

# Part IA — Groups

Based on lectures by R. Camina

Notes taken by Author

Michaelmas 2021

## Syllabus

### Examples of groups

Axioms for groups. Examples from geometry: symmetry groups of regular polygons, cube, tetrahedron. Permutations on a set; the symmetric group. Subgroups and homomorphisms. Symmetry groups as subgroups of general permutation groups. The Möbius group; cross-ratios, preservation of circles, the point at infinity. Conjugation. Fixed points of Möbius maps and iteration. [4]

### Lagrange's theorem

Cosets. Lagrange's theorem. Groups of small order (up to order 8). Quaternions. Fermat-Euler theorem from the group-theoretic point of view. [5]

### Group actions

Group actions; orbits and stabilizers. Orbit-stabilizer theorem. Cayley's theorem (every group is isomorphic to a subgroup of a permutation group). Conjugacy classes. Cauchy's theorem. [4]

### Quotient groups

Normal subgroups, quotient groups and the isomorphism theorem. [4]

### Matrix groups

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

### Permutations

Permutations, cycles and transpositions. The sign of a permutation. Conjugacy in  $S_n$  and in  $A_n$ . Simple groups; simplicity of  $A_5$ . [4]

# Contents

## Introduction

Dr Rachel Camina

Recommended books: Algebra & Geometry, Alan Beardon.

**Notation.**  $\nleftrightarrow$ - contradiction

## §1 Groups and homomorphisms

### §1.1 Motivation

Groups are the abstractions of symmetries, a unified way to investigate symmetries.

### §1.2 Basic Definitions and Examples

#### Definition 1.1 (Binary operation)

A binary operation  $*$  on a set  $X$  is a way of combining two elements of  $X$  to unambiguously give another element of  $X$ , i.e.  $*$  :  $X \times X \rightarrow X$ .

#### Definition 1.2 (Group)

If  $G$  is a set and  $*$  is a binary operation on  $G$  then  $(G, *)$  is a *group* if the following four axioms hold:

1.  $x, y \in G \implies x * y \in G$  (closure)
2.  $\exists$  an element  $e \in G$  satisfying  $x * e = x = e * x$  (existence of an identity)
3. for every  $x \in G$  there is a  $y \in G$  s.t.  $x * y = e = y * x$  (existence of inverses)
4. for every  $x, y, z \in G$ ,  $x * (y * z) = (x * y) * z$  (the associative law)

*Remark 1.*  $e$  is called the identity of  $G$  - see ?? for why it is unique. We will show in ?? that inverses are unique and we will write  $x^{-1}$  for the inverse of  $x$ .

#### Example 1.1

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

#### Example 1.2

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

#### Example 1.3

$(\mathbb{Q} \setminus \{0\}, *)$

**Non Example 1.1**  $(\mathbb{Z}, -)$  - associativity fails

**Non Example 1.2**  $(\mathbb{Z}, *)$  - no inverses

**Non Example 1.3**  $(\mathbb{Q}, *)$  -  $0^{-1}$  does not exist

These have all had an infinite number of elements, so onto some finite groups.

**Example 1.4** (The trivial group)

$$(e, *)$$

**Example 1.5**

$(\{\pm 1\}, \times)$ . A nice way to look at a group is to look at a multiplication table.

$\times$	1	-1
1	1	-1
-1	-1	1

We can see  $e = 1$  and  $(-1)^{-1} = -1$

**Example 1.6**

$(\{0, 1, 2\}, +_3)$ .  $+_3$  is addition modulo 3.

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

We can see  $e = 0$  and  $1^{-1} = 2$

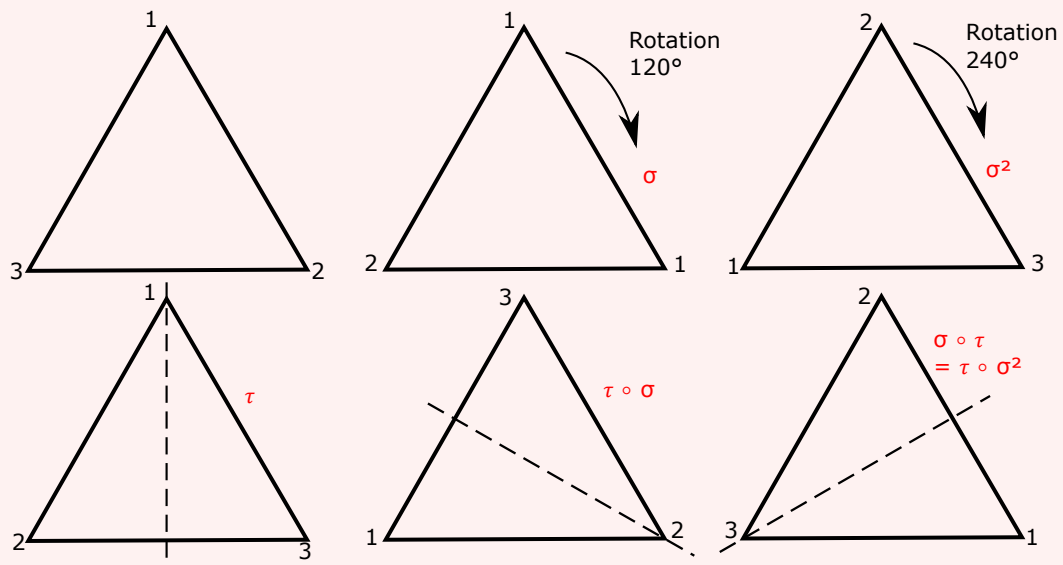
**Example 1.7**

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

You may notice that in any row no element is repeated, this is due to the cancellation law, ??.

### Example 1.8

Rotations and reflections of an equilateral triangle.



operation  $\circ$  = do right transformation then left transformation

**Claim:** This defines a group with 6 elements

### Example 1.9

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

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

under addition

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

A more interesting example is

### Example 1.10

$$GL_2(\mathbb{R}) = \{\text{invertible } 2 \times 2 \text{ matrices with entries in } \mathbb{R}\}.$$

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \det A = ad - bc \neq 0$$

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

Under multiplication this is a group.  $GL$  stands for general linear group.

### Lemma 1.1

Let  $(G, *)$  be a group.

- i. The identity element is unique.
- ii. Inverses are unique.

*Proof.*

- i. Suppose  $e$  and  $\hat{e}$  are both identities, so

$$a * e = a = e * a, \quad a * \hat{e} = a = \hat{e} * a \quad \forall a \in G.$$

In particular

$$e = e * \hat{e} = \hat{e}.$$

- ii. Suppose both  $y$  and  $z$  are inverses for  $x$ , so

$$x * y = e = y * x, \quad x * z = e = z * x$$

Then,  $y = y * e$

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

$$= (y * x) * z \quad (\text{associative law})$$

$$= e * z$$

$$= z.$$

□

*Remark 2.* Associativity means we don't need brackets,  $x * y * z$  is unambiguous. Furthermore, by induction,  $x_1 * x_2 * \cdots * x_n$  is unambiguous.

We know the statement is true for the case  $n = 3$ .

$$\begin{aligned} x_1 * (x_2 * \cdots * x_n) &= (x_1 * x_2) * (x_3 * \cdots * x_n) \\ &= (x_1 * x_2 * x_3) * (x_4 * \cdots * x_n) \end{aligned}$$

$$\begin{aligned}
&= \dots \\
&= (x_1 * x_2 * \dots * x_{n-1}) * x_n
\end{aligned}$$

*Remark 3.* We often omit ‘ $*$ ’ and write  $xy$  for  $x * y$  and  $G$  for  $(G, *)$ .

*Remark 4.*  $(xy)^{-1} = y^{-1}x^{-1}$ . Since it works:

$$\begin{aligned}
(xy)y^{-1}x^{-1} &= x(yy^{-1})x^{-1} \\
&= xex^{-1} \\
&= xx^{-1} \\
&= e
\end{aligned}$$

Note, inverses are unique

*Remark 5.*  $(x^{-1})^{-1} = x$

*Remark 6.*

$$\begin{aligned}
&x, y, z \in G \text{ and } xy = xz \\
\implies &x^{-1}xy = x^{-1}xz \\
\implies &y = z \qquad \qquad \qquad (\text{cancellation law})
\end{aligned}$$

### Definition 1.3 (Abelian group)

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

Note all our examples above are abelian except ?? and ??.

### Definition 1.4 (Order of group)

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

### Definition 1.5 (Subgroup)

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

- a)  $h, k \in H \implies h * k \in H$
- b)  $e_G \in H$
- c)  $h \in H \implies h^{-1} \in H$

(Note associativity is inherited)

i.e restricting operation to  $H$  still gives a group. We write  $H \leq G$ .

**Example 1.11**

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

**Example 1.12**

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

**Example 1.13**

In ?? if we just take the rotations we get a subgroup,  $\{1, \sigma, \sigma^2\}$  is a subgroup.

**Example 1.14**

In ??, we can take the matrices with determinant 1 which is  $\text{SL}_2(\mathbb{R})$  (SL stands for the special linear group).

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

We always have identity and whole thing as subgroups.

**Example 1.15**

If  $G$  is a group then  $\{e\} \leq G$  is the trivial subgroup.

**Example 1.16**

If  $G$  is a group then  $G \leq G$  is the improper subgroup.

**Proposition 1.1**

Subgroups of  $\mathbb{Z}$  are exactly  $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$  where  $n \in \mathbb{Z}_{\geq 0}$  (under addition).

*Proof.* First note  $n\mathbb{Z}$  is a subgroup of  $\mathbb{Z}$ .

a. If  $a, b \in n\mathbb{Z}$  then  $a = na'$  and  $b = nb'$  for some  $a', b' \in \mathbb{Z}$ . Then  $a + b =$



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

b.  $0 \in n\mathbb{Z}$ .

c. If we have  $a = na' \in n\mathbb{Z}$  then  $a^{-1} = -a = n(-a') \in n\mathbb{Z}$ .

Conversely assume  $H \leq \mathbb{Z}$ .

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

Otherwise choose  $0 < n \in H$  with  $n$  minimal (smallest positive element of  $H$ ). Then  $n\mathbb{Z} \in H$  by closure and inverses. We show  $H = n\mathbb{Z}$ . Suppose  $\exists h \in H \setminus n\mathbb{Z}$ , then we can write  $h = nk + h'$  with  $h' \in \{1, 2, \dots, n-1\}$ . But  $h' = h - nk \in H$ , contradicting minimality of  $n$ . Thus  $H = n\mathbb{Z}$ .  $\square$

## Aside: Functions

We need the notion of functions.

### Definition 1.6 (Function)

$f$  is a *function* between sets  $A$  and  $B$  if it assigns each element of  $A$  a unique element of  $B$ .

$$\begin{aligned} f : A &\rightarrow B \\ a &\mapsto f(a) \end{aligned}$$

### Example 1.17

$$\begin{array}{ll} \text{eg: } f : \mathbb{Z} \rightarrow \mathbb{Z} & g : \mathbb{Z} \rightarrow \mathbb{Z} \\ x \mapsto x + 1 & x \mapsto 2x. \end{array}$$

### Definition 1.7 (Composition of functions)

Suppose  $g : A \rightarrow B$  and  $f : B \rightarrow C$ , define

$$\begin{aligned} f \circ g : A &\rightarrow C \\ a &\mapsto (f \circ g)(a) = f(g(a)) \end{aligned}$$

### Example 1.18

$$(f \circ g)(x) = 2x + 1$$

$$(g \circ f)(x) = 2x + 2.$$

Suppose  $f_1 : A \rightarrow B$  and  $f_2 : A \rightarrow B$  then  $f_1 = f_2$  if  $f_1(a) = f_2(a) \quad \forall a \in A$ .

**Definition 1.8 (Bijective functions)**

$f : A \rightarrow B$  is a *bijection* if it defines a pairing between elements of  $A$  and elements of  $B$ . That is given  $b \in B \exists$  unique  $a \in A$  s.t.  $f(a) = b$ .

**Example 1.19**

$$\begin{aligned} f : \mathbb{Z} &\rightarrow \mathbb{Z} \\ x &\mapsto x + 1 \end{aligned}$$

**Definition 1.9 (Inverse function)**

If we have a bijection we can define

$$\begin{aligned} f^{-1} : B &\rightarrow A \\ b &\mapsto a \text{ where } f(a) = b. \end{aligned}$$

Then  $f \circ f^{-1} = id_B$   $f^{-1} \circ f = id_A$   
 $id_B(b) = b$

**Lemma 1.2**

If  $g : A \rightarrow B$  and  $f : B \rightarrow C$  are bijections then so is  $f \circ g : A \rightarrow C$ .

*Proof.* See Numbers and Sets

□

**Definition 1.10 (Group homomorphism)**

Let  $(G, *_G)$  and  $(H, *_H)$  be groups. Then the function

$$\theta : G \rightarrow H$$

is a *homomorphism* if

$$\theta(x *_G y) = \theta(x) *_H \theta(y) \quad \forall x, y \in G.$$

‘A map which respects the group operation’.

**Example 1.20**

$G = (\{0, 1, 2, 3\}, +_4)$ ,  $H = (\{1, e^{\pi i/2}, e^{\pi i}, e^{3\pi i/2}, \times\})$  (the 4th roots of unity).

$$\begin{aligned}
 \theta : G &\rightarrow H \\
 n &\mapsto e^{n\pi i/2} \\
 \theta(n +_4 m) &= e^{(n+4m)\pi i/2} \\
 &= e^{(n+m)\pi i/2} \text{ since } n + m = n +_4 m + 4k \text{ and } e^{4k\pi i/2} = 1 \\
 &= e^{n\pi i/2} \times e^{m\pi i/2} \\
 &= \theta(n) \times \theta(m)
 \end{aligned}$$

**Lemma 1.3**

Let  $G$  and  $H$  be groups and suppose we have a homomorphism  $\theta : G \rightarrow H$ . Then  $\theta(G) = \{\theta(g) : g \in G\}$ , the *image* of  $\theta$ , is a subgroup of  $H$ , written  $\theta(G) \leq H$ .

*Proof.*  $\theta(G) \subseteq H$  by definition of  $\theta$ .

*Closure:* Let  $x, y \in \theta(G)$ . Then  $x = \theta(g)$  and  $y = \theta(h)$  for some  $h, g \in G$ .

$$\begin{aligned}
 x *_H y &= \theta(g) *_H \theta(h) \\
 &= \theta(g *_G h) \text{ as } \theta \text{ is a homomorphism} \\
 &= \theta(G).
 \end{aligned}$$

*Identity:*

$$\begin{aligned}
 \theta(e_G) &= \theta(e_G *_G e_G) \\
 &= \theta(e_G) *_H \theta(e_G) \\
 \text{premultiplying by } \theta(e_G)^{-1} &\in H \\
 \mathbf{e}_H &= \theta(e_G) \in \theta(G)
 \end{aligned}$$

*Inverses:*

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

$$\begin{aligned} & \text{Inverses are unique} \\ \implies & \theta(g)^{-1} = \theta(g^{-1}) \in \theta(G) \end{aligned}$$

Associativity is inherited. □

### Definition 1.11 (Isomorphism)

A bijective homomorphism is called an isomorphism. If  $G$  and  $H$  are groups and  $\theta : G \rightarrow H$  is an isomorphism we say  $G$  and  $H$  are isomorphic and write  $G \cong H$ . The bijective part tells us the sets are the same and the homomorphism tells us the group operation is the same so an isomorphism tells us the groups are the “essentially the same”.

See ??

$$\begin{aligned} G = (\{0, 1, 2, 3\}, +_4) &\cong \{1, e^{\pi i/2}, e^{\pi i}, e^{3\pi i/2}, \times\} = H \\ \theta : G &\rightarrow H \\ n &\mapsto e^{n\pi i/2} \end{aligned}$$

$\theta$  is an isomorphism.

### Lemma 1.4

- i. The composition of two homomorphisms is a homomorphism, similarly for isomorphisms, thus if  $G_1 \cong G_2$  and  $G_2 \cong G_3$  then  $G_1 \cong G_3$ .
- ii. If  $\theta : G_1 \rightarrow G_2$  is an isomorphism then so is its inverse  $\theta^{-1} : G_2 \rightarrow G_1$ . So  $G_1 \cong G_2 \implies G_2 \cong G_1$ .

*Proof.*

- i. Suppose

$$\begin{aligned} \theta_1 : (G_1, *_1) &\rightarrow (G_2, *_2) \\ \theta_2 : (G_2, *_2) &\rightarrow (G_3, *_3) \end{aligned}$$

are isomorphisms. Thus  $\theta_2 \circ \theta_1$  is a function from  $G_1$  to  $G_3$ , we need to check if its a homomorphism.

$$\begin{aligned} & \text{Let } x, y \in G_1 \\ \theta_2 \circ \theta_1(x *_1 y) &= \theta_2(\theta_1(x) *_2 \theta_1(y)) && \text{since } \theta_1 \text{ is a homomorphism} \\ &= \theta_2(\theta_1(x)) *_3 \theta_2(\theta_1(y)) && \text{since } \theta_2 \text{ is a homomorphism} \\ &= (\theta_2 \circ \theta_1)(x) *_3 (\theta_2 \circ \theta_1)(y) \end{aligned}$$

ii.  $\theta$  is a bijection so  $\theta^{-1}$  exists, we need to show its a homomorphism.

Let  $y, z \in G_2$ .

Then  $\exists x, k \in G_1$ , s.t.

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

Note,  $\theta(x *_1 k) = \theta(x) *_2 \theta(k)$

$$= y *_2 z$$

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

□

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

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

### Definition 1.12 (Cyclic group)

A group  $H$  is *cyclic* if  $\exists h \in H$  such that each element of  $H$  is a power of  $h$ , i.e. for each  $x \in H \exists m \in \mathbb{Z}$  s.t.  $x = h^m$ . Then  $h$  is called a *generator* of  $H$  and we write  $H = \langle h \rangle$ .

### Example 1.21

$(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$ , the infinite cyclic group. We showed all subgroups of  $(\mathbb{Z}, +)$  are cyclic in ??.

### Example 1.22

$$(\{\pm 1\}, +) = \langle -1 \rangle$$

### Example 1.23

$$(\{0, 1, 2, 3\}, +_4) = \langle 1 \rangle = \langle 3 \rangle$$

Note a cyclic group is abelian.

**Definition 1.13 (Order of element)**

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

**Lemma 1.5**

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

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

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

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

( $\Rightarrow$ ) Suppose  $g^n = e$ . Write  $n = qm + r$  with  $0 \leq r < m$ ,  $q \in \mathbb{N}$ .

$$\begin{aligned} \implies e = g^n &= g^{qm+r} \\ &= (g^m)^q + g^r \\ &= e^q g^r \\ &= e g^r \\ &= g^r \\ \implies r &= 0 \text{ by minimality of } m \implies n = qm \text{ as required.} \end{aligned}$$

□

*Remark 7.*

- i. Suppose  $g \in G$ . Then  $\{g^n : n \in \mathbb{Z}\}$  is a subgroup of  $G$ , in fact it is the smallest subgroup of  $G$  containing  $g$ . We call it the subgroup of  $G$  generated by  $g$  and write  $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$ . Also  $|\langle g \rangle| = o(g)$  if finite. Since if  $o(g) = m$ ,  $\langle g \rangle = \{e, g, g^2, \dots, g^{m-1} = g^{-1}\}$ . Otherwise both infinite.
- ii. We can define the abstract cyclic group of order  $n$

$$C_n = \langle x \rangle, \text{ where } o(x) = n.$$

Then  $(\{0, 1, \dots, n-1\}, +_n)$  and  $(\{n^{\text{th}} \text{ roots of unity}\}, \times)$  are realisations of this group, they are all isomorphic.

- iii. Let  $G$  be a group and  $g_1, \dots, g_k \in G$ . Then the subgroup of  $G$  generated by  $g_1, \dots, g_k$  denoted  $\langle g_1, \dots, g_k \rangle$  is the smallest subgroup of  $G$  containing all the  $g_i$ 's. It is the intersection of all the subgroups of  $G$  containing all the  $g_i$ 's.

## §2 The Dihedral and Symmetric Groups

First note composition of functions is associative

$$\begin{aligned}
 f, g, h : X &\rightarrow X, \text{ let } x \in X \\
 (f \circ (g \circ h))(x) &= f((g \circ h)(x)) \\
 &= f(g(h(x))) \\
 &= (f \circ g)(h(x)) \\
 &= ((f \circ g) \circ h)(x) \\
 \implies f \circ (g \circ h) &= (f \circ g) \circ h.
 \end{aligned}$$

### §2.1 Dihedral Groups

#### Definition 2.1 (Dihedral groups $D_{2n}$ )

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

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

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

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

*Warning* - sometimes  $D_{2n}$  is denoted  $D_n$

We have already met  $D_6$  in ??.

