Groups - Lecture 1

9/10/20

A "symmetry" of an object preserves its structure and leaves it looking the same.

e.g. 

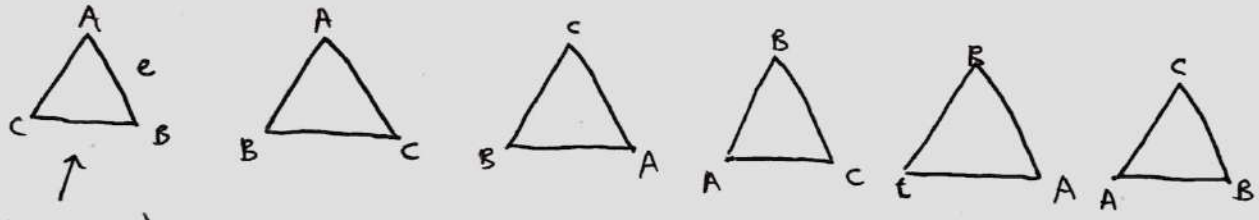
(reflection)

or 

(120° clockwise rotation)

For 

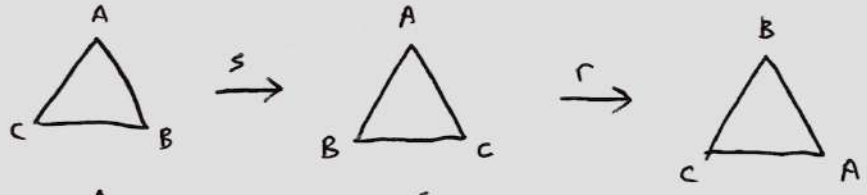
what are all possible symmetries?.



(do nothing)

Each symmetry can be reversed.

Doing 2 symmetries in a row makes another symmetry.

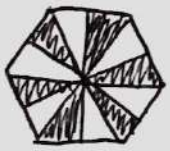


$rs(\Delta)$

$sr(\Delta)$

Note that order matters: $rs \neq sr$

$r^3 = e$ $\quad (r^2)^3 = e$ $\quad s^2 = e$



This also has 6 symmetries but behaves differently to Δ : here order doesn't matter and repeating a symmetry <6 times won't give the original back.

We need to study how the symmetries interact.

Groups are sets of elements (symmetries) with rules on how to compose them.

1. Always have identity element (do nothing)
2. Composing 2 elements gives another element in the set.
3. For each element we have an inverse
4. $(a*b)*c = a*(b*c)$: associative

Definition (Group) A group is a set G combined with a way of composing its elements $(*)$ satisfying

(0) - Closure: $g*h \in G \quad \forall g, h \in G$

(1) - Identity: $\exists e \in G$ s.t. $e*g = g*e = g$

(2) - Inverse: $\forall g \in G \quad \exists g^{-1} \in G$ s.t. $g*g^{-1} = g^{-1}*g = e$

(3) - Associativity: $\forall a, b, c \in G \quad (a*b)*c = a*(b*c)$

Formally we say G is a group if there is a binary operation $*: G \times G \to G$ satisfying conditions (1), (2) and (3).

Examples

0) $G = \{e\}$ "trivial group"

1) $G =$ symmetries of Δ, $*$ is composition

2) $G = \{\mathbb{Z}, +\}$ (can easily verify the axioms)

3) $G = \{\mathbb{R}, +\}, \{\mathbb{Q}, +\}, \{\mathbb{C}, +\}$ ← (should really use regular brackets)

4) $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ with multiplication

5) $(\mathbb{R}, *) \quad r*s = r+s+5$

6) $G = \{0, 1, 2, \dots, n-1\}$ with addition mod n $(\mathbb{Z}_n)$

7) A vector space with addition

8) $GL_2(\mathbb{R})$:= set of invertible 2×2 matrices with real coefficients with matrix multiplication

Non-examples

1) $G = \{0, 1, 2, \ldots, n-1\}$ with just addition

2) $(\mathbb{Z}, \times)$: no inverses : no $n \in \mathbb{Z}$ s.t. $2 \times n = 1$

3) $(\mathbb{R}, *)$ with $r * s = r^2 s$

No identity : if $\forall r \quad e^2 r = r^2 e = r$ then $e = \pm 1$

but $\exists r$ s.t. $r^2 \neq r$ and $-r^2 \neq r$ (as $e^2 = 1$)

contradicting $e^2 r = r^2 e = r$ for $e = \pm 1$. #

4) $G = \mathbb{N}$ with $n * m := |n - m|$

closure ✓ identity = 0 inverse : $n^{-1} = n$

associativity : $1 * 2 * 5$

$(1 * 2) * 5 = |\,|1-2| - 5\,| = 4$

$1 * (2 * 5) = |1 - |2 - 5|\,| = 2$ not associative.

Groups – Lecture 2

12/10/20

Notation: we often write $g \cdot h$ or gh for $g * h$.

Some easy consequences of the axioms:

Proposition 1.4 Let G be a group. Then

(i) the identity element is unique

(ii) $\forall g \in G$, the inverse of g is unique

(iii) if $g \cdot h = g$ then $h \cdot g = g$ (i.e. $h = e$)

(iv) if $g \cdot h = e$ then $h \cdot g = e$ (i.e. $h = g^{-1}$)

(v) $(gh)^{-1} = h^{-1} g^{-1}$

(vi) $(g^{-1})^{-1} = g$

Proof

(i) Suppose e, e' are both identity elements.
Then $ee' = e$ and $ee' = e'$
so $\underline{e = e'}$ so identity is unique.

(ii) Suppose $gh = e$ and $gk = e$
So $gh = gk \Rightarrow g^{-1}(gh) = g^{-1}(gk)$
(assoc.) $\Rightarrow (g^{-1}g)h = (g^{-1}g)k$
$\Rightarrow \underline{h = k}$ so inverse is unique.

(iii) If $gh = g$ then $gh = ge$
$\Rightarrow g^{-1}(gh) = g^{-1}(ge)$
$\Rightarrow eh = e$
$\Rightarrow h = e$ so it's also a left identity by def.

(iv) If $gh = e$ then $ghg = g$
$g^{-1}ghg = e \Rightarrow \underline{hg = e}$.
(so $h = g^{-1}$).

(v) $(gh)(h^{-1}g^{-1}) = geg^{-1} = gg^{-1} = e$

(vi) $gg^{-1} = e$ by definition so $g g^{-1}(g^{-1})^{-1} = (g^{-1})^{-1}$
$\Rightarrow ge = (g^{-1})^{-1}$ □

Definition 1.5 A group G is abelian (or commutative) if $\forall g, h \in G$, $gh = hg$.

Definition 1.6 A group G is finite if it has finitely many elements

The number of elements in G is the order of G, written $|G|$.

Definition 1.7 Let $(G, *)$ be a group. A subset $H \leq G$ is a subgroup of G if $(H, *)$ is a group.

Remark 1.8 To check $H < G$ is a subgroup, just check closure, identity, inverse (no need for associativity - inherited from G).

Note that $e_G = e_H$.

Examples 1.9

0) $\{e\} \leq G$ ("trivial subgroup")

1) $G \leq G$

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

3) If $G = \{\text{symmetries of } \Delta\}$ then $\{e, s\} \leq G$ and $\{e, r, r^2\} \leq G$.

Lemma 1.10 Let G be a group. $H < G$ is a subgroup iff

- H is non-empty and
- $\forall a, b \in H$, $ab^{-1} \in H$ (proof-exercise). ✓

Proposition 1.11 The subgroups of $(\mathbb{Z}, +)$ are precisely the ones of the form $n\mathbb{Z} \subset \mathbb{Z}$ (where $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$).

Proof Firstly, each $n\mathbb{Z}$ is a subgroup: fix $n \in \mathbb{N}$.
$n \in n\mathbb{Z}$ so it's nonempty, and $a, b \in n\mathbb{Z}$
$\Rightarrow a = nc$, $b = nd$ for $c, d \in \mathbb{Z}$, so $ab^{-1} = nc - nd$
$= n(c-d) \in n\mathbb{Z}$. So it's a subgroup.

Now we show that if $H \leq \mathbb{Z}$ then $H = n\mathbb{Z}$.

If $H = \{0\}$ then $H = 0\mathbb{Z}$.

Otherwise, take the smallest $n > 0$ in H. $H \leq \mathbb{Z}$ so is closed and contains inverses, so $n+n+\dots+n \in H$

$-n-n-n\dots-n \in H$.

So $n\mathbb{Z} \leq H$.

Suppose for contradiction that $\exists\, k \in H$ s.t. $k \notin n\mathbb{Z}$.

Then there is some $m \in \mathbb{Z}$ s.t. $n \cdot m < k < n \cdot (m+1)$

so $0 < k - n \cdot m < n$ but $k - n \cdot m \in H$ but is smaller than n. ✱ So $H = n\mathbb{Z}$. □

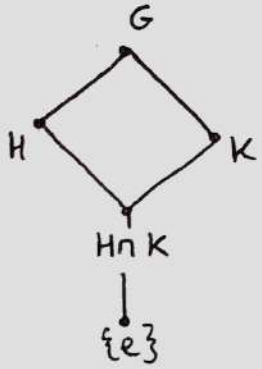
Proposition 1.12 (i) Let $H \leq G$, $K \leq G$. Then $H \cap K \leq G$.

(ii) If $K \leq H$ and $H \leq G$ then $K \leq G$. (transitivity)

(iii) If ~~$K \leq H$~~ $K \subseteq H$, $H \leq G$, $K \leq G$, then $K \leq H$.

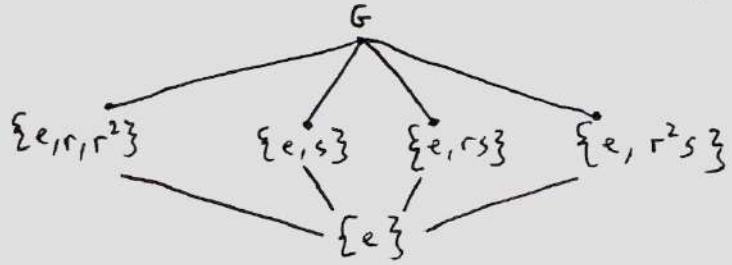
Proof Exercise.

A useful way to think about subgroups is via a diagram as follows.



"lattice of subgroups"

Example G = symmetries of $\Delta = \{e, r, r^2, s, rs, r^2s\}$



(can check cases to see these are all subgroups)

Definition 1.13 Let $X \neq \emptyset$ be a subset of a group G. The subgroup generated by X, denoted $\langle X \rangle$, is the intersection of all subgroups containing X.

Equivalently it's the smallest subgroup containing X. If $X \subseteq H \leq G$ then $\langle X \rangle \leq H$.

Groups – Lecture 3

14/10/20

$X \subseteq G$ $\quad \langle X \rangle :=$ smallest subgroup of G containing X

Proposition 1.14 Let $X \subseteq G$, $X \neq \emptyset$. Then $\langle X \rangle$ is the set of elements of G of the form $x_1^{\alpha_1} x_2^{\alpha_2} \dots x_k^{\alpha_k}$ where $x_i \in X$, $\alpha_i = \pm 1$, $k \geq 0$.

as all such elements of T must be in $\langle X \rangle$ ↓ (think closure)

Proof Let T be the set of such elements. Clearly $T \subseteq \langle X \rangle$.

T is a subgroup (can easily check) and $X \subseteq T$ so $\langle X \rangle \subseteq T$.

(if $X \subseteq H \leq G$ then $\langle X \rangle \leq H$). Hence $T = \langle X \rangle$. □

e.g. symmetries of Δ : $\langle r \rangle = \langle r^2 \rangle = \{e, r, r^2\}$

$\langle s \rangle = \{e, s\}$

$\langle r, s \rangle = \langle r^2, rs \rangle$

$\mathbb{Z} = \langle 1 \rangle = \langle 2, 3 \rangle$

Definition 1.15 Let $(G, *_G)$, $(H, *_H)$ be groups. A function $\phi : H \to G$ is a group homomorphism if $\forall a, b \in H$,

$$\phi(a *_H b) = \phi(a) *_G \phi(b).$$

A GHM is injective whenever $\phi(a) = \phi(b)$ we have $a = b$. $\quad (\phi : H \hookrightarrow G)$

A GHM is surjective whenever $\forall g \in G$, $\exists h \in H$: $\phi(h) = g$. $\quad (\phi : H \twoheadrightarrow G)$

A GHM is bijective if both injective and surjective.

Examples 1.16

0) $\phi : H \to G$ by $\phi(h) = e_G$. Injective iff $H = \{e_H\}$

Surjective iff $G = \{e_G\}$

1) The inclusion function $\iota : H \to G$ $(H \leqslant G)$ (is injective)

e.g. $\mathbb{Z} \to \mathbb{R}$

2) The function $\phi : \mathbb{Z} \to \mathbb{Z}_n$ given $\phi(k) = k \bmod n$ as

$$\phi(k+l) = k+l \bmod n = (k \bmod n) + (l \bmod n) \bmod n$$
$$= \phi(k) + \phi(l) \bmod n.$$

(Surjective)

3) $\phi : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \times)$ with $x \mapsto e^x$

$\phi(x+y) = e^{x+y} = e^x e^y$ (Bijective)

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

Consequences of definition

Proposition 1.17 Let $\phi : H \to G$ be a GHM.

(i) $\phi(e_H) = e_G$

(ii) $\phi(h^{-1}) = \phi(h)^{-1}$ $\forall\, h \in H$

(iii) if $\psi : G \to K$ is a GHM then $\psi\phi : H \to K$ is a GHM.

Proof (i) $e_H e_H = e_H$ so $\phi(e_H e_H) = \phi(e_H)\phi(e_H)$

$= \phi(e_H)$

so $\phi(e_H)\,\phi(e_H)\,\phi(e_H)^{-1} = \phi(e_H)\,\phi(e_H)^{-1}$

$\Rightarrow$ $\phi(e_H) = e_G$

(ii) Consider $\phi(h)\,\phi(h^{-1}) = \phi(hh^{-1}) = e_G$

so $\phi(h^{-1}) = \phi(h)^{-1}$ taking inverses.

(iii) $H \xrightarrow{\phi} G \xrightarrow{\psi} K$

$\forall\, a, b \in H \qquad \psi\phi(ab) = \psi(\phi(a)\phi(b))$ by definition of GHM used twice

$= \psi(\phi(a))\,\psi(\phi(b))$

as required. □

Definition 1.18 A bijective homomorphism is called an isomorphism.

H, G isomorphic: $H \cong G$ if $\exists$ a GIM $H \to G$.

2 descriptions of the same group - consider "the same"

Examples 1.19

(1) $G := \{1, i, -1, -i\} \leq \mathbb{C}^*$ (with $\times$)

Then $G \cong \mathbb{Z}_4$ with $\phi : G \to \mathbb{Z}_4$,

~~$\phi(1) = 0$~~
~~$\phi(i) = 1$~~
~~$\phi(-1) = 2$~~
~~$\phi(-i) = 3$~~

$\phi(1) = 0$
$\phi(i) = 1$
$\phi(-1) = 2$
$\phi(-i) = 3$

Generally $\{e^{2\pi i k/n} : 0 \leq k \leq n-1\} \cong \mathbb{Z}_n\}$.

(Check this is an isomorphism).

$\phi\left(e^{2\pi i k/n}\, e^{2\pi i m/n}\right) = \phi\left(e^{2\pi i (k+m)/n}\right) = k+m \bmod n$

$= \phi\left(e^{2\pi i k/n}\right) + \phi\left(e^{2\pi i m/n}\right) \bmod n.$

(2) $\phi : \mathbb{Z} \to n\mathbb{Z}$ by $k \mapsto nk$ (easy to check)

(3) $(\{1, -1\}, \times) \cong \{e, s\}$

Proposition 1.20 Let $f: H \to G$ be an isomorphism.

Then $f^{-1}: G \to H$ is also an isomorphism.

Proof $\forall a, b \in G$, $f^{-1}(ab) = f^{-1}\left(f\left(f^{-1}(a)\right) f\left(f^{-1}(b)\right)\right)$

$= f^{-1}\left(f\left(f^{-1}(a) f^{-1}(b)\right)\right)$ by GHM definition for f

$= f^{-1}(a) f^{-1}(b)$ as required. □

Groups – Lecture 4

16/10/20

Definition 1.21 Let $\phi : H \to G$ be a GHM.

Image of ϕ $\quad \operatorname{im}\phi = \{g \in G : g = \phi(h) \text{ for some } h \in H\}$

Kernel of ϕ $\quad \ker\phi = \{h \in H : \phi(h) = e_G\}$

Proposition 1.22 $\operatorname{im}\phi \leq G$, $\ker\phi \leq H$

$\operatorname{im}\phi \leq G$

Closure: if $a, b \in \operatorname{im}\phi$ then $\exists x, y \in H$ s.t. $a = \phi(x)$, $b = \phi(y)$

Then $ab = \phi(x)\phi(y) = \phi(xy)$, $xy \in H$ so $ab \in \operatorname{im}\phi$

Identity: $e_G \in \operatorname{im}\phi$ where $\phi(e_H) = e_G$

Inverse: if $a \in \operatorname{im}\phi$ then $a = \phi(x)$ $(x \in H)$

Then $\phi(x^{-1}) = \phi(x)^{-1} = a^{-1}$ so $a^{-1} \in \operatorname{im}\phi$.

$\ker\phi \leq H$

Closure: $x, y \in \ker\phi \Rightarrow \phi(x) = \phi(y) = e_G$.

$\phi(xy) = \phi(x)\phi(y) = e_G e_G = e_G$

so $xy \in \ker\phi$.

Identity: $\phi(e_H) = e_G$ so $e_H \in \ker\phi$

Inverse: if $x \in \ker\phi$ then $\phi(x^{-1}) = \phi(x)^{-1}$

$= e_G^{-1} = e_G$ so $x^{-1} \in \ker\phi$.

□

Examples 1.23

0) $\phi : H \to G$ $\quad \phi(h) = e_G \ \forall h \in H$

$\operatorname{im}\phi = e_G$, $\ker\phi = H$

1) Inclusion $\iota : H \to G$ for $H \leq G$ $\quad \operatorname{im}(\iota) = H$, $\ker\iota = \{e_H\}$

2) $\phi : \mathbb{Z} \to \mathbb{Z}_n$, $\phi(k) = k \bmod n$ has

$\operatorname{im}\phi = \mathbb{Z}_n$, $\ker\phi = n\mathbb{Z}$.

Proposition 1.24 Let $\phi : H \to G$ be a GHM.

(i) ϕ is surjective iff $\text{im}(\phi) = G$

(ii) ϕ is injective iff $\ker\phi = \{e\}$

Proof (i) by definition

(ii) Suppose ϕ is injective. We have $\phi(e_H) = e_G$. So no other element can be sent to e_G (injective) so $\ker\phi = \{e_H\}$.

Now suppose $\ker\phi = \{e_H\}$. Then if $\phi(a) = \phi(b)$ for $a, b \in H$, then

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

so $ab^{-1} = e_H \Rightarrow a = b$. So injective. □

Direct Products of Groups

How can we build a group with G, H as subgroups?

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

Definition 1.25 The direct product of two groups G, H is the set $G \times H$ with operation of component-wise composition:

$$(g_1, h_1) * (g_2, h_2) = (g_1 g_2, h_1 h_2)$$

Remark $G \times H$ contains subgroups isomorphic to G and H:

Take $G \times \{e_H\} = \{(g, e_H) : g \in G\}$

and similarly $\{e_G\} \times H$.

