

# 1a Lectures on Groups

Rachel Camina  
notes by  
Thomas Forster

November 4, 2017

## Contents

<b>1</b>	<b>Subgroups</b>	<b>4</b>
<b>2</b>	<b>Isomorphism and Homomorphism</b>	<b>5</b>
2.1	Homomorphism . . . . .	6
<b>3</b>	<b>Symmetric and Dihedral Groups</b>	<b>9</b>
3.1	Dihedral Groups . . . . .	15
3.2	Group Presentations . . . . .	16
<b>4</b>	<b>Cosets and Lagrange</b>	<b>17</b>
<b>5</b>	<b>Normal Subgroups, Quotient Groups and Homomorphisms</b>	<b>20</b>
5.1	Examples of normal subgroups . . . . .	22
<b>6</b>	<b>Direct (cartesian) Products</b>	<b>27</b>
<b>7</b>	<b>Small groups</b>	<b>30</b>
7.1	Realisations of $Q_8$ . . . . .	32
<b>8</b>	<b>Group Actions</b>	<b>34</b>
<b>9</b>	<b>Symmetries of Regular Solids</b>	<b>40</b>
9.1	The Tetrahedron . . . . .	40
9.2	The Cube . . . . .	41
9.3	The Dodecahedron . . . . .	42
9.4	Conjugacy Action . . . . .	44
9.5	Conjugation in $S_n$ . . . . .	45

<b>10 Matrix Groups</b>	<b>48</b>
10.0.1 some remarks . . . . .	50
10.0.2 Case 1 . . . . .	52
10.0.3 Case 2 . . . . .	52
10.1 Now consider the three-dimensional case . . . . .	52
<b>11 The Möbius Group</b>	<b>54</b>
11.0.1 Conjugacy classes in $M$ . . . . .	58

Dr. Rachel Camina, rdc26@dpmms.cam.ac.uk  
 Recommended reading: Alan Beardon Algebra and Geometry

Symbols:  $\forall \exists, \rightarrow$ , s.t.,  $\therefore$ ,  $\mathbb{Z}$ ,  $\mathbb{N}$ ,  $\mathbb{R}$ , and a  $\mathbb{C}$  for the complexes.

A binary operation is a way of combining two elements.

A group is a set  $G$  with an operation  $*$ .  $(G, *)$  is a group iff the following axioms are satisfied

- |   |                                   |
|---|-----------------------------------|
| (i) $x, y \in G \rightarrow x * y \in G$                      | closure                           |
| (ii) $(\exists e \in G)(\forall x \in G)(e * x = x = x * e)$  | Existence of an Identity element  |
| (iii) $(\forall x \in G)(\exists y \in G)(x * y = e = y * x)$ | Existence of [two-sided] inverses |
| (iv) $x * (y * z) = (x * y) * z$                              | Associativity                     |

Now for some illustrations (some of them are examples, some of them are failures)

1.  $\mathbb{Z}$  with  $+$  ... is a group
2.  $\mathbb{Q}$  with  $+$  ... is a group;  $\mathbb{R}$  with  $+$  ... is a group
3.  $\mathbb{Z}$  with  $-$ . Has closure, has an identity and has inverses but associativity fails.
4.  $\mathbb{Z}$  with  $\times$ . Has closure and identity and associativity but no inverses.
5.  $\mathbb{Q}$  with  $\times$ . Has closure and identity and associativity but 0 lacks an inverse.
6.  $\{1, -1\}$  with  $\times$ .

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

$e$  is 1 in this case.

7.  $\{0, 1, 2\}$  equipped with  $+_3$  (aka addition mod 3). It's a group.  $e$  is 0; inverse of 1 is 2 and vice versa.

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

8.  $\{e, a, b, c\}$  equipped with the following multiplication table:

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

It's closed; it has an identity; everything has an inverse—look down the main diagonal! [Dr C didn't say anything at this stage about associativity ...] We will see later that this is the group  $C_2 \times C_2$ .