Consider  $D_8$ <sup>1</sup>

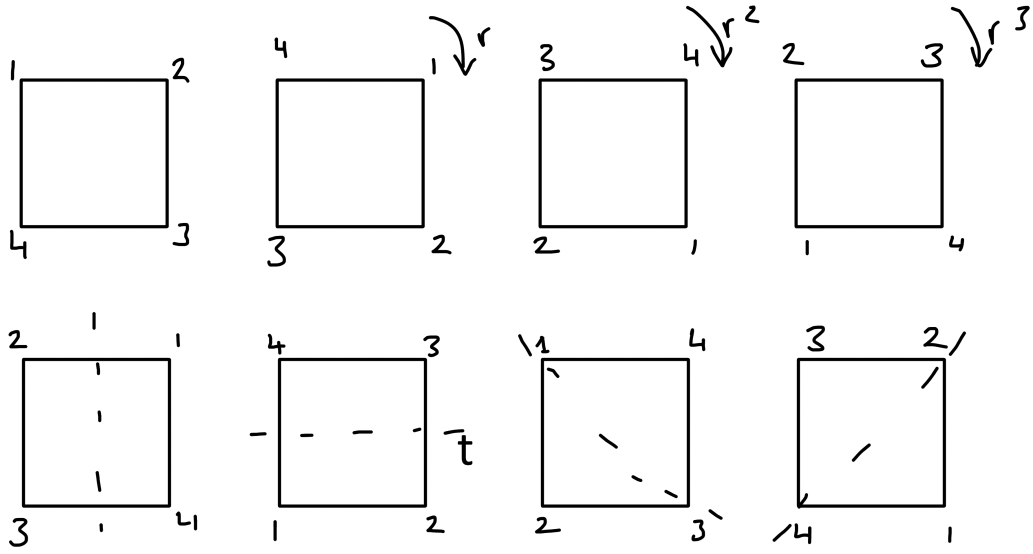
$$\begin{aligned}
 \text{Let } r : P &\rightarrow P \\
 z &\mapsto e^{2\pi i/n} z \\
 t : P &\rightarrow P \\
 z &\mapsto \bar{z}
 \end{aligned}$$

These are both isometries

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

---

<sup>1</sup>The subgroup generated by  $r^2$  and  $t$  includes the identity, as they are self inverses so no need for inverses, and by closure  $r^2 t = t r^2 t$  and so it is a subgroup of order 4.



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

$$\begin{aligned}
 &\text{Note, } r^n = \text{id} = \text{identity} \\
 \implies r^{-1} &= r^{n-1} \\
 t^2 &= \text{id} \\
 \implies t^{-1} &= t \\
 t * r * z &= e^{-2\pi i/n} \bar{z} = r^{-1} * t * z \\
 \implies tr &= r^{-1}t
 \end{aligned}$$

We show that the set of symmetries of  $P$  is precisely  $\{e, \underbrace{r, r^2, \dots, r^{n-1}}_{\text{rotations}}, \underbrace{t, rt, \dots, r^{n-1}t}_{\text{reflections}}\}$ .

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

Let  $f$  be a symmetry of  $P$ . Then  $f(1) = e^{2\pi i k/n}$  for some  $k$  ( $f(1)$  is mapping 1 to some vertex, so some element of  $V$ ).

$$\begin{aligned}
 \implies \underbrace{r^{-k} \circ f}_{g, \text{ symmetry of } P \text{ fixing } 1} (1) &= 1
 \end{aligned}$$



$$g = r^{-k} \circ f$$

So,  $g(e^{2\pi i/n}) = e^{2\pi i/n}$  or  $e^{-2\pi i/n}$  as the vertices next to 1 stay next to it.

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

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

So  $g$  fixes 0, 1 and  $e^{2\pi i/n} \implies g = \text{id} \implies f = r^k$ .

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

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

Algebraically we write,

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

Finally,  $D_2 \cong C_2$  and  $D_4$  is ???. Both are abelian. Also  $D_\infty$  exists.

## §2.2 Symmetric Groups

### Definition 2.2 (permutation)

Let  $X$  be a set. A bijection

$$f : X \rightarrow X$$

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

### Proposition 2.1

$\text{Sym } X$  is a group under composition of functions. It is called the symmetric group

on  $X$ .

*Proof.*

- closure - See ?? (Number's and Sets).
- identity, define  $\iota(x) = x \quad \forall x \in X$ .
- Let  $f \in \text{Sym}(X)$ . As  $f$  is a bijection,  $f^{-1}$  exists and is a bijection and satisfies  $f \circ f^{-1} = \iota = f^{-1} \circ f$ .
- composition of functions is associative.

□

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

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

If  $\sigma \in S_n$  write

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

### Example 2.1

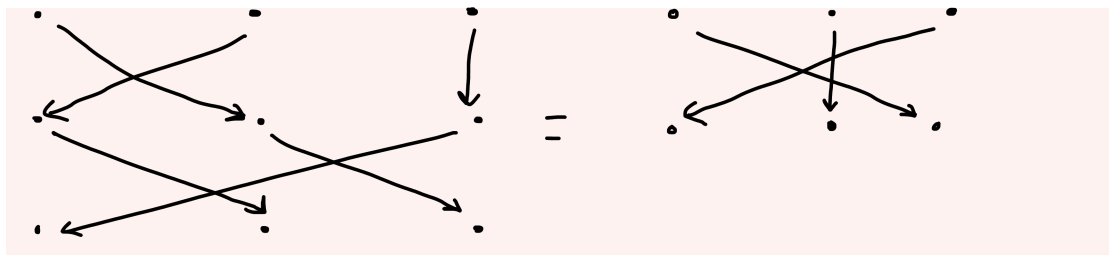
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in S_3$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \in S_5$$

### Example 2.2

Composition:

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

or:



### §2.2.1 Small n

#### Example 2.3

$$S_1 = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\} = \{\iota\} \quad \text{trivial group}$$

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$$

$$\cong (\{\pm 1\}, \times) \cong C_2$$

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

$$\cong D_6$$

Remark 8.

- i.  $|S_n| = n!$
- ii. For  $n \geq 3$   $S_n$  is not abelian. Consider

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

They don't commute in  $S_3$  so they won't in  $S_n$ .

- iii.  $D_{2n}$  naturally embeds in  $S_n$ . e.g.  $D_8 \lesssim S_4$  (isomorphic to a subgroup)

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

'Double row notation is cumbersome and hides what's going on, so we introduce cycle notation'.

#### Definition 2.3 (Cycle notation)

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

$$\sigma(a_i) = a_{i+1} \quad 1 \leq i \leq k-1$$

$$\sigma(a_k) = a_1$$

and  $\sigma(x) = x \ \forall \ x \in \{1, \dots, n\} \setminus \{a_1, \dots, a_k\}$ . Then  $\sigma$  is a  $k$ -cycle and we write  $\sigma = (a_1, a_2, \dots, a_k)$ . e.g.

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

is the 3-cycle  $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$  i.e.  $1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1$  and all of numbers map to themselves.

*Remark 9.*

i.

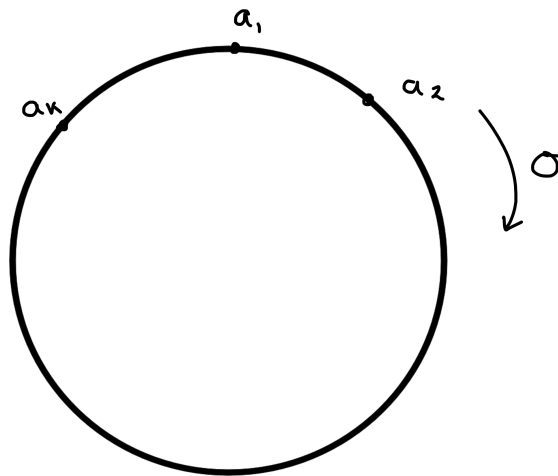
$$\begin{aligned} (a_1, a_2, \dots, a_k) &= (a_k, a_1, a_2, \dots, a_{k-1}) \\ &= \dots \end{aligned}$$

We usually write the smallest  $a_i$  first.

ii.

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

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



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

#### Definition 2.4 (Disjoint cycles)

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

### Lemma 2.1

If  $\sigma, \tau \in S_n$  are disjoint then  $\sigma\tau = \tau\sigma$

*Proof.* If  $x \in 1, \dots, n \setminus \{a_1, \dots, a_k\} \cup \{b_1, \dots, b_l\}$ ,  $(\sigma \circ \tau)(x) = \sigma(\tau(x)) = (\tau \circ \sigma)(x)$ .

Suppose  $1 \leq i \leq k-1$

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

And  $\sigma \circ \tau(a_k) = a_1$ ,  $\tau \circ \sigma(a_k) = a_1$ .

Similarly for  $b_j$   $\tau \circ \sigma(b_j) = \sigma \circ \tau(b_j)$

Thus  $\sigma \circ \tau$  and  $\tau \circ \sigma$  agree everywhere  $\implies \sigma \circ \tau = \tau \circ \sigma$ . □

### Example 2.4

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

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

### Example 2.5

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

### Example 2.6

$$\begin{aligned}
(1 \ 2 \ 3) (2 \ 3) &= (1 \ 2) (3) \\
&= (1 \ 2) \text{ suppress 1-cycles.} \\
(2 \ 3) (1 \ 2 \ 3) &= (1 \ 3)
\end{aligned}$$

### Theorem 2.1

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

### Example 2.7

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

*Proof.* Let  $a_1 \in \{1, 2, \dots, n\} = X$ . Consider  $a_1, \sigma(a_1), \sigma^2(a_1), \dots$ . Since  $X$  is finite  $\exists$  minimal  $j$  such that  $\sigma^j(a_1) \in \{a_1, \sigma(a_1), \sigma^2(a_1), \dots, \sigma^{j-1}(a_1)\}$ . We claim:  $\sigma^j(a_1) = a_1$ . Since if not

$$\begin{aligned}
&\sigma^j(a_1) = \sigma^i(a_1), \ j > i \geq 1 \\
\implies &\sigma^{j-i}(a_1) = a_1 \quad \text{! of minimality of } j.
\end{aligned}$$

So  $\{a_1, \sigma(a_1), \sigma^2(a_1), \dots, \sigma^{j-1}(a_1)\}$  is a cycle in  $\sigma$ .

If  $\exists b \in X \setminus \{a_1, \sigma(a_1), \sigma^2(a_1), \dots, \sigma^{j-1}(a_1)\}$ . Consider  $b, \sigma(b), \dots$

Note  $(b, \sigma(b), \sigma^2(b), \dots, \sigma^{j-1}(b))$  is disjoint from  $(a_1, \sigma(a_1), \sigma^2(a_1), \dots, \sigma^{j-1}(a_1))$  because  $\sigma$  is a bijection.<sup>a</sup>

Continue in this way until all elements of  $X$  are reached.  $\square$

<sup>a</sup>If  $\sigma^i(b) = \sigma^j(a_1)$  then  $b = \sigma^{j-i}(a_1)$  which contradicts  $b \in X \setminus \{a_1, \sigma(a_1), \sigma^2(a_1), \dots, \sigma^{j-1}(a_1)\}$ .

### Lemma 2.2

Let  $\sigma, \tau$  be disjoint cycles in  $S_n$ . Then  $o(\sigma\tau) = \text{lcm}\{o(\sigma), o(\tau)\}$

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

$$\begin{aligned}
(\sigma\tau)^k &= \sigma\tau\sigma\tau \dots \sigma\tau \\
&= \sigma^k \tau^k \quad ??
\end{aligned}$$

$$\begin{aligned}
&= e \cdot e \quad ?? \\
&= e \\
&\implies o(\sigma\tau) \mid k \quad ??
\end{aligned} \tag{1}$$

Now suppose  $o(\sigma\tau) = n$  so  $(\sigma\tau)^n = e \implies \sigma^n \tau^n = e$ . But  $\sigma, \tau$  move different elements of  $X \implies \sigma^n = e, \tau^n = e$ . By ??

$$\begin{aligned}
&\implies o(\sigma) \mid n \text{ and } o(\tau) \mid n \\
&\implies k = \text{lcm}\{o(\sigma), o(\tau)\} \\
&\quad \mid n = o(\sigma\tau) \\
&?, ? \implies o(\sigma\tau) = \text{lcm}\{o(\sigma), o(\tau)\}
\end{aligned} \tag{2}$$

□

### Proposition 2.2

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

*Proof.* By ?? it is enough to show a  $k$ -cycle can be written as a product of transpositions.

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

□

### Example 2.8

$$\begin{aligned}
(1 \ 2 \ 3 \ 4 \ 5) &= (1 \ 2)(2 \ 3)(3 \ 4)(4 \ 5) \\
&= (1 \ 2)(1 \ 2)(1 \ 2)(2 \ 3)(3 \ 4)(4 \ 5) \\
&= (1 \ 5)(1 \ 4)(1 \ 3)(1 \ 2)
\end{aligned}$$

*not unique.*

### Definition 2.5 (Sign of permutation)

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

### Lemma 2.3

The function

$$\begin{aligned}\text{sgn} : S_n &\rightarrow \{\pm 1\} \\ \sigma &\mapsto \text{sgn}(\sigma)\end{aligned}$$

is well defined.

i.e. if  $\sigma = \tau_1 \dots \tau_a = \tau'_1 \dots \tau'_b$  with  $\tau_i$  and  $\tau'_i$  transpositions then  $(-1)^a = (-1)^b$ .

$$\begin{aligned}\text{sgn}\left(\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \end{pmatrix}\right) &= (-1)^4 = (-1)^6 \\ &= 1\end{aligned}$$

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

Let  $\tau$  be a transposition. Claim:  $c(\sigma\tau) = c(\sigma) \pm 1 \equiv c(\sigma) + 1 \pmod{2}$ .

Let  $\tau = \begin{pmatrix} k & l \end{pmatrix}$ .

2 cases:

i.  $k, l$  lie in different cycles of  $\sigma$ :

$$\begin{aligned}\begin{pmatrix} k & a_1 & \dots & a_r \end{pmatrix} \begin{pmatrix} l & b_1 & \dots & b_s \end{pmatrix} \begin{pmatrix} k & l \end{pmatrix} &= \begin{pmatrix} k & b_1 & b_2 & \dots & b_s & l & a_1 & \dots & a_r \end{pmatrix} \\ \implies c(\sigma\tau) &= c(\sigma) - 1\end{aligned}$$

ii. i.  $k, l$  lie in the same cycle in  $\sigma$ :

$$\begin{aligned}\begin{pmatrix} k & a_1 & \dots & a_r & l & b_1 & \dots & b_s \end{pmatrix} \begin{pmatrix} k & l \end{pmatrix} &= \begin{pmatrix} k & b_1 & b_2 & \dots & b_s \end{pmatrix} \begin{pmatrix} l & a_1 & \dots & a_r \end{pmatrix} \\ \implies c(\sigma\tau) &= c(\sigma) + 1\end{aligned}$$

Assume

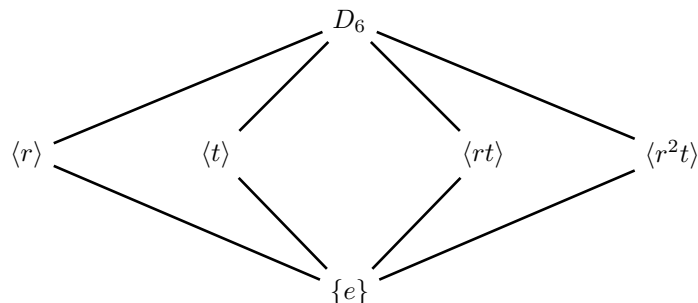
$$\begin{aligned}\sigma &= \text{id}\tau_1 \dots \tau_a \\ &= \text{id}\tau'_1 \dots \tau'_b \\ \implies c(\sigma) &\equiv n + a \pmod{2} \\ &\equiv n + b \pmod{2} \\ \implies a &\equiv b \pmod{2} \\ \implies (-1)^a &= (-1)^b\end{aligned}$$

□



## Aside: Subgroup Lattices

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



We put the largest subgroups at the top and work our way down.

### Theorem 2.2

Let  $n \geq 2$ . The map

$$\begin{aligned} \text{sgn} : (S_n, \circ) &\rightarrow (\{\pm 1\}, \times) \\ \sigma &\mapsto \text{sgn}(\sigma) \end{aligned}$$

is a well-defined non-trivial (doesn't just map to identity) homomorphism.

*Proof.*

- We know its well-defined by ??
- $\text{sgn}\left(\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\right) = -1$ , so non-trivial
- homomorphism:

Let  $\alpha, \beta \in S_n$  with  $\text{sgn}(\alpha) = (-1)^k$ ,  $\text{sgn}(\beta) = (-1)^l$ . So  $\exists$  transpositions  $\tau_i$  and  $\tau'_i$  such that  $\alpha = \tau_1 \dots \tau_k$  and  $\beta = \tau'_1 \dots \tau'_l$ . This implies

$$\begin{aligned} \alpha\beta &= \tau_1 \dots \tau_k \tau'_1 \dots \tau'_l \\ \implies \text{sgn}(\alpha\beta) &= (-1)^{k+l} \\ &= (-1)^k (-1)^l \\ &= \text{sgn}(\alpha) \text{sgn}(\beta) \end{aligned}$$

□

**Definition 2.6**

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

**Corollary 2.1**

The even permutations of  $S_n$  ( $n \geq 2$ ) form a subgroup called the *alternating group* and we denote it by  $A_n$ .

*Proof.*

- $\text{id} = \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix} \in A_n$
- 

$$\begin{aligned} \text{sgn}(\sigma) &= 1 = \text{sgn}(\rho) \\ \implies \text{sgn}(\sigma\rho) &= \text{sgn}(\sigma) \text{sgn}(\rho) \\ &= 1 \end{aligned}$$

by Theorem ??

- $\sigma = \tau_1 \dots \tau_k$  where  $\tau_i$  are transpositions. Then  $\sigma^{-1} = \tau_k \dots \tau_1 \implies \text{sgn}(\sigma) = \text{sgn}(\sigma^{-1})$
- associativity is inherited

□

**Example 2.9**

$$A_4 = \left\{ e, \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}, \right. \\ \left. \begin{pmatrix} 1 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 4 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 2 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 4 & 3 \end{pmatrix} \right\}.$$

*Remark 10.*

- $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$  (will be proved later on)
- cycles of even length are odd and cycles of odd length are even.
- $A_n = \ker(\text{sgn})$ , hence a subgroup (q9 - sheet 1).

### §3 Cosets and Lagrange

#### Definition 3.1 (Cosets)

Let  $H \leq G$  and  $g \in G$ . The *left coset*  $gH$  is defined to be  $\{gh : h \in H\}$ . Similarly the *right coset*  $Hg = \{hg : h \in H\}$

#### Example 3.1

$$\begin{aligned} S_3 &= \{e, (1 \ 2 \ 3), (1 \ 3 \ 2), (1 \ 2), (1 \ 3), (2 \ 3)\} \\ H &= \{\text{id}, (1 \ 2 \ 3), (1 \ 3 \ 2)\} = A_3 \\ (1 \ 2)H &= \{(1 \ 2), (1 \ 2)(1 \ 2 \ 3), (1 \ 2)(1 \ 3 \ 2)\} \\ &= \{(1 \ 2), (2 \ 3), (1 \ 3)\} \\ (1 \ 2 \ 3)H &= H \text{ (since } H \text{ is a subgroup)} \end{aligned}$$

Note,  $H \cup (1 \ 2)H = S_3$

#### Lemma 3.1

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

*Proof.*

$$\begin{aligned} \text{Define } \theta_g : H &\rightarrow gH \\ h &\mapsto gh. \end{aligned}$$

We show  $\theta_g$  is a bijection.

Surjectivity: if  $gh \in gH$  then  $\theta_g(h) = gh$ .

