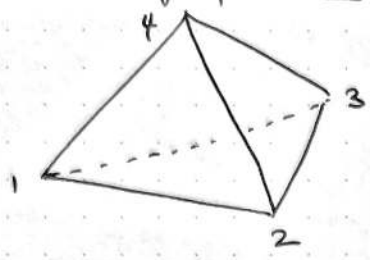
$$(g,h) \longrightarrow g.$$

It is surjective, so $\mathrm{Im}(\phi) = G$. $\mathrm{Ker}(\phi) = \{(g,h) \in G\times H : g = e\}$

$$= \{e\} \times H.$$

Isomorphism Theorem $\Rightarrow \dfrac{G\times H}{\{e\}\times H} \cong G$.

iv) Let G be the group of <u>all</u> symmetries of the regular tetrahedron.



(not just rotations)

G acts on the set $\{1,2,3,4\}$ of vertices, giving $\rho : G \to \mathrm{Sym}\{1,2,3,4\} \cong S_4$.

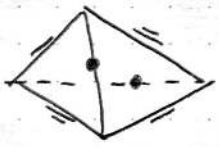
An isometry of $\mathbb{R}^3$ fixing 4 points which are not coplanar is Id, so ρ is injective.

$|S_4| = 4! = 24$

By the isomorphism theorem $G \cong G/\mathrm{Ker}(\rho)$
$\cong \mathrm{Im}(\rho)$
$\leq S_4$.

So $|G|$ divides $|S_4| = 24$. As $|G| > 12$, because it contains 12 rotations + ≥ 1 reflections, $|G| = 24$.

Therefore ρ is an isomorphism: $G \cong S_4$.



Let X denote the set of opposite pairs of edges on the tetrahedron: there are three. G acts on X, giving a homomorphism $\phi : G \to \mathrm{Sym}(X) \cong S_3$.

Have $|S_3| = 3! = 6$. Rotating around the vertical axis gives the permutation $(\backslash\ \backslash\ \bullet)$, of order 3.

Reflecting in the vertical plane gives $(\backslash\ \backslash)$, of order 2.

Thus 2 and 3 divide $|\mathrm{Im}(\phi)|$, so 6 divides this and hence $\mathrm{Im}(\phi) = S_3$ and ϕ is surjective.

Isomorphism theorem: $G/\mathrm{Ker}(\phi) \cong S_3$

Rephrasing: $\exists\ K \lhd S_4$ s.t. $S_4/K \cong S_3$.

<u>Def^n</u>: A non-trivial finite group is <u>simple</u> if its only normal subgroups are $\{e\}$ and G.

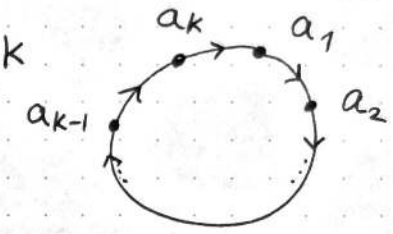
For such groups we cannot decompose them as $H \triangleleft G$ and G/H.

- Example: C_p is simple for p prime

Permutations For a set X, $\mathrm{Sym}(X)$ is the group of bijections $\sigma : X \to X$. Such a function is also called a permutation.
For $X = \{1, \dots, n\}$ call $\mathrm{Sym}(X) = S_n$. We have $|S_n| = n!$

Def^n Given a list $a_1, a_2, \dots, a_k \in \{1, \dots, n\}$ of distinct elements, the cycle $(a_1\ a_2 \cdots a_k) \in S_n$ is the permutation given by:

- $$(a_1 \cdots a_k)(i) = \begin{cases} a_{j+1} & \text{if } i = a_j \text{ and } j < k \\ a_1 & \text{if } i = a_k \\ i & \text{otherwise} \end{cases}$$



This is a bijection: $(a_k\ a_{k-1} \cdots a_2\ a_1)$ is an inverse for it.
It fixes exactly the elements not on the list: $\{1, \dots, n\} \setminus \{a_1, \dots, a_k\}$.
A transposition is a cycle of length 2: $(a\ b)$
Cycles $(a_1 \cdots a_k)$ and $(b_1 \cdots b_\ell)$ are called disjoint if $a_i \neq b_j\ \forall\ i, j$

Example: Cycles are permutations, so can be composed. Lets work out

- $(1234) \circ (324)$.

1 goes to 1 goes to 2
2 goes to 4 goes to 1 to give (12).
3 goes to 2 goes to 3
4 goes to 3 goes to 4

Now consider $(324)(1234)$ which is $(14) \neq (12)$.

Lemma i) Cycles can be cycled: $(a_1\ a_2 \cdots a_k) = (a_k\ a_1 \cdots a_{k-1})$
ii) Disjoint cycles commute: if $\sigma, \tau \in S_n$ are disjoint cycles, then $\sigma\tau = \tau\sigma$.

- Proof: i) Trivial

ii) Let $\sigma = (a_1 \cdots a_k)$, $\tau = (b_1 \cdots b_\ell)$.
For $i \in \{a_1, \dots, a_k\}$, we have

$\sigma(\tau(i)) = \sigma(i)$ as $i \notin \{b_1, \dots, b_\ell\}$ since σ, τ are disjoint

$\tau(\sigma(i)) = \sigma(i)$ as $\sigma(i) \in \{a_1, \dots, a_k\}$ outside of the b_js

For $i \notin \{a_1, \dots, a_k\}$, $\tau(\sigma(i)) = \tau(i)$ as σ fixes i, while

$\sigma(\tau(i)) = \tau(i)$ for $\tau(i) \notin \{a_1, \dots, a_k\}$ since i is not an a_i

So again $\sigma(\tau(i)) = \tau(\sigma(i))$ and hence $\sigma\tau = \tau\sigma$. □

Theorem (Disjoint Cycle Decomposition)

Every permutation in S_n is a composition of disjoint cycles

$$\sigma = (a_1^1\ a_2^1 \cdots a_{k_1}^1)(a_1^2 \cdots a_{k_2}^2) \cdots (a_1^r \cdots a_{k_r}^r)$$

in which every element $1, \dots, n$ appears exactly once.

write (12) as → (12)(3)(4)

Such a representation is unique up to cycling cycles and reordering cycles.