Example 1.26

$\mathbb{Z} \times \{1, -1\}$ has elements $(n, 1)$, $(n, -1)$ with $n \in \mathbb{Z}$

$(n, -1) * (m, -1) = (n + m, 1)$

$(n, -1) * (m, 1) = (n + m, -1)$ etc.

Remark In $G \times H$ everything in (the isomorphic copy of) G commutes with everything in (the isomorphic copy of) H.

$\forall (g, e_H) \in G \times \{e_H\}$, $\forall (e_G, h) \in \{e_G\} \times H$, we have $(g, e_H) * (e_G, h) = (e_G, h) * (g, e_H) = (g, h)$.

How can we recognise a group is a direct product?

Theorem 1.27 (Direct Product Theorem)

Let $H, K \leq G$ such that

(i) $H \cap K = \{e\}$

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

(iii) $\forall g \in G$, $\exists h \in H, k \in K$ s.t. $g = hk$

("$G = HK$" where $HK := \{hk : h \in H, k \in K\}$)

Then $G \cong H \times K$.

Proof Consider $f : H \times K \to G \quad (h, k) \mapsto hk$.

Show f is a GHM:

$$\begin{aligned} f((h_1, k_1) \cdot (h_2, k_2)) &= f(h_1 h_2, k_1 k_2) \\ &= h_1 h_2 k_1 k_2 \\ &= h_1 k_1 h_2 k_2 \quad (\text{commute - (ii)}) \\ &= f(h_1, k_1) f(h_2, k_2) \text{ so is a GHM.} \end{aligned}$$

f is surjective by (iii)

f is injective: Suppose $(h, k) \in \ker f$, then $f(h, k) = hk = e$.

So $h = k^{-1}$ so

$h = k^{-1} \in H \cap K = \{e\}$ by (i)

so $h = k = e \Rightarrow \ker f = \{e\}$ so injective.

So f is bijective and a homomorphism, so an isomorphism.

□

Examples

Cyclic Groups Recall $\langle X \rangle$ for $X \subseteq G$.

Definition 2.1 Let G be a group and $X \subseteq G$ $(X \neq \emptyset)$.
If $\langle X \rangle = G$ then X is a generating set of G.
G is cyclic if $\exists\, a \in G : \langle a \rangle = G$ $(|X| = 1)$.

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

Examples

0) $G = \{e\} = \langle e \rangle$
1) $(\mathbb{Z}, +)$: $\mathbb{Z} = \langle 1 \rangle$ or $\langle -1 \rangle$
2) $(\mathbb{Z}_n, +_n)$: $\mathbb{Z}_n = \langle 1 \rangle$ or $\langle k \rangle$ for k coprime to n
3) $\{ e^{2\pi i k/n} : 0 \leq k \leq n-1 \}$: $\langle e^{2\pi i k/n} \rangle$, k coprime to n (isomorphic to $\mathbb{Z}$))
4) $\{ e, a, a^2, \ldots, a^{n-1} \}$ with $a^k * a^j = a^{k+j}$ for $k+j < n$ and a^{k+j-n} if $k+j \geq n$ (again isomorphic to $\mathbb{Z}_n$)

Write C_n for (the isomorphism class of) this group 4).

These are the only examples.

$$C_n = \{e, a, a^2, \dots, a^{n-1}\} \cong \mathbb{Z}_n$$

$$a^k a^j = \begin{cases} a^{k+j} & \text{if } k+j < n \\ a^{k+j-n} & \text{if } k+j \geq n \end{cases}$$

Theorem 2.3

A cyclic group G is isomorphic to $\mathbb{Z}$ or to C_n for $n \in \mathbb{N}$.

Proof Let $G = \langle b \rangle$.

- Suppose $\exists n > 0 : b^n = e$. Take the smallest such n and define $\phi : C_n = \{e, a, \dots, a^{n-1}\} \to G$ by $\phi(a^k) = b^k \quad \forall \ 0 \leq k \leq n-1$.

  Then for any $a^j, a^k \in C_n$, if $j+k < n$

  $$\phi(a^j a^k) = \phi(a^{j+k}) = b^{j+k} = b^j b^k = \phi(a^j)\phi(a^k)$$

  If $j+k \geq n$

  $$\phi(a^j a^k) = \phi(a^{j+k-n}) = b^{j+k-n} = b^{j+k}(b^n)^{-1}$$
  $$= b^{j+k} e = b^j b^k = \phi(a^j)\phi(a^k).$$

  So ϕ is a GHM.

  $b^n = e \in G$ so all elements of G can be written as b^k, $0 \leq k < n$ so ϕ is surjective.

  ϕ is injective since $\phi(a^k) = e \Rightarrow b^k = e$ and so $k = 0$ (otherwise contradiction to minimality of n).

  So ϕ is a GIM $\to$ $G \cong C_n$.

- If no such n exists then define $\phi : \mathbb{Z} \to G$ by $k \to b^k$.

  Then $\phi(k+m) = b^{k+m} = b^k b^m = \phi(k)\phi(m)$ so GHM

  Clearly surjective (where $G = \langle b \rangle$)

  Suppose $m \in \ker\phi$. Then $\phi(m) = b^m = e$ and $\phi(-m) = b^{-m} = (b^m)^{-1} = e$ so if $m \neq 0$ then $\not\in$ to the fact that $\nexists\, n > 0$ s.t. $b^n = e$. So $m = 0$ so $\ker\phi = \{0\}$ so is injective. So ϕ is a GIM. $\square$

So all cyclic groups are essentially C_n or $\mathbb{Z}$.

Definition 2.4 The order of an element $g \in G$ is the smallest $n \in \mathbb{N}$ such that $g^n = e$ ($\text{ord}(g) = n$).
If there is no such n, then g has infinite order.
Write $\text{ord}(g) = \infty$.

Recall order of group is $|G|$.

Exercise If $g^m = e$, $m > 0$ then $\text{ord}(g) \mid m$.

Note that given $g \in G$, $\langle g \rangle$ is isomorphic to C_n if ord g is finite, isomorphic to $\mathbb{Z}$ if order is infinite. So $\text{ord}(g) = \langle g \rangle$.

Proposition 2.5 Cyclic groups are abelian.

Proof exercise

Dihedral Groups

Definition 2.6 The dihedral group D_{2n} is the group of symmetries of a regular n-gon.
Operation = composition of symmetries.

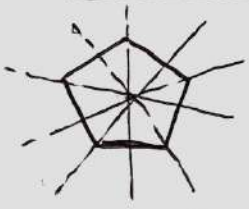
e.g. D_6 = group of symmetries of Δ

What are the symmetries of D_{2n}?

There are n clockwise rotations by angles $\frac{2\pi k}{n}$ $(0 \leq k < n)$

Also have n reflections.

Odd n



n reflection in axes through centre and each vertex

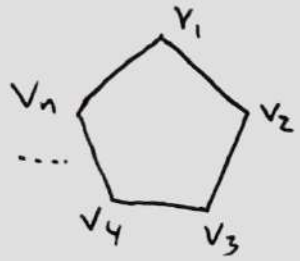
Even n

$\frac{n}{2}$ reflections in reflection axes between opposite vertices

$\frac{n}{2}$ reflections in lines between centres of opposite edges

We have listed $2n$ elements. Are these all the elements?

Let $g \in D_{2n}$



g is a symmetry of the n-gon so must send vertices to vertices.

So $g(v_1) = v_i \quad 1 \leq i \leq n$

g must send edges to edges so vertices adjacent to v_1 are sent to be adjacent to v_1.

Note that once we know $g(v_1)$ and $g(v_2)$, then $g(v_n)$ is determined and inductively every vertex is determined.
So we know exactly what g is.

Then since there are n possibilities for where v_1 is sent and 2 possibilities for where v_2 is sent, there are exactly $\underline{2n}$ elements in total.

Show D_{2n} is a group.

Closure — composition of symmetries gives another symmetry

Identity — "do nothing" rotation $0°$

Inverse — for a $\frac{2\pi k}{n}$ rotation, inverse is rotation by $\frac{2\pi(n-k)}{n}$. Reflection is own inverse.

Associativity — composition is associative

We can generate D_{2n} from 1 rotation and 1 reflection.

Let r = rotation $\frac{2\pi}{n}$

s = reflection in axis through v_1 and centre

Then r^k gives $\frac{2\pi k}{n}$ rotation

Consider $\underline{r^i s r^{-i}}$: $v_{i+1} \mapsto v_1 \mapsto v_1 \mapsto \underline{v_{i+1}}$

so v_{i+1} is fixed by this symmetry

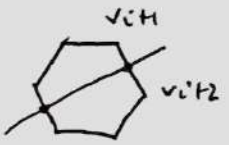
$v_{i+2} \mapsto v_2 \mapsto v_n \mapsto \underline{v_i}$

which determines the whole symmetry.

v_{i+1} is fixed so it's a reflection through v_{i+1} axis.

If n is odd then this is all reflections.

If n is even then we also need side-side reflections.



$r^{i+1} s r^{-i}$

$v_{i+1} \mapsto v_1 \mapsto v_1 \mapsto v_{i+2}$

$v_{i+2} \mapsto v_2 \mapsto v_n \mapsto v_{i+1}$

Switches v_{i+1} and v_{i+2} giving reflection.

These types of symmetries are called conjugations.

Can check this group is not abelian.

So $\boxed{D_{2n} = \langle r, s \rangle}$

with $rs = sr^{-1}$ (check what they do to vertices)

A small aside about "presentation" of groups.

$\langle$ generators | relations $\rangle$ e.g. $\langle a \mid a^n = e \rangle$ for C_n

$D_{2n} = \langle r, s \mid r^n = e,\ s^2 = e,\ rs = sr^{-1} \rangle$

(note this is important - must give info to deduce all relations)

(See Higman group (infinite))

Permutation Groups

Definition 2.7 Given a set X, a permutation of X is a bijective function $\sigma : X \to X$. The set of all permutations of X is $\mathrm{sym}(X)$.

Theorem 2.8 $\mathrm{Sym}(X)$ forms a group.

Proof Exercise

Definition 2.9 If $|X| = n$, we write S_n for isomorphism class of $\mathrm{sym}\, X$. (S_n: symmetric group on n elements)

Note $|S_n| = n!$ Usually we label $X = \{1, 2, 3, \ldots, n\}$.

One way to write permutations is two-row notation

e.g. $\sigma \in S_3$: $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$ we write

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$ – number is sent to the one below it.

Given $a_1, a_2, \ldots, a_k$ cycled and leaving the others unchanged,
$(a_1 \to a_2,\ a_2 \to a_3,\ \ldots,\ a_k \to a_1)$
we can write this permutation as $(a_1\ a_2\ a_3\ \ldots\ a_k)$

e.g. if $\sigma \in S_4$ then if $\sigma(1) = 3$, $\sigma(3) = 2$, $\sigma(2) = 1$, $\sigma(4) = 4$
then we can write $\sigma = (1\ 3\ 2)$

or sometimes $\sigma = (1\ 3\ 2)(4)$

Note that $(a_1\ a_2 \ldots a_k) = (a_2\ a_3 \ldots a_k\ a_1) = \ldots$ etc.

Definition 2.10 A permutation of the form $\sigma = (a_1\ a_2 \ldots a_k)$ is called a k-cycle.

If $k = 2$ it is called a transposition.

$(1\ 2\ 3\ 4)(3\ 2\ 4)$ is a permutation in S_4

$1 \mapsto 2$ $2 \mapsto 1$ $3 \mapsto 3$ $4 \mapsto 4$

so $1234 \to 2134$.

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

e.g. in S_5 $(2\ 5\ 4)(5\ 3\ 4) = (1)(2\ 5\ 3)(4) = (2\ 5\ 3)$

Note that the inverse of a cycle
$(a_1\ a_2 \ldots a_{k-1}\ a_k)$ is $(a_k\ a_{k-1} \ldots a_2\ a_1)$

Examples

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

Remarks $S_3 = D_6$ (permutation of the vertices)

But $S_n \not\subseteq D_{2n}$ in general

$D_{2n} \leq S_n$ however.

Definition 2.11 Two cycles are disjoint if no number (from 1 to n) appears in both.

Definition 2.12 For G a group, $g, h \in G$ commute if $gh = hg$.

Lemma 2.12 Disjoint cycles commute.

Proof Let $\sigma, \tau \in S_n$ be disjoint cycles. Want to show $\sigma\tau = \tau\sigma$. So we need to show $\forall x \in \{1, \dots, n\}$ $\sigma\tau(x) = \tau\sigma(x)$.

- If x is in neither of σ or τ then $\sigma\tau(x) = \tau\sigma(x) = x$.

WLOG: - If x is in τ but not σ (we know they're disjoint) then $\tau(x)$ is in τ. Since σ, τ disjoint, $\tau(x) \notin \sigma$. So $\sigma(\tau(x)) = \tau(\sigma(x))$. (since $\sigma(x) = x$).

These are all cases. □

Theorem 2.13 Any $\sigma \in S_n$ can be written as a composition of disjoint cycles. This expression is unique up to reordering or "cycling" cycles.

Proof Take $\sigma \in S_n$ and consider $1, \sigma(1), \sigma^2(1), \sigma^3(1), \dots$.

Since $\{1, \dots, n\}$ is finite, $\exists\ a > b$ s.t. $\sigma^a(1) = \sigma^b(1)$.

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

Let k be the smallest integer such that $\sigma^k(1) = 1$ ($k > 0$: we know $\exists k$ as $\sigma^{a-b}(1) = 1$).

Then for $0 \leq l < m < k$, if $\sigma^m(1) = \sigma^{(l)}(1)$ then $\sigma^{m-l}(1) = 1$ contradicting minimality of k. So up to k, $1, \sigma(1), \sigma^2(1), \ldots, \sigma^{k-1}(1)$ are all distinct.

This is our first cycle $(1\ \sigma(1)\ \sigma^2(1) \ldots \sigma^{k-1}(1))$.

We can then repeat this with the next number in $\{1, 2, \ldots, n\}$ that hasn't already appeared.

Since σ is a bijection, no number that has already appeared can reappear.

Then once we've exhausted all of $\{1, 2, \ldots, n\}$ we get a composition of disjoint cycles doing the same thing as σ.

Uniqueness: suppose we have 2 such decompositions

$$\sigma = (a_1 \ldots a_{k_1})(a_{k_1+1} \ldots a_{k_2}) \ldots (a_{k_{n-1}} \ldots a_{k_m})$$

$$= (b_1 \ldots b_{l_1})(b_{l_1+1} \ldots b_{l_2}) \ldots (b_{l_{s-1}} \ldots b_{l_s})$$

and each number from 1 to n appears exactly once in both of the expressions (including singletons)

Then we have $a_1 = b_t$ for some t and the other numbers appearing in the cycle of b_t are uniquely determined by $\sigma(a_1), \sigma^2(a_1), \ldots$

So $(a_1 \ldots a_{k_1})(\ldots) = (b_t \ldots)(\ldots)$ as disjoint cycles commute.

(a_{k_1} must match b_t — uniquely determined by where σ sends a_1.)

So they're unique up to reordering and cycling. □

Definition 2.14 The set of cycle lengths of the disjoint cycle decomposition of σ is its cycle type.

e.g. $(1\,2\,3)(5\,6)$ is $3,2$ (or $2,3$).

Theorem 2.15 The order of $\sigma \in S_n$ is the LCM of the cycle lengths in its cycle type.

Proof First note that the order of a k-cycle is k.

Suppose $\sigma = \tau_1 \tau_2 \dots \tau_r$ where τ_i are all disjoint

$\sigma^n = \tau_1^n \tau_2^n \dots \tau_r^n$ (as disjoint cycles commute)

Let τ_i have length k_i then if $\sigma^m = e$, then

$\tau_1^m \tau_2^m \dots \tau_r^m = e$

Hence $\tau_1^m = \tau_2^{-m} \dots \tau_r^{-m}$

The numbers permuted by LHS and RHS are disjoint so both sides must be $\underline{e}$. So $\tau_1^m = e$ so $k_1 \mid m$.

This holds for any k_i : $k_i \mid m \ \forall i$ so

$\mathrm{LCM}(k_i) \mid m$. So $\mathrm{ord}(\sigma)$ must be a multiple of the lcm.

$l = \mathrm{lcm}(k_1, \dots, k_r) \Rightarrow \sigma^l = \tau_1^l \dots \tau_r^l$

$= (\tau_1^{k_1})^{l/k_1} \dots (\tau_r^{k_r})^{l/k_r} = e$

So $\mathrm{lcm}(k_i) = \mathrm{ord}(\sigma)$. □

Disjoint cycle notation is one useful way to express elements of S_n. Another is as a product of transpositions.

Proposition 2.16 Let $\sigma \in S_n$. Then σ is a product of transpositions.

Proof By theorem 2.15, it's enough to do this for a cycle.

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

□

Note that this is not unique in general.

e.g. $(1\ 2\ 3\ 4) = (12)(23)(3\ 4) = (1\ 2)(2\ 3)(12)(3\ 4)(1\ 2)$

But the parity of the no. of transpositions is well-defined.

Theorem 2.17 Writing $\sigma \in S_n$ as a product of transpositions in different ways, σ is either always a product of an even no. of transpositions, or always a product of an odd no. of transpositions.

Proof Write $\#(\sigma)$ for the number of cycles in σ in (DCD) → disjoint cycle decomposition, including 1-cycles.

e.g. $(1\ 2)(3\ 4)(5) \in S_5 \quad \#(\sigma) = 3$

What happens to $\#(\sigma)$ if we multiply σ by a transposition $(c\ d)$?

This only affects cycles containing c and/or d.

If c, d are in the same cycle in DCD of σ

say $(c\ a_2\ a_3 \dots a_{k-1}\ d\ a_{k+1} \dots a_l)$

Multiply by $(c\ d)$ to give

$(c\ a_{k+1} \dots a_l)(d\ a_2\ a_3 \dots a_{k-1})$

So $\#(\sigma\tau) = \#(\sigma) + 1$ in this case.

If c, d in different cycles

$(c\ a_2 \dots a_k)(d\ b_2 \dots b_l)$

then multiplying by $(c\ d)$ gives

$(c\ b_2\ b_3 \dots b_l\ d\ a_2 \dots a_k)$ using reverse of case above so $\#(\sigma\tau) = \#(\sigma) - 1$ in this case.

So for any σ, any transposition τ,

$$\#(\sigma) \equiv \#(\sigma\tau) + 1 \mod 2.$$

Now suppose σ is two different products of transpositions

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

We know by theorem 2.15 that $\#(\sigma)$ is uniquely determined by σ (DCD uniqueness) and

$$\sigma = e\,\tau_1 \dots \tau_k = e\,\tau_1' \dots \tau_l'$$

Each time we multiply by τ_i we add 1 to the # value

$$\therefore \#(\sigma) \equiv \#(e) + k \mod 2$$

$$\#(\sigma) \equiv \#(e) + l \mod 2 \quad \Rightarrow \boxed{k \equiv l \mod 2}$$

as required. □

Definition 2.18 Writing $\sigma \in S_n$ as a product of transpositions $\sigma = \tau_1 \dots \tau_k$, the sign $(\sigma) = (-1)^k$.

$\operatorname{sign}(\sigma) = 1$: "even permutation"

$\operatorname{sign}(\sigma) = -1$: "odd permutation"

By Thm 2.17, this is well-defined.