Injectivity:

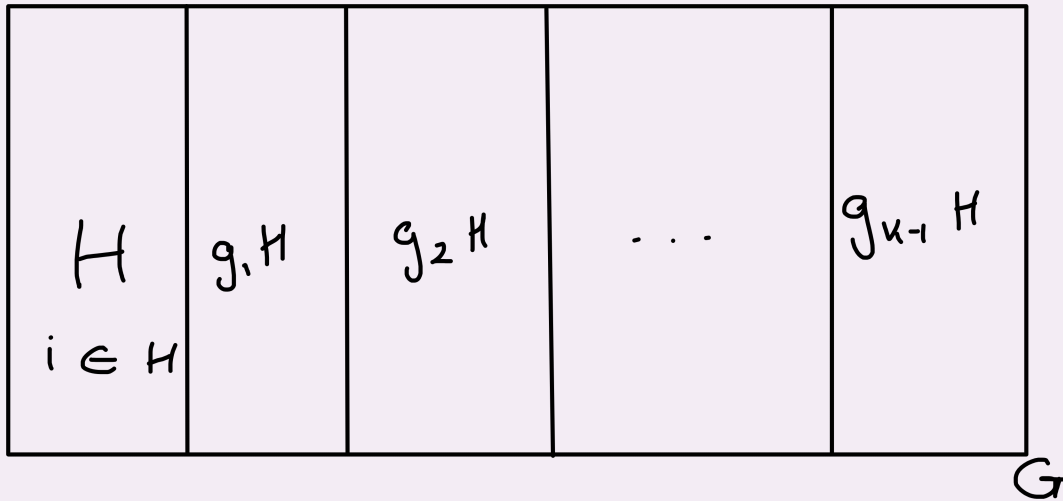
$$\begin{aligned} \theta_g(h_1) &= \theta_g(h_2) \\ gh_1 &= gh_2 \\ \implies h_1 &= h_2 \text{ (cancellation law)} \end{aligned}$$

□

**Lemma 3.2**

The left cosets of  $H$  in  $G$  form a partition of  $G$  i.e.

- i. each  $g \in G$  lies in some left coset of  $H$  in  $G$ .
- ii. if  $aH \cap bH \neq \emptyset$  (for some  $a, b \in G$ )  $\implies aH = bH$ .



*Proof.*

- i.  $g \in gH$  as  $e \in H$
- ii. Suppose  $c \in aH \cap bH$ .  
Claim:  $aH = cH = bH$ .

Now  $c \in aH$  so  $c = ak$  for some  $k \in H$ .

$$\begin{aligned} \implies cH &= \{ch : h \in H\} \\ &= \{akh : h \in H\} \subseteq aH. \end{aligned}$$

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

$$\implies aH \subseteq cH.$$

So  $aH = cH$ .

Similarly  $cH = bH$

□

**Example 3.2**

$$S_n = \underbrace{A_n}_{\text{even elements}} \dot{\cup} \underbrace{\begin{pmatrix} 1 & 2 \\ & \end{pmatrix} A_n}_{\text{odd elements}}$$

### Lemma 3.3

Let  $H \leq G$ ,  $a, b \in G$ . Then  $aH = bH \iff a^{-1}b \in H$ .

*Proof.* ( $\implies$ ):

$$\begin{aligned} b &\in bH = aH \\ \implies b &= ah \text{ for some } h \in H \\ \implies a^{-1}b &= h \in H \end{aligned}$$

( $\impliedby$ ):

$$\begin{aligned} \text{Suppose } a^{-1}b &= k \in H \\ \implies b &= ak \in aH \\ \text{also } b &\in bH. \\ \implies aH &= bH \end{aligned}$$

by ??

□

### Theorem 3.1 (Lagrange's Theorem)

Let  $H$  be a subgroup of the finite group  $G$ . Then the order of  $H$  divides the order of  $G$  (i.e.  $|H| \mid |G|$ ).

*Proof.* By ??  $G$  is partitioned into distinct cosets of  $H$ , say  $G = g_1H \dot{\cup} g_2H \dot{\cup} \dots \dot{\cup} g_kH$  (say  $g_1 = e$ ).

By ??<sup>a</sup>

$$\begin{aligned} |g_iH| &= |H| \quad 1 \leq i \leq k \\ \implies |G| &= |H|k \end{aligned}$$

□

---

<sup>a</sup>You would need to prove these lemma's in an exam q.

**Definition 3.2 (Index of a subgroup)**

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

*Remark 11.*

- i. If  $G$  is finite,  $|G : H| = \frac{|G|}{|H|}$ . But we can have  $|G : H|$  finite, even if  $G$  and  $H$  are infinite, e.g.  $\mathbb{Z}$  and  $n\mathbb{Z}$  where  $|G : H| = n$ .
- ii. We write  $(G : H)$  for the set of left cosets of  $H$  in  $G$ .

From Dexter's Notes:

The  $k$  in ?? is  $|G : H|$ , giving ??. 'The hard part of this proof is to prove that the left cosets partition  $G$  and have the same size. If you are asked to prove Lagrange's theorem in exams, that is what you actually have to prove.'

**Corollary 3.1 (Lagrange's Corollary)**

$G$  is a finite group,  $g \in G$ . Then  $o(g) \mid |G|$ . In particular,  $g^{|G|} = e$ .

*Proof.*

Note  $\langle g \rangle = \{e, g, \dots, g^{n-1}\}$  where  $o(g) = n$ .

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

$\implies g^{|G|} = e$  by ??

□

**Corollary 3.2**

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

*Proof.* Let  $e \neq g \in G$ . Then  $\{e\} \neq \langle g \rangle \leq G$ . By ??

$$1 \neq |\langle g \rangle| \mid |G| = p$$

$$\begin{aligned} \implies |\langle g \rangle| &= p = |G| \\ \implies \langle g \rangle &= G \end{aligned}$$

i.e.  $G$  cyclic. □

### Definition 3.3 (Euler's totient function)

Let  $n \in \mathbb{N}$  and  $\phi(n) = |\{1 \leq a \leq n : \text{hcf}(a, n) = 1\}|$ .

### Example 3.3

$$\phi(12) = |\{1, 5, 7, 11\}| = 4.$$

### Theorem 3.2 (Fermat-Euler Theorem)

Let  $n \in \mathbb{N}$ ,  $a \in \mathbb{Z}$  and  $\text{hcf}(a, n) = 1$ .

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

We can prove this by using Lagrange, but first we need to set it up.

Let  $n \in \mathbb{N}$ ,

$$\begin{aligned} R_n &= \{0, 1, \dots, n-1\} \\ R_n^* &= \{a \in R_n : \text{hcf}(a, n) = 1\} \end{aligned}$$

**Notation.**  $n \in \mathbb{Z}$  then  $\bar{u} \in R_n$  such that  $u \equiv \bar{u} \pmod{n}$ .

Define  $\times_n$  to be multiplication mod  $n$ .

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

Closure:

$$\begin{aligned} \text{hcf}(a, n) &= 1 = \text{hcf}(b, n) \\ \implies \text{hcf}(ab, n) &= 1 \\ \implies \text{hcf}(\overline{ab}, n) &= 1 \end{aligned}$$

Identity = 1

Associativity is fine.

Inverses: Let  $a \in R_n^*$ ,  $\text{hcf}(a, n) = 1$

$$\begin{aligned} \implies \exists u, v \in \mathbb{Z} \text{ s.t. } au + vn &= 1 \text{ (Bezout's Theorem)} \\ \implies au &\equiv 1 \pmod{n} \end{aligned}$$

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

*Proof.* Note  $|R_n^*| = \phi(n)$ .

$$a \equiv \bar{a} \pmod{n}, \bar{a} \in R_n^*$$

By ??

$$\begin{aligned} \bar{a}^{\phi(n)} &= \bar{a}^{|R_n^*|} = 1 \in R_n^* \\ \implies a^{\phi(n)} &\equiv 1 \pmod{n} \end{aligned}$$

□



## §4 Normal Subgroups, Quotient groups and Homomorphisms

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

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

When does this work? Consider  $gHkH$  if  $Hk = kH$  then we get  $gkHH = gkH$ . This motivates the following definition.

### Definition 4.1 (Normal subgroup)

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

### Example 4.1

$$\begin{aligned} K &= \{\text{id}, \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}\} \trianglelefteq S_3 \\ \begin{pmatrix} 1 & 2 \end{pmatrix} K &= \{\begin{pmatrix} 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 3 \end{pmatrix}\} = K \begin{pmatrix} 1 & 2 \end{pmatrix} \\ \begin{pmatrix} 1 & 3 \end{pmatrix} K &= K \begin{pmatrix} 1 & 3 \end{pmatrix} \\ \begin{pmatrix} 2 & 3 \end{pmatrix} K &= K \begin{pmatrix} 2 & 3 \end{pmatrix} \\ \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} K &= K = K \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \end{aligned}$$

But  $H = \{1, \begin{pmatrix} 1 & 2 \end{pmatrix}\}$  is not normal in  $S_3$ .

$$\begin{aligned} \begin{pmatrix} 1 & 3 \end{pmatrix} H &= \{\begin{pmatrix} 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}\} \\ H \begin{pmatrix} 1 & 3 \end{pmatrix} &= \{\begin{pmatrix} 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}\} \end{aligned}$$

### Proposition 4.1

Let  $K \trianglelefteq G$ . TFAE (The following are equivalent):

- i.  $gK = Kg \quad \forall g \in G$
- ii.  $gKg^{-1} = K \quad \forall g \in G$
- iii.  $gkg^{-1} \in K \quad \forall k \in K, g \in G$

*Proof.*

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

$$(ii) \implies (iii)$$

$$(iii) \implies (i)$$

For any  $k \in K$ ,  $g \in G \exists k' \in K$  s.t.  $gkg^{-1} = k'$

$$\begin{aligned}
 &\implies gk = k'g \in Kg \\
 &\implies gK \subseteq Kg
 \end{aligned}$$

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

$$\begin{aligned}
 &\implies kg = gk'' \\
 &\implies Kg \subseteq gK \\
 &\implies gK = Kg.
 \end{aligned}$$

□

#### Example 4.2

- $\{e\} \trianglelefteq G$ ,  $G \trianglelefteq G$ .
- If  $G$  is abelian, all subgroups are normal. Since if  $k \in K$ ,  $g \in G$  and  $K \leq G$  then  $gkg^{-1} = gg^{-1}k = k \in K$ .
- Kernels of homomorphisms are normal subgroups (Sheet 1, q9)  $\implies A_n \trianglelefteq S_n$  since  $A_n = \ker \text{sgn}$
- $D_{2n} = \left\langle \underbrace{r, t}_{\text{generators}} \mid \underbrace{r^n = e, t^2 = e, trt = r^{-1}}_{\text{relations}} \right\rangle$ . Then  $\langle r \rangle \trianglelefteq D_{2n}$ .

Clearly  $r^i r^j r^{-i} = r^j \in \langle r \rangle$ .

$$\begin{aligned}
 \text{Also, } (r^i t) r^j (r^i t)^{-1} &= r^i t r^j t r^{-i} \\
 &= r^i r^{-j} t t r^{-i} \text{ as } t r^k = r^{-1} t r^{k-1} \dots = r^{-k} t \\
 &= r^{-j} \in \langle r \rangle.
 \end{aligned}$$

Or use the following lemma.

**Lemma 4.1**

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

*Proof.*

$$G = K \dot{\cup} gK \text{ for any } g \in G \setminus K$$

as  $g$  is in  $gK$  but not  $K$  so  $gK \neq K$

$$= K \dot{\cup} Kg \text{ by } ??$$

as  $g$  is in  $Kg$  but not  $K$  so  $Kg \neq K$

$$\implies gK = Kg \forall g \in G, \text{ as if } g \in K \text{ then we just get } K = K.$$

□

**Theorem 4.1**

If  $K \trianglelefteq G$ , the set  $(G : K)$  of the left cosets of  $K$  in  $G$  is a group under coset multiplication i.e.  $gK \circ hK = ghK$ .

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

*Proof.* We need to check that coset multiplication is well defined.

$$\text{i.e. } gK = \hat{g}K$$

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

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

By  $??$ ,

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

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

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

$$\implies h^{-1}\hat{g}^{-1}gh \in K \text{ since } K \trianglelefteq G$$

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

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

$$\implies ghK = \hat{g}\hat{h}K \text{ by ??}.$$

So coset multiplication is well-defined. Group axioms now follow easily.

- By construction coset multiplication is closed as  $ghK \in (G : H)$  for  $g, h \in G$ .
- Identity given by  $eK = K$
- $(gK)^{-1} = g^{-1}K$
- Associativity holds since it does in  $G$ , to check:  $(gKhK)lK = (gh)lK = g(hl)K = gK(hKlK)$ .

□

### Example 4.3

i.

$$\begin{aligned} S_n/A_n &= \left( \left\{ A_n, \begin{pmatrix} 1 & 2 \\ & \end{pmatrix} A_n \right\}, \circ \right) \\ &\cong C_2. \end{aligned}$$

ii.

$$D_8 = \langle a, b : a^4 = e = b^2, bab = a^{-1} \rangle$$

Let  $K = \{1, a^2\}$ .

Claim:  $K \trianglelefteq D_8$ .

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

$$a^i a^2 a^{-i} = a^2 \in K.$$

$$|D_8|/|K| = 4 = |(D_8 : K)|.$$

4 distinct left cosets:

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

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

Note  $aKaK = a^2K = K$  This is isomorphic to ??.

- iii. Recall the subgroups of  $(\mathbb{Z}, +)$  are precisely the groups  $(n\mathbb{Z}, +)$  where  $n \in \mathbb{N} \cup \{0\}$ ,  $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ . Since  $(\mathbb{Z}, +)$  is abelian, all subgroups are normal,  $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ .

Suppose  $n = 5$ , cosets given by,

$$5\mathbb{Z} = \{5k : k \in \mathbb{Z}\}$$

$$1 + 5\mathbb{Z} = \{1 + 5k : k \in \mathbb{Z}\}$$

$$2 + 5\mathbb{Z} = \{2 + 5k : k \in \mathbb{Z}\}$$

$$3 + 5\mathbb{Z} = \{3 + 5k : k \in \mathbb{Z}\}$$

$$4 + 5\mathbb{Z} = \{4 + 5k : k \in \mathbb{Z}\}.$$

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

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

*Claim:*  $(\mathbb{Z}/5\mathbb{Z}, \underbrace{\circ}_{\text{coset 'addition'}}) \cong (\{0, 1, 2, 3, 4\}, +_5)^a$

We define a map  $\theta : n + 5\mathbb{Z} \rightarrow \bar{n}$  where  $n \equiv \bar{n} \pmod{5}$  and  $\bar{n} \in \{0, 1, 2, 3, 4\}$ .

Well-defined map:

$$\begin{aligned} & \text{if } n + 5\mathbb{Z} = m + 5\mathbb{Z} \\ \implies & -m + n \in 5\mathbb{Z} \text{ by ??} \\ \implies & -m + n \equiv 0 \pmod{5} \\ \implies & n \equiv m \pmod{5} \\ \implies & \bar{n} \equiv \bar{m} \end{aligned}$$

homomorphism:

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

In general  $(\mathbb{Z}/n\mathbb{Z}, \circ) \cong (\{0, 1, \dots, n-1\}, +_n)$ .

<sup>a</sup>It is coset 'addition' as it is abelian

Recall the definition of a homomorphism, ??,

$\text{Im}(\theta) = \{\theta(g) : g \in G\} \leq H$  (??).  $\ker(\theta) = \{g \in G : \theta(g) = e_H\} \trianglelefteq G$  (Sheet 1).

#### Theorem 4.2 (1st Isomorphism Theorem)

Let  $G, H$  be groups and  $\theta : G \rightarrow H$  a group homomorphism. Then

$$\begin{aligned}\text{Im } \theta &\leq H \\ \ker \theta &\trianglelefteq G \\ \text{and } G/\ker \theta &\cong \text{Im } \theta.\end{aligned}$$

#### Definition 4.2 (Simple group)

A group is called *simple* if its only normal subgroups are  $\{e\}$  and  $G$ , e.g.  $C_p$  where  $p$  is prime.

---

### Aside

#### Definition 4.3

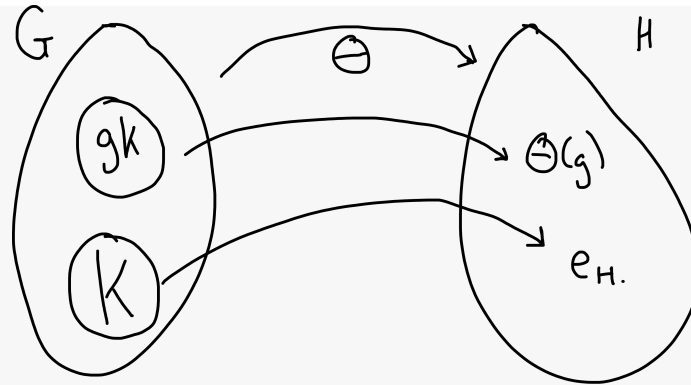
Suppose  $f : A \rightarrow B$

- i.  $f$  is *injective* (one-to-one) if  $a_1, a_2 \in A$ ,  $f(a_1) = f(a_2) \implies a_1 = a_2$  (each element of  $A$  maps to a different element of  $B$ ).
- ii.  $f$  is *surjective* (onto) if given  $b \in B \exists a \in A$  such that  $f(a) = b$  (every element in  $B$  is 'hit').
- iii.  $f$  is *bijective* if  $f$  is both injective and surjective.

---

*Proof (1st Isomorphism Theorem).* Let  $K = \ker \theta$ , we need to construct an isomorphism

$$\begin{aligned}\phi : G/\ker \theta &\rightarrow \text{Im } \theta \\ gK &\mapsto \theta(g).\end{aligned}$$



Need  $\phi$  well-defined:

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

Need  $\phi$  to be a homomorphism:

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

$\phi$  surjective: If  $\theta(g) \in \text{Im } \theta$  then  $\phi(gK) = \theta(g)$ .

$\phi$  injective: Suppose  $\phi(gK) = \phi(hK)$

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

□

*Remark 12.* By the ??,  $\text{Im } \theta \cong G/\ker \theta$ , a homomorphic image of  $G$  is isomorphic to a quotient of  $G$ .

## §4.1 Examples

### Example 4.4

$$\begin{aligned}\operatorname{sgn} : S_n &\rightarrow (\{\pm 1\}, \times) \\ \sigma &\mapsto \operatorname{sgn}(\sigma). \\ \operatorname{Im}(\operatorname{sgn}) &= (\{\pm 1\}, \times) \\ \ker(\operatorname{sgn}) &= A_n \\ \implies S_n/A_n &\cong (\{\pm 1\}, \times) \cong C_2 \\ \implies |A_n| &= \frac{|S_n|}{2}\end{aligned}$$

### Example 4.5

$$\begin{aligned}\theta : (\mathbb{R}, +) &\rightarrow (\mathbb{C} \setminus \{0\}, \times) \\ r &\mapsto e^{2\pi i r} \\ \text{Note, } \theta(r+s) &= \theta(r)\theta(s) \\ \operatorname{Im}(\theta) &= S^1 = \{z \in \mathbb{C} : |z| = 1\} \text{ unit circle} \\ \ker(\theta) &= (\mathbb{Z}, +) \trianglelefteq (\mathbb{R}, +). \\ (\mathbb{R}, +)/(\mathbb{Z}, +) &\cong S^1.\end{aligned}$$

### Example 4.6

Recall ?? and ??.

$$\begin{aligned}GL_2(\mathbb{R}) &= \{2 \times 2 \text{ matrices with entries in } \mathbb{R}, \det \neq 0\}. \\ \det : GL_2(\mathbb{R}) &\rightarrow (\mathbb{R} \setminus \{0\}, \times) \\ M &\mapsto \det(M) \\ \det(AB) &= \det A \det B \text{ so is a homomorphism.} \\ \operatorname{Im} \det &= (\mathbb{R} \setminus \{0\}, \times)\end{aligned}$$



$$\text{since } \det \begin{pmatrix} \alpha & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} = \alpha \in \mathbb{R} \setminus \{0\}$$

$$\ker \det = \mathrm{SL}_2(\mathbb{R}) = \{2 \times 2 \text{ matrices with entries in } \mathbb{R}, \det = 1\}.$$

$$\implies \mathrm{SL}_2(\mathbb{R}) \trianglelefteq \mathrm{GL}_2(\mathbb{R})$$

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

#### Example 4.7

$$\theta : (\mathbb{Z}, +) \rightarrow (\{0, 1, \dots, n-1\}, +_n)$$

$$n \mapsto \bar{n}$$

$$\ker \theta = n\mathbb{Z}.$$

#### Lemma 4.2

Given  $K \trianglelefteq G$ , the *quotient map*  $q : G \rightarrow G/K$  with  $g \mapsto gK$  is a surjective group homomorphism.

*Proof.*  $q(ab) = (ab)K = aKbK = q(a)q(b)$ . So  $q$  is a group homomorphism. Also for all  $aK \in G/K$ ,  $q(a) = aK$ . So it is surjective.  $\square$

Note that the kernel of the quotient map is  $K$  itself.

#### Lemma 4.3

A homomorphism  $\theta : G \rightarrow H$  is injective iff  $\ker \theta = \{e_G\}$ .

*Proof.* ( $\implies$ ): Suppose  $\theta(g) = e_H = \theta(e_G)$ . So injectivity  $\implies g = e_G$ .