Proof: Go by induction on n. For $n=1$, $e \in S_1$ is (1).

For $n>1$, first prove the following, for $\sigma \in S_n$

Claim: there is a $k \in \mathbb{N}$ s.t. $\sigma^k(1) = 1$ and

$$1, \sigma(1), \sigma^2(1), \ldots, \sigma^{k-1}(1)$$

are all distinct.

Proof: Consider the infinite sequence $1, \sigma(1), \sigma^2(1), \ldots$

As $\{1, \ldots, n\}$ is finite, the sequence must have a repeat:

$\sigma^a(1) = \sigma^b(1)$ for some $a, b \in \mathbb{N}$ with $a < b$.

So $1 = \sigma^{b-a}(1)$, by acting with $(\sigma^a)^{-1}$.

Therefore there exists a $k \in \mathbb{N}$ s.t. $\sigma^k(1) = 1$.

Let k be the smallest such number. If $0 \leq i < j \leq k-1$ were such that $\sigma^i(1) = \sigma^j(1)$, then $1 = \sigma^{j-i}(1)$. This contradicts the fact that k was the smallest such number. □

Consider the permutation $\tau = \sigma \circ (1\ \sigma(1) \cdots \sigma^{k-1}(1))^{-1}$.

This fixes $1, \sigma(1), \sigma^2(1), \ldots, \sigma^{k-1}(1)$ by inspection.

So τ is a permutation of $X = \{1, \ldots, n\} \setminus \{1, \sigma(1), \ldots, \sigma^{k-1}(1)\}$.

This has $< n$ elements, so τ can be written as a composition of disjoint cycles in the set X. As

$$\sigma = \tau \circ (1\ \sigma(1) \cdots \sigma^{k-1}(1))$$

we see that σ is a composition of disjoint cycles, as the sets X and $\{1, \sigma(1), \ldots, \sigma^{k-1}(1)\}$ are disjoint.

Suppose

$$(a_1^1\ a_2^1 \cdots a_{k(1)}^1)(a_1^2 a_2^2 \cdots a_{k(2)}^2) \cdots (a_1^r\ a_2^r \cdots a_{k(r)}^r) = (b_1^1\ b_2^1 \cdots b_{\ell(1)}^1)(b_1^2\ b_2^2 \cdots b_{\ell(2)}^2) \cdots (b_1^s\ b_2^s \cdots b_{\ell(s)}^s) \quad (*)$$

are two disjoint cycles decompositions where every number $1, \ldots, n$ appears.

Now $a_1^1 = b_i^j$ for some i, j. Then $a_2^1 = b_{i+1}^j$ and so on, cycling round if necessary. Applying the permutation to a_1^1 k_1 times brings it back to itself; applying to b_i^j ℓ_j times brings it back to itself.

L17.2 So $k_1 = l_j$ and

$$(a_1^1 a_2^1 \cdots a_{k_1}^1) = (b_1^j \; b_2^j \cdots b_{l_j}^j).$$

$$\overset{\text{renaming}}{=} (b_i^j \; b_{i+1}^j \cdots b_{l_j}^j \; b_1^j \cdots b_{i-1}^j) \quad \text{(cycling)}$$

Cancelling these cycles from both sides of (*) we arrive at the same problem for smaller n. □

Lemma: If $\sigma = (a_1^1 \cdots a_{k_1}^1) \cdots (a_1^r \cdots a_{k_r}^r)$ is a disjoint cycle decomposition, then the order of σ is

$$\text{lcm}(k_1, k_2, \ldots, k_r).$$

Example: in S_5, $(12)(345)$ has order 6

in S_6, $(1234)(56)$ has order 4

Proof: in any group, if $ab = ba$, then $(ab)^j = a^j b^j$.

$$\underbrace{abab\,ab \cdots ab}_{j \text{ times}}$$

So $\sigma^j = (a_1^1 \cdots a_{k_1}^1)^j \cdots (a_1^r \cdots a_{k_r}^r)^j$.

If $l = \text{lcm}(k_1, \ldots, k_r)$ then

$$(a_1^i a_2^i \cdots a_{k_i}^i)^l = \left[(a_1^i a_2^i \cdots a_{k_i}^i)^{k_i}\right]^{\frac{l}{k_i}} = e^{l/k_i} = e,$$

so $\sigma^l = e$. This just shows that the order of σ divides l.

Let m be the order of σ, so

$$e = \sigma^m = (a_1^1 \cdots a_{k_1}^1)^m \cdots (a_1^r a_2^r \cdots a_{k_r}^r)^m$$

and hence $(a_1^1 \cdots a_{k_1}^1)^m = \left[(a_1^2 a_2^2 \cdots a_{k_2}^2)^m \cdots (a_1^r \cdots a_{k_r}^r)^m\right]^{*_{k_1-1}}$.

The LHS fixes all a_n^j for $j \neq 1$

RHS fixes all a_n^j for $j = 1$.

Hence both sides fix <u>everything</u>, so the order k_1 of $(a_1^1 \cdots a_{k_1}^1)$ divides m.

Similarly, all k_i divide m, so $\text{lcm}(1, \ldots, k_r)$ divides m. □

The sign of a permutation

Proposition: Every permutation in S_n is a composition of transpositions.

Proof: Go by induction on n. Clear for $n \leq 2$.
For $\sigma \in S_n$, consider $(n\ \sigma(n)) \circ \sigma = \tau$ which fixes n, so is a permutation of $\{1, \dots, n-1\}$. Then τ is a composition of transpositions and $\sigma = (n\ \sigma(n)) \circ \tau$ is as well. □

We want to define the sign of a permutation σ as follows

$$\operatorname{sign}(\sigma) = (-1)^{\#\text{ transpositions necessary to write } \sigma \text{ as a composition of transpositions}}$$

Proof: If $\tau = (a_1^1\ a_2^1 \cdots a_{k_1}^1) \cdots (a_1^r\ a_2^r \cdots a_{k_r}^r)$

and $\sigma \in S_n$, then by the proposition

$$\sigma\tau\sigma^{-1} = (\sigma(a_1^1) \cdots \sigma(a_{k_1}^1)) \cdots (\sigma(a_1^r) \cdots \sigma(a_{k_r}^r))$$

which is again a composition of disjoint cycles, and has the same number of cycles of each length as τ.