Theorem 2.19 For $n \geq 2$ $\operatorname{sign}: S_n \to \{\pm 1\} \cong C_2$ is a surjective homomorphism.

Proof It's well defined by theorem 2.17.

Note that if σ can be written as a product of k transpositions, and σ' as a product of l transpositions then $\sigma\sigma'$ can be written as $k+l$ of them.

$$\operatorname{sign}(\sigma\sigma') = (-1)^{k+l} = (-1)^k (-1)^l = \operatorname{sign}\sigma \operatorname{sign}\sigma'.$$

PTO

Surjective for $n \geq 2$: $\operatorname{sign}(e) = 1$

$\operatorname{sign}(1\ 2) = -1$. □

Definition 2.20 The kernel of the homomorphism $\operatorname{sign} : S_n \to \{\pm 1\}$ is called the alternating group A_n.

(Recall kernel is a subgroup)

So $A_n \leq S_n$ is the subgroup of all the even permutations.

Proposition 2.21 $\sigma \in S_n$ is even iff its DCD has an even number of even cycles.
(even length)

Proof Exercise (Think: how many transpositions can a cycle with odd or even no. of elements be decomposed into?)

All groups can be seen as subgroups of symmetric groups.

$f: \mathbb{C} \to \mathbb{C}$, $\boxed{f(z) = \dfrac{az+b}{cz+d}}$ $a, b, c, d \in \mathbb{C}$, $ad-bc \neq 0$

$$f(z) - f(w) = \frac{az+b}{cz+d} - \frac{aw+b}{cw+d} = \frac{(ad-bc)(z-w)}{(cw+d)(cz+d)}$$

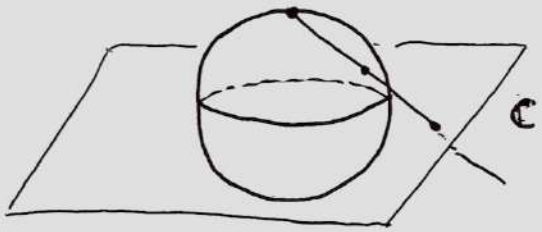
so if $ad-bc = 0$, then $f(z) = f(w)$ so f would be constant.

(We're trying to make a group so need invertible functions)

If $c \neq 0$, then $f\left(-\frac{d}{c}\right)$ gives zero denominator

To fix this, we introduce a new point "∞" to $\mathbb{C}$ to form the <u>extended complex plane</u>. ($\hat{\mathbb{C}}$) which is '$\mathbb{C} \cup \{\infty\}$.

We can visualise this via <u>stereographic projection</u>.



Get correspondence between points on sphere and points in $\mathbb{C}$ by drawing a line through "north pole" and sphere point and finding where it meets $\mathbb{C}$.

The north pole corresponds to ∞ in $\hat{\mathbb{C}}$.

<u>Definition 2.22</u> A Möbius map is a function $f: \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ of the form $f(z) = \dfrac{az+b}{cz+d}$ with $a, b, c, d \in \mathbb{C}$, $ad-bc \neq 0$, $f\left(-\frac{d}{c}\right) = \infty$

and $f(\infty) = \begin{cases} a/c & \text{if } c \neq 0 \\ \infty & \text{if } c = 0 \end{cases}$

<u>Lemma 2.23</u> Möbius maps are bijections $\hat{\mathbb{C}} \to \hat{\mathbb{C}}$.

<u>Proof</u> The inverse of $f(z) = \dfrac{az+b}{cz+d}$ is $f^{-1}(z) = \dfrac{dz-b}{-cz+a}$

(can check: $f(f^{-1}(z)) = \dfrac{a\left(\frac{dz-b}{-cz+a}\right)+b}{c\left(\frac{dz-b}{-cz+a}\right)+d} = \ldots = z$ $(z \neq \infty \text{ or } \frac{a}{c})$.

nonzero: $ad-bc \neq 0$

$$f\left(f^{-1}(\infty)\right) = f\left(-\frac{d}{c}\right) = \infty, \qquad f\left(f^{-1}\left(\frac{a}{c}\right)\right) = f(\infty) = \frac{a}{c}$$

so ff^{-1} = identity function $z \mapsto z$.

Similarly we can check $f^{-1}f$ = identity. □

Theorem 2.24 The set M of Möbius maps forms a group under composition.

Proof closure: Let $f_1(z) = \dfrac{a_1 z + b_1}{c_1 z + d_1}$ $\qquad f_2(z) = \dfrac{a_2 z + b_2}{c_2 z + d_2}$

$$(f_2 f_1)(z) = f_2(f_1(z)) = \frac{a_2\left(\frac{a_1 z + b_1}{c_1 z + d_1}\right) + b_2}{c_2\left(\frac{a_1 z + b_1}{c_1 z + d_1}\right) + d_2}$$

$$= \frac{(a_1 a_2 + b_2 c_1) z + (a_2 b_1 + b_2 d_1)}{(c_2 a_1 + d_2 c_2) z + (c_2 b_1 + d_1 d_2)} = \frac{az + b}{cz + d}$$

and $ad - bc = (a_1 a_2 + b_2 c_1)(c_2 b_1 + d_1 d_2)$

$$- (a_2 b_1 + b_2 d_1)(c_2 a_1 + d_2 c_2)$$

$$= (a_1 d_1 - b_1 c_1)(a_2 d_2 - b_2 c_2) \neq 0.$$

For $z \neq \infty$, $z \neq -\dfrac{d_1}{c_1}$, $z \neq f_1^{-1}\left(-\dfrac{d_2}{c_2}\right)$

Special cases:

$$f_2(f_1(\infty)) = f_2\left(\frac{a_1}{c_1}\right) = \frac{a_2\left(\frac{a_1}{c_1}\right) + b_2}{c_2\left(\frac{a_1}{c_1}\right) + d_2} = \frac{a_1 a_2 + b_2 c_1}{c_2 a_1 + d_2 c_1}$$

This matches $\dfrac{a\infty + b}{c\infty + d}$

$f_2\left(f_1\left(\frac{-d_1}{c_1}\right)\right) = f_2(\infty) = \frac{a_2}{c_2}$ matching $\frac{a\left(\frac{-d_1}{c_1}\right)+b}{c\left(\frac{-d_1}{c_1}\right)+d}$ (check)

$f_2\left(f_1\left(f_1^{-1}\left(\frac{-d_2}{c_2}\right)\right)\right) = f_2\left(\frac{-d_2}{c_2}\right) = \infty$

which matches $\frac{a\left(\frac{-d}{c}\right)+b}{c\left(\frac{-d}{c}\right)+d} = \infty$. Note $f_1^{-1}\left(\frac{-d_2}{c_2}\right) = \frac{-d}{c}$.

Identity: $id: z \mapsto z = \frac{1(z)+0}{0(z)+1}$, $ad-bc = 1 \neq 0$

Inverse: follows from bijection

Associativity: Function composition is associative. □

Note M is not abelian e.g. $f_1(z) = z+1$, $f_2(z) = 2z$.

Remark For working with Möbius maps in $\hat{\mathbb{C}}$, use conventions

"$\frac{1}{\infty} = 0$", "$\frac{1}{0} = \infty$", "$\frac{a\infty}{c\infty} = \frac{a}{c}$"

Proposition 2.25 Every Möbius map can be written as a composition of maps of the following forms

(i) $f(z) = az$, $a \neq 0$ "dilation/rotation"

(ii) $f(z) = z+b$ "translation"

(iii) $f(z) = \frac{1}{z}$ "inversion"

Proof $f(z) = \frac{az+b}{cz+d}$ If $c \neq 0$ then

$$z \xmapsto{(ii)} z + \frac{d}{c} \xmapsto{(iii)} \frac{1}{z+\frac{d}{c}} \xmapsto{(i)} \frac{(-ad+bc)c^{-2}}{z+d/c}$$

$$\xmapsto{(ii)} \frac{a}{c} + \frac{(-ad+bc)c^{-2}}{z+\frac{d}{c}} = \frac{az+b}{cz+d}.$$

If $c=0$, $z \overset{(i)}{\mapsto} \frac{a}{d}z \overset{(ii)}{\mapsto} \frac{a}{d}z + \frac{b}{d} \mapsto \frac{az+b}{d}$. □

In particular, the set of all dilations/rotations, translations and inversion generates M, i.e. $\langle f \rangle = M$.

Lagrange's Theorem

Definition 3.1 Let H be a subgroup of a group G, $g \in G$. A set of the form

$gH = \{gh : h \in H\}$ is called a left coset of H in G.

$Hg = \{hg : h \in H\}$ is a right coset.

($gH, Hg \subseteq G$ but not necessarily subgroups).

Think of a coset as being a "translated copy" of H that may no longer be a subgroup.

Examples 3.2

0) Let $H = \{e\} \leq G$. Then $gH = \{g\} = Hg$

1) Let $H = 2\mathbb{Z} \leq \mathbb{Z}$. Then $0 + 2\mathbb{Z} = \{0+k : k \in 2\mathbb{Z}\}$
$= 2\mathbb{Z}$

$1 + 2\mathbb{Z} = \{\ldots, -3, -1, 1, 3, \ldots\}$

2) $H = \{e, (12)\} \leq S_3 = \{e, (12), (13), (23), (123), (132)\}$

$eH = \{e, (12)\} = H$

$(12)H = \{(12)e, (12)(12)\} = \{(12), e\} = H$

$(13)H = \{(13), (13)(12)\} = \{(13), (123)\}$.

$(23)H = \{(23), (132)\}$

$(123)H = \{(123), (13)\} = (13)H$

$(132)H = \{(132), (23)\} = (23)H$.

Note

$\bigcup_{g \in G} gH = G$

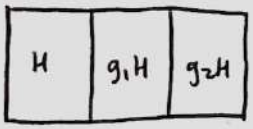
$|H| = |gH|$

Groups - Lecture 9

28/10/20

Last time: $H \leq G$, $g \in G$

$gH \subseteq G := \{gh : h \in H\}$ $\quad$ $Hg \subseteq G := \{hg : h \in H\}$



"G is union of equally-sized, non-overlapping cosets"

Theorem 3.3 (Lagrange's Theorem) Given H, a subgroup of a finite group G:

(i) $|H| = |gH| \quad \forall g \in G$

and

(ii) for $g_1, g_2 \in G$, either $g_1H = g_2H$ or $g_1H \cap g_2H = \emptyset$.

(iii) $G = \bigcup_{g \in G} gH$

In particular, defining the **index** of H in G $|G:H|$ is the number of distinct cosets of H in G, we have

$$|G| = |G:H|\,|H|.$$

"Cosets pave the group"

Proof

(i) The function $H \to gH$ $\quad h \mapsto gh$ defines a bijection between H and gH so $|H| = |gH|$.

(ii) Suppose $g_1H \cap g_2H \neq \emptyset$. Then $\exists g \in g_1H \cap g_2H$.

So $g = g_1h_1 = g_2h_2$

Then $g_1 = g_2h_2h_1^{-1}$ so for any $h \in H$ we have $g_1h = g_2\underbrace{h_2h_1^{-1}h}_{\in H} \in g_2H$ so $g_1H \subseteq g_2H$.

Similarly $g_2H \subseteq g_1H$ so $g_1H = g_2H$ if the intersection is nontrivial.

(iii) Given $g \in G$, we have $g \in gH$.

So $G \subseteq \bigcup_{g \in G} gH$. Certainly $\bigcup gH \subseteq G$ so they are equal.

So $|G| = (\text{no. of distinct cosets of } H) \cdot |H| = |G:H| \cdot |H|$. □

Note that in general $gH \neq Hg$.

When are two left cosets the same?

Proposition 3.4 $g_1 H = g_2 H$ iff $g_1^{-1} g_2 \in H$

Proof Exercise

In particular, taking $g' \in gH$ gives $g^{-1} H = gH$.

Take an element from each of the distinct cosets

$g_1, g_2, \ldots, g_{|G:H|}$. Then $G = \bigsqcup_{i=1}^{|G:H|} g_i H$ (disjoint union)

The g_i are <u>coset representatives</u> of H in G.

Corollary 3.5 Let G be a finite group and $g \in G$. Then $\text{ord}(g) \mid |G|$.

Proof Take $H = \langle g \rangle$, then $\text{ord}(g) = |H| \mid |G|$ (LT)
so $\text{ord}(g) \mid |G|$. □

Corollary 3.6 Let G be a finite group, $g \in G$. Then $g^{|G|} = e$.

Proof $g^{|G|} = g^{|G:H||H|}$ with $H = \langle g \rangle$

$= g^{|G:H| \, \text{ord}(g)} = e^{|G:H|} = e$. □

★ **Corollary 3.7** A group of <u>prime</u> order must be cyclic and generated by any non-identity element.

Proof Let $|G| = p$ (p prime).

Take $g \in G$. Then $|\langle g \rangle| \mid |G|$ so as $|G| = p$,

$|\langle g \rangle| = 1$ or p for all g. If $g \neq e$ then

$|\langle g \rangle| = p$ so $\langle g \rangle = G$.

□

An application in NT

Consider $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$

Define multiplication: $a * b = ab \bmod n$. Is this well defined?

If $a_1 \equiv a_2 \bmod n$, $b_1 \equiv b_2 \bmod n$

then $a_1 = a_2 + nk$, $b_1 = b_2 + n\ell$, so

$a_1 b_1 = (a_2 + nk)(b_2 + n\ell) = a_2 b_2 + n(n\ell k + a_2 \ell + b_2 k)$

So $a_1 b_1 \equiv a_2 b_2 \bmod n$. So is well-defined.

The set $\{0, 1, \ldots, n-1\}$ is not a group wrt multiplication as some elements don't have inverses (multiplicative), e.g. 0.

Let $\mathbb{Z}_n^*$ be $\mathbb{Z}_n \setminus \{\text{non-invertible elements}\}$ (not just 0)

In fact $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : a \text{ coprime to } n\}$

Then can easily check $(\mathbb{Z}_n^*, * \bmod n)$ is a group.

Define Euler totient function $\phi(n) = |\mathbb{Z}_n^*|$

e.g. $\phi(5) = |\{1, 2, 3, 4\}| = 4$

$\phi(6) = |\{1, 5\}| = 2$

Theorem 3.8 (Fermat-Euler theorem) Let $n \geq 1$, $N \in \mathbb{Z}$ coprime to n. Then $N^{\phi(n)} \equiv 1 \bmod n$.

Proof N coprime to $n \Rightarrow$ the element a of $\mathbb{Z}_n$ corresponding to N is in $\mathbb{Z}_n^*$, so $a^{|\mathbb{Z}_n^*|} = a^{\phi(n)} = 1$ in $\mathbb{Z}_n^*$ by corollary 3.6.

Since $N = a + kn$, $N^{\phi(n)} = (a + kn)^{\phi(n)} = a^{\phi(n)} + n(\ldots)$

$\equiv a^{\phi(n)} \equiv 1 \bmod n$.

□

In particular, for p prime, $N^{p-1} \equiv 1 \bmod p$ for any N not divisible by p.

Exploring groups using Lagrange

Example 3.9 D_{10} : possible subgroup sizes are 1, 2, 5, 10

1 : $\{e\}$

2 : Generated by each of the 5 possible reflections

5 : must be cyclic as 5 is prime so rotations

10 : D_{10}

Study groups of order up to 8

$|G| = 1 \Rightarrow G = \{e\}$

$|G| = 2 \Rightarrow G \cong C_2$ by Corollary 3.7

$|G| = 3 \Rightarrow G \cong C_3$ similarly

$|G| = 4$?

Proposition 3.10 If $|G| = 4$ then either $G \cong C_4$ or $G \cong C_2 \times C_2$.

Proof By LT, possible orders of elements of G are 1, 2 or 4.

If there is an element of order 4 g, then

$G = \langle g \rangle$ as g, g^2, g^3 all distinct: $G = C_4$.

If there is no such element then all non-identity elements have order 2. Then G is abelian (see sheet 1 Q7).

Take two distinct order 2 elements b, c. Then

$\langle b \rangle \cap \langle c \rangle = \{e, b\} \cap \{e, c\} = \{e\}$

$bc = cb$ (G abelian)

bc is in neither b nor c and $bc \neq e \neq b \neq c$

so bc is 4th element and $G = \langle b \rangle \times \langle c \rangle$. □

$|G| = 5 \Rightarrow G \cong C_5$ again by Corollary 3.7.

Quotients of Groups

How and when does it make sense to divide a group by another? We are interested in subgroups where left and right cosets coincide.

Definition (Normal subgroup) A subgroup $N \leq G$ is normal if $\forall g \in G$, $gN = Ng$. Write $N \trianglelefteq G$.

Exercise Show that the following are equivalent:

- $\forall g \in G \quad gN = Ng$
- $\forall g \in G \quad \cancel{\forall n \in N} \; \forall n \in N, \; g^{-1} n g \in N$
- $\forall g \in G, \; g^{-1} N g = N$

Examples 4.2

0) $\{e\}$ and G are always normal subgroups of G.

1) $n\mathbb{Z} \trianglelefteq \mathbb{Z}$: $\forall a \in \mathbb{Z}, \quad a + n\mathbb{Z} = n\mathbb{Z} + a$

2) $A_3 \trianglelefteq S_3$ (A_3 = even permutations)

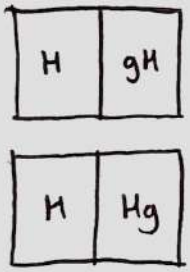
Proposition 4.3

(i) Any subgroup of an abelian group is normal

(ii) Any subgroup of index 2 is normal

Proof (i) If G abelian, then $g^{-1} n g = n \quad \forall g \in G, \; n \in N$.

(ii)



2 cosets "pave" the group

If $H \leq G$ with $|G:H| = 2$ then there are only 2 different cosets, one is H. Cosets are disjoint by Lagrange, so the other coset is $G \setminus H$, both for left and right cosets. So H is normal. □

Proposition 4.4 If $\phi : G \to H$ is a homomorphism, then $\ker \phi \trianglelefteq G$.

Proof $\ker \phi \leq G$. Given $k \in \ker \phi$ we want $g^{-1} k g \in \ker \phi$

$$\phi(g^{-1} k g) = \phi(g^{-1}) \phi(k) \phi(g) = \phi(g)^{-1} e \phi(g)$$

$$= \phi(e) = e \quad \text{so } g^{-1} k g \in \ker \phi.$$ □

Example 4.5

1) $SL_2(\mathbb{R}) \trianglelefteq GL_2(\mathbb{R})$

↑ 2×2 matrices of det. 1

↑ 2×2 invertible matrices

$\det : GL_2(\mathbb{R}) \to \mathbb{R}^\times$

identity 1

so $SL_2(\mathbb{R}) = \ker(\det)$

2) $A_n \trianglelefteq S_n$ ($A_n = \ker(\text{sign})$ and an index 2 subgroup)

3) $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ ($n\mathbb{Z}$ abelian; $n\mathbb{Z}$ = kernel of $\phi : \mathbb{Z} \to \mathbb{Z}_n$)

We can use this to study small-order groups.

If $|G| = 6$ then $G \cong C_6$ or $G \cong D_6$. (Proposition 4.6)

Proof By Lagrange, element orders are 1, 2, 3, 6.

- If there's an element of order 6 then $G \cong C_6 = \langle g \rangle$ where $g^6 = e$
- If not, then by Q7 on sheet 1 then there must be an element not of order 1 or 2 (or group order would be a power of 2). So there's an element r of order 3.