( $\impliedby$ ):

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

$$\begin{aligned} \implies h^{-1}g &= e_G \\ \implies h &= g. \end{aligned}$$

□

$$\begin{aligned} \text{Recall if } N \trianglelefteq G, g \in G, n \in N \\ \implies gng^{-1} &\in N \\ \implies gng^{-1} &= \hat{n} \text{ for some } \hat{n} \in N \\ \implies gn &= \hat{n}g. \end{aligned}$$

This allows us to reorder our elements and helps in proving the following lemma.

**Lemma 4.4**

- i. Let  $N \trianglelefteq G, H \leq G$ . Then  $NH = \{nh : n \in N, h \in H\} \leq G$ .
- ii. Let  $N \trianglelefteq G, M \trianglelefteq G$  then  $NM \trianglelefteq G$ .

*Proof.*

- i. Closure,  $nh, \overline{nh} \in NH$

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

$$\text{id} = e = ee \in NH$$

inverse:

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

- ii. we need to check normality

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

□

## §5 Direct Products and Small Groups

### §5.1 Direct Products

#### Definition 5.1 ((External) direct product of groups)

Let  $H$  and  $K$  be groups. We can construct the (external) *direct product*,  $H \times K$ , with a set  $\{(h, k), h \in H, k \in K\}$  and an operation:

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

i.e. component wise multiplication. Then  $(H \times K, *)$  is a group

*Proof.* closure:  $H$  is a group  $\implies h_1 h_2 \in H$ ,  $K$  is a group  $\implies k_1 k_2 \in K$

identity:  $(e_H, e_K)$

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

associativity since group operation in both  $H$  and  $K$  are associative.  $\square$

*Remark 13.*

1. If  $H$  and  $K$  are both finite,  $|H \times K| = |H||K|$ .
2.  $H \times K$  is abelian iff  $(h_1, k_1) * (h_2, k_2) = (h_2, k_2) * (h_1, k_1) \quad \forall h_1, h_2 \in H, k_1, k_2 \in K$   
 iff  $(h_1 h_2, k_1 k_2) = (h_2 h_1, k_2 k_1)$   
 iff  $h_1 h_2 = h_2 h_1$  and  $k_1 k_2 = k_2 k_1$   
 iff  $H$  is abelian and  $K$  is abelian.
- 3.

$$\begin{aligned}H &\cong \{(h, e_K) : h \in H\} \leq H \times K \\ K &\cong \{(e_H, k) : k \in K\} \leq H \times K\end{aligned}$$

#### Example 5.1

1.

$$\begin{aligned}C_2 \times C_2 &= \langle x \rangle \times \langle y \rangle \\ &= \{e, x\} \times \{e, y\} \\ \text{elements : } &(e, e), (x, e), (e, y), (x, y)\end{aligned}$$

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

This is the called the Klein 4-group and is  $\cong$  to ??.

Note  $o((x, e)) = o((e, y)) = o((x, y)) = 2$ . So  $C_2 \times C_2 \not\cong C_4$ , as there is no element of order 4.

2. However,  $C_2 \times C_3 \cong C_6$  (Sheet 2, qn 10).

### Lemma 5.1

Let  $(h, k) \in H \times K$  where  $H, K$  are groups. Then  $o((h, k)) = \text{lcm}(o(h), o(k))$ .

*Proof.* Let  $n = o((h, k))$  and  $m = \text{lcm}(o(h), o(k))$ .  
Then  $h^m = e_H, k^m = e_K$  by ??.

$$\begin{aligned} \text{So } (h, k)^m &= (h^m, k^m) \\ &= (e_H, e_K) \end{aligned}$$

$$\implies n \mid m \text{ by ??}.$$

$$\begin{aligned} \text{Also, } (h, k)^n &= (h^n, k^n) \\ &= (e_H, e_K) \end{aligned}$$

$$\implies o(h) \mid n \text{ and } o(k) \mid n \text{ by ??}.$$

$$\implies \mid n.$$

Thus we know when  $C_m \times C_n \cong C_{mn}$  (Sheet 2, qn 10). □

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

### Proposition 5.1 (Direct Product Theorem)

Let  $G$  be a group with subgroups  $H$  and  $K$ , if:

1. each element of  $G$  can be written as  $hk$ , for some  $h \in H, k \in K$ ,
2.  $H \cap K = \{e\}$
3.  $hk = kh \forall h \in H, k \in K$

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

*Proof.*

$$\begin{aligned}\text{Let } \theta : H \times K &\rightarrow G \\ (h, k) &\mapsto hk.\end{aligned}$$

$\theta$  is a homomorphism:

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

$\theta$  is injective:

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

$\theta$  is surjective by ??.

So  $\theta$  is an isomorphism as required.  $\square$

*Remark 14.* There are alternative equivalent definitions of internal direct product.  $G$  is the internal direct product of subgroups  $H$  and  $K$  if:

- 1'.  $H \trianglelefteq G, K \trianglelefteq G$
- 2'.  $H \cap K = \{e\}$
- 3'.  $HK = G$

*Proof.* We need to show  $??, ??, ?? \iff ??, ??, ??$ .

( $\implies$ ) we show  $K \trianglelefteq G$ .

Let  $k \in K, g = h_1 k_1 \in G$  by ??.

$$\begin{aligned}gkg^{-1} &= h_1 \underbrace{k_1 k k_1^{-1}}_{\bar{k} \in K} h_1^{-1} \\ &= \bar{k} \in K \text{ by ??}\end{aligned}$$

Similarly  $H \trianglelefteq G$ .

And  $?? \implies ??$ .

( $\Leftarrow$ ) need to show ??.

$h \in H, k \in K$  consider

$$\begin{aligned} h^{-1} \underbrace{k^{-1}hk}_{\in H} &\in H, \text{ since } H \trianglelefteq G \\ &\in K, \text{ since } K \trianglelefteq G \\ \implies h^{-1}k^{-1}hk &= H \cap K = \{e\} \text{ by ??} \\ \implies hk &= kh \end{aligned}$$

□

### Example 5.2

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

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

## §5.2 Small Groups

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

$$\begin{aligned} r : z &\mapsto e^{2\pi i/n} z \\ t : z &\mapsto \bar{z} \end{aligned}$$

elements of

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

### Lemma 5.2

Now suppose  $G$  is a group,  $n \geq 3$ , with  $|G| = 2n$ , and  $\exists b \in G$  with  $o(b) = n$  and  $a \in G$ ,  $o(a) = 2$  and  $aba = b^{-1}$ . Then  $G \cong D_{2n}$ .

*Proof.* Note  $\langle b \rangle \trianglelefteq G$  since of index two, ??.

Also  $a \notin \langle b \rangle$ , since  $aba = aab = b$  as  $a \in \langle b \rangle \implies ab = ba$ .

$$\begin{aligned}\text{So } G &= \langle b \rangle \cup \langle b \rangle a \\ &= \{e, b, \dots, b^{n-1}, a, ba, \dots, b^{n-1}a\}\end{aligned}$$

Furthermore

$$\begin{aligned}ab &= b^{-1}a \\ \implies ab^k &= (ab)b^{k-1} \\ &= b^{-1}ab^{k-1} \\ &= b^{-2}ab^{k-2} \\ &\vdots \\ &= b^{-k}a \\ \text{So } (b^k a)(b^k a) &= b^k b^{-k} aa \\ &= e.\end{aligned}$$

We can check

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

is an isomorphism. □

### §5.2.1 Classifying groups of small order

#### Example 5.3

- If  $|G| = 1$ ,  $G = \{e\}$
- If  $|G| = 2 \implies G \cong C_2$ , as we have identity and an another element which must be a self inverse or we can prove by ??.
- If  $|G| = 3 \implies G \cong C_3$  by ?? (3 is prime).
- If  $|G| = 5 \implies G \cong C_5$  by ?? (5 is prime).
- If  $|G| = 7 \implies G \cong C_7$  by ?? (7 is prime).

#### Lemma 5.3

If  $|G| = 4$ ,  $G$  is isomorphic to  $C_4$  and  $C_2 \times C_2$ , both abelian.

*Proof.* By ??, if  $1 \neq g \in G$  then  $o(g) \mid 4$ .

$$\begin{aligned} \text{If } \exists g \in G \text{ s.t. } o(g) = 4 \\ \implies G \cong C_4 \end{aligned}$$

Suppose not, then let

$$\begin{aligned} 1 \neq a \in G &\implies o(a) = 2 \\ &\implies G \text{ is abelian (qn 7, sheet 1)} \\ &\implies C_2 \cong \langle a \rangle \trianglelefteq G. \end{aligned}$$

Let  $b \in G \setminus \langle a \rangle$ , then  $1 \neq b \in G$  so  $C_2 \cong \langle b \rangle \trianglelefteq G$ .

Also,  $\langle a \rangle \cap \langle b \rangle = \{e\}$ .

Consider the element  $ab$ :

if  $ab = e \implies a = b^{-1} = b \nmid$ .

if  $ab = a \implies b = e \nmid$ .

if  $ab = b \implies a = e \nmid$ .

So

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

□

#### Lemma 5.4

If  $|G| = 6$ ,  $G$  is isomorphic to  $C_6$  and  $D_6 \cong S_3$ . Note  $C_6 \not\cong D_6$  as  $C_6$  is abelian and  $D_6$  is not.

*Proof.* Let  $1 \neq g \in G \implies o(g) = 2, 3$  or  $6$  by ??. If all non-identity elements have order 2  $\implies |G|$  is a 2-power  $\nmid$  (qn 7, Sheet 1).

So  $\exists b \in G, o(b) = 3$  (Note if  $o(g) = 6$  then  $o(g^2) = 3$ ).

$C_3 \cong \langle b \rangle \trianglelefteq G$ , RHS by ?? (since of index 2).

Let  $a \in G \setminus \langle b \rangle$ ,

$$\implies a^2 \in \langle b \rangle.$$

As  $a\langle b \rangle \in G/\langle b \rangle$  and  $|G/\langle b \rangle| = 2$ , the group has order 2. So  $(a\langle b \rangle)^2 = a^2\langle b \rangle = e = \langle b \rangle$  by ??. Then  $a^2 \in \langle b \rangle$  by ??.



If  $a^2 = b$  or  $b^2$  then  $o(a) = 6$ , as if  $a^2 = b$ ,  $a^3 = ab$  and if  $ab = e$ ,  $a = b^{-1} \in \langle b \rangle \nmid$ .  
 $o(a) = 6 \implies G \cong C_6$ .

Suppose  $a^2 = 1$ .

Also,  $aba^{-1} = aba \in \langle b \rangle$  as  $\langle b \rangle \trianglelefteq G$ .

$$\begin{aligned} \text{If } aba^{-1} = e &\implies b = e \nmid \\ &= b \implies ab = ba \\ &\implies o(ab) = 6 \\ &\implies G \cong C_6. \\ &= b^2 = b^{-1}. \end{aligned}$$

So  $o(a) = 2$ ,  $o(b) = 3$ ,  $aba^{-1} = b^{-1} \implies G \cong D_6$ . □

## §5.2.2 Groups of order 8

### Lemma 5.5

If  $G$  has order 8, then either  $G$  is abelian (i.e.  $\cong C_8, C_4 \times C_2$  or  $C_2 \times C_2 \times C_2$ ), or  $G$  is not abelian and isomorphic to  $D_8$  or  $Q_8$  (dihedral or quaternion).

*Proof.* Consider the different possible cases:

- If  $G$  contains an element of order 8, then  $G \cong C_8$ .
- If all non-identity elements have order 2  $\implies G$  is abelian (Sheet 1, Q7). If all non-identity elements have order 2  $\implies G$  abelian (qn7, Sheet 1). Let  $1 \neq a \in G$ , then  $C_2 \cong \langle a \rangle \trianglelefteq G$ , RHS as  $G$  is abelian. Choose  $b \notin \langle a \rangle$ ,  $\langle a, b \rangle = \{1, a, b, ab\}$

$$\begin{aligned} \text{Choose } b \notin \langle a \rangle, \\ \langle a, b \rangle &= \{1, a, b, ab\} \\ &= \langle a \rangle \langle b \rangle \\ &\cong \langle a \rangle \times \langle b \rangle \text{ by ??}. \end{aligned}$$

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

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

- Now suppose  $\exists g \in G, o(g) > 2 \implies \exists a \in G, o(a) = 4$  (if we have  $o(a) = 8$ , then  $o(a^2) = 4$ ).  $C_4 \cong \langle a \rangle \trianglelefteq G$ , RHS by ?? (since of index 2).

$$\begin{aligned} & \text{Let } b \in G \setminus \langle a \rangle \\ & \implies b^2 \in \langle a \rangle. \end{aligned}$$

(Same reasoning as in  $n = 6$ , alternative proof is  $b^2 \in \langle a \rangle$  or  $b^2 \in b\langle a \rangle$ , if  $b^2 = ba^n \implies b = a^n \nmid$  so  $b^2 \in \langle a \rangle$ ).

$$\begin{aligned} & \text{If } b^2 = a \text{ or } a^3 \\ & \implies o(b) = 8 \implies G \cong C_8. \end{aligned}$$

$$\begin{aligned} & \text{Else } b^2 = e \text{ or } a^2 \\ & \text{Now } bab^{-1} \in \langle a \rangle \text{ since } \langle a \rangle \trianglelefteq G \\ & \quad = a^i \text{ for some } i. \\ & \implies b^2ab^{-2} = b(bab^{-1})b^{-1} \\ & \quad = ba^ib^{-1} \\ & \quad = (bab^{-1})^i \text{ as } (bab^{-1})(bab^{-1}) = ba^2b \\ & \quad = a^{i^2} \\ & \text{But } b^2 \in \langle a \rangle \implies b^2ab^{-2} = a \end{aligned}$$

as  $b^2 = a^m$  so must commute with  $a$ .

$$\begin{aligned} & \implies i^2 \equiv 1 \pmod{4} \\ & \implies i \equiv \pm 1 \pmod{4}. \end{aligned}$$

- When  $i \equiv 1 \pmod{4}$ ,  $bab^{-1} = a \implies ba = ab$ . So  $G = \langle a \rangle \cup b\langle a \rangle$  is abelian.
  - \* If  $b^2 = e$ , then  $G = \langle a \rangle \langle b \rangle \cong \langle a \rangle \times \langle b \rangle \cong C_4 \times C_2$ .
  - \* If  $b^2 = a^2$ , then  $(ba^{-1})^2 = e$ . So  $G = \langle a, ba^{-1} \rangle \cong C_4 \times C_2$ .
- If  $i \equiv -1 \pmod{4}$ , then  $bab^{-1} = a^{-1}$ .
  - \* If  $b^2 = e$ , then  $G = \langle a, b : a^4 = e = b^2, bab^{-1} = a^{-1} \rangle$ . So  $G \cong D_8$  by definition.
  - \* If  $b^2 = a^2$ , then we have  $G \cong Q_8$ , a new group called the quaternion group.

To show all 5 groups are different,  $C_8$  has an element of order 8,  $C_4 \times C_2$  does not.  $C_4 \times C_2$  has an element of order 4 whilst  $C_2 \times C_2 \times C_2$  does not have elements of order 2 or 4.

$D_8$  and  $Q_8$ ,  $Q_8$  has 6 elements of order 4, but  $D_8$  only has 2, so non-isomorphic.  $\square$

### §5.2.3 Realisations of $Q_8$

1.

$$\begin{aligned} Q_8 &= \{\pm 1, \pm i, \pm j, \pm k\} \\ \text{with } ij &= k, jk = i, ki = j \\ ji &= -k, kj = -i, ik = -j \\ i^2 &= j^2 = k^2 = -1 \\ \text{so } o(i) &= o(j) = o(k) = 4, o(-1) = 2. \end{aligned}$$

2.

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \right\} \leq \text{SL}_2(\mathbb{C})$$

3.

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

If  $|G| = 9$ , we will show later that groups of order  $p^2$  (where  $p$  is prime) are abelian, so either  $G \cong C_9$ .

Or all non-identity elements have order 3 by ?? Choose  $e \neq a \in G, b \in G \setminus \langle a \rangle$

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

If  $|G| = 10 \implies G \cong C_{10}$  or  $D_{10}$  (qn 12, Sheet 2, use proof similar to order 8 not 6).

*Remark 15.* There are lots of groups of order  $2^k$ . e.g. 10 of order 16 and approximately 50,000,000,000 of order  $2^{10}$ .

## §6 Group Actions

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

### Definition 6.1 (Group action)

Let  $G$  be a group and  $X$  a non-empty set. We say that  $G$  *acts* on  $X$  if there is a mapping

$$\begin{aligned}\rho : G \times X &\rightarrow X \\ (g, x) &\mapsto \rho(g, x) = g(x)\end{aligned}$$

such that

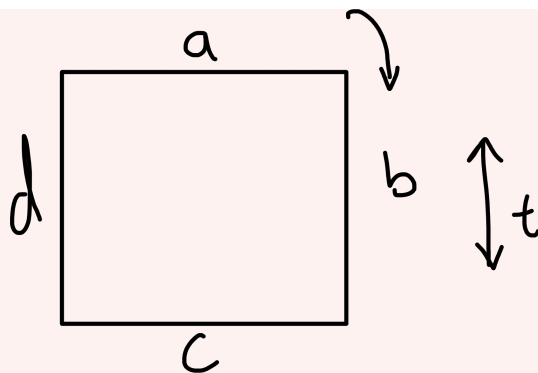
0. if  $g \in G, x \in X$ , then  $\rho(g, x) = g(x) \in X$  (implied by notation, but something we should check).
1.  $\rho(gh, x) = \rho(g, \rho(h, x))$ . shorthand:  $gh(x) = g(h(x))$ .
2.  $\rho(e, x) = x$ , shorthand:  $e(x) = x$ .

When  $G$  acts on a set it maps elements of  $X$  to  $X$  in a way that the multiplication of  $G$  is respected.

### Example 6.1

- i. trivial action  $\rho(g, x) = x \quad \forall x \in X, g \in G$ .
- ii.  $S_n$  acts on  $X = \{1, 2, \dots, n\}$  by permuting the elements of  $X$ . e.g.  $S_3$  acts on  $\{1, 2, 3\}$ ,  $\sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \in S_3 : \sigma(1) = 2, \sigma(2) = 1, \sigma(3) = 3$ .  $\tau = \begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix} \in S_3$ ,  $\tau\sigma = \begin{pmatrix} 1 & 3 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$   
 $(\tau\sigma)(1) = 2, \tau(\sigma(1)) = \tau(2) = 3$ .  
 Similarly subgroups of  $S_n$  act on  $X$ .

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



$$t(a) = c$$

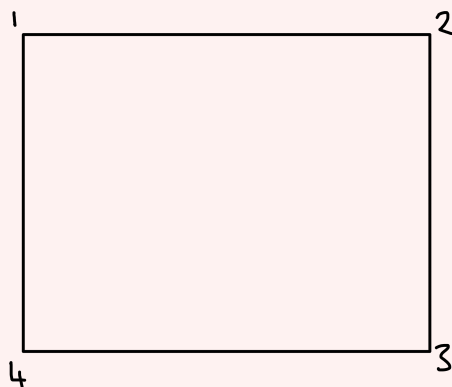
$$t(b) = b$$

$$r(a) = b.$$

$$t(c) = a$$

$$t(d) = d.$$

Also acts on the vertices of a square.



$$t(1) = 4$$

$$t(2) = 3$$

$$t(4) = 1$$

$$t(3) = 2.$$

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

$$G \times G \rightarrow G$$

$$(g, k) \mapsto gk.$$

Check:

0.  $gk \in G$  (by closure)

1.

$$\begin{aligned}\rho(gh, k) &= ghk \\ \rho(g, \rho(h, k)) &= \rho(g, hk) = ghk\end{aligned}$$

Or in shorthand:

$$\begin{aligned}gh(k) &= ghk \\ g(h(k)) &= g(hk) = ghk.\end{aligned}$$

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

v. We also have the  $G$  right regular action

$$\begin{aligned}G \times G &\rightarrow G \\ (g, k) &\mapsto kg^{-1}.\end{aligned}$$

(we need inverse for ?? to hold.)

vi.  $G$  acts on itself by *conjugation*

$$\begin{aligned}G \times G &\rightarrow G \\ (g, k) &\mapsto gkg^{-1}.\end{aligned}$$

Check:

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

1.

$$\begin{aligned}\rho(gh, k) &= ghk(gh)^{-1} \\ &= ghkh^{-1}g^{-1}\rho(g, \rho(h, k)) = \rho(g, hkh^{-1}) = g(hkh^{-1})g^{-1}\end{aligned}$$

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

vii. Let  $N \trianglelefteq G$ , then  $G$  acts on  $N$  by conjugation

$$\begin{aligned}G \times N &\rightarrow N \\ (g, n) &\mapsto gng^{-1}.\end{aligned}$$

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

(1) and (2) as above.