Conversely, if τ and τ' have the same number of cycles of each length, then we can write them as

$$\tau = (a_1^1\ a_2^1 \cdots a_{k_1}^1)(a_1^2\ a_2^2 \cdots a_{k_2}^2) \cdots (a_1^r\ a_2^r \cdots a_{k_r}^r)$$

$$\tau' = (b_1^1\ b_2^1 \cdots b_{k_1}^1)(b_1^2\ b_2^2 \cdots b_{k_2}^2) \cdots (b_1^r\ b_2^r \cdots b_{k_r}^r)$$

where every number $1, 2, \ldots, n$ appears. Let

$$\sigma : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}$$
$$a_j^i \longrightarrow b_j^i.$$

This is a bijection (it is clearly surjective as every $1, \ldots, n$ is some b_j^i). Then $\sigma\tau\sigma^{-1} = \tau'$ by construction, so τ and τ' are conjugate. □

We can record conjugacy classes as

$$1^{a_1} 2^{a_2} \cdots n^{a_n} \longleftrightarrow \{\sigma \in S_n \mid \text{when } \sigma \text{ is disjoint cycle decomposed it has } a_i \ i\text{-cycles } \forall i\}$$

"cycle type"

Recall that conjugacy classes are orbits of the conjugation action of a group G on itself. The stabiliser of $g \in G$ is called the centraliser, and is $C_G(g) = \{h \in G : hgh^{-1} = g\}$.

Lemma: if $\sigma \in S_n$ has cycle type $1^{a_1} 2^{a_2} \cdots n^{a_n}$, then

$$|C_{S_n}(\sigma)| = 1^{a_1} \cdot a_1!\ 2^{a_2} \cdot a_2! \cdots n^{a_n} \cdot a_n!$$

Proof: By the uniqueness of disjoint cycle notation, two ways of writing σ as disjoint cycles can only differ by cycling the cycles and reordering the cycles. The number of ways to do this is

$$\prod_{i=1}^{n} i^{a_i} a_i!$$

(i^{a_i}: # ways cycling i-cycles; $a_i!$: # ways reordering i-cycles)

If $h \in C_{S_n}(\sigma)$ then $\sigma = h\sigma h^{-1}$, giving two different ways of writing the same permutation as disjoint cycles. But we just counted these. □

So by OST, if σ has cycle type $1^{a_1} \cdots n^{a_n}$, then

$$|cl(\sigma)| = \frac{n!}{1^{a_1} a_1! \cdots n^{a_n} a_n!}$$ which is neat. ●

Example Consider S_4. The conjugacy classes are indexed by $1^{a_1} 2^{a_2} \cdots 4^{a_4}$ such that $\sum i a_i = 4$.

So 1^4, $1^2 2^1$, 2^2, $1^1 3^1$, 4^1 are the 5 conjugacy classes.

The class 1^4 consists of permutations having 4 1-cycles: this consists just of $\{e\}$, a conjugacy class of size 1.

The conjugacy class $1^2 2^1$ consists of transpositions, e.g. $(12)(3)(4)$.

This has size $\frac{4!}{1^2 2! 2^1 1!} = 6 = \binom{4}{2}$ so is ●

$(12)(3)(4)$ $(13)(2)(4)$ $(14)(2)(3)$

$(23)(1)(4)$ $(24)(1)(3)$ $(34)(1)(2)$.

What is the centraliser of $(12)(3)(4)$? It must have 4 elements:

e, $(12)(3)(4)$, $(1)(2)(34)$, $(12)(34)$

The conjugacy class 2^2 consists of double transpositions, e.g. $(12)(34)$

This has size $\frac{4!}{2^2 2!} = 3$ so is $(12)(34)$, $(13)(24)$, $(14)(23)$

The centraliser of $(12)(34)$ has order 8: it is an exercise to work out what it is.

L19.3

The conjugacy class $1^1 3^1$ consists of 3-cycles, e.g. $(123)(4)$.
It has size $\frac{4!}{1^1 1! 3^1 3!} = 8$. The centraliser of $(123)(4)$ has 3 elements, so is e, (123), $(123)^2 = (132)$.

The conjugacy class 4^1 consists of 4-cycles, of which there are $\frac{4!}{4^1 1!} = 6$. The centraliser of (1234) has order 4, so is e, (1234), $(1234)^2 = (13)(24)$, $(1234)^3 = (1432)$.

If H is a normal subgroup of G, and $h \in H$, then $ghg^{-1} \in H$ for any $g \in G$. So H is a union of conjugacy classes in G.

Example: What are the normal subgroups of S_4?
H contains e, so contains the conjugacy class 1^4.
If the conjugacy class $1^2 2^1$ lies in H, then all transpositions lie in H, so H is the whole group, as any permutation is a composition of transpositions.
If H contains 2^2, the 3 double transpositions, then it contains at least e, $(12)(34)$, $(13)(24)$, $(14)(23)$.
This is a subgroup, called K, by inspection. So $K \triangleleft S_4$.
If H contains $1^1 3^1$ of 3-cycles, then it contains 8 3-cycles + e, so ≥ 9 elements. By Lagrange $|H|$ divides $|S_4| = 24$, so $|H| = 12$ or $|H| = 24$ and $H = S_4$. In the first case we must have $H = A_4 \triangleleft S_4$. (produce double transpositions, so all even)
If H contains 4^1, then it contains all 4-cycles, but
$(1234)(1324) = (142)(3)$
so this reduces to the previous case.
So the normal subgroups of S_4 are $\{e\}$, K, A_4, S_4.

The quotient groups of S_4 are

- $S_4/\{e\} = S_4$, $S_4/K = S_3$ (c.f. lecture 16 tetrahedron)
- $S_4/A_4 = C_2$, $S_4/S_4 = \{e\}$ △

Lets discuss conjugation in $A_n \leq S_n$

Remark: recall $ccl(\sigma)$ denotes the conjugacy class of $\sigma \in G$. Lets denote this by $ccl_G(\sigma)$ for now.