By Lagrange $|G| = 6 = |G : \langle r \rangle| \cdot |\langle r \rangle| = 3\,|G : \langle r \rangle|$

so $|G : \langle r \rangle| = 2$ so $\langle r \rangle \trianglelefteq G$ by Prop. 4.3.

There must also be an element s of order 2 since $|G|$ is even (Q8 sheet 1).

What can $s^{-1}rs \in \langle r \rangle$ be?

If $s^{-1}rs = e$ then $r = e$ but r has order 3 ✱

If $s^{-1}rs = r$ then $sr = rs$ and so sr has order 6 (since $(sr)^n = s^n r^n$ if they commute) ✱

So $s^{-1}rs = r^2 \Rightarrow G = \langle r, s \rangle$ with

$r^3 = e$, $s^2 = e$, $sr = r^2 s = r^{-1}s$ so $G \cong D_6$.

□

Recall $N \leq G$ is normal if $gN = Ng \quad \forall g \in G$

$(g^{-1}Ng = N)$

Quotients

Motivation: consider $n\mathbb{Z} \trianglelefteq \mathbb{Z}$. Cosets are

$0 + n\mathbb{Z}, \quad 1 + n\mathbb{Z}, \quad 2 + n\mathbb{Z}, \quad \ldots, \quad (n-1) + n\mathbb{Z}$

These cosets behave a lot like elements of $\mathbb{Z}_n$.

If we try to "add" them then we can define

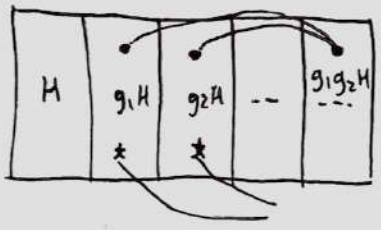
$(k + n\mathbb{Z}) + (m + n\mathbb{Z}) := (k+m) + n\mathbb{Z}$

For a general subgroup $H \leq G$, could try to do the same:

$g_1 H \, g_2 H = g_1 g_2 H$

This may not be well-defined:

may depend on choice of g_1, g_2.



Do these other two coset representatives still give the same new coset?

To have it well-defined, we need

$g_1' H = g_1 H, \quad g_2' H = g_2 H \Rightarrow g_1' g_2' H = g_1 g_2 H.$

If $g_1' H = g_1 H, \; g_2' H = g_2 H$ then $g_1' = g_1 h_1, \; g_2' = g_2 h_2$ for some $h_1, h_2 \in H$.

So $g_1' g_2' H = g_1 h_1 g_2 \underbrace{h_2 H}_{H} = g_1 h_1 g_2 H$

So in order for $g_1' g_2' H = g_1 g_2 H$, we need $g_1 h_1 g_2 H = g_1 g_2 H$

$\Rightarrow h_1 g_2 H = g_2 H$

$\Rightarrow g_2^{-1} h_1 g_2 H = H \Rightarrow g_2^{-1} h_1 g_2 \in H$

$\Leftrightarrow$ H is a normal subgroup.

Proposition 4.7 The set of (left) cosets of N in G forms a group under operation $g_1N \cdot g_2N = g_1g_2N$ if $N \trianglelefteq G$.

Proof Well-defined operation: normal subgroup ensures this

Closure if g_1N, g_2N are cosets then so is g_1g_2N

Identity $eN = N$

Inverse $(gN)^{-1} = g^{-1}N$

Associativity inherited from G □

Definition 4.8 If $N \trianglelefteq G$, the group of left cosets of N in G is called the quotient group of G by N, written G/N.

Examples 4.9

1) cosets of $n\mathbb{Z}$ in $\mathbb{Z}$, as seen above. In fact $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

2) $A_3 \trianglelefteq S_3$ gives S_3/A_3 – has 2 elements as $|S_3 : A_3| = 2$.
So $S_3/A_3 \cong C_2$
Indeed, take a nontrivial coset e.g. $(1\,2)A_3$:
$(1\,2)A_3 \cdot (1\,2)A_3 = (1\,2)^2 A_3 = A_3$.

Note in general $\left|\frac{G}{N}\right| = |G : N|$.

3) If $G = H \times K$ then both H and K are normal in G.
$G/H \cong K$ and $G/K \cong H$ (Exercise)

4) Consider $N := \langle r^2 \rangle \leq D_8$. Can check it's normal:
$r^{-1}r^2r \in N$ and $s^{-1}r^2s = r^{-2} = r^2 \in N$

Since $\langle r, s \rangle = D_8$, we have that if $g^{-1}ng \in N$ for g generators then it holds for the whole group.

Then $|N| = 2$ so $|D_8/N| = |D_8 : N| = \frac{|D_8|}{|N|}$ by Lagrange

$= 8/2 = 4.$

By Proposition 3.10, $D_8/N \cong C_2 \times C_2$ or C_4.

$D_8/N = \{N, sN, rN, srN\}$

Can check sN, rN, srN all have order 2 so

$D_8/N \cong C_2 \times C_2$.

Non-example

$H := \langle (1\,2) \rangle \leq S_3$ - not normal: $(1\,2\,3)H \neq H(1\,2\,3)$

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

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

Then $(1\,2\,3)H \cdot (1\,3\,2)H = (1\,2\,3)(1\,3\,2)H = H$

but choose different representatives:

$(1\,3)H \cdot (1\,3\,2)H = (1\,3)(1\,3\,2)H = (2\,3)H \neq H.$

(as $(2\,3)$ isn't in H). So "multiplication" is not well defined.

Remarks

- It's interesting to investigate which properties pass from G to its quotients. Being abelian and being finite are some examples.
- Quotients are not subgroups in general. May not even be isomorphic to a subgroup.
- With normality $gN = Ng \ \forall g \in G$ need to specify in which group a subgroup is normal e.g. if $K \leq N \leq G$ with $K \trianglelefteq N$, K may not be normal in G (even if N is normal in G).

Normality is not transitive.

However, if $N \leq H \leq G$ and $N \trianglelefteq G$, then $N \trianglelefteq H$.

Theorem 4.10 Given $N \trianglelefteq G$, the function $\pi : G \to \frac{G}{N}$, $\pi(g) = gN$, is a surjective homomorphism (called the the quotient map) with $\ker \pi = N$.

Proof π is a homomorphism:

$$\pi(g)\,\pi(h) = gN \cdot hN = ghN = \pi(gh)$$

Surjective: everything in G/N is a coset

$$\pi(g) = gN = N \iff g \in N \quad \text{so} \quad \ker \pi = N.$$

So together with Prop. 4.4, we have that normal subgroups are exactly the kernels of homomorphisms.

Theorem 4.11 (1st Isomorphism Theorem)

Let $\phi : G \to H$ be a HM. Then $G/\ker \phi \cong \operatorname{im} \phi$.

Theorem 4.11 (1st Isomorphism Theorem)
Let $\phi : G \to H$ be a homomorphism. Then
$G/\ker\phi \cong \operatorname{Im}\phi$.

Proof Define $\bar{\phi} : G/\ker\phi \to \operatorname{Im}\phi$ via
$$g\ker\phi \mapsto \phi(g)$$

Well-defined: if $g_1\ker\phi = g_2\ker\phi$, then
$g_1 = g_2 k$ for some $k \in \ker\phi$
$$\bar{\phi}(g_1\ker\phi) = \phi(g_1) = \phi(g_2 k) = \phi(g_2)\phi(k) = \phi(g_2) = \bar{\phi}(g_2\ker\phi)$$

Homomorphism:
$$\bar{\phi}(g\ker\phi\, g'\ker\phi) = \bar{\phi}(gg'\ker\phi) = \phi(gg') = \phi(g)\phi(g') = \bar{\phi}(g\ker\phi)\,\bar{\phi}(g'\ker\phi)$$

Surjective: all elements in $\operatorname{Im}\phi$ are of the form $\phi(g)$ for some $g \in G$

Injective: if $\bar{\phi}(g\ker\phi) = e = \phi(g)$ in $\operatorname{Im}(\phi)$ then $g \in \ker\phi$ so $g\ker\phi = \ker\phi$

□

Examples 4.12

1) $\det : GL_2(\mathbb{R}) \to \mathbb{R}^*$, $\operatorname{Im}(\det) = \mathbb{R}^*$
$\ker(\det) = SL_2(\mathbb{R})$ by definition
so $GL_2(\mathbb{R})/SL_2(\mathbb{R}) \cong \mathbb{R}^*$

2) Consider $\phi : \mathbb{R} \to \mathbb{C}^*$, $\phi(r) = e^{2\pi i r}$
$\operatorname{Im}\phi$ = circle of radius 1 in $\mathbb{C}$ (S^1)
$\phi(r) = e^{2\pi i r} = 1 \iff r \in \mathbb{Z}$ so $\ker\phi = \mathbb{Z}$
so $\mathbb{R}/\mathbb{Z} \cong S^1$

Something to help us understand subgroup structure of quotient groups:

Theorem 4.13 (Correspondence Theorem)

Let $N \trianglelefteq G$. The subgroups of G/N are in bijective correspondence with subgroups of G containing N.

Proof Given $N \leq M \leq G$, $N \trianglelefteq G$, then $N \trianglelefteq M$ and clearly $M/N \leq G/N$.

Conversely, for every subgroup $H \leq G/N$, we can take the preimage of H under the quotient map $\pi : G \to G/N$ i.e. $\pi^{-1}(H) = \{g \in G : gN \in H\}$

This is a subgroup of G:

closure: if $g_1, g_2 \in \pi^{-1}(H)$ then

$$g_1 g_2 N = \underbrace{g_1 N}_{\in H} \underbrace{g_2 N}_{\in H} \quad \text{so } g_1 g_2 N \in H.$$

(id., inverses easy to check)

$\pi^{-1}(H)$ contains N since $\forall n \in N$, $nN = N \in H$ (identity coset)

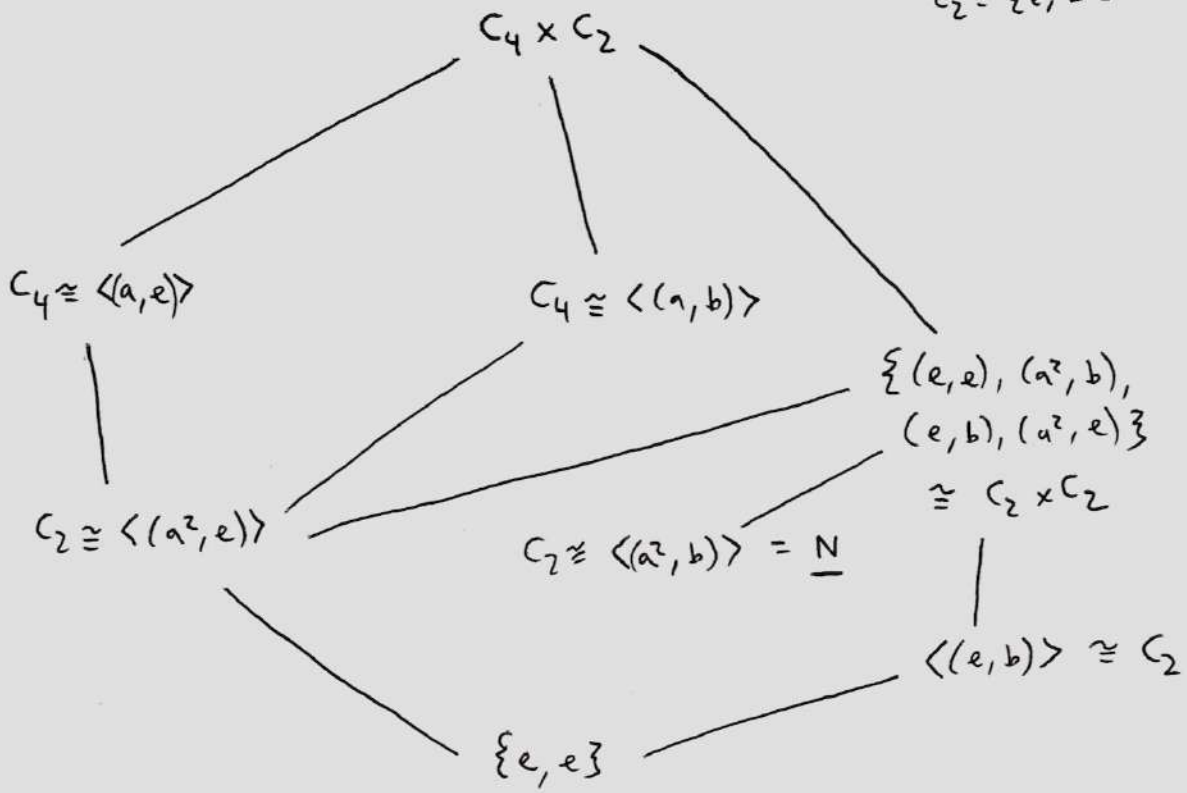
Now can check for $N \leq M \leq G$, $\pi^{-1}(M/N) = M$ and for any $H \leq G/N$, $\pi^{-1}(H)/N = H$

So correspondence is bijective. $\square$

Correspondence preserves indices, normality, containments.

e.g. $C_4 \times C_2$

$C_4 = \{e, a, a^2, a^3\}$
$C_2 = \{e, b\}$



$C_4 \times C_2 / N$ ← order 4 by Lagrange
$\cong C_4$ as $C_2 \times C_2$ has 2 more subgroups

$C_2 \cong \{N, (e,b)N\}$

$\{N\}$

What if we had a subgroup $H \leq G$ that didn't contain $N \trianglelefteq G$?
We can actually still make a normal subgroup of H by intersecting.

Corollary 4.14 (2nd Isomorphism Theorem)

Let $H \leq G$, $N \trianglelefteq G$. Then $H \cap N \trianglelefteq H$ and

$$H / H \cap N \cong HN / N$$

Proof When $N \trianglelefteq G$, $H \leq G$, then $HN = \{hn : h \in H, n \in N\}$ is a subgroup of G and $HN = \langle H, N \rangle$.

Consider $\phi : H \to HN/N$, $\phi(h) = hN$

This is a well-defined surjective homomorphism.

$\phi(h) = hN = N \iff h \in N$ (but $h \in H$ so kernel is $N \cap H$).

Then by 1st isomorphism theorem, $H/N \cap H \cong HN/N$. $(\leq G/N)$ □

We mentioned after Thm 4.13 that normality is preserved. We can even say something about quotients.

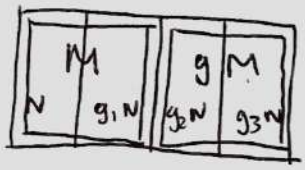
Corollary 4.15 (3rd Isomorphism Thm)

Let $N \leq M \leq G$ s.t. $N \trianglelefteq G$, $M \trianglelefteq G$.

Then $M/N \trianglelefteq G/N$ and $(G/N)/(M/N) \cong G/M$.

Proof ~~Define $\phi : G \to N$~~

Define $\phi : G/N \to G/M$ by $\phi(gN) = gM$.



ϕ is well-defined as $N \leq M$ and is a surjective HM.

Kernel: $\phi(gN) = gM = M \iff g \in M$, so $\ker\phi = \frac{M}{N}$

and by Thm 4.11, $(G/N)/(M/N) \cong G/M$. □

Example 4.16 1) Consider $\mathbb{Z}$: $H = 3\mathbb{Z}$, $N = 5\mathbb{Z}$. Then by 2nd Isomorphism Thm ($H/H\cap N \cong HN/N$), we have $H\cap N \trianglelefteq H$ i.e. $15\mathbb{Z} \trianglelefteq 3\mathbb{Z}$ and $H/H\cap N \cong \underset{\uparrow}{HN}/N = \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}_5$.
$\langle H, N\rangle$

2) (See $C_4 \times C_2$) – $C_4 = \langle a\rangle$, $C_2 = \langle b\rangle$

$N = \langle (a^2, b)\rangle$ $\quad M = \langle (e,b), (a^2, e)\rangle$

$N \leq M \leq G$, $N, M \trianglelefteq G$

By 3rd Isomorphism thm, $(C_4 \times C_2 / N)/(M/N)$
$\cong C_4 \times C_2 / M$
$\cong C_4 \times C_2 / C_2 \times C_2 \cong \underline{C_2}$.

Definition (simple group) A group $\overset{G}{\uparrow}$ is simple if its only normal subgroups are $\{e\}$ and G.

Example C_p with p prime

A_5 (proof later in course)

Section 5 : Group Actions

For many groups we've met we identified elements by their effect on a set e.g. S_n permuting $\{1, 2, \ldots, n\}$, Möbius group as functions $\hat{\mathbb{C}} \to \hat{\mathbb{C}}$, D_{2n} as symmetries of n-gon

Definition Let G be a group and X be a set. An action of G on X is a function $\alpha : G \times X \to X$ with $\alpha_g(x) = \alpha(g, x)$ satisfying :

$$\begin{cases} \alpha_g(x) \in X & \forall g \in G, x \in X \\ \alpha_e(x) = x & \forall x \in X \\ \alpha_g \alpha_h(x) = \alpha_{gh}(x) & \forall g, h \in G, x \in X \end{cases}$$

i.e. $\alpha(g, \alpha(h, x)) = \alpha(gh, x)$

Notation $G \curvearrowright X$ (G acts on X)

Example 5.2

0) Take any G, X and define the trivial action $\alpha_g(x) = x$ $\forall g \in G$, $\forall x \in X$.

1) $S_n \curvearrowright \{1, 2, \dots, n\}$ by permutation
$\alpha_g : X \to X$

2) $D_{2n} \curvearrowright \{$vertices of regular n-gon$\}$
labelled $\{1, 2, \dots, n\}$:
$D_{2n} \curvearrowright \{1, 2, \dots, n\}$ recall $D_{2n} \leq S_n$

3) $M \curvearrowright \hat{\mathbb{C}}$ (Möbius maps)

4) Symmetries of a cube act on set of vertices and set of edges, set of faces, pairs of opposite faces

Remarks
- More than one group can act on the same set
- One group can act on many sets
- Actions give information about the group

Lemma 5.3 $\forall g \in G$, $\alpha_g : X \to X$, $x \mapsto \alpha_g(x)$ is a bijection.

Proof $\alpha_g(\alpha_{g^{-1}}(x)) = \alpha_{gg^{-1}}(x) = \alpha_e(x) = x$

Similarly $\alpha_{g^{-1}}(\alpha_g(x)) = \alpha_{g^{-1}g}(x) = \alpha_e(x) = x$

So $\alpha_g \alpha_{g^{-1}}$ = identity function on X = $\alpha_{g^{-1}} \alpha_g$

So α_g is bijective. □

Also can define actions by linking G to $\mathrm{Sym}(X)$, the permutations of X.

Proposition 5.4 Let G be a group, X be a set. Then $\alpha : G \times X \to X$ is an action iff the function $\rho : G \to \mathrm{Sym}(X)$ with $\rho(g) = \alpha_g$ is a homomorphism.

Proof $\Rightarrow$: α is an action. By Lemma 5.3 α_g is a bijection $X \to X$ so $\alpha_g \in \mathrm{Sym}\, X$.
$\rho(gh) = \alpha_{gh}$ and for all $x \in X$, $\alpha_{gh}(x) = \alpha_g \alpha_h(x)$

so $\rho(gh) = \alpha_{gh} = \alpha_g \alpha_h = \rho(g)\rho(h)$

so $\rho(g)$ is a homomorphism.