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

$$\begin{aligned} G \times (G : H) &\rightarrow (G : H) \\ (g, kH) &\mapsto gkH. \end{aligned}$$

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

1.

$$\begin{aligned} \rho(gh, kH) &= (gh)kH = ghkH. \\ \rho(g, \rho(h, kH)) &= \rho(g, hkH) \\ &= ghkH \end{aligned}$$

$$2. \quad \rho(e, kH) = ekH = kH.$$

*Remark 16.* Recall a permutation of a set  $X$  is a bijection of  $X$ ,  $??$ . We have commented that a bijection  $f : X \rightarrow X$  has a 2-sided inverse, i.e.  $\exists g : X \rightarrow X$  s.t.

$$\begin{aligned} f \circ g(x) &= x \quad \forall x \in X \\ g \circ f(x) &= x \quad \forall x \in X. \end{aligned}$$

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

$f \circ g(x) = x \quad \forall x \in X \implies f$  is surjective, as  $f$  is mapping to all elements in  $X$   
 $g \circ f(x) = x \quad \forall x \in X \implies f$  is injective, as if  $f$  took two elements to the same place then  $g$  wouldn't be able to split them up.

Note 2-sided is necessary:

$$\begin{array}{ll} \phi : \mathbb{Z} \rightarrow \mathbb{Z} & \psi : \mathbb{Z} \rightarrow \mathbb{Z} \\ x \mapsto 2x & 2x \mapsto x \\ & 2x + 1 \mapsto 0 \\ \phi\psi = \text{id}. & \end{array}$$

### Lemma 6.1

Suppose the group  $G$  acts on the non-empty set  $X$ . Fix  $g \in G$ , then the map

$$\begin{aligned} \phi_g : X &\rightarrow X \\ x &\mapsto \rho(g, x) = g(x) \end{aligned}$$

is a permutation of  $X$ , i.e.  $\phi_g \in \text{Sym}(X)$ .

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

$$\begin{aligned}\phi_{g^{-1}} \circ \phi_g(x) &= \phi_{g^{-1}}(\rho(g, x)) \\ &= \rho(g^{-1}, \rho(g, x)) \\ &= \rho(g^{-1}g, x) \text{ since } \rho \text{ is a group action, } ?? \\ &= \rho(e, x) \\ &= x \quad \forall x.\end{aligned}$$

Similarly,  $\phi_g \circ \phi_{g^{-1}}(x) = x \quad \forall x \in X$ . □

### Proposition 6.1

Suppose  $G$  acts on the set  $X$ . Then the map

$$\begin{aligned}\Phi : G &\rightarrow \text{Sym}(X) \\ g &\mapsto \phi_g\end{aligned}$$

as in ??, is a homomorphism.

*Proof.* We need to show  $\Phi$  is a homomorphism i.e. need

$$\begin{aligned}\Phi(gh) &= \Phi(g) \circ \Phi(h) \\ \text{i.e. } \phi_{gh} &= \phi_g \circ \phi_h.\end{aligned}$$

Let  $x \in X$

$$\begin{aligned}\phi_{gh}(x) &= \rho(gh, x) \\ &= \rho(g, \rho(h, x)) \\ &= \phi_g \circ \phi_h(x).\end{aligned}$$

This is true  $\forall x \in X$ . □

*Remark 17.*

1. ?? gives us an equivalent definition of a group action. If  $G$  is a group and  $X$  a set such that  $\Phi : G \rightarrow \text{Sym}(X)$  is a group homomorphism, then

$$\begin{aligned}\rho : G \times X &\rightarrow X \\ (g, x) &\mapsto \phi_g(x)\end{aligned}$$

where  $\Phi(g) = \phi_g$ , is group action.



2. Using notation of ??, by ??

$$G/\ker \Phi \cong \text{Im } \Phi \leq \text{Sym}(X).$$

Note

$$\begin{aligned} \ker \Phi &= \{g \in G : \Phi(g) = \text{id}_X \in \text{Sym}(X)\} \\ &= \{g \in G : \phi_g(x) = \rho(g, x) = x \ \forall x \in X\} \\ &\leq G, \text{ Kernels of homomorphisms are normal subgroups (Sheet 1, q9).} \end{aligned}$$

I.e. The kernel of the homomorphism is all those elements of  $G$  that fix every element of  $X$ , that act ‘trivially’.

### Definition 6.2 (Kernel of an Action)

The kernel of an action  $\rho : G \times X \rightarrow X$  is the kernel of the homomorphism  $\Phi : G \rightarrow \text{Sym}(X)$ .

### Definition 6.3 (Faithful Action)

An action of  $G$  on  $X$  is faithful if  $\ker \rho = \ker \Phi = \{e\}$ .

### Example 6.2

The kernels of ??

1. trivial action -  $\ker \Phi = G$ .
2.  $S_n$  acts on  $\{1, \dots, n\}$  - faithful.
3.  $D_8$  acts on the edges of a square - faithful.
4. left regular action - faithful.
5. conjugation -  $\ker \Phi = \{g \in G : \underbrace{gkg^{-1}}_{gk=kg} = k \ \forall k \in G\} = Z(G)$ , the centre of  $G$  are ‘the elements that commute with everything’.
6. conjugation of  $N \leq G$ .  $\ker \Phi = \{g \in G : gng^{-1} = n \ \forall n \in N\} = C_G(N)$ , the centraliser of  $N$  in  $G$ .
7. left coset action -

$$\begin{aligned} \ker \Phi &= \{g \in G : gkH = kH \ \forall k \in G\} \\ &= \{g \in G : k^{-1}gk \in H \ \forall k \in G\} \\ &= \{g \in G : g \in kHk^{-1} \ \forall k \in G\} \end{aligned}$$

$$\begin{aligned}
&= \bigcap_{k \in G} kHk^{-1} \\
&= \text{Core}_G(H) \trianglelefteq G \\
&\text{and } \underbrace{\text{Core}_G(H)}_{\text{core of } H} \leq H \text{ (we can set } k = e\text{)}.
\end{aligned}$$

*Useful Note for exam sheet:* If  $\ker \Phi = \{e\}$ , then  $G$  is isomorphic to a subgroup of  $\text{Sym}(X)$ , we write  $G \lesssim \text{Sym}(X)$ . So if  $|G| \nmid |\text{Sym}(X)|$  then  $\ker \Phi \neq \{e\}$ .

### Theorem 6.1 (Cayley's Theorem)

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

*Proof.* We take  $X$  to be  $G$  and consider the left regular action

$$\begin{aligned}
G \times G &\rightarrow G \\
(g, h) &\mapsto gh.
\end{aligned}$$

This is a faithful action as  $gh = h \ \forall h \in G \implies g = e$ . Thus we have an injective homomorphism

$$\Phi : G \rightarrow \text{Sym}(G)$$

and  $G \lesssim \text{Sym}(G)$ . □

### Definition 6.4 (Orbit)

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

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

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

### Example 6.3

The orbits of ??.

1. trivial action,  $\text{Orb}_G(x) = \{x\}$
2.  $S_n$  acts on  $\{1, \dots, n\}$  -  $\text{Orb}_G(1) = X$  (we can get  $(1 \ a)$  which maps  $x$  to any  $a$ ).  
If  $H = \langle (1 \ 2)(3 \ 4 \ 5) \rangle \leq S_n$  acting on  $X = \{1, 2, 3, 4, 5\}$  then  $\text{Orb}_G(1) = \{1, 2\}$  and  $\text{Orb}_G(3) = \{3, 4, 5\}$ .

3.  $D_8$  acts on the edges of a square -  $\text{Orb}_{D_8}(a) = \{a, b, c, d\}$ .
4. left regular action -  $\text{Orb}_G(k) = G$ , since  $g = g(k^{-1}k) = (gk^{-1})k$  for any  $g \in G$ .
5. conjugation -  $\text{Orb}_G(k)$

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

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

### Definition 6.5 (Transitive orbits)

We say  $G$  acts *transitively* on  $X$  if for any  $x \in X$ ,  $\text{Orb}_G(x) = X$ . Equivalently, if given any pair  $x_1, x_2 \in X \exists g \in G$  s.t.  $g(x_1) = x_2$ .

So the left regular action is a transitive action.

### Lemma 6.2

The distinct  $G$ -orbits form a partition of  $X$

*Proof.* Let  $x \in X$ , then  $x \in \text{Orb}_G(x)$  since  $x = ex$ .

Suppose  $z \in \text{Orb}_G(x) \cap \text{Orb}_G(y)$ , we show  $\text{Orb}_G(x) = \text{Orb}_G(z) = \text{Orb}_G(y)$ .

$z \in \text{Orb}_G(x) \implies \exists g \in G$  s.t.  $g(x) = z$ .

$$\begin{aligned}\text{Suppose } t \in \text{Orb}_G(z) &\implies \exists h \in G \text{ s.t. } h(z) = t \\ &\implies t = h(g(x)) = (hg)(x) \\ &\implies t \in \text{Orb}_G(x) \implies \text{Orb}_G(z) \subseteq \text{Orb}_G(x)\end{aligned}$$

Similarly  $g(x) = z$

$$\begin{aligned}x &= e(x) = (g^{-1}g)(x) = g^{-1}(z) \\ &\implies \text{Orb}_G(x) \subseteq \text{Orb}_G(z).\end{aligned}$$

Thus  $\text{Orb}_G(x) = \text{Orb}_G(z)$ . Similarly,  $\text{Orb}_G(z) = \text{Orb}_G(y)$ . □

*Remark 18.*

1. We could have proved ?? by noticing that  $x_1 \sim x_2$  if  $\exists g \in G$  s.t.  $g(x_1) = x_2$  is an equivalence relation.
2.  $\text{Orb}_G(x)$  is  $G$ -invariant, i.e.  $g(\text{Orb}_G(x)) \subseteq \text{Orb}_G(x)$ . Since if  $y \in \text{Orb}_G(x)$ ,  $y = hx$  for some  $h \in G \implies g(y) = g(h(x)) = (gh)(x) \in \text{Orb}_G(x)$ .

3.  $G$  is transitive on  $\text{Orb}_G(x)$ .

Let  $y, z \in \text{Orb}_G(x)$

$y = g(x), z = h(x)$ , for some  $g, h \in G$ .

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

### Definition 6.6 (Stabiliser)

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

$$\begin{aligned}\text{Stab}_G(x) &= \{g \in G : g(x) = x\} \\ &\subseteq G.\end{aligned}$$

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

### Example 6.4

The stabilisers of ??.

1. trivial action -  $\text{Stab}_G(x) = G$ .
2.  $S_n$  on  $X = \{1, 2, \dots, n\}$  -  $\text{Stab}_G(1) \cong S_{n-1}$ .
3.  $H = \langle \begin{pmatrix} 1 & 2 \\ 3 & 4 & 5 \end{pmatrix} \rangle$  on  $X$  -  $\text{Stab}_H(1) = \langle \begin{pmatrix} 3 & 4 & 5 \end{pmatrix} \rangle$ .
4.  $D_8$  -  $\text{Stab}_{D_8}(b) = \{e, t\}$ .
5. left regular action -  $\text{Stab}_G(k) = \{e\}$ ,  $gk = k \implies g = e$ .
6. conjugation -

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

I.e. all those elements of  $G$  that commute with  $k$ .

### Lemma 6.3

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

*Proof.*

- $e(x) = x \implies e \in \text{Stab}_G(x).$

- 

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

- 

$$\begin{aligned} & g \in \text{Stab}_G(x) \\ g(x) &= x \\ x &= e(x) = (g^{-1}g)(x) = g^{-1}(gx) \\ &= g^{-1}(x) \\ \implies g^{-1} &\in \text{Stab}_G(x). \end{aligned}$$

- Associativity is inherited from  $G$ .

□

*Remark 19.* Recall, ??

$$\begin{aligned} \Phi : G &\rightarrow \text{Sym}(X) \\ \ker \Phi &= \{g \in G : g(x) = x \forall x \in X\} \\ &= \bigcap \text{Stab}_G(x). \end{aligned}$$

### **Theorem 6.2 (Orbit-Stabiliser Theorem)**

Let  $G$  be a finite group acting on a non-empty set  $X$ . Then  $\text{Stab}_G(x) \leq G$  and

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

*Remark 20.* We actually prove that  $|G : \text{Stab}_G(x)|$ , the number of left cosets of  $\text{Stab}_G(x)$  in  $G$ , is equal to  $|\text{Orb}_G(x)|$ , a more general statement.

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

$$\begin{aligned} \theta : \text{Orb}_G(x) &\rightarrow (G : \text{Stab}_G(x)) \\ g(x) &\mapsto g \text{Stab}_G(x). \end{aligned}$$

$\theta$  is well-defined:

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

$\theta$  is injective:

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

$\theta$  is surjective:

$$\begin{aligned}
 &\text{Given } g \text{Stab}_G(x) \in (G : \text{Stab}_G(x)) \\
 &\text{then } g(x) \in \text{Orb}_G(x) \\
 &\text{and } \theta(g(x)) = g \text{Stab}_G(x).
 \end{aligned}$$

Thus  $\theta$  is a well-defined bijection. □

## §6.1 Application to Symmetry Groups of Regular Solids

Let  $S$  be a regular solid and  $V$  its vertices. The the symmetries of  $S$  are the isometries (distance preserving maps) of  $\mathbb{R}^2$  or  $\mathbb{R}^3$  that maps  $S$  to itself. The dual is the solid with vertices in the middle of each face of the input.

### §6.1.1 Tetrahedron (self-dual)

faces are 4 equilateral triangles.

Let  $G$  be group of symmetries of  $T$ , and  $X = \{\text{vertices of } T\} = \{1, 2, 3, 4\}$ . Then  $\exists$  a homomorphism

$$\Phi : G \rightarrow \text{Sym } X \cong S_4 \text{ ??}$$

Note  $\ker \Phi = \{e\}$ , if all vertices are fixed, then  $T$  fixed.

Consider  $G^+ \leq G$  be the subgroup of all rotations. The elements of  $G^+$  are as follows:

There are 4 such axes, giving 8 rotations of order 3 (these are all the 3-cycles in  $S_4$ ).

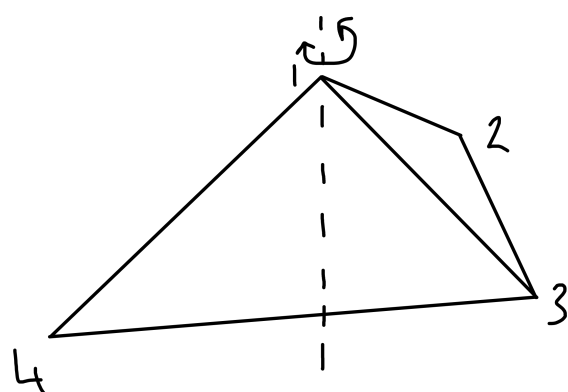
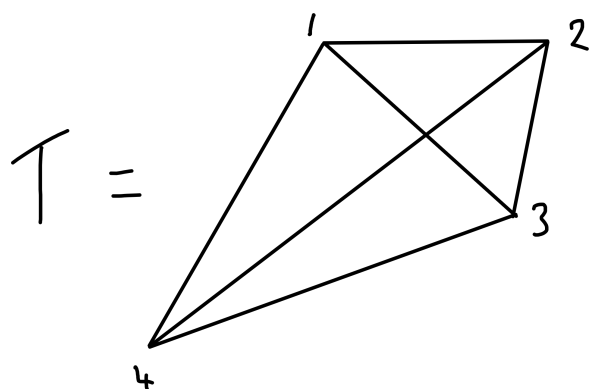


Figure 1: Rotation of  $2\pi/3$ , a 3-cycle  $(2 \ 3 \ 4)$ , and  $4\pi/3$  gives  $(2 \ 4 \ 3)$ .

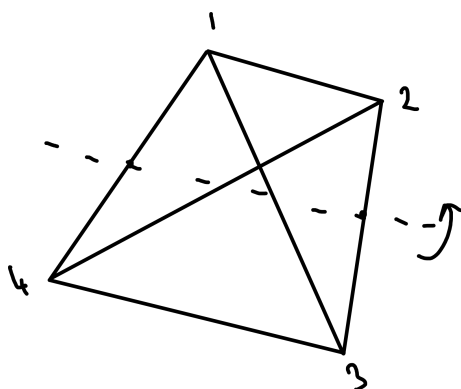


Figure 2: Rotation of  $\pi$ , a double transposition  $(1 \ 4)(2 \ 3)$ . We have one rotation for each pair of axes and we have 6 axes, so 3 such double transpositions.

and identity,

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

(only subgroup of order 12)

Now consider  $G$  (all symmetries). Clearly  $\text{Orb}_G(1) = \{1, 2, 3, 4\} = \text{Orb}_{G^+}(1)$ . Consider  $\text{Stab}_G(1)$ .

- Note if 3 vertices are fixed then  $T$  is fixed.
- Suppose vertices 1 and 2 are fixed

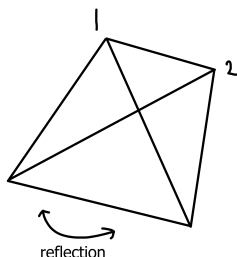


Figure 3: reflection through 1, 2 giving  $\begin{pmatrix} 3 & 4 \end{pmatrix} = \tau$ . We have such a reflection for each of the 6 edges.

- If just 1 is fixed we have order 3 rotation from before,  $\sigma$ .

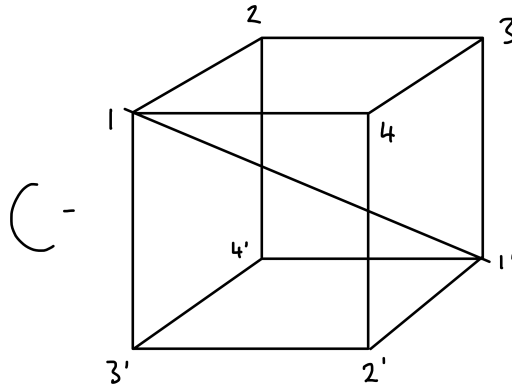
These are all elements in  $G$

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

(consider the effects of  $\sigma$  and  $\tau$  on the bottom face to see why  $\langle \sigma, \tau \rangle \cong D_6$ ).

Note  $\text{Stab}_{G^+}(1) = \langle \sigma \rangle$ . Also  $\begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 2 & 3 & 4 \end{pmatrix}$ .





### §6.1.2 Cube (dual to octahedron)

Let  $G^+$  be the group of rotations of  $C$ . Then  $G^+$  acts on set of diagonals  $X = \{D_1, D_2, D_3, D_4\}$ .

If a rotation,  $\sigma$ , that fixes all the diagonals, then  $\sigma = \text{id}$ . So we have an injective homomorphism

$$\Phi : G^+ \rightarrow \text{Sym}(X) \cong S_4.$$

Rotations:

- id

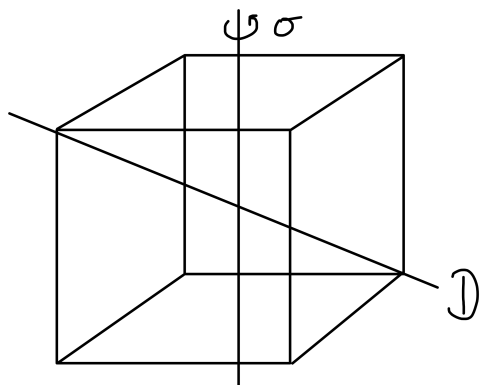


Figure 4:  $\sigma$  rotation of  $\pi/2$  corresponds to  $\begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix}$  in action on diagonals. There are 3 such axes giving 6 elements of order 4 and 3 of order 2.

- 
- 
-

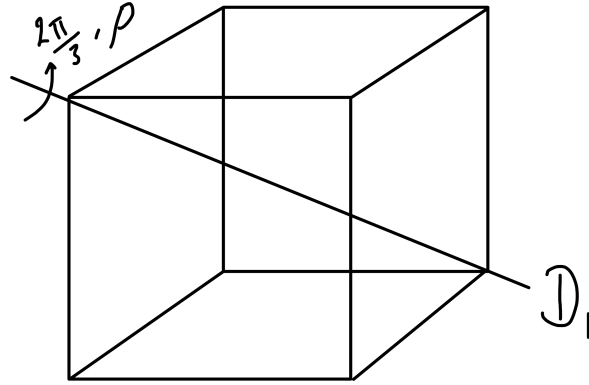


Figure 5:  $o(\rho) = 3$  corresponds to  $\begin{pmatrix} 2 & 3 & 4 \end{pmatrix}$ , we have 4 such axes giving eight elements of order 3  $(\rho, \rho^2)$ .