If $\sigma \in A_n$ and τ is conjugate to σ in A_n, then it is also conjugate to σ in S_n: so $ccl_{A_n}(\sigma) \subset ccl_{S_n}(\sigma)$

- but these need not be equal.

Example: consider $(123), (132) \in A_3$. These are conjugate in S_3 as they have the same cycle type, 3^1. But $A_3 \cong C_3$ is abelian, so elements are conjugate in A_3 iff they are equal.

On the other hand, if $(123), (132) \in A_5$ then

$\underbrace{((12)(45))}_{\in A_5}(123)((12)(45))^{-1} = (213) = (132)$

so (123) and (132) are conjugate in A_5. △

- Using OST for the conjugation action of A_n or S_n on themselves, get

$$|A_n| = |ccl_{A_n}(\sigma)|\,|C_{A_n}(\sigma)|$$
$$|S_n| = |ccl_{S_n}(\sigma)|\,|C_{S_n}(\sigma)|$$

but also $|S_n| = 2|A_n|$. So there are two possibilities:

1) $|ccl_{A_n}(\sigma)| = |ccl_{S_n}(\sigma)|$ and $|C_{A_n}(\sigma)| = \frac{1}{2}|C_{S_n}(\sigma)|$
2) $|ccl_{A_n}(\sigma)| = \frac{1}{2}|ccl_{S_n}(\sigma)|$ and $|C_{A_n}(\sigma)| = |C_{S_n}(\sigma)|$

Note $C_{A_n}(\sigma) = A_n \cap C_{S_n}(\sigma)$, so the possibilities are

- i) $C_{S_n}(\sigma)$ contains an odd element and $|ccl_{A_n}(\sigma)| = |ccl_{S_n}(\sigma)|$ so $ccl_{A_n}(\sigma) = ccl_{S_n}(\sigma)$.

ii) $C_{S_n}(\sigma)$ consists entirely of even elements, and $|ccl_{S_n}(\sigma)|$ is the union

of $\mathrm{ccl}_{A_n}(\sigma)$ and another ccl of the same size.

Example: conjugacy classes in A_4

The conjugacy class 1^4 in S_4 consists of the identity, which is also a conjugacy class in A_4.

The conjugacy class $1^3 2^1$ consists of odd elements so is not in A_4.

The conjugacy class 2^2 of double transpositions does lie in A_4. The element $(12)(34)$ is centralised by (12), an odd element, so this remains a single ccl.

The conjugacy class $1^1 3^1$ of 3-cycles is even so lies in A_n. Know

$C_{S_4}((123)) = \{e, (123), (132)\}$ as we know this group has order 3

consists of even elements, so this ccl in S_4 splits into two ccls in A_4, of size 4 each. They are

$\{(123), (142), (134), (243)\}$

$\{(132), (143), (124), (234)\}$.

The ccl 4^1 in S_4 consists of odd elements so does not lie in A_4.

Example: Normal subgroups of A_4

If $H \triangleleft A_4$ contains the conjugacy class 2^2, then can have $H = K = \{e, (12)(34), (13)(24), (14)(23)\}$.

If $H \triangleleft A_4$ contains one of the two conjugacy classes of 3-cycles, then as these conjugacy classes are related to each other by inversion it must contain both conjugacy classes of 3-cycles. This gives ≥ 9 elements in H, so $H = A_4$ by Lagrange.

So normal subgroups are $\{e\}$, K, A_4

with quotient groups $A_4/\{e\} = A_4$, $A_4/K = A_3$, $A_4/A_4 = \{e\}$.

Theorem: the group A_5 is simple, i.e. it has no non-trivial normal subgroups

Proof: the group S_5 has $5! = 120$ elements. The conjugacy classes can be summarised as

cl	1^5	$1^3 2^1$	$1^1 2^2$	$1^2 3^1$	$1^1 4^1$	5^1	$2^1 3^1$
element	e	(12)	$(12)(34)$	(123)	(1234)	(12345)	$(12)(345)$
sign	+	−	+	+	−	+	−
size	1	10	15	20	30	24	20

In A_5, only have conjugacy classes of even elements. Need to work out whether conjugacy classes in S_5 remain conjugacy classes or split into two.

The cl $1^1 2^2$ is centralised by (12) which is odd, so remains a single cl.

The cl $1^2 3^1$: (123) is centralised by (45), so remains a single cl.

The class 5^1: $C_{S_5}((12345)) = \langle (12345) \rangle$, so consists of even elements. So this splits into 2 cls, of size 12 each.

So	cl	1^5	$1^1 2^2$	$1^2 3^1$	5^1	$\neq$	5^1
	size	1	15	20	12		12

If $H \triangleleft A_5$, then its order would

i) divide $|A_5| = 60$,

ii) be a sum of the sizes of these cls containing 1^5.

There are no such numbers other than 1 and 60.

Hence A_5 is simple. □

Groups of matrices

Write $\mathbb{F}$ for $\mathbb{R}$ or $\mathbb{C}$ in this section.

The general linear and special linear groups

$$M_{n\times n}(\mathbb{F}) = \{ n\times n \text{ matrices with entries in } \mathbb{F} \}$$

Matrix multiplication is a function

$$\cdot : M_{n\times m}(\mathbb{F}) \times M_{m\times k}(\mathbb{F}) \longrightarrow M_{n\times k}(\mathbb{F})$$

which gives a binary operation

$$\cdot : M_{n\times n}(\mathbb{F}) \times M_{n\times n}(\mathbb{F}) \longrightarrow M_{n\times n}(\mathbb{F}).$$

This is associative.(G1) The identity matrix

$$I_n = \begin{pmatrix} 1 & & 0 \\ & 1 & \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

is an identity element for $\cdot$: $A \cdot I_n = A$.(G2)

Not all matrices have inverses. A is invertible iff $\det(A) \neq 0$.(G3)

Def^n: The n^{th} general linear group is

$$GL_n(\mathbb{F}) = \{ A \in M_{n\times n}(\mathbb{F}) \text{ with } \det(A) \neq 0 \}.$$

Lemma: the data $(GL_n(\mathbb{F}), \cdot, I_n)$ is a group. → so is closed since $(AB)^{-1} = B^{-1}A^{-1}$

We know $\det(AB) = \det(A)\det(B)$, so

$$\det : (GL_n(\mathbb{F}), \cdot, I_n) \longrightarrow (\mathbb{F}\setminus\{0\}, \times, 1) \qquad (*)$$

is a homomorphism.