$\Leftarrow$: Given $\rho : G \to \mathrm{Sym}\, X$ (a HM), can define $\alpha : G \times X \to X$ by $\alpha(g, x) = \alpha_g(x) = \rho(g)(x)$

α is an action as

- $\rho(g) \in \mathrm{Sym}\, X \Rightarrow \rho(g)(x) = \alpha_g(x) \in X$
- $\rho(e)$ = identity element in $\mathrm{Sym}\, X$
  so $\alpha_e(x) = \rho(e)(x) = x$
- $\rho(gh) = \rho(g)\rho(h) \Rightarrow \alpha_{gh}(x) = \alpha_g \alpha_h(x)$.

□

"every element of G induces a ~~for~~ bijection on X"

Write $g(x)$ for $\alpha_g : X \to X$.

Definition 5.5 The kernel of an action $\alpha : G \times X \to X$ is the kernel of the homomorphism $\rho : G \to \mathrm{Sym}\, X$ (as above).

These are all the elements of G that act as the identity of $\mathrm{Sym}\, X$ i.e. do nothing to all $x \in X$.

Note that by IIT, $G/\ker\rho \cong \operatorname{Im}\rho \leq \operatorname{sym} X$

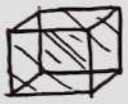
so in particular if $\ker\rho = \{e\}$, then $G \leq \operatorname{sym} X$.

Example 5.6

1) D_{2n} acting on $\{1,\dots,n\}$ (labelled vertices)
has $\ker\rho = \{e\}$: every nontrivial element of D_{2n} moves at least one vertex so $D_{2n} \leq S_n$.

2) G symmetries of cube, X = unordered pairs of opposite faces

$\{F_1, F_2\} = \{F_2, F_1\}$



$|X| = 3$ so $\rho: G \to S_3$ is a homomorphism

There are symmetries of the cube that realise all permutations of X.

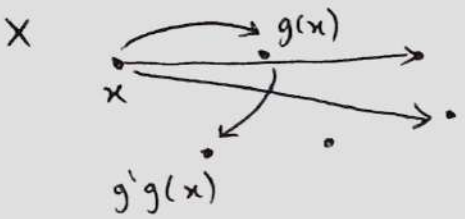
So $G/\ker\rho \cong S_3$. Notice $|G| > |S_3| = 6$ so $\ker\rho$ is nontrivial.

Definition 5.7 An action $G \curvearrowright X$ is called faithful if $\ker\rho = \{e\}$. Careful: "only e fixes everything"

NOT "only e fixes anything"

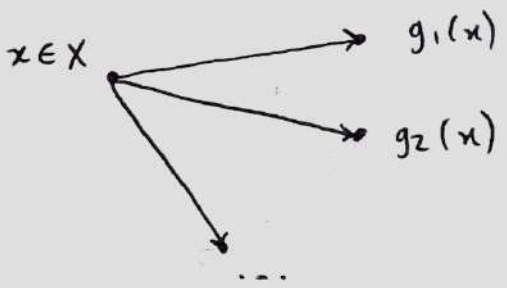
Orbits and Stabilisers

Which elements of X can we "get to" from a certain $x \in X$ using the action of G.



Which group elements leave x unchanged for a given x?

Orbits and Stabilisers



Definition 5.8

Let $G \curvearrowright X$, $x \in X$. The orbit of x, $\mathrm{Orb}(x)$ is

$$\{g(x) : g \in G\} \subseteq X.$$

The stabiliser of x is $\mathrm{Stab}(x) = \{g \in G : g(x) = x\} \leq G$

The action is transitive if $\mathrm{orb}(x) = X$.

Example

$G = S_3 = \{e, (1\,2), (2\,3), (1\,3), (1\,2\,3), (1\,3\,2)\} \leq S_4$

$G \curvearrowright \{1, 2, 3, 4\}$

$\mathrm{Orb}_G(1) = \{1, 2, 3\} = \mathrm{Orb}_G(2) = \mathrm{Orb}_G(3)$

as we can send each of 1, 2, 3 to anything in $\{1, 2, 3\}$ using permutations in G.

$\mathrm{Orb}_G(4) = 4$

$\mathrm{Stab}(1) = \{e, (2\,3)\}$ $\quad \mathrm{Stab}(2) = \{e, (1\,3)\}$

$\mathrm{Stab}(3) = \{e, (1\,2)\}$, $\quad \mathrm{Stab}(4) = G$

Lemma 5.9

For any $x \in X$, $\mathrm{stab}(x) \leq G$.

Proof closure: $g, h \in \mathrm{Stab}(x) \Rightarrow (gh)(x) = g(h(x)) = x$.

Identity: $e(x) = x$ so $e \in \mathrm{Stab}(x)$

Inverse: if $g \in \mathrm{Stab}(x)$ then $g(x) = x$

so $x = g^{-1}(x)$ as it's bijective so $g^{-1} \in \mathrm{Stab}(x)$

Associativity: inherited from G. □

Recall from N&S: a partition of a set X is a set of subsets of X s.t. each $x \in X$ belongs to exactly one subset in the partition.

Lemma 5.10 Let $G \curvearrowright X$. Then the orbits partition X.

Proof Firstly for any $x \in X$, $x \in Orb(x)$.

Suppose $z \in Orb(x) \cap Orb(y)$. Then $\exists g_1 \in G$ with $g_1(x) = z$ and $g_2 \in G$ with ~~$g_2(x) =$~~ $g_2(y) = z$

$\Rightarrow y = g_2^{-1}(z)$. so $y = g_2^{-1} g_1(x)$ so then for any $g \in G$,

$g(y) = (g g_2^{-1} g_1)(x) \in Orb(x) \Rightarrow Orb(y) \leq Orb(x)$.

By symmetry $Orb(x) \leq Orb(y)$. So $Orb(x) = Orb(y)$.

So orbits are either equal or disjoint, so distinct orbits partition X. □

Recall proof of disjoint cycle notation for $\sigma \in S_n$: what we were really doing was finding the orbits in $\{1, 2, \ldots, n\}$ under $\langle \sigma \rangle$ which are disjoint.

e.g. $(1\,2\,3)(4\,5\,6\,7)(8\,9) \in S_9$

Orbits: $\{1,2,3\}$, $\{4,5,6,7\}$, $\{8,9\}$.

Note that sizes of orbits can be different (unlike cosets).

Theorem 5.11 (Orbit-Stabiliser Theorem)

Let $G \curvearrowright X$, G finite. Then for any $x \in X$, have

$$|G| = |Orb(x)| \cdot |Stab(x)|.$$

Proof This follows from Lagrange.

PTO

$g(x) = h(x) \iff h^{-1}g(x) = x \iff h^{-1}g \in \mathrm{Stab}(x)$

$\iff g\,\mathrm{Stab}(x) = h\,\mathrm{Stab}(x)$ as cosets (Prop. 3.4).

So distinct points in $\mathrm{orb}(x)$ are in bijection with distinct cosets of $\mathrm{stab}(x)$.

So $|\mathrm{Orb}(x)| = |G : \mathrm{Stab}(x)| = \dfrac{|G|}{|\mathrm{Stab}(x)|}$ by LT

so $\underline{|G| = |\mathrm{Orb}(x)|\,|\mathrm{Stab}(x)|}$. □

Notice that all elements in a given coset $g\,\mathrm{Stab}(x)$ do the same thing to x as g does.

An element of $g\,\mathrm{Stab}(x)$ has form gh $(h \in \mathrm{Stab}(x))$

so $gh(x) = g(h(x)) = \underline{g(x)}$ as $h \in \mathrm{Stab}(x)$.

We can use orbit-stabiliser to investigate groups, e.g. we know $|D_{2n}| = 2n$ but now we can do it via orbit-stabiliser:.

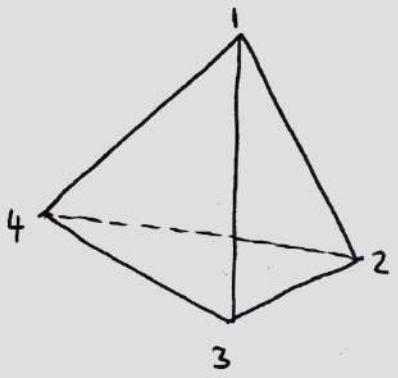
D_{2n} acts transitively on vertices $\{1, 2, \ldots, n\}$: any vertex can be sent to any other. So $|\mathrm{Orb}(1)| = n$.

$\mathrm{Stab}(1) = \{e, s\}$ so $|\mathrm{Stab}(1)| = 2$.

↑ reflection through vertex 1

So $|D_{2n}| = |\mathrm{Orb}(1)|\,|\mathrm{Stab}(1)| = \underline{2n}$.

Symmetries of the tetrahedron



4 faces (eq. triangles)

4 vertices, 6 edges

(vertices $\{1,2,3,4\}$

Let G be the group of symmetries.

G acts transitively on the vertices and there is no non-identity symmetry that fixes all the vertices. So have $\rho: G \to S_4$ injective (kernel = identity)

$\text{Orb}(1) = \{1,2,3,4\}$

$\text{Stab}(1)$ = symmetries of face $234 = \{e, (2\,3\,4), (2\,4\,3), (2\,3), (3\,4), (2\,4)\}$
$\cong D_6$. $(\cong S_3)$.

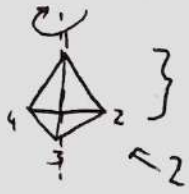
Then $|G| = |\text{Orb}(1)||\text{Stab}(1)| = 4 \times 6 = \underline{24}$.
$(= |S_4|)$

$G \leq S_4$ and $|G| = |S_4|$ so $\underline{|G| = |S_4|}$.

We have determined the group by orbits/stabilisers.

Let $G^+ \leq G$ with G^+ being only rotations.

$\text{Orb}(1) = \{1,2,3,4\}$

$\text{Stab}(1) = \{e,$ rotations through 1  $\}$ so $|\text{Stab}(1)| = 3$.

$\leftarrow$ 2 such rotations

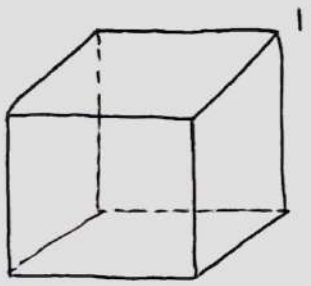
So $|G^+| = 3 \times 4 = \underline{12}$

$G^+ \leq G = S_4$ so $|G^+| = 12 \Rightarrow \underline{G^+ = A_4 \leq S_4}$.

(Note odd-order rotations $\Rightarrow$ even permutations)

Rotations through axis line joining midpts of opposite edges have form of 2 transpositions.

Symmetries of the Cube



Label vertices

$\{1, 2, \ldots, 7, 8\}$

Let G = group of symmetries of cube, acting on vertices.

This is transitive so WLOG, $|Orb(1)| = 8$.

$Stab(1)$ = { e, 2 rotations with axis through 1, 3 reflections in planes through 1 and an outgoing edge)

Size 6

so $|G| = 8 \times 6 = \underline{48}$ (we'll determine the group later)

Let G^+ be the rotations, acting on the 8 vertices

$|Orb(1)| = 8$, $|Stab(1)| = 3$ so $|G^+| = 24$.

(exclude 3 reflections)

Now let G^+ act on the 4 diagonals: $\rho : G^+ \to S_4$.

All 4-cycles are in $Im(\rho)$, as are all transpositions.

4-cycles 

transpositions 

Sheet 2: $\langle (1\,2), (1\,2\,3\,4) \rangle = S_4$ so ρ is surjective

But since $|G^+| = 24 = |S_4|$ have $G^+ \cong S_4$.

5 Platonic solids in $\mathbb{R}^3$ have polygonal faces, straight edges and vertices s.t. their group of symmetries acts transitively on triples of form (vertex, incident edge, incident face)

Cube and octahedron are dual - can be inscribed in each other with vertices in the middle of faces.

Dodecahedron and icosahedron are also dual: each pair has same sym. group.

So only 3 groups can be symmetries of Platonic solids

We have already seen that if $2 \mid |G|$ then G contains an element of order 2.

Theorem 5.12 (Cauchy's Theorem) Let G be a finite group. If a prime p divides $|G|$, then G contains an element of order p.

Proof Let $p \mid |G|$. Consider $G^p = \underbrace{G \times G \times \cdots \times G}_{p \text{ times}}$

This is the group of p-tuples of elements of G, with coordinate-wise composition.

Consider subset $X \subseteq G^p$ with $X = \{(g_1, g_2, \cdots, g_p) \in G^p : g_1 g_2 \cdots g_p = e\}$ (p-tuples multiplying to e)

Note that if $g \in G$ has order p, then $(g, g, \cdots, g) \in X$ and if $(g, g, \ldots, g) \in X$ then g has order p if $g \neq e$ (note need p prime).

Now take group $C_p = \langle a \rangle$ and let C_p act on X by "cycling": $a(g_1, \ldots, g_p) = (g_2, g_3, \ldots, g_p, g_1)$

Check this is an action:

- if $g_1 \cdots g_p = e$ then $e = g_1^{-1} e g_1 = g_1^{-1} \underbrace{g_1 g_2 \cdots g_p}_{e} g_1$
  $= g_2 \cdots g_p g_1 = e$ so cycled tuple is in X.
  (Inductively holds for a^k) tuples
- $e(g_1, \cdots, g_p) = (g_1, \cdots, g_p)$
- $a^k(g_1, \cdots, g_p) = (g_{k+1}, \ldots, g_k) = a \cdot a \cdot a \cdots a(g_1, \ldots, g_p)$

so it is an action.

PTO

Since orbits partition X, the sum of the sizes of distinct orbits must be size of X. But $|X| = |G|^{p-1}$ because you can choose any of the $|G|$ elements for each of the first $p-1$ elements in the tuple freely, and then the last one must be their product's inverse.

So since $p \mid |G|$, have $p \mid |G|^{p-1} \Rightarrow p \mid |X|$.

We apply Orbit-Stabiliser Theorem:

$$|\mathrm{Orb}(g_1, \dots, g_p)| \, |\mathrm{Stab}(g_1, \dots, g_p)| = |C_p| = p$$

Size of any orbit divides p, so any orbit has size 1 or p and sum to size of $X = kp$ $(k \in \mathbb{Z})$ as $p \mid |X|$

$$|X| = kp = \underbrace{\sum_{\substack{\text{orbits} \\ \text{size 1}}} 1}_{\text{so \# of size-1 orbits divides } p.} + \sum_{\substack{\text{orbits} \\ \text{size } p}} p \quad \leftarrow \text{a multiple of } p.$$

This isn't 0: $|\mathrm{Orb}(e, e, \dots, e)| = 1$

so there must be other orbits of size 1. (At least $p-1$ others)

But orbits of size 1 must be of form

$\{(g, g, \dots, g)\}$ so $\exists\, g \neq e$ in G with this element in X, i.e. $g^p = e$. (So $\mathrm{ord}\, g = p$). $\square$

Left Multiplication Actions

Lemma 5.13 Let G be a group. Then G acts on itself by left multiplication. This action is faithful and transitive.

Proof – $\forall g \in G$, $\forall x \in G$, have $gx \in G$.

– $e(x) = e \cdot x = x \quad \forall x \in G$

– $(gh)(x) = g(h(x))$ by associativity.

So it is an action.

This action is faithful: $g(x) = x \iff gx = x \iff g = e$

Transitive: given $x, y \in G$, set $g = yx^{-1}$

so $g(x) = yx^{-1}x = y$. □

Definition 5.14 The left multiplication action is called the left regular action.

Theorem 5.15 (Cayley's Theorem) Every group is isomorphic to a subgroup of a symmetric group.

Proof Let $G \curvearrowright G$ (left reg. action). This gives a homomorphism $\rho : G \to \mathrm{Sym}(G)$ with $\ker \rho = \{e\}$ (as faithful) since action is faithful, so by 1st isomorphism theorem, $G/\ker\rho = G \cong \mathrm{Im}\,\rho \leq \mathrm{Sym}\, G$ (as image must be a subgroup. So $G \cong$ (some subgroup of $\mathrm{Sym}\, G$). □

Proposition 5.16 Let $H \leq G$. Then G acts on the set of left cosets by left multiplication, and action is transitive. "Left coset action"

$g(xH) = gxH$

PTO

Proof - $g(g_1H) = gg_1H$, so $g(g_1H)$ is a left coset.

- $e(g_1H) = eg_1H = g_1H$

- $gg'(g_1H) = gg'g_1H = g(g'(g_1H))$ so is an action.

Transitive: given g_1H, g_2H, have $g_1g_2^{-1}(g_2H) = g_1H$. □

Note: this is the left-regular if $H = \{e\}$.

This induces actions of G on its quotient groups G/N

Conjugation Actions

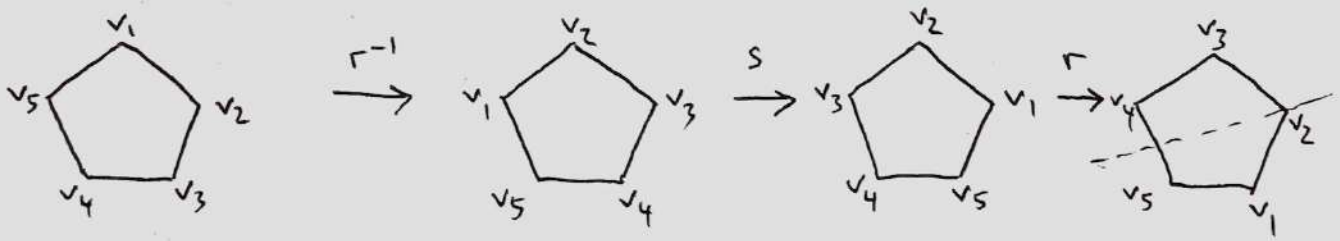
Definition 5.17 Given $g, h \in G$, the element $hgh^{-1} \in G$ is the conjugate of g by h.

We should think of conjugate elements as doing the same thing but from different points of view. This will become particularly clear when we look at Möbius maps and matrices later.

Example Consider D_{10} and consider the conjugate s and rsr^{-1} (s: reflection through v_1 and centre).

Have r as rotation by $2\pi/5$ clockwise.

What does rsr^{-1} do?



The end result is the same as reflecting in axis through centre and v_2 so result of conjugation of a reflection is still a reflection, but from a different point of view.

Another example is matrix groups e.g. $GL_n\mathbb{R}$ where a conjugate matrix represents the same transformation wrt a different basis.

Proposition 5.18 A group G acts on itself by conjugation.

Proof $g(x) = gxg^{-1} \in G$

$e(x) = exe^{-1} = x$

$gh(x) = ghx(gh)^{-1} = ghxh^{-1}g^{-1} = g(hxh^{-1})g^{-1}$
$= g(h(x))$.

So it's an action.

The kernel, orbits and stabilisers have special names:

Definition 5.19 - The kernel of the conjugation action of G on itself is called the centre $Z(G)$ of G:

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

(note $ghg^{-1} = h \iff gh = hg$ so this is the set of elements that commute with every other)

- The orbit of the action is called a conjugacy class

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

- Stabilisers are called centralisers

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

"elements that commute with this particular h"

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

Definition 5.20 If $H \leq G$, $g \in G$, then the conjugate of H by g is $gHg^{-1} = \{ ghg^{-1} : h \in H \}$

Proposition 5.21 Let $H \leq G$, $g \in G$. Then $gHg^{-1} \leq G$.