9. Rotations and reflections of an equilateral triangle. Label the vertices '1', '2' and '3'. There is a rotation thru'  $2\pi/3$  radians, and for each vertex, a reflection about the perpendicular bisector thru' that vertex.

The operation  $*$  is composition [which makes it obvious that associativity holds] and we get a group with 6 elements. Might be an idea to write out a multiplication table. (For you, Dear Reader, not me!)

10.  $M_2(\mathbb{R})$ :  $2 \times 2$  matrices "over"  $\mathbb{R}$  (with entries in  $\mathbb{R}$ .)  $*$  is matrix addition (aka "pointwise" or "co-ordinatewise" addition)
11.  $GL_2(\mathbb{R})$ : Invertible  $2 \times 2$  matrices over  $\mathbb{R}$  where  $*$  is matrix multiplication.

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \notin \mathbb{R} \wedge (ad - bc \neq 0) \right\} \quad ()$$

Recall that

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

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

- (1) *The identity is unique.*  
(2) *Inverses are unique.*

*Proof:*

[Dear Reader: try to work this one out for yourself. Then check your answer against what i copied off the blackboard.]

(1) Suppose  $e$  and  $\hat{e}$  are both identities. Then  $e * \hat{e} = e$  (beco's  $\hat{e}$  is an identity) and  $e * \hat{e} = \hat{e}$  (beco's  $e$  is an identity) so  $e = \hat{e}$ .

(2) Suppose  $x$  has two inverses:  $y$  and  $z$ . Both these inverses are two-sided.

$yxz = z$  beco's  $y$  is a left inverse;

$yxz = y$  beco's  $z$  is a right inverse;

whence  $y = z$ . ■

Observe that what we have actually shown is that if  $x$  has both a left inverse and a right-inverse then they are the same.

## Remarks

- Associativity means we can omit brackets. We can prove this by induction on the number of brackets. [Dear Reader: do not worry about this proof *pro tem*. Check the details if you like but don't stress]
- Often, when it's clear from context what the group operation is, we simply drop the ' $*$ '.
- Use uniqueness of inverses to prove  $(xy)^{-1} = y^{-1}x^{-1}$
- Prove  $(x^{-1})^{-1} = x$ . (Premultiply by  $x^{-1}$ )

**DEFINITION 1** A group  $(G, *)$  is abelian if  $*$  is commutative.

[end of first lecture]

What's purple and commutes? An Abelian grape.

The multiplication table of an abelian grape is symmetric about the main diagonal.

Multiplication of matrices and the composition of the operations on triangles above are not commutative.

We use ' $\circ$ ' or ' $\cdot$ ' for composition.

$(G, *)$  is a *finite* group iff  $G$  is finite.  $|G|$  is the *order* of the group  $(G, *)$ , the number of elements in the set  $G$ .

miniexercise: which of the groups in the list in the first lecture are finite.

A: 1, 2, 6, 11 and 12 are all infinite, and the others are finite.

7) has order 2; 8) has order 3; 9) has order 4 and 10) has order 6.

## 1 Subgroups

This is our first encounter with the notion of *substructure*.

$(H, *)$  is a subgroup of  $(G, *)$  if

- (i)  $H \subseteq G$
  - (ii)  $(H, *)$  is a group
  - (iii) The operation  $*$  on  $H$  is the restriction of the operation  $*$  on  $G$ .
- We say  $(H, *)$  "inherits" the operation from  $(G, *)$ .

We write " $(H, *)$  is a subgroup of  $(G, *)$ " as " $(H, *) \leq (G, *)$ ". (There is a certain amount of abuse of notation going on: people often write ' $H$ ' instead of  $(H, *)$ .)

It's obvious that if  $*$  was associative on  $G$ , and  $H \subseteq G$  then the restriction of  $*$  to  $H$  is associative too.