Def^n: the n^{th} special linear group is

$$SL_n(\mathbb{F}) = \{ A \in GL_n(\mathbb{F}) \text{ with } \det(A) = 1 \}.$$

This is the kernel of $(*)$, so is a normal subgroup.

The homomorphism is surjective: for $\lambda \in \mathbb{F} \setminus \{0\}$,

$$\det \begin{pmatrix} \lambda & 0 & \\ 1 & 1 & \\ & \ddots & \\ 0 & & 1 \end{pmatrix} = \lambda.$$

So by the isomorphism theorem,

$$GL_n(\mathbb{F}) / SL_n(\mathbb{F}) \cong \mathbb{F} \setminus \{0\}.$$

The group $GL_n(\mathbb{F})$ acts on the vector space $\mathbb{F}^n$, where if we consider $\mathbb{F}^n$ as column vectors of length n, then

$$A * v := Av.$$

This corresponds to a homomorphism $\rho : GL_n(\mathbb{F}) \to Sym(\mathbb{F}^n)$.

This is injective, as if $Av = v$ for all vectors v, then $A = I_n$.

$$Im(\rho) = \left\{ \alpha : \mathbb{F}^n \to \mathbb{F}^n \text{ s.t. } \alpha \text{ is an invertible linear map} \right\}.$$

So $GL_n(\mathbb{F}) \cong \{ \text{linear isomorphisms } \alpha : \mathbb{F}^n \to \mathbb{F}^n \}$.

Change of basis

In V+M have seen that if $A \in M_{n \times n}(\mathbb{F})$ represents a linear map α in the standard basis $\{\underline{e}_1, \dots, \underline{e}_n\}$ of $\mathbb{F}^n$, then the matrix for α in a second basis $\{\underline{f}_1, \dots, \underline{f}_n\}$ is $P^{-1}AP$ where P is the invertible matrix determined by

$$\underline{f}_j = \sum_{i=1}^{n} P_{ij} \underline{e}_i.$$

Proposition: the group $GL_n(\mathbb{F})$ acts on the set $M_{n \times n}(\mathbb{F})$ on the right via $A \cdot P =: P^{-1}AP$.

Matrices $A, B \in M_{n \times n}(\mathbb{F})$ lie in the same orbit of this action iff A and B represent the same linear map $\mathbb{F}^n \to \mathbb{F}^n$ in different bases.

Proof: $(A \cdot P) \cdot Q = (P^{-1}AP) \cdot Q$

$= Q^{-1}P^{-1}APQ$

$= (PQ)^{-1}APQ$

$= A \cdot (PQ)$ so (A1) holds.

$A \cdot I_n = I_n^{-1} A I_n = A$ so (A2) holds.

The second part is an interpretation of the previous discussion.

Example In V+M, Jordan normal/canonical form says that any $A \in M_{\frac{n}{2}\times\frac{n}{2}}(\mathbb{C})$ is conjugate to one of

$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ with $\lambda_1 \neq \lambda_2$, ①

$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$, ②

$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$. "Jordan block" ③

We have $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \lambda_2 & 0 \\ 0 & \lambda_1 \end{pmatrix}$

so in case ① the order of the λ_i is not determined.

The matrices on this list are not conjugate to each other, apart from $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ and $\begin{pmatrix} \lambda_2 & 0 \\ 0 & \lambda_1 \end{pmatrix}$.

We have a complete description of the orbits of $GL_2(\mathbb{C})$ on $M_{2\times 2}(\mathbb{C})$ via this. What about stabilisers?

P stabilises A $\Leftrightarrow$ $P^{-1}AP = A$

$\Leftrightarrow$ $AP = PA$.

① $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ stabilises $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ $\Leftrightarrow$ $AP = PA$, so

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} = \begin{pmatrix} \lambda_1 a & \lambda_2 b \\ \lambda_1 c & \lambda_2 d \end{pmatrix}$

$$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \lambda_1 a & \lambda_1 b \\ \lambda_2 c & \lambda_2 d \end{pmatrix}$$

Comparing non-diagonal entries, using $\lambda_1 \neq \lambda_2$, gives $b = c = 0$.

So stabiliser of $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ is

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in GL_2(\mathbb{C}) \right\}.$$

② $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} = \lambda I_2$ commutes with all matrices, so

stabiliser is $GL_2(\mathbb{C})$.

③ $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ stabilises $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ if

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} \lambda a & a+\lambda b \\ \lambda c & c+\lambda d \end{pmatrix}$$

$$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \lambda a + c & \lambda b + d \\ \lambda c & \lambda d \end{pmatrix}$$

are equal. So $c = 0$, $a = d$ and hence stabiliser is

$$\left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in GL_2(\mathbb{C}) \right\}.$$

△

Le Möbius group

Recall that a $f \in \mathcal{M}$ can be written as $f(z) = \dfrac{az+b}{cz+d}$

where $a, b, c, d \in \mathbb{C}$ and $ad - bc \neq 0$.

We saw that if $f'(z) = \dfrac{a'z+b'}{c'z+d'}$, then

$$f'(f(z)) = \frac{a''z+b''}{c''z+d''} \quad \text{where} \quad \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

In other words, $\phi : SL_2(\mathbb{C}) \to \mathcal{M}$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \frac{az+b}{cz+d}$$

is a homomorphism.

Proposition: ϕ is surjective, and its kernel is $\{I_2, -I_2\}$.

Proof: For $f(z) = \frac{az+b}{cz+d}$, form $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ whose determinant $ad-bc \neq 0$ by definition. So it lies in $GL_2(\mathbb{C})$, but may not lie in $SL_2(\mathbb{C})$.