Proof Closure: $gh_1g^{-1}, gh_2g^{-1} \in gHg^{-1}$

$$\Rightarrow (gh_1g^{-1})(gh_2g^{-1}) = gh_1g^{-1}gh_2g^{-1}$$
$$= gh_1h_2g^{-1} \in gHg^{-1}$$

Identity: $geg^{-1} = e \in gHg^{-1}$

Inverses: given $ghg^{-1} \in gHg^{-1}$, $gh^{-1}g^{-1} \in gHg^{-1}$ is the inverse of ghg^{-1}

Associativity: inherited from G. □

Note: $gHg^{-1} \cong H$ (Exercise)

Proposition 5.22 A group G acts by conjugation on the set of its subgroups. The singleton orbits are exactly the normal subgroups.

Proof Exercise (recall $N \trianglelefteq G \iff gNg^{-1} = N$).

Groups - Lecture 17

Proposition 5.23 Normal subgroups are those subgroups that are unions of conjugacy classes.

Proof Let $N \trianglelefteq G$. If $h \in N$ then $ghg^{-1} \in N \quad \forall g \in G$.
So $ccl(h) \subseteq N$. So N is a union of ccls of its elements

i.e. $$N = \bigcup_{h \in N} ccl(h)$$

Conversely if $H \leq G$ is a union of ccls then $\forall g \in G$, $\forall h \in H$, $ghg^{-1} \in H$, so $H \trianglelefteq G$. □

Example $A_3 = \{e, (123), (132)\} \trianglelefteq S_3$

$A_3 = \{e\} \cup \{(123), (132)\}$

Note that $(123), (132)$ are conjugate in S_3 but not A_3.

Lemma 5.24 Given a k-cycle $(a_1, \dots, a_k)$ and $\sigma \in S_n$, we have $\sigma(a_1 \dots a_k)\sigma^{-1} = (\sigma(a_1)\ \sigma(a_2) \dots \sigma(a_k))$

Proof $\sigma(a_1 \dots a_k)\sigma^{-1}$:
$$\sigma(a_1) \mapsto a_1 \mapsto a_2 \mapsto \sigma(a_2)$$
$$\sigma(a_2) \mapsto a_2 \mapsto a_3 \mapsto \sigma(a_3)$$
$$\dots$$
$$\sigma(a_k) \mapsto a_k \mapsto a_1 \mapsto \sigma(a_1)$$

so $\sigma(a_1 \dots a_k)\sigma^{-1}$ and $(\sigma(a_1) \dots \sigma(a_k))$ do the same thing to $\{\sigma(a_1), \dots, \sigma(a_k)\}$.

For any $a \notin \{\sigma(a_1), \dots, \sigma(a_k)\}$, have $(\sigma(a_1) \dots \sigma(a_k))$ leaves a unchanged, so so does $\sigma(a_1 \dots a_k)\sigma^{-1}$ since $\sigma^{-1}(a) \notin \{a_1, \dots, a_k\}$.

□

Proposition 5.25 Two elements of S_n are conjugate (in S_n) iff they have the same cycle type.

Proof Two elements that are conjugate will certainly have the same cycle type: given $\sigma \in S_n$, write σ in disjoint cycles: $\sigma = \sigma_1 \sigma_2 \dots \sigma_m$. Then if $\rho \in S_n$

$$\rho \sigma \rho^{-1} = \rho \sigma_1 \rho^{-1} \rho \sigma_2 \rho^{-1} \dots \rho \sigma_m \rho^{-1}$$

by 5.24 each $\rho \sigma_i \rho^{-1}$ is a cycle of the same length as σ_i and $\rho \sigma_i \rho^{-1}$ still disjoint - ρ bijective.

Conversely if σ and τ have same cycle type, then

$$\sigma = (a_1 \dots a_{k_1})(a_{k_1+1} \dots a_{k_2})(a_{k_2+1} \dots a_{k_3}) \dots$$

$$\tau = (b_1 \dots b_{k_1})(b_{k_1+1} \dots b_{k_2})(b_{k_2+1} \dots b_{k_3}) \dots$$

in disjoint cycle notation including singletons. So all of $\{1, \dots, n\}$ appear in both σ and τ.

Then setting ρ as $\rho(a_i) = b_i \ \forall i$, obtain $\rho \sigma \rho^{-1} = \tau$. (again using 2.54). □

Example 5.26 Conjugacy classes of S_4

cycle type	example element	size of cl	size of C_{S_4}	sign
1,1,1,1	(1)(2)(3)(4) = e	1	24	1
2,1,1	(12)	6	4	-1
2,2	(12)(34)	6/2 = 3	8	1
3,1	(123)	2x3x4/3 = 8	3	1
4	(1234)	6	4	-1

Can find normal subgroups from this.

$N \trianglelefteq S_4$ must contain e and be a union of conjugacy classes

Must have $|N| \mid 24$

Possibilities: look through divisors of 24: 1, 2, 3, 4, 6, 8, 12, 24

Order 1: $\{e\}$

Order 2 impossible

Order 3 impossible

Order 4: $\{e, (12)(34), (13)(24), (14)(23)\}$ $\cong C_2 \times C_2$ or "V_4" Klein four group

Order 8 impossible

Order 12: $\{e, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\} \cong A_4$

Order 24: S_4

All possible quotients of S_4 are:

$S_4/\{e\} \cong S_4$ $\quad S_4/V_4 \cong S_3$ $\quad S_4/A_4 \cong C_2$

$S_4/S_4 \cong \{e\}$

Exercise Do this for S_5.

What about conjugation in A_n? Note $ccl_{S_n}(\sigma) = \{\tau\sigma\tau^{-1} : \tau \in S_n\}$

$ccl_{A_n}(\sigma) = \{\tau\sigma\tau^{-1} : \tau \in A_n\}$

so have $ccl_{A_n}(\sigma) \subseteq ccl_{S_n}(\sigma)$ as $A_n \leq S_n$.

But elements that are conjugate in S_n may not be conjugate in A_n.

e.g. $(23)(123)(23) = (132)$ in S_3 so $(123), (132)$ conj. in S_3

but $(23) \notin A_3$ and there are no $\tau \in A_3$ (other) that are such that $\tau(123)\tau^{-1} = (132)$.

However in S_5 $\quad (23)(45)(123)(45)(23) = (132)$

and $(23)(45)$ is in A_5.

Some conjugacy classes of S_n will split into smaller conjugacy classes in A_n. How?

By Orbit-Stabiliser, $|S_n| = |ccl_{S_n}(\sigma)||C_{S_n}(\sigma)|$

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

But $|S_n| = 2|A_n|$ and $|ccl_{A_n}(\sigma)| \leq |ccl_{S_n}(\sigma)|$ so either

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

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

Definition 5.27 When $|ccl_{A_n}(\sigma)| = \frac{1}{2}|ccl_{S_n}(\sigma)|$, we say that the conjugacy class of σ <u>splits</u> in A_n.

Proposition 5.28 The ccl of $\sigma \in A_n$ splits in A_n iff there are no odd permutations that commute with σ.

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

$C_{A_n}(\sigma) = A_n \cap C_{S_n}(\sigma)$ intrinsically

and $A_n \cap C_{S_n}(\sigma) = C_{S_n}(\sigma)$ iff C_{S_n} contains no odd elements. (i.e. no odd permutation commutes with σ - under conjugation action $\tau\sigma\tau^{-1} = \sigma \iff \tau\sigma = \sigma\tau$).

□

Example 5.29 ccls in A_4

cycle type	example element	odd element in C_{S_4}?	size of ccl_{S_4}	size of ccl_{A_4}
1, 1, 1, 1	e	✓ e.g. (1 2)	1	1
2, 2	(12)(34)	✓ e.g. (1 2)	3	3
3, 1	(123)	× as $\lvert C_{S_4}(123)\rvert = 3$ and $C_{S_4}(123)$ contains exactly $\langle(123)\rangle$ - none are odd	8	4, 4

Example 5.30 ccls in A_5

cycle type	example element	odd el. in C_{S_5} ?	size of ccl_{S_5}	size of ccl_{A_5}
1, 1, 1, 1	e	✓	1	1
2, 2, 1	$(12)(34)$	✓	15	15
3, 1, 1	(123)	✓	20	20
5	(12345)	×	24	12/12

↗ as $C_{S_5}(12345) = \langle (12345) \rangle$ exercise

Theorem 5.32 A_5 is a simple group.

Proof Normal subgroups must be unions of ccls, must contain e, and order must divide $|A_5| = 60$.

Sizes of ccl_{A_5} are 1, 15, 20, 12, 12

The only ways of adding $1 +$ (some of 15, 20, 12, 12) to get a divisor of 60 are

$$1, \quad 1 + 15 + 20 + 12 + 12 \quad \text{(can check: no other ways)}$$
$$\downarrow \qquad\qquad \downarrow$$
$$1 \qquad\qquad 60$$

so only normal subgroups of A_5 are $\{e\}$ and A_5. □

Remark All A_n ($n \geq 5$) are simple: proved in IB GRM.

Section 6 Möbius groups revisited

Recall: $f : \hat{\mathbb{C}} \to \hat{\mathbb{C}}$

$$f(z) = \frac{az+b}{cz+d} \qquad a, b, c, d \in \mathbb{C}$$

$$ad - bc \neq 0 \qquad f\left(-\frac{d}{c}\right) = \infty,$$

$$f(\infty) = \begin{cases} a/c & \text{if } c \neq 0 \\ \infty & \text{if } c = 0 \end{cases}.$$

Remark This definition defines an action $M \curvearrowright \hat{\mathbb{C}}$.

Proposition 6.1 This action $M \curvearrowright \hat{\mathbb{C}}$ is faithful, and so $M \leq \mathrm{Sym}\,\hat{\mathbb{C}}$.

Proof Consider $\rho : M \to \mathrm{Sym}(\hat{\mathbb{C}})$ given by $\rho(f)(z) = f(z)$
Then if $\rho(f) =$ id. permutation of $\hat{\mathbb{C}}$ $(z \mapsto z)$ then f is the identity in M. So ρ is injective and the action is faithful. □

Definition 6.2 A fixed point of a Möbius map $f: \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ is a point $z \in \hat{\mathbb{C}}$ with $f(z) = z$.

Theorem 6.3 A Möbius map with at least 3 fixed points is the identity.

Proof Let $f(z) = \dfrac{az+b}{cz+d}$ have $\geqslant 3$ fixed points.

If ∞ is not a fixed point, then $\dfrac{az+b}{cz+d} = z$ for $\geqslant 3$ complex numbers i.e. $cz^2 + (d-a)z - b = 0$ which can't have 3 roots in $\mathbb{C}$ by FTA, unless $c = b = 0$, $d = a$ i.e. $z = z$, $f =$ identity.

If ∞ is a fixed point, then $\dfrac{a\infty+b}{c\infty+d} := \dfrac{a}{c} = \infty$
So $c = 0$. So $\dfrac{az+b}{d} = z$ for $\geqslant 2$ complex numbers, so $(a-d)z + b = 0$ for $\geqslant 2$ complex numbers. But it can't have > 1 (linear) so we have $a - d = b = 0$ so f is the identity with $a = d$, $b = c = 0$. □

PTO

Corollary 6.4 If two Möbius maps coincide on 3 distinct points in $\hat{\mathbb{C}}$, then they are equal.

Proof Let $f, g \in M$ be such that

$$f(z_1) = g(z_1)$$
$$f(z_2) = g(z_2)$$
$$f(z_3) = g(z_3)$$

for 3 distinct points $z_1, z_2, z_3 \in \hat{\mathbb{C}}$.

Then $g^{-1} f(z_i) = g^{-1}(g(z_i)) = z_i$

(true for $i = 1, 2, 3$)

So $g^{-1} f$ fixes ≥ 3 points, so it must be the identity.

So in M, $g^{-1} f = e \Rightarrow \underline{f = g}$ so the maps are equal. □

We can rephrase this corollary as

"Knowing what a Möbius map does on 3 distinct points in $\hat{\mathbb{C}}$ uniquely determines the map".

Theorem 6.5 There is a unique Möbius map sending any 3 distinct points of $\hat{\mathbb{C}}$ to any 3 distinct points of $\hat{\mathbb{C}}$.

i.e. given $z_1, z_2, z_3 \in \hat{\mathbb{C}}$ and $w_1, w_2, w_3 \in \hat{\mathbb{C}}$ (distinct): $\exists!$ (unique) f : $f(z_i) = w_i \quad i = 1,2,3$

Proof Suppose first that $w_1 = 0,\ w_2 = 1,\ w_3 = \infty$

Then $f(z) = \dfrac{(z_2 - z_3)(z - z_1)}{(z_2 - z_1)(z - z_3)}$ satisfies $f(z_i) = w_i \ \forall i$.

[Special cases: if $z_1 = \infty$, use $f(z) = \dfrac{z_2 - z_3}{z - z_3}$, if $z_2 = \infty$ use $f(z) = \dfrac{z - z_1}{z - z_3}$, if $z_3 = \infty$ use $f(z) = \dfrac{z - z_1}{z_2 - z_1}$]

Then can find f_1 sending (z_1, z_2, z_3) to $(0, 1, \infty)$

and f_2 sending (w_1, w_2, w_3) to $(0, 1, \infty)$

Then $f := f_2^{-1} f_1$ sends (z_1, z_2, z_3) to (w_1, w_2, w_3) as required.

Uniqueness follows immediately from Corollary 6.4. □

We saw on Sheet 2: conjugate hfh^{-1} of a Möbius map f satisfies

- $\operatorname{ord}(hfh^{-1}) = \operatorname{ord}(f)$
- f fixes $z \iff hfh^{-1}$ fixes $h(z)$

In particular, the number of fixed points of a conjugate is the same as the number of fixed points of the original map.

PTO

Theorem 6.6 Every non-identity element $f \in M$ has 1 or 2 fixed points. If f has 1 fixed point, then it is conjugate to $z \mapsto z+1$. If f has 2 fixed points, then it is conjugate to a map of the form $z \mapsto az$, $a \in \mathbb{C} \setminus \{0\}$.

Proof Theorem 6.3 $\Rightarrow$ non-identity element has < 3 fixed points.

If $f(z) = \dfrac{az+b}{cz+d}$, by considering the quadratic $cz^2 + (d-a)z - b = 0$ (from $f(z) = z$) must have at least one distinct root in $\mathbb{C}$, so $f(z)$ has ≥ 1 fixed point. So it has 1 or 2 fixed points.

If f has exactly 1 fixed point z_0, choose $z_1 \in \mathbb{C}$ not fixed by f. Then $(z_1, f(z_1), z_0)$ are all distinct. (Check)

So there is some $g \in M$ s.t. $(z_1, f(z_1), z_0) \mapsto (0, 1, \infty)$.

Consider gfg^{-1} : $0 \mapsto z_1 \mapsto f(z_1) \mapsto 1$

$\infty \mapsto z_0 \mapsto z_0 \mapsto \infty$ ∞ fixed

$gfg^{-1}(0) = 1$, $gfg^{-1}(\infty) = \infty$, so map gfg^{-1} must be equal to $z \mapsto az+1$ $(a \in \mathbb{C})$. Exercise: check a map with these properties has such a form.

If $a \neq 1$ then this fixes $\dfrac{1}{1-a} \neq \infty$. ※ as ∞ must be the only fixed point of gfg^{-1}, as assumed initially that f has only one fixed point so so must gfg^{-1}.

So have $a = 1$ so $z \mapsto z+1$.

If f has exactly 2 fixed points z_0 and z_1, then let g be any Möbius map sending $(z_0, z_1) \mapsto (0, \infty)$.
(can find this : Thm 6.5)

So gfg^{-1} : $0 \mapsto z_0 \mapsto z_0 \mapsto 0$

$\infty \mapsto z_1 \mapsto z_1 \mapsto \infty$

i.e. gfg^{-1} fixes 0 and ∞.

So gfg^{-1} has form $z \mapsto az$ (exercise: check this)

with $a = gfg^{-1}(1)$. □

Can use this to efficiently work out f^n given $f \in M$.

$gf^n g^{-1} = (gfg^{-1})^n$ which can be computed easily:

1 fixed point: $z \mapsto z+n$

2 fixed points: $z \mapsto a^n z$

So f^n will be conjugate to one of the above by g^{-1}.

Circles and Lines

The image under $f \in M$ of 3 points in $\hat{\mathbb{C}}$ uniquely determine f. 3 points also uniquely determine lines/circles in $\hat{\mathbb{C}}$.

Eqn of a circle, centre $b \in \mathbb{C}$, radius $r > 0$ in $\mathbb{C}$ is

$|z-b| = r$

$\iff |z-b|^2 = r^2 \iff (z-b)(z-b)^* - r^2 = 0$

$\iff zz^* - b^*z - bz^* + bb^* - r^2 = 0 \qquad (*)$

Eqn of a straight line in $\mathbb{C}$ $(a, b, c \in \mathbb{R})$

$a\,\mathrm{Re}(z) + b\,\mathrm{Im}(z) = c$

$\iff \overline{\frac{a+ib}{2}}\, z + \frac{a+ib}{2}\, \bar{z} - c = 0 \qquad (\dagger)$

For a straight line in $\hat{\mathbb{C}}$, ∞ is always on the line.

Both $(*)$ and $(\dagger)$ have the form in the next definition.

Definition 6.7 A circle in $\hat{\mathbb{C}}$ satisfies

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

(consider ∞ a solution iff $A = 0$).

Exercise Show that this is either a circle in $\mathbb{C}$ or a line $\cup \{\infty\}$.
(Note: line in $\mathbb{C}$ corresponds to circle on Riemann sphere)

Theorem 6.8 Möbius maps send circles in $\hat{\mathbb{C}}$ to circles in $\hat{\mathbb{C}}$.

Proof By Prop. 2.25 (generating set of M) it's enough to check this for $z \mapsto az$, $z \mapsto z+b$, $z \mapsto \frac{1}{z}$.

Writing $S(A, B, C)$ for $Az\bar{z} + \bar{B}z + B\bar{z} + C = 0$ $(**)$

can check that under $z \mapsto az$ $\quad S(A,B,C) \mapsto S\left(\frac{A}{\bar{a}a}, \frac{B}{\bar{a}}, C\right)$

under $z \mapsto z+b$ $\quad S(A, B, C) \to S(A, B-Ab, C + Ab\bar{b} - B\bar{b} - \bar{B}b)$

under $z \mapsto \frac{1}{z}$ solutions to $(**)$ become solutions to

$Cw\bar{w} + Bw + \bar{B}\bar{w} + A = 0$ so $S(A,B,C) \to S(C, \bar{B}, A)$. □

Remark Both circles and Möbius maps are "determined" by 3 points. So in practice, easy to find a Möbius map sending a given circle to another given circle.

e.g. $f \in M$ with unit circle $\to \mathbb{R} \cup \{\infty\}$

Pick 3 points on unit circle: $\{-1, i, 1\}$

Pick 3 points on $\mathbb{R} \cup \{\infty\}$: $\{-1, 0, 1\}$

need f with $-1, 1$ fixed and $i \mapsto 0$

e.g. by inspection $f(z) = \dfrac{z-i}{1-iz}$ works.