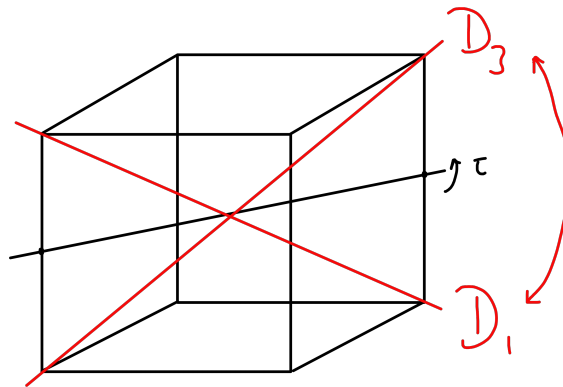


Figure 6: rotation of  $\pi$ ,  $o(\tau) = 2$  corresponds to  $\begin{pmatrix} 1 & 3 \end{pmatrix}$ . There are 6 such axes

I.e.  $G^+ \cong S_4$ . Note  $\text{Orb}_{G^+}(D_1) = \{D_1, D_2, D_3, D_4\}$ .  $\text{Stab}_{G^+}(D_1) = \{\rho, \tau'\}$  or consider  $G^+$  acting on vertex 1

$$\begin{aligned} |\text{Orb}_{G^+}(1)| &= 8 \\ |\text{Stab}_{G^+}(1)| &= |\langle \rho \rangle| = 3. \\ \implies |G^+| &= 24. \end{aligned}$$

Now consider full symmetry group of  $C$ , call it  $G$ .

Consider action on faces  $F_1, \dots, F_6$ , this yields an injective (or faithful) homomorphism as fixing all the faces fixes everything.

$$\begin{aligned} \Phi : G &\rightarrow \text{Sym}(F_i) \cong S_6. \\ |\text{Orb}(F_1)| &= 6. \\ \text{Stab}(F_1) &\cong D_8. \text{ Consider the opposite face} \\ \implies |G| &= 6 \times 8 = 48. \end{aligned}$$

So, action on diagonals is not faithful;  $\exists g \in G$   $g(D_i) = D_i$   $1 \leq i \leq 4$  but  $g \neq \text{id}$ .  $g$  can swap vertex  $i$  with  $i'$ , the diagonals will stay unchanged however. Alternatively, label vertices of  $C$  as  $\{(\pm 1, \pm 1, \pm 1)\}$ , then

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

If we label the faces of the cube like a dice (1 opposite 6, 2 opposite 5, 3 opposite 4) then  $g = \begin{pmatrix} 1 & 6 \\ 2 & 5 \\ 3 & 4 \end{pmatrix}$ .

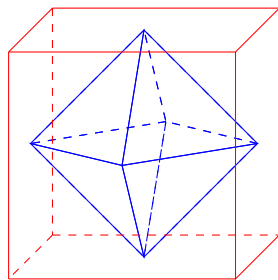
Then  $G \cong G^+ \times \langle g \rangle$ .

*Proof.*

$$\begin{aligned} G^+ &\trianglelefteq G \text{ by ?? (since of index 2)} \\ \langle g \rangle &\trianglelefteq G \text{ commutes with all rotations} \\ G^+ \cap \langle g \rangle &= \{e\} \\ |G^+ \langle g \rangle| &= 48 = |G|. \end{aligned}$$

□

In fact, we have also proved that the group of symmetries of an octahedron is  $S_4 \times C_2$  since the octahedron is the dual of the cube. (if you join the centres of each face of the cube, you get an octahedron)



### §6.1.3 Dodecahedron (dual to Icosahedron) - Non examinable

Let  $D$  be the dodecahedron.

- 12 regular pentagonal faces
- 30 edges
- 20 vertices

Let  $G^+$  = group of rotations of  $D$ .

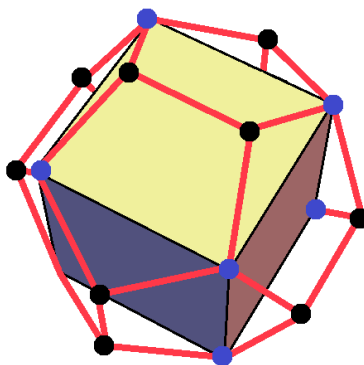
Let  $F$  be a face of  $D$ .

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

$$|\text{Stab}_{G^+}(F)| = 5 \text{ just rotating about face}$$

$$\implies |G^+| = 5 \times 12 = 60 \text{ by ??}.$$

There are five cubes embedded in  $D$ .



15 pairs of edges, 3 pairs per cube  $\implies$  5 cubes.

$G^+$  acts faithfully on cubes, giving us an injective map  $\Phi : G^+ \rightarrow S_5$ . And  $|G^+| = 60 \implies G^+ \cong A_5$  ( $A_5$  is the only subgroup of order 60 of  $S_5$ ). The smallest non-abelian simple group comes up as the rotational group of a dodecahedron.

We can find the elements of  $A_5$

- Rotations through opposite faces - 5 cycles (6 axes, 4 elements per axis giving 24 elements).
- Rotations through opposite vertices - 3 cycles.
- Rotations through opposite edges - double transpositions (15 such).

## §6.2 Another Application of ??

### Theorem 6.3 (Cauchy's Theorem)

Let  $G$  be a finite group and  $p$  a prime that divides  $|G|$ . Then there exists an element in  $G$  of order  $p$ .

*Proof.* Let

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

Let  $H = \langle h : o(h) = p \rangle \cong C_p$  acts on  $X$  as follows:

$$\begin{aligned} H \times X &\rightarrow X \\ (h, (x_1, x_2, \dots, x_p)) &\mapsto (x_2, x_3, \dots, x_p, x_1) \end{aligned}$$

in general

$$(h^i, (x_1, x_2, \dots, x_p)) \mapsto (x_{1+i}, x_{2+i}, \dots, x_{p+i})$$

suffices are taken modulo  $p$ .

Check this is a group action

0.

$$\begin{aligned} x_1 x_2 \dots x_p &= e \\ x_{i+1} x_{2+i} \dots, x_{p+i} &= [(x_1 x_2 \dots x_i)^{-1} (x_1 x_2 \dots x_i)] x_{i+1} x_{2+i} \dots, x_p x_1 x_2 \dots x_i \\ &= (x_1 x_2 \dots x_i)^{-1} x_1 x_2 \dots x_p (x_1 x_2 \dots x_i) \\ &= (x_1 x_2 \dots x_i)^{-1} e (x_1 x_2 \dots x_i) \\ &= e. \end{aligned}$$

1.

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

2.

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

Let  $\bar{x} = (x_1, x_2, \dots, x_p) \in X$ . As distinct orbits partition  $X$  (??)

$$\implies \sum_{\text{distinct orbits}} |\text{Orb}_H(\bar{x})| = |X|.$$

Note  $|X| = |G|^{p-1}$  (choose  $x_1, \dots, x_{p-1}$  then  $x_p$  is determined, we have  $|G|$  choices for each free variable).

$$\begin{aligned} p \mid |G| &\implies p \mid |X| \\ &\implies p \mid \sum_{\text{distinct orbits}} |\text{Orb}_H(\bar{x})| \end{aligned} \tag{3}$$

But by ??

$$\begin{aligned} |\text{Orb}_H(\bar{x})| \mid |H| &= p \\ \implies |\text{Orb}_H(\bar{x})| &= 1 \text{ or } p. \end{aligned}$$

Now,  $\bar{e} = (e, e, \dots, e) \in X$  and  $|\text{Orb}_H(\bar{e})| = 1$ . So  $\exists$  at least  $p - 1$  other orbits of length 1 by (??). So  $\exists \bar{x} \in X$  s.t  $|\text{Orb}_H(\bar{x})| = 1 \implies \bar{x} = (x, x, \dots, x)$  (has to look the same after permutation) with  $x \neq e$  and  $x^p = e$ .  $\square$

### §6.3 Conjugacy Action

$$\begin{aligned} G \times G &\rightarrow G \\ (g, h) &\mapsto ghg^{-1}. \end{aligned}$$

Orbits are called conjugacy classes

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

stabilisers are called centralisers

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

*Remark 21.*

1. By ?? the conjugacy classes partition  $G$ .

2. By ??,  $h \in G$

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

In particular  $(C_G(h))$  is a subgroup

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

3. If  $k \in \text{ccl}_G(h)$  then  $o(k) = o(h)$ .

*Proof.* Since  $k = ghg^{-1}$  for some  $g \in G$ , so

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

Similarly,  $h = g^{-1}kg \implies o(h) \mid o(k)$ . □

4. Recall the centre of  $G$  is

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

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

Note  $z \in Z(G) \iff |\text{ccl}_G(z)| = 1$ .

*Proof.* If  $z \in Z(G)$

$$\begin{aligned} \implies \text{ccl}_G(z) &= \{ \underbrace{gzg^{-1}}_{gg^{-1}z=z} : g \in G \} \\ &= \{z\} \end{aligned}$$

If  $|\text{ccl}_G(z)| = 1$ , note  $z = eze^{-1} \in \text{ccl}_G(z)$ . So  $gzg^{-1} = z \forall g \in G$ . □

5. Let  $H \leq G$ , then  $H$  is normal iff it is a union of conjugacy classes (Sheet 3, Q3).

6.  $G$  is abelian iff  $G = Z(G)$ .

### Proposition 6.2

Let  $p$  be a prime and  $G$  a group of order  $p^n$ . Then  $Z(G)$  is nontrivial, i.e.  $Z(G) > \{e\}$  (not equal to).

*Proof.* Let  $G$  act on  $G$  by conjugation. Then the conjugacy classes of  $G$  partition  $G$ ,

$$G = \dot{\bigcup}_{\text{distinct conj classes}} \text{ccl}_G(x) \text{ by ??}.$$

By ??

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

Either  $|\text{ccl}_G(x)| = 1$  or  $p \mid |\text{ccl}_G(x)|$ . By ??,

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

Now  $p \mid |G|$  and  $p \mid RHS$

$$\implies p \mid \sum_{x \in Z(G)} |\text{ccl}_G(x)| = |Z(G)|$$

□

#### Lemma 6.4

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

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

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



$$= hg \\ \implies G \text{ is abelian.}$$

□

### Corollary 6.1

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

*Proof.* (Q10, Sheet 3).

□

*Remark 22.*

A group of order  $p^n$  for a prime  $p$  is called a finite  $p$ -group.

If all the elements have  $p$ -power order,  $G$  is called a  $p$ -group. E.g.  $C_{p^\infty}$  is the Prüfer group.

### §6.3.1 Conjugation in $S_n$

#### Definition 6.7 (Cycle type)

Let  $\sigma \in S_n$  and write  $\sigma$  as a product of disjoint cycles including 1-cycles. Then the *cycle type* of  $\sigma$  is  $(n_1, n_2, \dots, n_k)$  where  $n_1 \geq n_2 \geq \dots \geq n_k \geq 1$  and the cycles in  $\sigma$  have length  $n_i$ .

Note  $n = n_1 + n_2 + \dots + n_k$ .

#### Example 6.5

$$\begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix} \begin{pmatrix} 5 & 6 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix} \begin{pmatrix} 5 & 6 & 7 \end{pmatrix} \begin{pmatrix} 8 \end{pmatrix} \\ = S_8$$

has cycle type  $(4, 3, 1)$ .

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

#### Theorem 6.4

The permutations  $\pi$  and  $\sigma$  in  $S_n$  are conjugate in  $S_n$  (i.e.  $\exists g \in S_n$  s.t.  $g\pi g^{-1} = \sigma$ ) iff they have the cycle type.

*Proof.* Suppose  $\sigma$  has cycle type  $(n_1, n_2, \dots, n_k)$ . Write

$$\sigma = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n_1} \end{pmatrix} \begin{pmatrix} a_{21} & a_{22} & \dots & a_{2n_2} \end{pmatrix} \dots \begin{pmatrix} a_{k1} & a_{k2} & \dots & a_{kn_k} \end{pmatrix}.$$

Let  $\tau \in S_n$ .

Then

$$\begin{aligned} \tau\sigma\tau^{-1}(\tau(a_{ij})) &= \tau\sigma(a_{ij}) \\ &= \begin{cases} \tau(a_{ij+1}) & j < n_i \\ \tau(a_{i1}) & j = n_i \end{cases}. \end{aligned}$$

So

$$\begin{aligned} \tau\sigma\tau^{-1} &= \begin{pmatrix} \tau(a_{11}) & \tau(a_{12}) & \dots & \tau(a_{1n_1}) \end{pmatrix} \\ &\quad \begin{pmatrix} \tau(a_{21}) & \tau(a_{22}) & \dots & \tau(a_{2n_2}) \end{pmatrix} \dots \begin{pmatrix} \tau(a_{k1}) & \tau(a_{k2}) & \dots & \tau(a_{kn_k}) \end{pmatrix}. \end{aligned}$$

So if two elements of  $S_n$  are conjugate they have the same cycle type.

Furthermore if  $\pi$  has the same cycle type as  $\sigma$ , we can write

$$\pi = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n_1} \end{pmatrix} \dots \begin{pmatrix} b_{k1} & b_{k2} & \dots & b_{kn_k} \end{pmatrix}.$$

Define  $\tau(a_{ij}) = b_{ij}$  then  $\pi = \tau\sigma\tau^{-1}$ . Thus 2 permutations of the same cycle type are conjugate.  $\square$

### Example 6.6

$$\begin{aligned} \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 4 \end{pmatrix}^{-1} &= \begin{pmatrix} 4 & 2 & 3 \end{pmatrix} \\ \begin{pmatrix} 1 & l \end{pmatrix} \begin{pmatrix} 1 & k \end{pmatrix} \begin{pmatrix} 1 & l \end{pmatrix} &= \begin{pmatrix} l & k \end{pmatrix} \end{aligned}$$

Consider  $S_4$ : Let  $x \in S_4$ , recall

$$24 = |S_4| = |\text{ccl}_{S_4}(x)| |C_{S_4}(x)| \text{ by ??}.$$

example member, $x$	cycle type	no. of	sgn	$ C_{S_4}(x) $	$C_{S_4}(x)$
$e$	$(1, 1, 1, 1)$	1	1	24	$S_4$
$\begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 4 \end{pmatrix}$	$(2, 1, 1)$	6	-1	4	$\langle \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 4 \end{pmatrix} \rangle \cong C_2 \times C_2$
$\begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 4 \end{pmatrix}$	$(3, 1)$	8	1	3	$\langle \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \rangle \cong C_3$
$\begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 4 \end{pmatrix}$	$(2, 2)$	3	1	8	$\langle \begin{pmatrix} 1 & 3 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 \end{pmatrix} \rangle \cong D_8$
$\begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix}$	$(4)$	6	-1	4	$\langle \begin{pmatrix} 1, 2, 3, 4 \end{pmatrix} \rangle \cong C_4.$

### Corollary 6.2

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

However in  $A_n$  conjugation is less clear. Certainly

$$\begin{aligned} \text{ccl}_{A_n}(x) &= \{gxg^{-1} : g \in A_n\} \\ &\subseteq \{gxg^{-1} : g \in S_n\} = \text{ccl}_{S_n}(x) \end{aligned}$$

since  $A_n \leq S_n$ . So if two elements are conjugate in  $A_n$  they have the same cycle type. But having the same cycle type in  $A_n$  does not guarantee being conjugate.

E.g.  $(1\ 2\ 3)$  is not conjugate to  $(1\ 3\ 2)$  in  $A_4$ .

If  $\tau(1\ 2\ 3)\tau^{-1} = (1\ 3\ 2)$  then  $\tau = (1\ 2)$  or  $(3\ 2)$  or  $(1\ 3) \in S_4 \setminus A_4$ .

Or consider

$$\begin{aligned} C_{A_4}((1\ 2\ 3)) &= C_{S_4}((1\ 2\ 3)) \cap A_4 \\ C_{S_4}((1\ 2\ 3)) &= \langle (1\ 2\ 3) \rangle \leq A_4 \\ \text{So, } C_{A_4}((1\ 2\ 3)) &= C_{S_4}((1\ 2\ 3)) \\ \implies |\text{ccl}_{A_4}((1\ 2\ 3))| &= \frac{|A_4|}{|C_{A_4}((1\ 2\ 3))|} \text{ by ??} \\ &= \frac{|S_4|/2}{|C_{S_4}((1\ 2\ 3))|} \\ &= \frac{|\text{ccl}_{S_4}((1\ 2\ 3))|}{2}. \end{aligned}$$

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

*Key point* Let  $x \in A_n$ . If  $C_{A_n}(x) = C_{S_n}(x) \implies |\text{ccl}_{A_n}(x)| = \frac{|\text{ccl}_{S_n}(x)|}{2}$  by ??.

If  $C_{A_n}(x) \subsetneq C_{S_n}(x)$ , then  $C_{S_n}$  contains an odd permutation and  $|C_{A_n}(x)| = |C_{S_n} \cap A_n| = \frac{|C_{S_n}|}{2}$  (Q4, Sheet 2)  $\implies |\text{ccl}_{A_n}(x)| = |\text{ccl}_{S_n}(x)|$ .

$A_4$ :

example member, $x$	cycle type	$C_{A_4}(x)$	size of ccl
$e$	$(1, 1, 1, 1)$	$A_4$	1
$(1\ 2\ 3)$	$(3, 1)$	$\langle (1\ 2\ 3) \rangle$	4
$(1\ 3\ 2)$	$(3, 1)$	$\langle (1\ 3\ 2) \rangle$	4
$(1\ 2)(3\ 4)$	$(2, 2)$	$\{e, (1\ 2)(2\ 4), (1\ 4)(2\ 3)\} \cong C_2 \times C_2$	3

*Remark 23.* The number of elements in  $S_n$  with  $k_l$  cycles of length  $l$  is given by

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

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

### Example 6.7

E.g. Number of cycles in  $S_5$  of type  $(\cdot \cdot)(\cdot \cdot)(\cdot)$ , so  $k_2 = 2$  and  $k_1 = 1$ .

$$\text{no. of} = \frac{5!}{2! 2^2 1! 1} = 15$$

Or  $(\cdot \cdot \cdot)(\cdot \cdot)$ ,  $k_3 = 1, k_2 = 1$

$$\text{no. of} = \frac{5!}{1! 3^1 1! 2^1} = 20.$$

Let us consider  $S_5$ ,  $|S_5| = 120$ .

example member, $x$	cycle type	no. of	sgn	$ C_{S_5}(x) $	$C_{S_5}(x)$
$e$	$(1, 1, 1, 1, 1)$	1	1	120	$S_5$
$(1 \ 2)$	$(2, 1, 1, 1)$	10	-1	12	$\langle (1 \ 2) \rangle \times \text{Sym}\{3, 4, 5\} \cong C_2 \times S_3$
$(1 \ 2)(3 \ 4)$	$(2, 2, 1)$	15	1	8	$\langle (1 \ 3 \ 2 \ 4), (1 \ 2) \rangle \cong D_8$
$(1 \ 2 \ 3)$	$(3, 1, 1)$	20	1	6	$\langle (1 \ 2 \ 3), (4 \ 5) \rangle \cong C_6$
$(1 \ 2 \ 3)(4 \ 5)$	$(3, 2)$	20	-1	6	"
$(1 \ 2 \ 3 \ 4)$	$(4, 1)$	30	-1	4	$\langle (1 \ 2 \ 3 \ 4) \rangle$
$(1 \ 2 \ 3 \ 4 \ 5)$	$(5)$	24	1	5	$\langle (1 \ 2 \ 3 \ 4 \ 5) \rangle$

Now consider  $A_5$ ,  $|A_5| = 60$ .

example member, $x$	cycle type	$C_{A_5}(x)$	$ \text{ccl}_{A_5}(x) $
$e$	$(1, 1, 1, 1, 1)$	$A_5$	1
$(1 \ 2)(3 \ 4)$	$(2, 2, 1)$	$\langle (1 \ 2)(3 \ 4), (1 \ 3)(2 \ 4) \rangle$	15
$(1 \ 2 \ 3)$	$(3, 1, 1)$	$\langle (1 \ 2 \ 3) \rangle$	20
$(1 \ 2 \ 3 \ 4 \ 5)$	$(5)$	$\langle (1 \ 2 \ 3 \ 4 \ 5) \rangle$	12
$(2 \ 1 \ 3 \ 4 \ 5)$	$(5)$	$\langle (2 \ 1 \ 3 \ 4 \ 5) \rangle$	12

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

### Theorem 6.5

$A_5$  is a simple group.