If we write $ad-bc = \Delta^2$, then $\Delta \neq 0$ and

$$\det \begin{pmatrix} a/\Delta & b/\Delta \\ c/\Delta & d/\Delta \end{pmatrix} = \frac{ad-bc}{\Delta^2} = 1$$

so $\begin{pmatrix} a/\Delta & b/\Delta \\ c/\Delta & d/\Delta \end{pmatrix} \in SL_2(\mathbb{C})$.

$$\phi \begin{pmatrix} a/\Delta & b/\Delta \\ c/\Delta & d/\Delta \end{pmatrix} = \frac{(a/\Delta)z + b/\Delta}{(c/\Delta)z + d/\Delta} = \frac{az+b}{cz+d} = f(z).$$

Hence ϕ is surjective.

If $\phi \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ = identity Möbius transformation, then

$$\frac{az+b}{cz+d} = z \qquad \forall z$$

$$\Rightarrow \quad 0 = cz^2 + (d-a)z - b \qquad \forall z$$

$$\Rightarrow \quad c = 0, \; a = d, \; b = 0$$

So $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$. This is in $SL_2(\mathbb{C})$, so $\det = 1$, $a^2 = 1$.

So it must be I_2 or $-I_2$, as claimed. □

Applying the Isomorphism Theorem,

$$\mathcal{M} \cong \frac{SL_2(\mathbb{C})}{\{I_2, -I_2\}} = PSL_2(\mathbb{C})$$

"projective special linear group"

Orthogonal and special orthogonal group

The transpose of $A \in M_{n\times m}(\mathbb{F})$ is $A^T \in M_{m\times n}(\mathbb{F})$ given by

$(A^T)_{ij} = A_{ji}$. It satisfies $(AB)^T = B^T A^T$.

Def: The n^{th} orthogonal group is $O(n) = \{P \in GL_n(\mathbb{R}) : P^T P = I_n\}$.

Lemma: $O(n) \leq GL_n(\mathbb{R})$

Proof: $I_n \in O(n)$, since $I_n^T = I_n \Rightarrow I_n^T I_n = I_n^2 = I_n$.

If $P \in O(n)$, $P^{-1} = P^T$ and $(P^{-1})^T = P \Rightarrow (P^{-1})^T P^{-1} = I_n$.

If $P, Q \in O(n)$, $(PQ)^T PQ = Q^T P^T P Q = I_n$. □

Recall that $\mathbb{R}^n$ has the standard inner product given by

$$x \cdot y = \sum_{i=1}^{n} x_i y_i = x^T y$$

where we consider elements of $\mathbb{R}^n$ as column vectors.

If we consider $P \in GL_n(\mathbb{R})$ as a change of basis matrix from the standard basis $\{e_1, e_2, \ldots, e_n\}$ to the basis $\{f_1, f_2, \ldots, f_n\}$ given by f_i being the i^{th} column of P. Then

$$(P^T P)_{ij} = \sum_{k=1}^{n} (P^T)_{ik} (P)_{kj} = \sum_{k=1}^{n} (P)_{ki} (P)_{kj} = f_i \cdot f_j$$

So $P \in O(n) \iff f_i \cdot f_j = \delta_{ij}$

$\iff \{f_1, \ldots, f_n\}$ is orthonormal

Example: $A, B \in M_{n\times n}(\mathbb{R})$ lie in the same orbit of the action of $O(n)$ by conjugation $\iff$ they represent the same linear map in two orthogonal bases.

Prop: A matrix $P \in GL_n(\mathbb{R})$ lies in $O(n)$ iff $Px \cdot Py = x \cdot y$ $\forall\, x, y \in \mathbb{R}^n$. In particular P preserves lengths and angles, since these are defined as $|x| = \sqrt{x \cdot x} = \sqrt{Px \cdot Px} = |Px|$

and $\cos\theta_1 = \dfrac{x \cdot y}{|x||y|} = \dfrac{Px \cdot Py}{|Px||Py|} = \cos\theta_2$.

Proof: Let $P \in O(n)$, $x, y \in \mathbb{R}^n$. Then

$$Px \cdot Py = (Px)^T Py = x^T P^T P y = x^T y = x \cdot y$$

Conversely, suppose $Q \in GL_n(\mathbb{R})$ satisfies $Qx \cdot Qy = x \cdot y$ $\forall\, x, y$.

Then $Qe_i \cdot Qe_j = e_i \cdot e_j = \delta_{ij}$.

But Qe_i = i^{th} column of matrix, so the columns of Q form an orthonormal basis. Then $Q \in O(n)$. □

A standard property of det is $\det(A^T) = \det(A)$. So if $P^TP = I_n$, then $1 = \det I_n = \det(P^TP) = \det P^T \det P = (\det P)^2$

$\Rightarrow \det(P) = \pm 1$. Also

$$\begin{pmatrix} -1 & & 0 \\ & 1 & \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$ has det -1.

Def^n the n^{th} special orthogonal group $SO_n(n)$ is $\{ P \in GL_n(\mathbb{R}) : P^TP = I_n \text{ and } \det P = 1 \}$, i.e. $\ker(\det : O(n) \to \{\pm 1\})$.

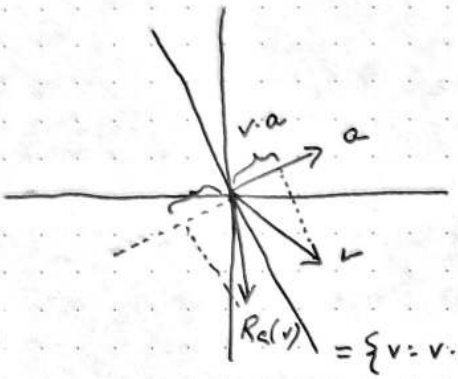
So $SO(n) \triangleleft O(n)$ has index 2.

Reflection

Def^n: For a vector $a \in \mathbb{R}^n$ of length 1 $[= |a| = \sqrt{a \cdot a}]$, the reflection in the plane normal to a is the linear map

$R_a : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ given by

$v \longrightarrow v - 2(v \cdot a)a$.