Cross-Ratios

Recall that given distinct points $z_1, z_2, z_3 \in \hat{\mathbb{C}}$, $\exists!$ $f \in M$ with $f(z_1) = 0$, $f(z_2) = 1$, $f(z_3) = \infty$

Definition 6.9

If $z_1, z_2, z_3, z_4 \in \hat{\mathbb{C}}$ are distinct, then their cross-ratio $[z_1, z_2, z_3, z_4]$ is defined to be $f(z_4)$ where $f \in M$ is the unique Möbius map with $f(z_1) = 0$, $f(z_2) = 1$, $f(z_3) = \infty$

so in particular $[0, 1, \infty, w] = w \quad \forall w \in \hat{\mathbb{C}} \setminus \{0, 1, \infty\}$ (as it's identity)

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

Special cases when $z_i = \infty$ for some i e.g. $[\infty, z_2, z_3, z_4]$

$$= \frac{(\cancel{z_4 - \infty})(z_2 - z_3)}{(\cancel{z_2 - \infty})(z_4 - z_3)} = \frac{z_2 - z_3}{z_4 - z_3}$$

(Follows from proof of Thm 6.5)

There are 4! different conventions for cross-ratio depending on order of $0, 1, \infty$

Proposition 6.10

Double transpositions of the z_i fix cross-ratio

e.g. $[z_1, z_2, z_3, z_4] = [z_2, z_1, z_4, z_3]$

$= [z_3, z_4, z_1, z_2] = [z_4, z_3, z_2, z_1]$

Proof Check by inspection of $(*)$. □

Theorem 6.11 Möbius maps preserve the cross-ratio

i.e. $[z_1, z_2, z_3, z_4] = [f(z_1), f(z_2), f(z_3), f(z_4)]$

Proof Let $f \in M$ be the unique Möbius map with

$f : (z_1, z_2, z_3) \mapsto (0, 1, \infty)$ so

$f(z_4) = [z_1, z_2, z_3, z_4]$

$f \circ g^{-1} : g(z_1) \mapsto 0 \qquad g(z_2) \mapsto 1$

$g(z_3) \mapsto \infty$

and $f \circ g^{-1}$ is the unique map with this property

So $[g(z_1), g(z_2), g(z_3), g(z_4)] = (f \circ g^{-1})(g(z_4))$

$= f(z_4)$

$= [z_1, z_2, z_3, z_4]$. □

Corollary 6.12 Four distinct points in $\hat{\mathbb{C}}$ lie on a circle iff the cross ratio $[z_1, z_2, z_3, z_4] \in \mathbb{R}$.

Proof Let f be the unique map $(z_1, z_2, z_3) \mapsto (0, 1, \infty)$ with $f(z_4) = [z_1, z_2, z_3, z_4]$

The circle through z_1, z_2, z_3 is sent to the circle through $(0, 1, \infty)$ i.e. $\mathbb{R} \cup \{\infty\}$

so z_4 lies on C iff $f(z_4)$ lies on $\mathbb{R} \cup \{\infty\}$

but $f(z_4) \neq \infty$ because $f(z_3) = \infty$, $z_3 \neq z_4$.

So true when $f(z_4)$ is real. □

Section 7 Matrix Groups

Some matrix groups: $M_{n\times n}(\mathbb{F})$ is the set of $n\times n$ matrices over the field $\mathbb{F}$ (usually $\mathbb{R}$ or $\mathbb{C}$)

Definition 7.1 $GL_n(\mathbb{F}) = \{A \in M_{n\times n}(\mathbb{F}) : A \text{ invertible}\}$ is the general linear group over $\mathbb{F}$.

Note $\det : GL_n(\mathbb{F}) \to \mathbb{F}^* = \mathbb{F}\setminus\{0\}$ is a surjective HM.

Definition 7.2 $SL_n(\mathbb{F})$ (special linear group) $SL_n(\mathbb{F}) \leq GL_n(\mathbb{F})$ is kernel of det HM.

Definition 7.3 The orthogonal group $O_n = O_n(\mathbb{R})$ is $\{A \in GL_n(\mathbb{R}) : A^TA = I\}$. Have $O_n \leq GL_n(\mathbb{R})$.

Proposition 7.4 $\det : O_n \to \{\pm 1\}$ is a surjective homomorphism.

Proof If $A \in O_n$ then $A^TA = I$ so

$\det(A)^2 = \det A^T \det A = \det(A^TA) = \det I = 1$

so $\det(A) = \pm 1$.

surjective: $\det I = 1$, $\det \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = -1$ (a HM as above). □

Definition 7.5 The special orthogonal group $SO_n(\mathbb{R})$ is the kernel of det HM: $SO_n = \{A \in O_n : \det A = 1\}$.

Möbius maps via matrices

Proposition 7.6 Function $\phi : SL_2(\mathbb{C}) \to M$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto f$ with $f(z) = \frac{az+b}{cz+d}$

is a surjective HM with kernel $\{I, -I\}$.

Proof ϕ a HM: $f_1(z) = \frac{a_1z+b_1}{c_1z+d_1}$, $f_2(z) = \frac{a_2z+b_2}{c_2z+d_2}$

have $f_2(f_1(z)) = \frac{az+b}{cz+d}$. $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$ as required.

ϕ surjective: if $\frac{az+b}{cz+d}$ is a Möbius map then $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{C})$ as $ad - bc \neq 0$.

But $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ may not be 1, so take $D^2 = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and consider $\begin{pmatrix} a/D & b/D \\ c/D & d/D \end{pmatrix}$ with $\det = 1$ and $\frac{\frac{a}{D}z + \frac{b}{D}}{\frac{c}{D}z + \frac{d}{D}} = \frac{az+b}{cz+d}$

so $\exists$ matrix in $SL_2(\mathbb{C})$ with image $\frac{az+b}{cz+d}$ of ϕ.

If $\phi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = id \in M$ then $\frac{az+b}{cz+d} = z \quad \forall z \in \hat{\mathbb{C}}$.

$\Leftrightarrow c = b = 0$, $a = d$ so $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$

Since it's in $SL_2(\mathbb{C})$, have $a^2 = 1 \Rightarrow a = \pm 1$ so kernel is $\{I, -I\}$.

Corollary 7.7 $M \cong SL_2(\mathbb{C}) / \{I, -I\}$ by 1st isomorphism theorem. □

This is called the projective special linear group.

Actions of Matrix Groups

All above groups act on corresponding vector spaces.

Example 7.8 Let $G \leq GL_2(\mathbb{R})$ act on $\mathbb{R}^2$. What are the orbits?

$\{0\}$ is a singleton orbit

If $G = GL_2(\mathbb{R})$ then it acts transitively on $\mathbb{R}^2 \setminus \{0\}$ as can complete any $\underline{v} \neq \underline{0}$ to a basis and have an invertible change of basis matrix sending any basis to any basis. So orbits $\{0\}$, $\mathbb{R}^2 \setminus \{0\}$.

Now if $G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in GL_2(\mathbb{R}) \right\}$

$$= \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, d \neq 0 \right\}$$

have $\text{orb} \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\}$

$$\text{orb} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} : \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in G \right\}$$

$$= \left\{ \begin{pmatrix} a \\ 0 \end{pmatrix} : a \neq 0 \right\} \quad (x \text{ axis without } 0)$$

$$\text{orb} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} : \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in G \right\} = \left\{ \begin{pmatrix} b \\ d \end{pmatrix} : d \neq 0 \right\}$$

which is all vectors in $\mathbb{R}^2$ excluding "x-axis"

which covers the <u>whole of $\mathbb{R}^2$</u> (3 orbits, not same size).

(see sheet 4 for more examples).

We will now interpret the conjugation action of $GL_n(\mathbb{F})$ on $n \times n$ matrices. Use changes of basis.

Change of Basis

Recall from V&M: if $\alpha : \mathbb{F}^n \to \mathbb{F}^n$ is a linear map, then we can represent α as a matrix A wrt a basis $\{\underline{e}_1, \underline{e}_2, \dots, \underline{e}_n\}$. If we choose a different basis $\{\underline{f}_1, \dots, \underline{f}_n\}$ then α can also be represented wrt this basis by the matrix $\underline{P^{-1}AP}$ where P is the change of basis matrix defined by

$$\underline{f}_j = \sum_{i=1}^{n} P_{ij} \underline{e}_i .$$

This is an example of conjugation.

Proposition 7.9 $GL_n(\mathbb{F})$ acts on $M_{n\times n}(\mathbb{F})$ by conjugation. The orbit of a matrix $A \in M_{n\times n}(\mathbb{F})$ is the set of matrices representing the same linear map as A wrt different bases.

Proof

- $P(A) = PAP^{-1} \in M_{n\times n}(\mathbb{F})$. $\forall A \in M_{n\times n}(\mathbb{F}),\ \forall P \in GL_n(\mathbb{F})$
- $I(A) = IAI^{-1} = A \quad \forall A$
- $(QP)(A) = QPAP^{-1}Q^{-1} = Q(P(A))$ so is an action.

By discussion above, A, B in same orbit iff $A = PBP^{-1}$ for some $P \in GL_n(\mathbb{F})$

$\Leftrightarrow$ $B = P^{-1}AP$ $\Leftrightarrow$ B represents the same linear map but wrt a different basis. $\square$

Example 7.10 In V&M, we've seen that any matrix in $M_{n\times n}(\mathbb{C})$ is conjugate to a matrix in Jordan normal form (JNF) i.e. conjugate to one of the following types of matrix for 2×2:

PTO

$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ $(\lambda_1 \neq \lambda_2)$ $\quad \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ or $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$

In case $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$, values λ_1, λ_2 uniquely determined by the matrix (the eigenvalues) but the order of eigenvalues is not unique

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \lambda_2 & 0 \\ 0 & \lambda_1 \end{pmatrix}$$

Other than this, no two matrices on this JNF list are conjugate.

$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ only conjugate to itself (as it's λI)

$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ characterised by having a repeated eigenvalue λ but only a 1-dim. eigenspace (independent of basis).

and $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ is characterised by having 2 distinct eigenvalues.

This gives a complete description of the orbits of $GL_n(\mathbb{C}) \curvearrowright M_{n\times n}(\mathbb{C})$.

What are the stabilisers?

$P \in \text{stab}(A) \iff PAP^{-1} = A \iff PA = AP$

For $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} = \begin{pmatrix} \lambda_1 a & \lambda_2 b \\ \lambda_1 c & \lambda_2 d \end{pmatrix}$$

$$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \lambda_1 a & \lambda_1 b \\ \lambda_2 c & \lambda_2 d \end{pmatrix}$$

so $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{stab}\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \iff \lambda_1 c = \lambda_2 c,\ \lambda_1 b = \lambda_2 b$

but $\lambda_1 \neq \lambda_2$

so need $\underline{b = c = 0}$.

So $\text{stab}\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in GL_2(\mathbb{C}) \right\}$.

For $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ have $\operatorname{stab}\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} = GL_2(\mathbb{C})$

For $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$: $\operatorname{stab}\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in GL_2(\mathbb{C}) \right\}$

(exercise : check)

Geometry of orthogonal groups

Consider standard inner product in $\mathbb{R}^n$: $\underline{x} \cdot \underline{y} = \sum_{i=1}^{n} x_i y_i$

$= \underline{x}^T \underline{y}$

Consider $\underline{P}_1, \ldots, \underline{P}_n$ of $P \in O_n$, have $(P^T P)_{ij}$ is

$\underline{P}_i^T \underline{P}_j = \underline{P}_i \cdot \underline{P}_j$

Since $P \in O_n \iff P^T P = I$, we have that $P \in O_n$ iff

$\underline{P}_i \cdot \underline{P}_j = \delta_{ij}$.

We have obtained :

Proposition 7.11 $P \in O_n \iff$ columns of P form an orthonormal basis.

Proof shown above. □

Thinking of $P \in O_n$ as a change of basis matrix :

Proposition 7.12 Consider $O_n \curvearrowright M_{n\times n}(\mathbb{R})$ by conjugation. Two matrices lie in the same orbit iff they represent the same linear map wrt 2 orthonormal bases.

Proof again seen above □

Proposition 7.13 $P \in O_n \iff P\underline{x} \cdot P\underline{y} = \underline{x} \cdot \underline{y} \quad \forall x, y \in \mathbb{R}^n$.

Proof $\Rightarrow (P\underline{x}) \cdot (P\underline{y}) = (P\underline{x})^T P\underline{y} = \underline{x}^T P^T P \underline{y} = \underline{x}^T \underline{y}$

$\Leftarrow$ If $P\underline{x} \cdot P\underline{y} = \underline{x} \cdot \underline{y} \quad \forall \underline{x}, \underline{y} \in \mathbb{R}^n$:

PTO

Taking basis vectors $\underline{e}_i, \underline{e}_j$ we have

$$P\underline{e}_i \cdot P\underline{e}_j = \underline{e}_i \cdot \underline{e}_j = \delta_{ij}$$

So vectors $P\underline{e}_1, \ldots, P\underline{e}_n$ are orthonormal. These are the columns of P, so $P \in O_n$ by 7.11. □

Corollary 7.13 For $P \in O_n$, $\underline{x}, \underline{y} \in \mathbb{R}^n$, have (i) $|P\underline{x}| = |\underline{x}|$ & (ii) $P\underline{x} \angle P\underline{y} = \underline{x} \angle \underline{y}$ (angle preserved)

Proof (i) Follows: $|\underline{x}|^2 = \underline{x} \cdot \underline{x} = P\underline{x} \cdot P\underline{x} = |P\underline{x}|^2$ (lengths > 0)

(ii) Angles defined from inner product. □

Note $\cos : [0, \pi] \to [-1, 1]$ injective.

Definition 7.14 If $\underline{a} \in \mathbb{R}^n$ with $|\underline{a}| = 1$, then the reflection in the plane normal to $\underline{a}$ is the linear map

$$R_{\underline{a}} : \mathbb{R}^n \to \mathbb{R}^n \qquad \underline{x} \mapsto \underline{x} - 2(\underline{x} \cdot \underline{a})\,\underline{a}$$

Lemma 7.15 $R_{\underline{a}}$ lies in O_n.

Proof Let $\underline{x}, \underline{y} \in \mathbb{R}^n$ $\quad R_{\underline{a}}(\underline{x}) \cdot R_{\underline{a}}(\underline{y}) = (\underline{x} - 2(\underline{x} \cdot \underline{a})\,\underline{a}) \cdot (\underline{y} - 2(\underline{y} \cdot \underline{a})\,\underline{a})$

$$= \underline{x} \cdot \underline{y} - 2(\underline{x} \cdot \underline{a})(\underline{a} \cdot \underline{y}) - 2(\underline{y} \cdot \underline{a})(\underline{x} \cdot \underline{a}) + 4(\underline{x} \cdot \underline{a})(\underline{y} \cdot \underline{a})(\underline{a} \cdot \underline{a})$$

$= \underline{x} \cdot \underline{y}$ since $\underline{a} \cdot \underline{a} = 1$

So $R_a \in O_n$ by Prop. 7.13. □

Conjugates of reflections are also reflections.

Lemma 7.16 Given $P \in O_n$, $PR_{\underline{a}}P^{-1} = R_{P\underline{a}}$.

Proof We have $PR_{\underline{a}}P^{-1}(\underline{x}) = P(P^{-1}(\underline{x})) - 2(P^{-1}(\underline{x}) \cdot \underline{a})\,\underline{a})$

$= \underline{x} - 2(P^{-1}(\underline{x}) \cdot \underline{a})(P\underline{a})$ but $P \in O_n$ so $P^{-1} = P^T$

so $P^{-1}(\underline{x})\,\underline{a} = P^T\underline{x} \cdot \underline{a} = \underline{x}^T P\underline{a} = \underline{x} \cdot P\underline{a}$

so $PR_{\underline{a}}P^{-1}(\underline{x}) = \underline{x} - 2(\underline{x} \cdot P\underline{a})(P\underline{a})$ a reflection wrt $P(a)$. □

Can a reflection lie in $SO_n \leq O_n$?
($\uparrow$ det = 1)

We know that the determinant is the product of the eigenvalues.

What are e.vals of $R_{\underline{a}}$? $\underline{x} \mapsto \underline{x} - 2(\underline{x}\cdot\underline{a})\,\underline{a}$

Can spot e.vecs: $R_{\underline{a}}(\underline{a}) = \underline{a} - 2(\underline{a}\cdot\underline{a})\,\underline{a} = -\underline{a}$

(e.vec with e.val -1)

and for $\underline{x} \in$ (plane normal to $\underline{a}$) have $R_{\underline{a}}(\underline{x}) = \underline{x} - 2(\underline{x}\cdot\underline{a})\,\underline{a}$ ($\underline{x}\cdot\underline{a} \uparrow 0$)

$= \underline{x}$

so $\underline{x}$ is an e.vec with e.val 1.

Eigenvalue 1 has multiplicity $n-1$ so these are all the eigenvectors.

So determinant of $R_{\underline{a}}$ is -1 so $R_{\underline{a}} \notin SO_n$.

So $R_{\underline{a}} \in O_n \setminus SO_n$. (Prop. 7.17).

What about SO_n?

Theorem 7.18 Every element of SO_2 has the form $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ for some $\theta \in [0, 2\pi]$. (A/C rotation about origin).

Conversely, every such element lies in SO_2.

Proof Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SO_2$. Have $A^TA = I$ (orthogonal)

and $\det A = 1$ so $A^T = A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ (as $\det = 1$)

so as $A^T = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, have $a = d$, $b = -c$

with $ad - bc = 1$

$\Rightarrow a^2 + c^2 = 1$ so $a = \cos\theta$, $c = \sin\theta$ for some θ.

Conversely $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ has det. 1 and is orthogonal (check) so lies in SO_2. $\square$

Theorem 7.19 The elements of $O_2 \setminus SO_2$ are the reflections in lines through the origin.

Proof Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in O_2 \setminus SO_2$, so $A^T A = I$ and $\det A = -1$.

Again: $A^T = \begin{pmatrix} a & c \\ b & d \end{pmatrix} = -\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = A^{-1}$

so $a = -d$, $b = c$ and as $ad - bc = -1$, have $a^2 + c^2 = 1$ so $a = \cos\theta$, $c = \sin\theta$ for some θ.

So $A = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$: check it's a reflection by double angle formulas.

$$A \begin{pmatrix} \sin\frac{\theta}{2} \\ -\cos\frac{\theta}{2} \end{pmatrix} = -\begin{pmatrix} \sin\theta/2 \\ -\cos\theta/2 \end{pmatrix}, \quad A \begin{pmatrix} \cos\theta/2 \\ \sin\theta/2 \end{pmatrix} = \begin{pmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2} \end{pmatrix}$$

so A is the reflection in the plane orthogonal to unit vector $\begin{pmatrix} \sin\frac{\theta}{2} \\ -\cos\frac{\theta}{2} \end{pmatrix}$.

Conversely a ~~vector~~ reflection in a line through the origin also has this form. □

Corollary 7.20 Every element of O_2 is the composition of at most two reflections.

Proof Every element of $O_2 \setminus SO_2$ is itself a reflection ✓.

If $A \in SO_2$, then $A = A \underbrace{\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}}_{I}$ ↙ $\det = -1$

so $A \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ are in O_2 but not SO_2 so are reflections. □

Theorem 7.21 If $A \in SO_3$, then $\exists\ \underline{v} \in \mathbb{R}^3$ with $|\underline{v}| = 1$ and $A\underline{v} = \underline{v}$.

Proof It's enough to show that 1 is an eigenvalue of A (as we can normalise the eigenvector).

So need $\det(A - I) = 0$

so $\det(A-I) = \det(A - AA^T) = \det A \det(I - A^T)$ ($\det A = 1$)

$= \det(I - A^T) = \det((I-A)^T) = \det(I-A)$

$= -\det(A-I)$ so $\underline{\det(A-I) = 0}$. □

Corollary 7.22 Every element A in SO_3 is conjugate in SO_3 to a matrix of the form $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$.