Some illustrations

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

2.  $(\{1, -1\}, \times) \leq (\mathbb{Q} \setminus \{0\}, \times)$ ;
3. In example 9 from lecture 1  $\{1, \sigma, \sigma^2\}$  equipped with composition is a subgroup. (Remark:  $\sigma$  is the rotation;  $\tau_i$  is the reflection in vertex  $i$ . Further remark: she wrote ‘1’ instead of ‘ $e$ ’ out of force of habit ... it’s common to use the letter ‘1’ to denote the identity of a group.)
4. In example 12 we have the subgroup of matrices of determinant 1. This works because the determinant of the product of two matrices is the product of the determinants. Write out a proof if you are not sure. This subgroup is called  $SL_2(\mathbb{R})$ , where the ‘ $S$ ’ means *Special*.
5.  $(\{e\}, *)$  is a subgroup of every group (at least if we pretend that all groups have the same identity element, which we sort-of can). It’s the *trivial* subgroup;
6.  $(G, *) \leq (G, *)$ . It’s the “improper” subgroup.

## 2 Isomorphism and Homomorphism

When are two groups the same group? if we took example 9) from lecture 1 and systematically replaced all the Roman letters by Greek letters it would still (in the sense we are interested in) be the same group. Let’s spell out what we might mean by this.

We need to say a bit about functions

$f : A \rightarrow B$  is a function if  $(\forall a \in A)(\exists! b \in B) f$  sends  $a$  to  $b$ .

Here are some examples:

$$f : \mathbb{Z} \rightarrow \mathbb{Z}: f(x) = x + 1$$

$$g : \mathbb{Z} \rightarrow \mathbb{Z}: g(x) = 2x$$

$$h : \mathbb{Z} \rightarrow \mathbb{Z}: f(x) = x^2$$

$$j : \{0, 1, 2, 3, 4\} \rightarrow \{0, 1, 2, 3, 4\} \text{ by: if } X < 4 \text{ then } x \mapsto x + 1; 4 \mapsto 4;$$

$$k : \{0, 1, 2, 3, 4\} \rightarrow \{0, 1, 2, 3, 4\} \text{ by: if } X < 4 \text{ then } x \mapsto x + 1; 4 \mapsto 0.$$

If  $f, g$  both  $A \rightarrow B$  with  $(\forall a \in A)(f(a) = g(a))$ , then we say  $f = g$ . [ $f$  and  $g$  have the same *extent* or *extension* and we say they are the same *function-in-extension*.]

### Composition of functions

If  $g : A \rightarrow B$  and  $f : B \rightarrow C$  then  $f \circ g : A \rightarrow C$  and  $f \circ g(a) = f(g(a))$ .

Consider the two function  $f, g : \mathbb{Z} \rightarrow \mathbb{Z}$  as above. Then  $f \circ g(x) = 2x + 1$ .

At this point one should draw  $j$  and  $k$  as digraphs, but don’t know how to do digraphs in L<sup>A</sup>T<sub>E</sub>X!

$k$  is *injective* and  $j$  isn't. An injective function never sends distinct arguments to the same value.

$k$  is *surjective* and  $j$  isn't. An injective function never sends distinct arguments to the same value. A function is surjective if “everything [in the target] gets hit”. We sometimes use a special arrow: thus “ $f : A \twoheadrightarrow B$ ” means that  $f$  is surjective

A function is bijective iff it is both injective and surjective.

$f, g$  and  $k$  are injective;  $f$  and  $k$  are surjective;  $f$  and  $k$  are bijective.

Key point: if  $f : A \rightarrow B$  it has an inverse! The inverse is written ‘ $f^{-1}$ ’.  $f \circ f^{-1} = 1_B$ ;  $f^{-1} \circ f = 1_A$ . This makes  $f^{-1}$  a *two-sided* inverse. The inverse we find in groups are also two-sided. [You might like to reflect on the possibility of a surjection  $A \twoheadrightarrow B$  having a right-sided inverse but no left-sided inverse.]