Lemma: For any vector a of length 1, $R_a \in O(n)$

Proof: let $v, w \in \mathbb{R}^n$ and consider

$R_a(v) \cdot R_a(w)$

$= (v - 2(v \cdot a)a) \cdot (w - 2(w \cdot a)a)$

$= v \cdot w - 2(w \cdot a)(v \cdot a) - 2(v \cdot a)(a \cdot w) + 4(v \cdot a)(w \cdot a)(a \cdot a)$ ($a \cdot a = 1$ as a has length 1)

$= v \cdot w$. This holds for all v, w, so by the previous prop^n, $R_a \in O(n)$. □

Lemma: for $P \in O(n)$, $P R_a P^{-1} = R_{Pa}$

Proof: apply $P R_a P^{-1}$ to v, giving $P(P^{-1}v - 2(P^{-1}v \cdot a)a)$

$= v - 2(P^{-1}v \cdot a)Pa$

Note $(P^{-1}v) \cdot a = (P^{-1}v)^T a = v^T (P^{-1})^T a$

but since P is orthogonal, $P^{-1} = P^T$ ($P^T P = I_n$), this gives

$v^T Pa = v \cdot (Pa)$. Hence

$(P R_a P^{-1})(v) = v - 2(v \cdot Pa)Pa = R_{Pa}(v)$. □

More basic properties of reflections:

i) $R_a(R_a(v)) = R_a(v - (v \cdot a)a) = R_a(v) - 2(R_a(v) \cdot a)a$

$= v - 2(v \cdot a)a - 2((v - 2(v \cdot a)a) \cdot a)a$

$= v - 2(v \cdot a)a - 2[v \cdot a - 2(v \cdot a)(a \cdot a)]a$ ($a \cdot a = 1$)

$= v - 2(v \cdot a)a + 2(v \cdot a)a$

$= v$ ☺ $\therefore R_a R_a = I$

The only possible eigenvalues are ± 1.

ii) Both eigenvalues arise:

$$R_a(a) = a - 2(a\cdot a)a = -a$$

so a is an eigenvector with eigenvalue -1

On the other hand, if w is orthogonal to a, then

$$R_a(w) = w - 2(w\cdot a)a = w$$

so w is an eigenvector with eigenvalue $+1$

If we choose a basis $\{f_2, f_3, \dots, f_n\}$ for the plane orthogonal to a, and set $f_1 = a$, then in the basis $\{f_1, \dots, f_n\}$, the matrix for R_a is $\begin{pmatrix} -1 & & 0 \\ & 1 & \\ 0 & & \ddots \\ & & & 1 \end{pmatrix}$

This shows $\det(R_a) = -1$, so $R_a \notin SO(n)$.

Reflections & Rotations in $\mathbb{R}^2$

Theorem: every element of $SO(2)$ is of the form $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ for some $0 \le \theta < 2\pi$. This is an anticlockwise rotation about the origin by an angle θ.

Proof: Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SO(2)$, so $A^TA = I_n$ and $\det A = 1$. So $A^T = A^{-1}$, i.e.

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

so $a = d$, $b = -c$. As $ad - bc = 1$, this gives $a^2 + c^2 = 1$. Thus there is a $0 \le \theta < 2\pi$ with $a = \cos\theta$, $c = \sin\theta$. So

$$A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$ as claimed. □

Theorem: every element of $O(2) \setminus SO(2)$ is a reflection.

Proof: Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in O_k(2) \setminus SO(2)$, so $A^TA = I_n$ and $\det A = -1$. So $A^T = A^{-1}$, i.e. $\begin{pmatrix} a & c \\ b & d \end{pmatrix} = \frac{1}{-1}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

hence $a=-d$, $b=c$. Using $ad-bc=-1$, get $a^2+c^2=1$

so $a=\cos\theta$, $c=\sin\theta$ for some $0\le\theta<2\pi$. Then

$A=\begin{pmatrix}\cos\theta & \sin\theta\\ \sin\theta & -\cos\theta\end{pmatrix}$. One can check with double-angle formulae that

$$\begin{pmatrix}\cos\theta & \sin\theta\\ \sin\theta & -\cos\theta\end{pmatrix}\begin{pmatrix}\sin\theta/2\\ -\cos\theta/2\end{pmatrix}=-\begin{pmatrix}\sin\theta/2\\ -\cos\theta/2\end{pmatrix}$$

and

$$\begin{pmatrix}\cos\theta & \sin\theta\\ \sin\theta & -\cos\theta\end{pmatrix}\begin{pmatrix}\cos\theta/2\\ \sin\theta/2\end{pmatrix}=\begin{pmatrix}\cos\theta/2\\ \sin\theta/2\end{pmatrix}.$$

So $\begin{pmatrix}\cos\theta/2\\ \sin\theta/2\end{pmatrix}$ and $\begin{pmatrix}\sin\theta/2\\ -\cos\theta/2\end{pmatrix}$ are orthogonal eigenvectors with eigenvalues 1 and -1, respectively.

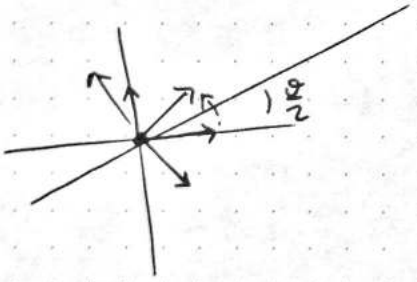
So A is R_a with $a=\begin{pmatrix}\sin\theta/2\\ -\cos\theta/2\end{pmatrix}$, a reflection. △▽ □

Corollary: every element of $O(2)$ is a composition of at most two reflections.

Proof: let $A\in O(2)$. If $A\notin SO(2)$, A is a reflection by the previous theorem. If $A\in SO(2)$, then

$$A=\underbrace{\left(A\begin{pmatrix}-1&0\\0&1\end{pmatrix}\right)}_{\det A=-1,\ \text{so in } O(2)\setminus SO(2)}\begin{pmatrix}-1&0\\0&1\end{pmatrix}.$$

Now $A\begin{pmatrix}-1&0\\0&1\end{pmatrix}$ is a reflection by previous theorem. So A is a product of two reflections. □



Reflections & Rotations in $\mathbb{R}^3$

Theorem: if $A \in SO(3)$, then there is a unit vector $v \in \mathbb{R}^3$ such that $Av = v$.