Proof By Theorem 7.21, $\exists\ \underline{v}_1 \in \mathbb{R}^3$ with $|\underline{v}_1| = 1$, $A\underline{v}_1 = \underline{v}_1$

We can extend $\underline{v}_1$ to an orthonormal basis $\{\underline{v}_1, \underline{v}_2, \underline{v}_3\}$ (see V&M earlier) of $\mathbb{R}^3$. Then for $i = 2, 3$ we have

~~$A\underline{v}_1 \cdot \underline{v}_1$~~ $A\underline{v}_i \cdot \underline{v}_1 = A\underline{v}_i \cdot A\underline{v}_1 = \underline{v}_i \cdot \underline{v}_1 = 0$

(A preserves inner product)

So $A\underline{v}_2$, $A\underline{v}_3$ lie in span $\{\underline{v}_2, \underline{v}_3\}$

so A maps span $\{\underline{v}_2, \underline{v}_3\}$ to itself and we can hence consider restriction of A to this subspace

This still has determinant 1 (as A will have matrix $\begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix}$ wrt basis $\{\underline{v}_1, \underline{v}_2, \underline{v}_3\}$.)

So A restricted to $\langle \underline{v}_2, \underline{v}_3 \rangle$ = span $\{\underline{v}_2, \underline{v}_3\}$ is in SO_2

so has form $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$. So A has required form wrt $\{\underline{v}_1, \underline{v}_2, \underline{v}_3\}$.

The change of basis matrix P lies in O_3 since $\{\underline{v}_1, \underline{v}_2, \underline{v}_3\}$ is an orthonormal basis.

If $P \notin SO_3$, then can use the basis $\{-\underline{v}_1, \underline{v}_2, \underline{v}_3\}$ instead. □

Geometrically: every element in SO_3 is a rotation about some axis. ($\underline{v}_1$ above).

Corollary 7.23 Every element of O_3 is the composition of at most 3 reflections.

Proof If $A \in SO_3$ then $\exists P \in SO_3$ with $PAP^{-1} = B$,

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

since $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ is a composition of at most 2 reflections by Cor. 7.20,

so is B: $B = B_1 B_2$. Then A is too, since the conjugate of a reflection is a reflection and

$$A = P^{-1}BP = P^{-1}B_1B_2P = P^{-1}B_1PP^{-1}B_2P$$
$$= (P^{-1}B_1P)(P^{-1}B_2P)$$

If $A \in O_3 \setminus SO_3$, then $\det A = -1$ and

$$A = A \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$\det = 1$, lies in SO_3, comp. of at most 2 reflections

$\det = -1$, a reflection in y,z plane

So A is product of at most 3 reflections.

Symmetries of cube - revisited

We can think of symmetry groups of platonic solids as subgroups of O_3.

By Q11 on sheet 4: $O_3 \cong SO_3 \times C_2$ where C_2 is generated by the map $\underline{v} \mapsto -\underline{v}$.

So if $\underline{v} \mapsto -\underline{v}$ is a symmetry of the platonic solid, then its group of symmetries will also split as the direct product

$G^+ \times C_2$ (G^+ : rotations)

So we have that symmetry group of cube is $G^+ \times C_2 \cong S_4 \times C_2$ by chapter 5 results.

Section 8 - Groups of order 8

We've already seen all possibilities for groups of order ≤ 7.

Order 8:

Definition 8.1 Consider the subset of matrices of $GL_2(\mathbb{C})$ given by

$$\underline{1} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \underline{i} := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \underline{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \underline{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

The set $\{ \pm \underline{1}, \pm \underline{i}, \pm \underline{j}, \pm \underline{k} \}$ forms a group wrt matrix multiplication called quaternions, Q_8.

Exercise: check it's a group.

Can verify elements satisfy:

$g^4 = \underline{1} \quad \forall g \in Q_8$

$(-\underline{1})^2 = \underline{1}$

$\underline{i}^2 = \underline{j}^2 = \underline{k}^2 = -\underline{1}$

$\underline{i} \cdot \underline{j} = \underline{k}, \quad \underline{j} \cdot \underline{k} = \underline{i}, \quad \underline{k} \cdot \underline{i} = \underline{j}$

$\underline{j} \cdot \underline{i} = -\underline{k} \qquad \underline{k} \cdot \underline{j} = -\underline{i} \qquad \underline{i} \cdot \underline{k} = -\underline{j}$.

(not abelian).

Lemma 8.2 If a finite group has all non-identity elements of order 2, then it is isomorphic to $C_2 \times C_2 \times \dots \times C_2$.

Proof By Q7 on sheet 1, such a group G is abelian and order of $G = 2^n$ for some n.

If $|G| = 2$, have $G \cong C_2$

If $|G| > 2$, then choose a_1 of order 2.

$\exists\, a_2 \notin \langle a_1 \rangle$ and by DPT, have $\langle a_1, a_2 \rangle \cong \langle a_1 \rangle \times \langle a_2 \rangle$
$\cong C_2 \times C_2$.

If $|G| = 2^2$, done: if not, take $a_3 \notin \langle a_1, a_2 \rangle$

then $\langle a_1, a_2, a_3 \rangle \cong (\langle a_1 \rangle \times \langle a_2 \rangle) \times \langle a_3 \rangle$
$\cong C_2 \times C_2 \times C_2$

Can continue in this way to get $G \cong C_2 \times C_2 \times \dots \times C_2$. □

Theorem 8.3 All groups of order 8 are isomorphic to one of C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_8 or Q_8.

Proof Check above groups are not isomorphic.

Let $|G| = 8$. If $g \in G$ then $\operatorname{ord} g \mid 8$ so $\operatorname{ord} g = 1, 2, 4$ or 8.

- If there's an element of order 8 then $G = \langle g \rangle \cong C_8$.
- If all non-id. elements have order 2 then $G \cong C_2 \times C_2 \times C_2$.
- Remaining cases: have order 4 elements. Then $\langle h \rangle \cong C_4$

$|G : \langle h \rangle| = 2$ so $\langle h \rangle \trianglelefteq G$.

Then $g^2 \in \langle h \rangle$ by Q4 sheet 3.

So $g^2 = e, h, h^2$ or h^3.

If $g^2 = h$ or h^3 then $g^4 = h^2 \neq e$ so g has order 8 ✱

So $g^2 = e$ or $g^2 = h^2$.

If $g^2 = e$ consider $ghg^{-1} \in \langle h \rangle$ and has order 4.

So $ghg^{-1} = h$ or h^3.

If $ghg^{-1} = h$ then g, h commute. Also have $\langle h \rangle \cap \langle g \rangle = \{e\}$ and $G = \langle h \rangle \cdot \langle g \rangle$ so by DPT, $G \cong \langle h \rangle \times \langle g \rangle$

so $G \cong \underline{C_4 \times C_2}$.

If $ghg^{-1} = h^3 = h^{-1}$ then since $g^2 = e$, have $\underline{G \cong D_8}$.

If $g^2 = h^2$, then have $ghg^{-1} = h$ or h^3 as before

If $ghg^{-1} = h$ then $(gh)^2 = g^2h^2 = h^4 = e$ so $\text{ord}(gh) = 2$.

Apply DPT again to $\langle h \rangle$, $\langle gh \rangle$: $G \cong \langle h \rangle \times \langle gh \rangle \cong \underline{C_4 \times C_2}$.

If $ghg^{-1} = h^3$ then we define $\phi : G \to Q_8$ with

$e \mapsto 1$, $h \mapsto i$, $h^2 \mapsto -1$, $h^3 \mapsto -i$, $g \mapsto j$, $gh \mapsto -k$,

$gh^2 \mapsto -j$, $gh^3 \mapsto k$

Bijective and can check it's a homomorphism

So $\underline{G \cong Q_8}$. □

<u>Remark</u> We know that in an abelian group, every subgroup is normal. The converse is <u>not</u> true:

every subgroup is normal $\not\Rightarrow$ abelian.

Q_8 is an example: 3 subgroups of order 4 (index 2 so normal) and subgroup $\{1, -1\}$ are normal but Q_8 is not abelian.

The end of the course

Geometric Group Theory

A branch of group theory that exploits connections between properties of groups and ~~geo~~ geometric properties of spaces on which they act.

Groups can even be turned into geometric objects themselves.

Free Groups

Let S be a set called an alphabet and let S^{-1} be the set of "formal inverses" of elements of S.

A word in alphabet S is a finite sequence of elements of $S \cup S^{-1}$ e.g. $s_1 s_2 s_3 \dots s_n$

(we also consider the empty word to be a word).

A word is reduced if it does not contain occurences of subwords of the form ss^{-1} or $s^{-1}s$. Any word can be reduced.

e.g. $S = \{a, b, c\}$: $aa^{-1}bcb^{-1}bc^{-1}b \to bcc^{-1}b \to b^2$

Definition 9.1 The free group on the alphabet S, denoted $F(S)$ is the set of reduced words in the alphabet S with the operation of concatenation.

- Free groups are characterised by the universal property: for any group G, homomorphisms from a free group to G are in bijective correspondence with functions $S \to G$.
- If $G = \langle X \rangle$ then there's a surjective homomorphism $F(X) \twoheadrightarrow G$ (see Q16, sheet 1)

  In particular, every group is the quotient of a free group.

  If $|S| = |T|$ then $F(S) \cong F(T)$. We write F_n for $F(S)$ when $|S| = n$.

Group Presentations

Definition 9.2 Let X be a subset of a group G. The **normal closure** $\langle\langle X \rangle\rangle$ of X in G is the smallest normal subgroup of G containing X.

(note: if $X \subset N$, $N \trianglelefteq G$ then $\langle\langle X \rangle\rangle \leq N$).

$\langle\langle X \rangle\rangle$ is generated by $\{ gxg^{-1} : g \in G, x \in X \}$

"products of conjugates of elements in X"

Given a free group $F(S)$ and $R \subseteq F(S)$, we write $\langle S | R \rangle$ for the group $F(S) / \langle\langle R \rangle\rangle$.

Definition 9.3 A presentation of a group G is an isomorphism of G with a group written in the form $\langle S | R \rangle$.

$\langle S | R \rangle$

generators ↑ ↑ relation(s)

G is **finitely presented** if it admits a finite presentation i.e.

$\langle s_1, \ldots, s_n \mid r_1, \ldots, r_m \rangle$

n, m finite

Informally, in free group we can cancel ss^{-1}, $s^{-1}s$ and get the same element. In $\langle S | R \rangle$ we can also cancel any words in R.

Examples 9.4 24:00 in lecture

0) If $R = \emptyset$ then $\langle S | R \rangle \cong F(S)$

If $R = S$ then $\langle S | R \rangle \cong \{e\}$

1) $C_n \cong \langle a \mid a^n \rangle \cong F(a) / \langle\langle a^n \rangle\rangle$ elements $e, a, aa \ldots a, a^{-1}a^{-1} \ldots a^{-1}$

$\cong \mathbb{Z}/n\mathbb{Z}$ (note any subgroup is normal).

2) $D_{2n} \cong \langle r, s \mid r^n, s^2, srs^{-1} r \rangle$

3) $\langle a, b \mid aba^{-1}b^{-2}, a^{-2}b^{-1}ab \rangle \cong \{e\}$

A group can have many presentations e.g.

C_n as $\langle a \mid a^n \rangle$ or $\langle a, b \mid a^n, b \rangle$ so not unique

In general it's difficult to recognise which group a given presentation represents. (Even the trivial group!)

Indeed, there does not exist an algorithm such that upon input of a presentation, it can tell you whether or not it's the trivial group. "word problem"

There are uncountably many isomorphism classes of finitely generated groups, but only countably many isomorphism classes of finitely presented groups.

Cayley Graphs (A way to visualise groups)

Focus on finitely generated groups.

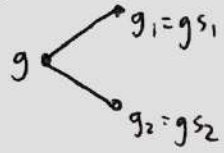
Definition 9.5 Let G be a finitely generated group, and $S \subseteq G$. The Cayley graph of G wrt S, denoted $Cay(G, S)$ is given by

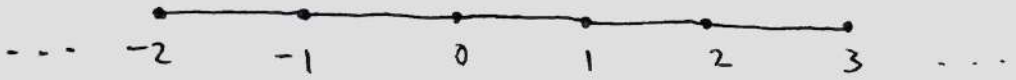
vertices of $Cay(G, S) = G$

edges of $Cay(G, S) = \{(g, gs) : g \in G, s \in S\}$

Example $\mathbb{Z}$, $S = \langle 1 \rangle$

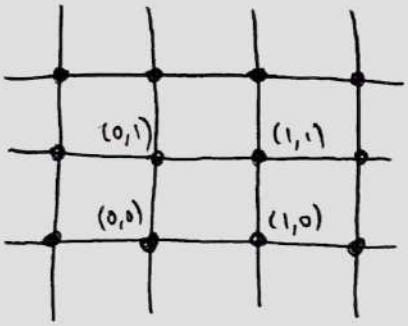
(generated by $\{1\}$)





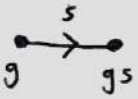
PTO

$\mathbb{Z}^2$ $\quad S = \{(1,0), (0,1)\}$

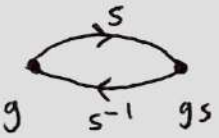


or could take $S = \{(1,0)\}$

(not connected)

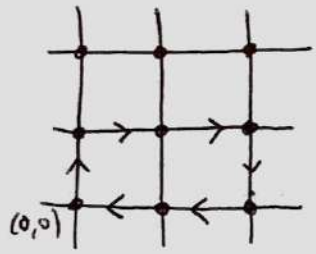
Remarks Could use directed edges / labelled edges e.g. 

- $Cay(G,S)$ is a $2|S|$-regular graph (no. of edges from each vertex is $2|S|$)

Note: usually don't write double edges 

- $Cay(G,S)$ is connected exactly when $\langle S \rangle = G$.
- Relators in elements of S give rise to cycles in the graph

recall $\mathbb{Z}^2 = \langle (0,1), (1,0) \rangle$



shows $(0,1) + (1,0) + (1,0) - (0,1) - (1,0) - (1,0)$
$= (0,0)$.

- If $\langle S \rangle = G$, then paths from e to a vertex correspond to words in S which represent the corresponding element in G.
- $Cay(G,S)$ allows us to put a distance function on G:

"word metric" $d_S(g,h) :=$ length of the shortest path from g to h in $Cay(G,S)$.

- G acts on $Cay(G,S)$ by isometries "distance preserving transformation" i.e. $d(x,y) = d(g(x), g(y))$ via left multiplication.

$h(g) = hg$, $d_S(h(g_1), h(g_2)) = d_S(g_1, g_2)$

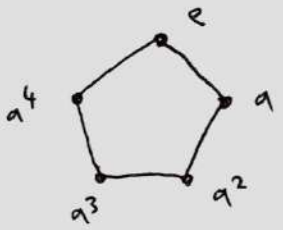
G acts by graph isomorphisms.

- Cayley graphs do <u>not</u> uniquely determine the group!

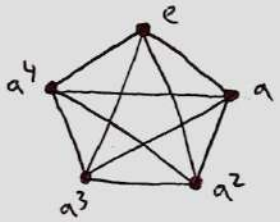
<u>Examples 9.6</u>

0) $G = \{e\}$ $\quad e \quad$ or $\quad e$ (not usually drawn this way)

1) $C_5 = \langle a \rangle$

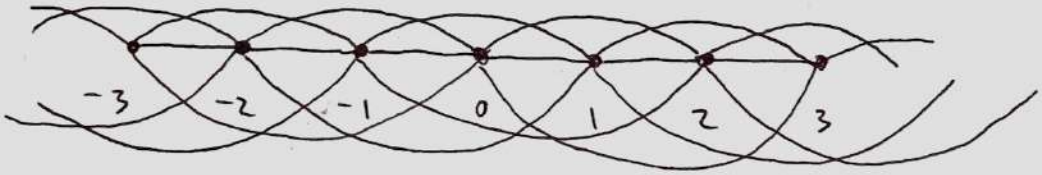


$C_5 = \langle a, a^2 \rangle$

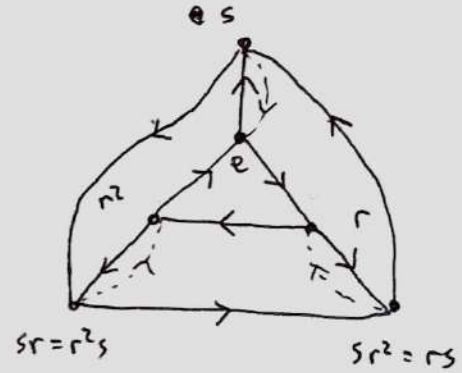


Cayley graph for a group not unique – depends on the generating set.

2) $\mathbb{Z} = \langle 2, 3 \rangle$



3) $D_6 = \langle r, s \rangle$

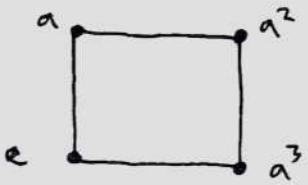


Can read off relations

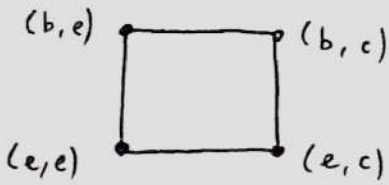
e.g. $r^3 = e$

$rsrs = e$

4) $C_4 = \langle a \rangle$

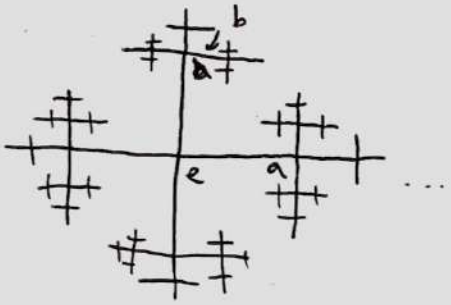


$C_2 \times C_2 = \langle (b,e), (e,c) \rangle$



give same graph - Cayley graph not unique.

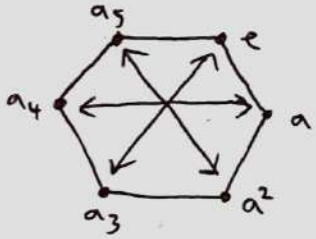
5) $F_2 = F(a,b)$



no relations

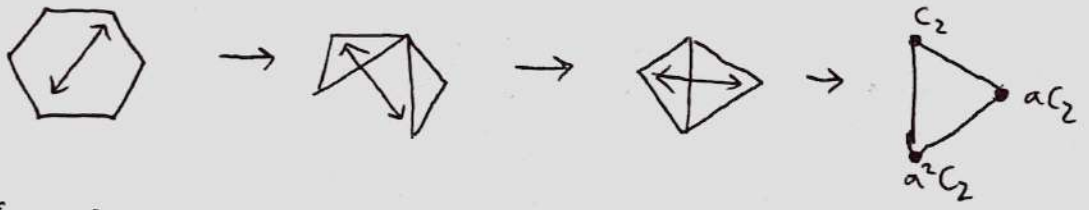
Can use Cayley graphs to visualise quotients e.g. $C_6 / C_2 \cong \underline{C_3}$

$C_6 = \langle a \rangle$, $C_2 = \langle a^3 \rangle$



"identify the vertices that differ by an element of C_2"

e.g. g, h, g_1 when taking quotient of G by H



Cayley graph of C_3

For infinite groups, there are lots of nice connections between geometric properties of $Cay(G,S)$ and algebraic properties of groups.

e.g. growth (number of elements at a certain distance from e)

ends - removing parts of graph - what happens going to infinity