*Proof.* Suppose  $N \trianglelefteq A_5$ . Then  $N$  is a union of conjugacy classes (Sheet 3, Q3(a)).  
 $\implies |N| = 1 + 15a + 20b + 12c + 12d$  where  $a, b, c, d \in \{0, 1\}$ . But by ??  $|N| \mid |A_5| = 60 \implies |N| = 1$  or  $60$ .  $\square$

#### *Comments*

1.  $A_5$  is the smallest non-abelian simple group.
2.  $A_n$  is simple  $\forall n \geq 5$  (GRM), but  $A_4$  is not simple.
3. Classification of finite simple groups exists, includes  $\infty$  families
  - $C_p$  where  $p$  is prime (only abelian simple groups)
  - $A_n$  for  $n \geq 5$
  - groups of 'Lie type', matrix groups
  - 26 sporadic groups, include Monster and Baby Monster

## §7 Matrix Groups

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

### Definition 7.1 (General Linear Group)

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

### Proposition 7.1

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

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

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

inverse:  $\det A \neq 0 \implies A^{-1}$  exists,  $\det A^{-1} = \frac{1}{\det A} \neq 0$ .

matrix multiplication is associative:

$$\begin{aligned} (A(BC))_{ij} &= A_{ik}(BC)_{kj} \\ &= A_{ik}B_{kt}C_{tj} \\ ((AB)C)_{ij} &= (AB)_{ik}C_{kj} \\ &= A_{it}B_{tk}C_{kj}. \end{aligned}$$

□

### Example 7.1

$$\begin{aligned} \mathrm{GL}_2(\mathbb{R}) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\} \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} &= \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & -a \end{pmatrix}. \end{aligned}$$

### Proposition 7.2

$$\mathrm{Det} : \mathrm{GL}_n(\mathbb{R}) \rightarrow (\mathbb{R} \setminus \{0\}, \times)$$

$$A \mapsto \det A.$$

is a surjective group homomorphism.

*Proof.* Note  $(\mathbb{R} \setminus \{0\}, \times)$  is a group.  $\text{Det}$  is clearly a map to  $(\mathbb{R} \setminus \{0\}, \times)$ , we need to check it's a group homomorphism,

$$\begin{aligned} \text{Det}(AB) &= \det(AB) \quad (AB \text{ is multiplication in } \text{GL}_n) \\ &= \det A \cdot \det B \quad (\text{multiplication in } (\mathbb{R} \setminus \{0\}, \times)) \\ &= \text{Det } A \text{ Det } B \end{aligned}$$

and that  $\text{Det}$  is surjective. Let  $r \in (\mathbb{R} \setminus \{0\}, \times)$  then

$$A = \begin{pmatrix} r & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \in \text{GL}_n(\mathbb{R}) \mapsto \det(A) = r.$$

□

By ??  $\ker(\text{Det}) \leq \text{GL}_n(\mathbb{R})$ .

$$\begin{aligned} \ker(\text{Det}) &= \{A \in \text{GL}_n(\mathbb{R}) : \det A = 1\} \\ &= \text{SL}_n(\mathbb{R}) \text{ the special linear group.} \end{aligned}$$

Furthermore, by ??

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

*Remark 24.* More generally we can define the general linear group and special linear group over any field.

Examples of fields:

$\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{F}_p$  where  $\mathbb{F}_p = (\{0, 1, 2, \dots, p-1\}, +_p, \times_p)$  and  $p$  is prime. Note  $\text{GL}_n(\mathbb{F}_p)$  and  $\text{SL}_n(\mathbb{F}_p)$  are finite groups.

What is  $|\text{GL}_3(\mathbb{F}_p)|$ ?

Non-zero determinant means we have linearly independent columns. The no. of choices for the first column is  $p^3 - 1$  (can't be  $\begin{pmatrix} 0 & 0 & 0 \end{pmatrix}^T$ ). The second column is not a multiple of first so  $p^3 - p$  (there are  $p$  multiples of first column). Third column not in space spanned by first two columns, this space has size  $p^2$  (consider  $\alpha c_1 + \beta c_2$  with  $\alpha, \beta \in \mathbb{F}_p$ ), so  $p^3 - p^2$ .

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

We can still consider

$$\begin{aligned}\text{Det} : \text{GL}_3(\mathbb{F}_p) &\rightarrow (\mathbb{F}_p \setminus \{0\}, \times) \\ A &\mapsto \det(A).\end{aligned}$$

Note  $(\mathbb{F}_p \setminus \{0\}, \times)$  is a group: we have closure, identity = 1 and associativity. Let  $a \in \mathbb{F}_p \setminus \{0\}$ , by Bezout's Thm  $\exists x, y$  s.t.

$$\begin{aligned}ax + py &= 1 \\ \therefore ax &\equiv 1 \pmod{p} \\ \text{Choose } \bar{x} &\equiv x \pmod{p}, \\ 1 \leq \bar{x} &\leq p-1, \quad a^{-1} = x\end{aligned}$$

Det is a surjective homomorphism to  $(\mathbb{F}_p \setminus \{0\}, \times)$  so by ??

$$\begin{aligned}|\text{GL}_3(\mathbb{F}_p)|/|\text{SL}_3(\mathbb{F}_p)| &= p-1 \\ \implies |\text{SL}_3(\mathbb{F}_p)| &= \frac{(p^3-1)(p^3-p)(p^3-p^2)}{p-1}.\end{aligned}$$

## §7.1 Actions of $\text{GL}_n(\mathbb{C})$

1. Let  $\mathbb{C}^n$  denote vectors of length  $n$  with entries in  $\mathbb{C}$ :

$$\begin{aligned}\text{GL}_n(\mathbb{C}) \times \mathbb{C}^n &\rightarrow \mathbb{C}^n \\ (A, v) &\mapsto Av.\end{aligned}$$

Note  $Iv = v$ ,  $(AB)v = A(Bv)$ . This action is faithful:  $Av = v \forall v \in \mathbb{C}^n \implies A = I_n$  (consider  $v = e_i$ ). The action has two orbits

$$\begin{aligned}\text{Orb}_{\text{GL}_n(\mathbb{C})}(\underline{0}) &= \{\underline{0}\} \\ \text{Orb}_{\text{GL}_n(\mathbb{C})}(v) &= \mathbb{C}^n \setminus \{\underline{0}\} \text{ for } v \neq \underline{0},\end{aligned}$$

i.e. given  $w \neq 0 \exists A \in \text{GL}_n(\mathbb{C})$  s.t.  $Av = w$ .

2. Conjugation action of  $\text{GL}_n(\mathbb{C})$  on  $M_n(\mathbb{C})$  (set of all matrices)

$$\begin{aligned}\text{GL}_n(\mathbb{C}) \times M_n(\mathbb{C}) &\rightarrow M_n(\mathbb{C}) \\ (P, A) &\mapsto PAP^{-1}.\end{aligned}$$

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

*Remark 25.* Matrices  $A$  and  $B$  are conjugate if they represent the same linear map. If  $PAP^{-1} = B$ , then  $P$  represents a change of basis matrix. (See LA next year)



**Example 7.2**

$$A : e_1 \mapsto 2e_1$$

$$e_2 \mapsto 3e_2$$

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

$$\text{Let } P : e_1 \mapsto e_2$$

$$e_2 \mapsto e_1$$

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

$$= P^{-1}$$

$P$  is a change of basis

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

$$\text{i.e. } e_2 \mapsto 3e_2$$

$$e_1 \mapsto 2e_1.$$

We will use the following result from V&M when investigating Möbius groups.

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

1. The orbit of  $A$  contains a diagonal matrix  $\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$  with  $\lambda \neq \mu$ .
2. The orbit of  $A$  is  $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} = \lambda I$  for some  $\lambda$ .
3. The orbit of  $A$  contains a matrix  $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$  for some  $\lambda$ .

*Proof.* See V&M but essentially

1. In this case  $A$  has 2 distinct eigenvalues  $\lambda \neq \mu$ , take a basis consisting of an eigenvector for  $\lambda$  and an eigenvector for  $\mu$ . Distinct pairs given distinct orbits.
2.  $PAP^{-1} = \lambda I \implies A = P\lambda IP^{-1} = \lambda I$ , eigenvalues  $\lambda, \lambda$ , 2 linearly independent eigenvectors.

3. In this case  $A$  has a repeated eigenvalue, but just one linearly independent eigenvector.

□

## §7.2 Orthogonal Group

### Aside: Recalling transpose properties

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

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

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

*Note*

1.

$$\begin{aligned} (AB)^T &= B^T A^T \\ [(AB)^T]_{ij} &= (AB)_{ji} \\ &= A_{jk} B_{ki} \\ [B^T A^T]_{ij} &= B_{ik}^T A_{kj}^T \\ &= B_{ki} A_{jk} \checkmark \end{aligned}$$

2.

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

3.

$$\begin{aligned} AA^T = I &\iff A^T A = I. \\ \implies A^T A &= A^{-1} \underbrace{AA^T}_I A \end{aligned}$$

$$\begin{aligned}
&= A^{-1}A \\
&= I.
\end{aligned}$$

4.

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

5.

$$\det A^T = \det A.$$

### Definition 7.2 (Orthogonal group)

$$O_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : A^T A = I\}$$

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

### Proposition 7.3

$O_n(\mathbb{R})$  is a subgroup of  $GL_n(\mathbb{R})$  called the *orthogonal group*.

*Proof.*

- $\det A \neq 0 \implies O_n(\mathbb{R}) \subseteq GL_n(\mathbb{R})$ .
- closure:

$$\begin{aligned}
&A, B \in O_n(\mathbb{R}) \\
(AB)^T(AB) &= B^T A^T AB \\
&= B^T B = I \\
\implies AB &\in O_n(\mathbb{R})
\end{aligned}$$

- $I_n \in O_n(\mathbb{R})$
- Associativity is inherited.
- inverse:  $A^T A = I_n \implies A^T = A^{-1}$  and  $A^T \in O_n(\mathbb{R})$  since  $(A^T)^T = A$  and  $AA^T = I$ .

□

Note  $1 = (\det A)^2 \implies \det A = \pm 1$  if  $A \in O_n(\mathbb{R})$ .

So,

$$\begin{aligned} \text{Det} : O_n(\mathbb{R}) &\rightarrow (\{\pm 1\}, \times) \\ A &\mapsto \det A \end{aligned}$$

is a surjective homomorphism as,  $\begin{pmatrix} -1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \in O_n(\mathbb{R})$ .

$$\begin{aligned} \text{So } \ker(\text{Det}) &= \{A \in O_n(\mathbb{R}) : \det A = 1\} \\ &= SO_n(\mathbb{R}) \trianglelefteq O_n(\mathbb{R}). \end{aligned}$$

By ??:

$$O_n(\mathbb{R})/SO_n(\mathbb{R}) \cong C_2.$$

### Lemma 7.1

Let  $A \in O_n(\mathbb{R})$  and  $\underline{x}, \underline{y} \in \mathbb{R}^n$ . Then

1.  $A\underline{x} \cdot A\underline{y} = \underline{x} \cdot \underline{y}$
2.  $|A\underline{x}| = |\underline{x}|$ .

So  $A$  is an isometry (distance preserving map) of Euclidean space  $\mathbb{R}^n$ .

*Proof.*

1.

$$\begin{aligned} A\underline{x} \cdot A\underline{y} &= (A\underline{x})^T (A\underline{y}) \\ &= \underline{x}^T A^T A \underline{y} \\ &= \underline{x}^T \underline{y} \\ &= \underline{x} \cdot \underline{y}. \end{aligned}$$

2.

$$\begin{aligned} |A\underline{x}|^2 &= A\underline{x} \cdot A\underline{x} \\ &= \underline{x} \cdot \underline{x} \\ &= |\underline{x}|^2 \end{aligned}$$

□

Note by ?? if  $\lambda$  is an eigenvalue of  $A$ ,  $A\underline{x} = \lambda\underline{x} \implies |\lambda\underline{x}| = |\underline{x}|$  i.e.  $|\lambda| = 1$ .

### §7.2.1 In 2 dimensions

Let  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{R})$  and

$$\begin{aligned} I &= AA^T \\ &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} \\ \implies 1 &= a^2 + b^2 = c^2 + d^2 \\ 0 &= ac + bd. \\ I &= A^T A \\ &= \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ \implies 1 &= a^2 + c^2 = b^2 + d^2 \\ 0 &= ab + cd. \end{aligned}$$

For  $0 \leq \theta < 2\pi$  let

$$\begin{aligned} \begin{pmatrix} a \\ c \end{pmatrix} &= \begin{pmatrix} \cos \theta \\ \sin \theta \end{pmatrix} \\ \text{so } \begin{pmatrix} b \\ d \end{pmatrix} &= \begin{pmatrix} \mp \sin \theta \\ \pm \cos \theta \end{pmatrix}. \end{aligned}$$

$$A = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$$

$\det A = 1$  so a rotation and all elements of  $SO_2(\mathbb{R})$  are of this form.

$$\text{Or } A = \begin{pmatrix} \cos \theta & \sin \theta \\ \sin \theta & -\cos \theta \end{pmatrix}$$

$$\det A = -1$$

$$A \begin{pmatrix} x \\ y \end{pmatrix} = e^{i\theta} \overline{x + iy} = e^{i\theta} \bar{z}$$

What are the fixed points?

$$z = e^{i\theta} \bar{z} \iff e^{-i\theta/2} z = e^{i\theta/2} \bar{z}$$

$$\begin{aligned}
&\iff e^{-i\theta/2}z = t \in \mathbb{R} \\
&\iff z = e^{i\theta/2}t. \\
&\implies \text{a reflection in line } e^{i\theta/2}
\end{aligned}$$

All elements of  $O_2(\mathbb{R}) \setminus SO_2(\mathbb{R})$  of this form.

$$\text{So, } O_2(\mathbb{R}) = \underbrace{SO_2(\mathbb{R})}_{\text{rotations}} \cup \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} SO_2(\mathbb{R})}_{\text{reflections}}$$

Note any element of  $O_2(\mathbb{R})$  is a product of at most two reflections. Since if  $A \in SO_2(\mathbb{R})$  then  $A = \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}}_{\text{reflection}} \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}}_{\text{reflection}}.$

### §7.2.2 In 3 dimensions

#### Proposition 7.4

Let  $A \in SO_3(\mathbb{R})$ . Then  $A$  has an eigenvector with eigenvalue 1.

*Proof.*

$$\begin{aligned}
\det(A - I) &= \det(A - AA^T) \\
&= \det A \det(I - A^T) \\
&= 1 \cdot \det(I - A)^t \\
&= \det(I - A) \\
&= (-1)^3 \det(A - I) \\
&= -\det(A - I) \\
\implies \det(A - I) &= 0 \text{ and } A \text{ has an eigenvalue } = 1.
\end{aligned}$$

□

*Alternative Proof.* Consider  $\chi_A(x)$  (characteristic poly of  $A$ ), it is a cubic in  $\mathbb{R}$  and its roots multiply to 1 ( $\det A = 1 = \prod_i \lambda_i$ ). Thus it has a real root, and  $|\lambda| = 1 \implies \lambda = \pm 1$ . But the other eigenvalues are either a complex conjugate pair, then  $\lambda = 1$  as product of eigenvalues give  $\det A = 1$ , or all are real so either 1, -1, -1 or 1, 1, 1. □

### Theorem 7.1

Let  $A \in SO_3(\mathbb{R})$  then  $A$  is conjugate (i.e. there is a change of basis) to a matrix of the form  $\begin{pmatrix} \cos \theta & -\sin \theta & 0 \\ \sin \theta & \cos \theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$  for some  $\theta \in [0, 2\pi]$ . In particular,  $A$  is a rotation around an axis through the origin.

*Proof.* By ??  $\exists \underline{v} \in \mathbb{R}^3$  with  $A\underline{v} = \underline{v}$ , we can assume  $|\underline{v}| = 1$ . Let  $\{e_1, e_2, e_3\}$  be the standard orthonormal basis for  $\mathbb{R}^3$ . There exists  $P \in SO_3(\mathbb{R})$  s.t.  $P\underline{v} = e_3$ . So  $PAP^{-1}(e_3) = e_3$  and for  $\Pi$  plane perpendicular to  $e_3$  then  $PAP^{-1}(\Pi)$  is perpendicular to  $e_3$ . So,

$$\begin{aligned} PAP^{-1} &= \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ on } \Pi \\ &= \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} Q \end{aligned}$$

$$\det(PAP^{-1}) = \det A = 1$$

$$\implies \det Q = 1$$

$$(PAP^{-1})(PAP^{-1})^T = I \implies QQ^T = I.$$

$$\text{So, } Q \in SO_2(\mathbb{R}).$$

□

Suppose  $\underline{r}$  is a reflection in a plane  $\Pi$  through 0. Let  $\underline{n}$  be a unit vector perpendicular to  $\Pi$ .

Then  $r(\underline{x}) = \underline{x} - 2(\underline{x} \cdot \underline{n})\underline{n}$ ,  $\underline{n} \mapsto -\underline{n}$ ,  $\Pi$  is fixed. So  $\underline{r}$  is conjugate to  $\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in O_3(\mathbb{R})$

by taking basis  $\underline{n}$  and two orthogonal unit vectors in  $\Pi$ .

$$O_3(\mathbb{R}) = \underbrace{SO_3(\mathbb{R})}_{\text{rotations, det} = 1} \cup \underbrace{\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} SO_3(\mathbb{R})}_{\text{det} = -1}$$

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} SO_3(\mathbb{R}) \text{ includes}$$

- reflections

- inversion in origin,  $-I_3$
- combinations of rotations and reflections

### Theorem 7.2

Any element of  $O_3(\mathbb{R})$  is a product of at most 3 reflections.

*Proof.* Let  $\{e_1, e_2, e_3\}$  be the standard orthonormal basis for  $\mathbb{R}^3$ . Let  $A \in O_3(\mathbb{R})$ .

$$|Ae_3| = |e_3| = 1 \text{ since } A \text{ is an isometry.}$$

So  $\exists$  a reflection  $r_1$  s.t.  $r_1 A(e_3) = e_3$ . Let  $\Pi = \langle e_1, e_2 \rangle \perp e_3$ . So  $r_1 A(\Pi) = \Pi$ , as angles are preserved.

$\exists$  a reflection  $r_2$  s.t.  $r_2(e_3) = e_3$ ,  $r_2(r_1 A(e_2)) = e_2$ . So  $r_2 r_1 A$  fixes  $e_2$  and  $e_3$ .

So  $r_2 r_1 A(e_1) = \pm e_1$ , if  $e_1 = e_1$ , set  $r_3 = \text{id}$ . Else  $e_1 = -e_1$ , let  $r_3$  be the reflection in the plane  $\perp$  to  $e_1$ .

So  $r_3 r_2 r_1 A$  fixes  $e_1, e_2, e_3$ , so  $r_3 r_2 r_1 A = \text{id} \implies A = r_1^{-1} r_2^{-1} r_3^{-1} = r_1 r_2 r_3$ .  $\square$

Alternatively, any element in  $SO_3(\mathbb{R})$  is a product of at most 2 reflections, via 2-dimensional case. Thus any element of  $\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} SO_3(\mathbb{R})$  is a product of at most 3 reflections. Note we do need 3, e.g.  $-I_3$ .



## §8 Möbius Groups

### Definition 8.1 (Möbius transformation)

A Möbius transformation (or map) is a function of a complex variable  $z$  that can be written in the form

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

for some  $a, b, c, d \in \mathbb{C}$  with  $ad - bc \neq 0$ .

Why  $ad - bc \neq 0$ ?

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

So,  $ad - bc = 0 \implies f$  is constant (not interesting). If,  $ad - bc \neq 0 \implies f$  is injective.

When does  $f(z) = g(z)$  ( $g(z)$  is  $f(z)$  with different  $a, b, c, d$ )? Suppose  $\exists$  at least 3 values of  $z$  in  $\mathbb{C}$  s.t.

$$\begin{aligned} \frac{az + b}{cz + d} &= \frac{\alpha z + \beta}{\gamma z + \delta} \\ ad - bc &\neq 0, \quad \alpha\delta - \beta\gamma \neq 0. \end{aligned}$$

Then  $\exists \lambda \neq 0, \lambda \in \mathbb{C}$  s.t.

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

Since, we have 3 distinct values of  $z$  for which

$$(az + b)(\gamma z + \delta) = (\alpha z + \beta)(cz + d)$$

so these quadratics are identical

$$\implies \alpha\gamma = \alpha c, \quad b\delta = \beta d$$

$$a\delta + \beta\delta = \alpha d + \beta c$$

$$\text{Let } \mu = a\delta - \beta c = \alpha d - b\gamma$$

$$(\text{so } \mu^2 = (ad - bc)(\alpha\delta - \beta\gamma) \neq 0).$$

$$\begin{aligned} \text{Then } \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} &= \begin{pmatrix} \mu & 0 \\ 0 & \mu \end{pmatrix} \\ \implies \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} &= \frac{\mu}{ad - bc} \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \end{aligned}$$

Problem:  $f$  is not defined at  $z = -\frac{d}{c}$ . We would like  $f(-\frac{d}{c}) = \infty$ . We consider  $f$  defined on  $\mathbb{C} \cup \{\infty\} = \mathbb{C}_\infty$  the extended complex plane. So if  $f(z) = \frac{az+b}{cz+d}$ , domain is now  $\mathbb{C}_\infty$ . If  $c \neq 0$ ;  $f(\infty) = \frac{a}{c}$ ;  $f(-\frac{d}{c}) = \infty$  else  $c = 0$ ;  $f(\infty) = \infty$ .