Proof: we need to show that 1 is an eigenvalue of A, with v just being its eigenvector. This is equivalent to showing

$$\det(A - 1I_3) = 0$$

We have
$$\begin{aligned}
\det(A - I_3) &= \det(A - A^TA) \quad \text{as } A \in O(3) \\
&= \det(I_3 - A^T) \cdot \det A^{-1} \quad \text{as } A \in SO(3) \\
&= \det(I_3 - A) \quad \text{as } \det(B^T) = \det(B) \\
&= \det((A - I_3)(-I_3)) \\
&= \det(A - I_3)\det(-I_3) \quad -1 \text{ as } (-1)^3 = -1 \\
&= -\det(A - I_3).
\end{aligned}$$

So $\det(A - I_3) = 0$. □

Corollary: every matrix $A \in SO(3)$ is conjugate (in $SO(3)$) to a matrix of the form
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix},$$

i.e. every $A \in SO(3)$ is a rotation.

Proof: by the Theorem we can find a vector $\underline{f}_1$ such that $A\underline{f}_1 = \underline{f}_1$. Extend this to an orthonormal basis $\{\underline{f}_1, \underline{f}_2, \underline{f}_3\}$.

For $i = 2$ or 3,
$$\begin{aligned}
(A\underline{f}_i) \cdot \underline{f}_1 &= (A\underline{f}_i) \cdot (A\underline{f}_1) \\
&= \underline{f}_i \cdot \underline{f}_1 \quad \text{as } A \text{ is orthogonal} \\
&= 0 \quad \text{as basis orthonormal.}
\end{aligned}$$

So $A\underline{f}_i$ is orthogonal to $\underline{f}_1$ and lies in the 2-dim vector space spanned by $\underline{f}_2$ and $\underline{f}_3$. In this basis A is represented by the matrix B, so the matrix A is
$$X = \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & & \\ 0 & & B \end{array}\right)$$
for some matrix B. So, as $\det(A) = 1$, orthogonal, so is B. Also, as $\det(B) = 1$, and $B \in SO(2)$.

By our proposition about $SO(2)$, we must have

$$B = \begin{pmatrix} \cos\vartheta & -\sin\vartheta \\ \sin\vartheta & \cos\theta \end{pmatrix} \text{ for some } \vartheta.$$

If P is the change of basis matrix from the standard basis to $\{\underline{f}_1, \underline{f}_2, \underline{f}_3\}$, then $P \in O(3)$ as these are both orthonormal basis. So $A = P^{-1}XP$ for $P \in O(3)$. If this lies in $SO(3)$ we're done. If not, let P' be the change of basis matrix for $\{-\underline{f}_1, \underline{f}_2, \underline{f}_3\}$. Then $\det(P') = 1$ and P' also conjugates X to A. Hence X and A are conjugate in $SO(3)$. □

Corollary: every matrix in $O(3)$ is a composition of at most 3 reflections.

Proof: suppose first $A \in SO(3)$. By the previous corollary, A is conjugate to $X = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\vartheta & -\sin\theta \\ 0 & \sin\vartheta & \cos\theta \end{pmatrix}$ via $P \in SO(3)$.

If $X = R_a R_b$ for some $a, b \in \mathbb{R}^3$, then A is as well:

$$\begin{aligned} A = P^{-1}XP &= P^{-1} R_a R_b P \\ &= P^{-1} R_a P P^{-1} R_b P \\ &= R_{P^{-1}a} R_{P^{-1}b} \end{aligned}$$

so is a product of two reflections.

But elements in $SO(2)$ such as $\begin{pmatrix} \cos\vartheta & -\sin\vartheta \\ \sin\vartheta & \cos\theta \end{pmatrix}$ are products of two reflections by our previous work in $\mathbb{R}^2$. So indeed X is a product of two reflections.

If $A \in O(3) \setminus SO(3)$, then

$$A = \left[A \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right] \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$\underbrace{\qquad\qquad}$ has det 1, so in $SO(3)$, hence two reflections

$\underbrace{\qquad\qquad}$ reflection

is a product of 3 reflections. □

L24.3

Consider $GL_2(\mathbb{Z}/5\mathbb{Z}) = \{$ 2×2 matrices with entries in $\mathbb{Z}/5\mathbb{Z}$ and which are invertible $\}$

A matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible iff $ad - bc \neq 0$, or equivalently $ad-bc$ having a multiplicative inverse.

There are $5^4 = 625$ matrices in total.

The non-invertible ones are those where $ad-bc = 0$.

Case 1: $a = 0 \longrightarrow b = 0$, c or d no matter (25 choices)
$\longrightarrow c = 0$, " (25 choices)
take 5 away for overcounting $b = c = 0$.

Case 2: $a \neq 0$, $d = \frac{bc}{a}$, so b, c are anything and so is a (as long as not 0).

$\therefore$ 145 non-invertible

So there are 480 invertible matrices, and this is the order of $GL_2(\mathbb{Z}/5\mathbb{Z})$.

$SL_2(\mathbb{Z}/5\mathbb{Z}) = \ker(\det : GL_2(\mathbb{Z}+/5\mathbb{Z}) \xrightarrow[\text{surjective}]{} U_5)$

so $|SL_2(\mathbb{Z}/5\mathbb{Z})| = \frac{480}{4} = 120$.

Let $PSL_2(\mathbb{Z}/5\mathbb{Z}) = SL_2(\mathbb{Z}/5\mathbb{Z}) / \{I_2, -I_2\}$,
and then $*PSL_2(\mathbb{Z}/5\mathbb{Z})*$ has order 60, i.e. $2^2 \cdot 3 \cdot 5$

The conjugacy classes:	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}$
order:	1	2	3	5	5
centraliser size:	60	~~4~~	3	~~5~~ 5	~~5~~ 5
ccl size:	1	~~20~~ 15	20	~~12~~ 12	~~12~~ 12

BS

So 24 elements of order 5, each subgroup of order 5 has 1 of order 1 and 4 of order 5 $\Rightarrow$ 5 subgroups of order 5. NANI? So $PSL_2(\mathbb{Z}/5\mathbb{Z})$ acts on its subgroups of order 5. This gives an injective hom. to S_5.

So its image is a subgroup of S_5 of index 2. This subgroup must be normal, and hence of it is A_5.

$\therefore \quad PSL_2(\mathbb{Z}/5\mathbb{Z}) \cong A_5.$