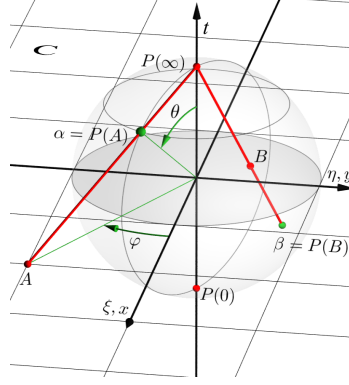


Figure 7: Stereographic projection of a complex number  $A$  onto a point  $\alpha$  of the Riemann sphere

### Theorem 8.1

The set  $\mathcal{M}$  of all Möbius maps on  $\mathbb{C}_\infty$  is a group under composition. It is a subgroup of  $\text{Sym}(\mathbb{C}_\infty)$ .

*Proof.* • Composition of maps is associative.

- $I(z) = z \in \mathcal{M}$  ( $a = d = 1, c = d = 0$ )
- closure:

$$\text{Let } f(z) = \frac{az + b}{cz + d}, \quad g(z) = \frac{\alpha z + \beta}{\gamma z + \delta}$$

Suppose  $c \neq 0, \delta \neq 0$

First suppose  $z \in \mathbb{C} \setminus \{-\delta/\gamma\}$

$$\begin{aligned} \text{Then } f(g(z)) &= \frac{a \left( \frac{\alpha z + \beta}{\gamma z + \delta} \right) + b}{c \left( \frac{\alpha z + \beta}{\gamma z + \delta} \right) + d} \\ &= \frac{(a\alpha + b\gamma)z + (a\beta + b\delta)}{(c\alpha + d\gamma)z + (c\beta + \delta d)} \\ &\in \mathcal{M} \end{aligned}$$

$$\text{since } (a\alpha + b\gamma)(c\beta + \delta d) - (a\beta + b\delta)(c\alpha + d\gamma) = (ad - bc)(\alpha\delta - \beta\gamma) \neq 0$$

$$\text{Also, } f\left(g\left(-\frac{\delta}{\gamma}\right)\right) = f(\infty) = \frac{a}{c}$$

$$\text{and } \frac{(a\alpha + b\gamma)\left(-\frac{\delta}{\gamma}\right) + (a\beta + b\delta)}{(c\alpha + d\gamma)\left(-\frac{\delta}{\gamma}\right) + (c\beta + \delta d)} = \frac{a\alpha\left(-\frac{\delta}{\gamma}\right) + \alpha\beta}{c\alpha\left(-\frac{\delta}{\gamma}\right) + c\beta}$$

$$= \frac{a}{c} \checkmark$$

Need to check  $c = 0$

- Inverses:

$$f(z) = \frac{az + b}{cz + d}, \quad ad - bc \neq 0$$

$$\text{Let } f^*(z) = \frac{dz - b}{-cz + a}$$

$$\text{Then } f(f^*(z)) = z = f^*(f(z)) \text{ for } z \neq -\frac{d}{c}, -\frac{a}{c}, \infty$$

These cases are ok.

If  $c = 0$

$$f(f^*(\infty)) = f(\infty) = \infty = f^*(f(\infty)).$$

□

### Theorem 8.2

$\text{GL}_2(\mathbb{C})/Z \cong \mathcal{M}$  where  $Z = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \lambda \in \mathbb{C} \setminus \{0\} \right\}$  ( $Z$  is the centre of  $\text{GL}_2(\mathbb{C})$ ).

*Proof.* We construct a surjective homomorphism from  $\text{GL}_2(\mathbb{C})$  onto  $\mathcal{M}$  with kernel  $Z$ .

Let  $\Phi : \text{GL}_2(\mathbb{C}) \rightarrow \mathcal{M}$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto f(z) = \frac{az + b}{cz + d}$$

Note  $\Phi$  is a homomorphism

$$\begin{aligned} f(z) &= \frac{az + b}{cz + d}, \quad g(z) = \frac{\alpha z + \beta}{\gamma z + \delta} \\ \Phi \left( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) \Phi \left( \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \right) (z) &= f \circ g(z) \\ &= \frac{(a\alpha + b\gamma)z + (a\beta + b\delta)}{(c\alpha + d\gamma)z + (c\beta + d\delta)} \text{ from proof of ??} \\ &= \Phi \left( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \right) (z). \end{aligned}$$

Clearly  $\Phi$  is surjective.

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\in \ker \Phi \\ \iff \frac{az+b}{cz+d} &= z \quad \forall z \in C_\infty \\ \text{Let } z = \infty &\implies c = 0 \\ z = 0 &\implies b = 0 \\ z = 1 &\implies a = d \\ \implies \ker \Phi &= Z \end{aligned}$$

Finally apply ??.

□

### Corollary 8.1

$$\frac{\mathrm{SL}_2(\mathbb{C})}{\{\pm I\}} = \mathcal{M}.$$

*Proof.* Restrict  $\phi$  to  $\mathrm{SL}_2(\mathbb{C})$

$$\begin{aligned} \phi : \mathrm{SL}_2(\mathbb{C}) &\rightarrow \mathcal{M} \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\mapsto \frac{az+b}{cz+d} \end{aligned}$$

We require  $\phi$  to be surjective:

$$\begin{aligned} f(z) &= \frac{az+b}{cz+d} \\ &= \frac{\frac{a}{\sqrt{ad-bc}}z + \frac{b}{\sqrt{ad-bc}}}{\frac{c}{\sqrt{ad-bc}}z + \frac{d}{\sqrt{ad-bc}}}. \end{aligned}$$

And  $\ker \phi = \{\pm I\}$ .

□

### Proposition 8.1

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

1.  $z \mapsto az$ ,  $a \neq 0$ ; represents a dilation or a rotation
2.  $z \mapsto z + b$ ; a translation
3.  $z \mapsto \frac{1}{z}$ ; inversion.

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

$$\text{If } c = 0; \quad z \mapsto \underbrace{\left(\frac{a}{d}\right)z}_{f_1, ??} \mapsto \underbrace{\left(\frac{a}{d}\right)z + \frac{b}{d}}_{f_2, ??}$$

$$f = f_2 \circ f_1$$

If  $c \neq 0$

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

$$= \left(\frac{a}{c}\right) + \frac{\frac{-ad+bc}{c^2}}{z + \frac{d}{c}}$$

$$= A + \frac{B}{z + \frac{d}{c}}, \quad B \neq 0$$

$$z \xrightarrow{f_1, ??} z + \frac{d}{c}$$

$$\xrightarrow{f_2, ??} \frac{1}{z + \frac{d}{c}}$$

$$\xrightarrow{f_3, ??} \frac{B}{z + \frac{d}{c}}$$

$$\xrightarrow{f_4, ??} A + \frac{B}{z + \frac{d}{c}}$$

$$f = f_4 \circ f_3 \circ f_2 \circ f_1$$

□

### Definition 8.2 (Triply transitive action)

A group  $G$  acts *triply transitively* on a set  $X$  if given  $x_1, x_2, x_3 \in X$  all distinct and  $y_1, y_2, y_3 \in X$  all distinct there exists  $g \in G$  such that  $g(x_i) = y_i$ ,  $i = 1, 2, 3$ .

A group  $G$  acts *sharply triply transitively* if such a  $g$  is unique.

### Theorem 8.3

The action of  $\mathcal{M}$  on  $\mathbb{C}_\infty$  is sharply triply transitive.

*Proof.* Label first triple  $\{z_0, z_1, z_\infty\}$  and second triple  $\{w_0, w_1, w_\infty\}$ . We construct

$g \in \mathcal{M}$  s.t.

$$\begin{aligned} g : z_0 &\mapsto 0 \\ z_1 &\mapsto 1 \\ z_\infty &\mapsto \infty. \end{aligned}$$

First suppose  $z_0, z_1, z_\infty \neq \infty$

$$g(z) = \frac{(z - z_0)(z_1 - z_\infty)}{(z - z_\infty)(z_1 - z_0)}$$

Check: “ $ad - bc$ ” =  $(z_0 - z_\infty)(z_1 - z_\infty)(z_1 - z_0) \neq 0$ .

If  $z_\infty = \infty$

$$g(z) = \frac{(z - z_0)}{(z_1 - z_0)}$$

If  $z_1 = \infty$

$$g(z) = \frac{(z - z_0)}{(z - z_\infty)}$$

If  $z_0 = \infty$

$$g(z) = \frac{(z_1 - z_\infty)}{(z - z_\infty)}$$

Similarly find  $h$  s.t.

$$\begin{aligned} g : w_0 &\mapsto 0 \\ w_1 &\mapsto 1 \\ w_\infty &\mapsto \infty. \end{aligned}$$

Then  $f = h^{-1}g : z_i \rightarrow w_i$

Now to prove uniqueness.

Suppose  $f' : z_i \mapsto w_i$

Then  $f^{-1} \circ f' : z_i \mapsto z_i$

Let  $g$  be as above

$$\begin{aligned} gf^{-1}f'g^{-1} : 0 &\mapsto 0 \implies b = 0 \\ &: 1 \mapsto 1 \implies a = d \end{aligned}$$

$$\begin{aligned}
& : \infty \mapsto \infty \implies c = 0 \\
\implies & gf^{-1}f'g^{-1} = \text{id} \\
\implies & f^{-1}f' = \text{id} \\
\implies & f = f'.
\end{aligned}$$

So, the image of just three points determines the map □

### §8.1 Conjugacy classes in $\mathcal{M}$

Recall  $\Phi : \text{GL}_2(\mathbb{C}) \twoheadrightarrow \mathcal{M}$  from proof of ?? ( $\twoheadrightarrow$  means its a surjective homomorphism). Suppose  $A, B$  are conjugate in  $\text{GL}_2(\mathbb{C})$ , i.e.  $\exists P \in \text{GL}_2(\mathbb{C})$  s.t.  $PAP^{-1} = B$  then

$$\begin{aligned}
\Phi(P)\Phi(A)\Phi(P)^{-1} &= \Phi(PAP^{-1}) \\
&= \Phi(B) \in \mathcal{M}
\end{aligned}$$

i.e.  $\Phi(A)$  and  $\Phi(B)$  are conjugate in  $\mathcal{M}$ .

Use knowledge of conjugacy classes in  $\text{GL}_2(\mathbb{C})$ .

#### Theorem 8.4

Any non-identity Möbius map is conjugate to  $f(z) = \nu z$  for some  $\nu \neq 0, 1$  or to  $f(z) = z + 1$ .

*Proof.*

1.

$$\begin{aligned}
& \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} \text{ where } \lambda \neq \mu, \lambda \neq 0 \neq \mu. \\
& \Phi \left( \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} \right) = f, f(z) = \frac{\lambda}{\mu}z = \nu z, \nu \neq 0, 1.
\end{aligned}$$

2.

$$\begin{aligned}
& \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} \text{ where } \lambda \neq 0 \\
& \Phi \left( \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \right) = \text{id}.
\end{aligned}$$

3.

$$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \text{ where } \lambda \neq 0$$

$$\Phi \left( \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \right) = f, \quad f(z) = \frac{\lambda z + 1}{\lambda} = z + \frac{1}{\lambda}$$

$$\text{i.e. } f = \Phi \left( \begin{pmatrix} 1 & \frac{1}{\lambda} \\ 0 & 1 \end{pmatrix} \right).$$

$$\text{And } \begin{pmatrix} 1 & \frac{1}{\lambda} \\ 0 & 1 \end{pmatrix} \text{ is conjugate to } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$\text{via } \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \frac{1}{\lambda} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{\lambda} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

So  $f$  is conjugate to  $g$  where  $g(z) = z + 1$ .

□

### Corollary 8.2

A non-identity Möbius map has either

1. 2 fixed points or
2. 1 fixed point.

*Proof.* Suppose  $gf g^{-1} = h$ . Then  $\alpha$  is a fixed point of  $f$  (i.e.  $f(\alpha) = \alpha$ )  $\iff$   $g(\alpha)$  is a fixed point of  $h$  (i.e.  $h(g(\alpha)) = g(\alpha)$ ).<sup>a</sup>

So number of fixed points of  $f$  = number of fixed points of  $h$  as  $g$  is a bijection. By ?? either,  $f$  conjugate to  $z \mapsto \nu z$  which has two fixed points:  $0, \infty$ ; or  $f$  conjugate to  $z \mapsto z + 1$  which has one fixed point:  $\infty$ . □

<sup>a</sup>  $f(\alpha) = \alpha \iff gf(\alpha) = g(\alpha) \iff h(g(\alpha)) = gf g^{-1}(g(\alpha)) = g(\alpha)$  or  $gf = hg \implies h(g(\alpha)) = g(\alpha)$  if  $f(\alpha) = \alpha$  and conversely  $g(f(\alpha)) = h(g(\alpha)) \implies g(f(\alpha)) = g(\alpha)$ .

## §8.2 Circles in $\mathbb{C}_\infty$

A Euclidean circle is the set of points in  $\mathbb{C}$  given by some equation  $|z - z_0| = r$ ,  $r > 0$ . A Euclidean line is the set of points in  $\mathbb{C}$  given by some equation  $|z - a| = |z - b|$ ,  $a \neq b$ .

### Definition 8.3 (Circle in $\mathbb{C}_\infty$ )

A circle in  $\mathbb{C}_\infty$  is either a Euclidean circle of a set  $L \cup \{\infty\}$  where  $L$  is a Euclidean



line. Its general equation is of the form

$$Az\bar{z} + \bar{B}z + B\bar{z} + C = 0, \quad (4)$$

where  $A, C \in \mathbb{R}$  and  $|B|^2 > AC$ .

Where  $z = \infty$  is a solution iff  $A = 0$ .

$A = 0$ : line

$C = 0$ : goes through the origin.

There is a unique circle passing through any 3 distinct points in  $\mathbb{C}_\infty$ .

### Theorem 8.5

Let  $f \in \mathcal{M}$  and  $C$  a circle in  $\mathbb{C}_\infty$ , then  $f(C)$  is a circle in  $\mathbb{C}_\infty$ .

*Proof.* By ??, just need to consider  $f(z) = az$ ,  $z + b$  or  $\frac{1}{z}$ . Let  $S_{A,B,C}$  be the circle defined by ??.

$$f(z) = az : S_{A,B,C} \mapsto S_{A/a\bar{a}, B/\bar{a}, C}$$

$$f(z) = z + b : S_{A,B,C} \mapsto S_{A, B-Ab, C+Ab\bar{b}-\bar{B}b-B\bar{b}}$$

$$f(z) = \frac{1}{z} = w : S_{A,B,C} \mapsto A + Bw + \bar{B}\bar{w} + Cw\bar{w} = 0 = S_{C, \bar{B}, A}.$$

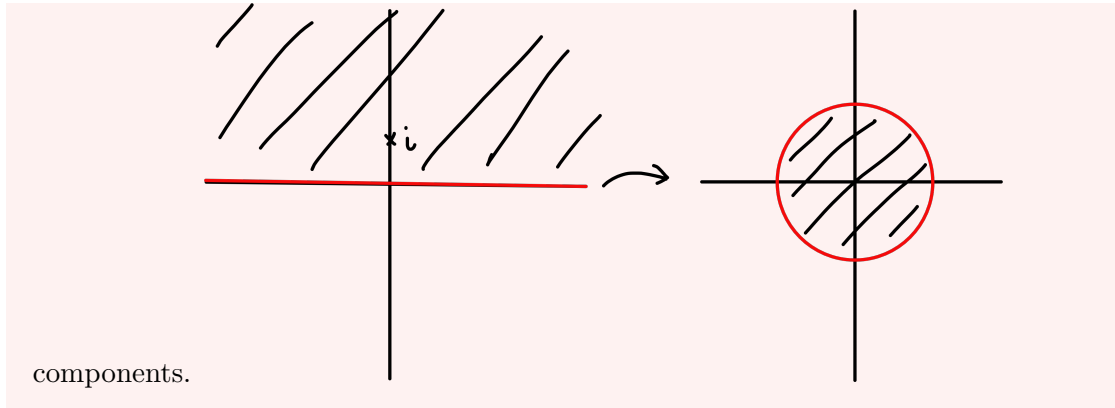
□

### Example 8.1

Consider the image of  $\mathbb{R} \cup \{\infty\}$  (a circle in  $\mathbb{C}_\infty$ ) under

$$f(z) = \frac{z-i}{z+i}.$$

It is thus a circle in  $\mathbb{C}_\infty$  containing  $f(0) = -1$ ,  $f(\infty) = 1$ ,  $f(1) = -i$  so  $f(\mathbb{R} \cup \{\infty\}) =$  unit circle. Furthermore, complimentary components are mapped to complementary



### §8.3 Cross-Ratios

#### Definition 8.4

The cross-ratio of distinct points  $z_1, z_2, z_3, z_4 \in \mathbb{C}$ .

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

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

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

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

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

Note  $[0, 1, w, \infty] = \frac{-w}{-1} = w$

*Warning:* different authors use different permutations of 1, 2, 3, 4 in the definition.

#### Theorem 8.6

Given  $z_1, z_2, z_3, z_4 \in \mathbb{C}_\infty$  distinct  $w_1, w_2, w_3, w_4 \in \mathbb{C}_\infty$  distinct then  $\exists f \in \mathcal{M}$  s.t.  $f(z_i) = w_i \iff [z_1, z_2, z_3, z_4] = [w_1, w_2, w_3, w_4]$ . In particular, Möbius maps preserve cross-ratios  $[z_1, z_2, z_3, z_4] = [f(z_1), f(z_2), f(z_3), f(z_4)]$

*Proof.* ( $\implies$ ): Suppose  $f(z_j) = w_j$  and  $z_i, w_i \neq \infty \forall i$  and  $f(z) = \frac{az+b}{cz+d}$ , then

$$cz_j + d \neq 0 \quad \forall j.$$

$$\begin{aligned} \text{So, } w_j - w_k &= f(z_j) - f(z_k) \\ &= \frac{(ad - bc)(z_j - z_k)}{(cz_j + d)(cz_k + d)} \\ \implies [z_1, z_2, z_3, z_4] &= [w_1, w_2, w_3, w_4] \\ &= [f(z_1), f(z_2), f(z_3), f(z_4)] \end{aligned}$$

Need to check other cases;  $z_1 = \infty, w_1 = f(\infty) = \frac{a}{c}$  etc.

( $\Leftarrow$ ): Suppose  $[z_1, z_2, z_3, z_4] = [w_1, w_2, w_3, w_4]$ . Let  $g \in \mathcal{M}$  s.t.  $g(z_1) = 0, g(z_2) = 1, g(z_4) = \infty$  as triple transitive. Let  $h \in \mathcal{M}$  s.t.  $h(w_1) = 0, h(w_2) = 1, h(w_4) = \infty$ .

$$\begin{aligned} g(z_3) &= [0, 1, g(z_3), \infty] \\ &= [g(z_1), g(z_2), g(z_3), g(z_4)] \\ &= [z_1, z_2, z_3, z_4] \text{ by above} \\ &= [w_1, w_2, w_3, w_4] \\ &= [h(w_1), h(w_2), h(w_3), h(w_4)] \\ &= [0, 1, h(w_3), \infty] \\ &= h(w_3). \end{aligned}$$

So  $h^{-1}g$  is required map. □

So  $[z_1, z_2, z_3, z_4] = f(z_3)$  where  $f$  is the unique Möbius map that sends  $z_1 \mapsto 0, z_2 \mapsto 1, z_4 \mapsto \infty$ .

### Corollary 8.3

$z_1, z_2, z_3, z_4$  lie in some circle in  $\mathbb{C}_\infty \iff [z_1, z_2, z_3, z_4] \in \mathbb{R}$ .

*Proof.* Let  $C$  be a circle through  $z_1, z_2, z_4$ .

Let  $g : C \rightarrow \mathbb{R} \cup \{\infty\}$  s.t.  $g(z_1) = 0, g(z_2) = 1, g(z_4) = \infty$ .

$$\begin{aligned} g(z_3) &= [0, 1, g(z_3), \infty] \\ &= [g(z_1), g(z_2), g(z_3), g(z_4)] \\ &= [z_1, z_2, z_3, z_4] \text{ by ??} \\ \text{So, } [z_1, z_2, z_3, z_4] \in \mathbb{R} &\iff g(z_3) \in \mathbb{R} \\ &\iff z_3 \in C. \end{aligned}$$

□