**REMARK 1** *If  $A$  is finite and  $f : A \rightarrow A$  is injective then  $f$  is surjective.*

Indeed the converse is Dedekind’s definition of finite: a set  $X$  is infinite iff there is an injection  $X \rightarrow X$  that is not a surjection.

**LEMMA 2** *Suppose  $g : A \rightarrow B$  and  $f : B \rightarrow C$ . Then they are both (in)(sur)(bi)jective iff  $g \circ f$  is (in)(sur)(bi)jective.*

Proof omitted. [Dear Reader, i have one written out somewhere if you need it]

## 2.1 Homomorphism

We are interested in maps that “respect” the group operations.

**DEFINITION 2** *Let  $(G, *_G)$  and  $(H, *_H)$  be groups.*

*We say  $\theta : G \rightarrow H$  is a homomorphism if*  
 $(\forall g_1, g_2 \in G)(\theta(g_1) *_H \theta(g_2) = \theta(g_1 *_G g_2))$

[Of course we also want  $\theta(e_G) = e_H$  and we want  $\theta$  to preserve complements but we’re going to ignore those for the moment while we press on with some illustrations].

Let  $G$  be  $\{0, 1, 2, 3\}$  and let  $H$  be  $\{1, e^{\pi i/2}, e^{\pi i}, e^{3\pi i/2}\}$ , the set of the fourth roots of unity. Equip  $G$  with  $+_3$  (addition mod 3) and equip  $H$  with (complex) multiplication. Both are groups, and there is a bijection between them given by  $n \mapsto e^{n\pi i/2}$ . This bijection respects the group operations. These two groups are—in the sense we are interested in—the same group. (The form of words that used to be used and sometimes still is, is that they are the same *abstract* group. Distinct as concrete groups.)

[end of second lecture]

**LEMMA 3** *Let  $(G, *_G)$ ,  $(H, *_H)$  be groups with  $\theta : G \rightarrow H$  a homomorphism. Then the image of  $G$  in  $\theta$  is a subgroup of  $H$ .*

[Dear Reader: lots of things to be careful of here. (i) The word ‘image’ is overloaded or frankly misused. People sometimes talk of image (of a function) when they mean a value of the function. You should use ‘image’ only when you mean *set of values*, as here. The image of  $G$  in  $\theta$  is  $\{\theta(g) : g \in G\}$ , and Dr Camina writes ‘ $\theta(G)$ ’ for this. This widespread deplorable habit is sort-of OK: you can tell that  $\theta(g)$  is a group *element* while  $\theta(G)$  is a group (a *set* of elements) beco’s of context, but this kind of disambiguation is not always possible and the overloading of the parenthesis notation is bad practice, tho’ almost universal. I was brought up to write ‘ $\theta“G$ ’ for the image of  $G$  in  $\theta$  and that’s what i shall consistently do here.]

Closure: If  $x, y \in \theta“G$  then there are  $g, h \in G$  (not neccessarily distinct) with  $x = \theta(g)$  and  $y = \theta(h)$ . Then  $x *_H y = \theta(g) *_H \theta(h) = \theta(g *_G h)$  and this last thing is in the range of  $\theta$  as desired.

[Dear Reader: the **range** of a function  $f$  defined on a set  $A$  is  $f“A$ . I don’t seem to have defined it earlier]

■ I should probably supply some more details here

**DEFINITION 3** *A group homomorphism that is a bijection is an isomorphism. If  $\theta : G \rightarrow H$  is a bijection we say  $G$  and  $H$  are isomorphic and we write ‘ $G \cong H$ ’.*

Example: The integers mod 4 with addition and the 4th roots of unity with multiplication are isomorphic.  $n \mapsto e^{2n\pi/2}$  is the obvious isomorphism. [Are there any others, Dear Reader?]

You can think of two isomorphic groups as being the same group with the elements labelled differently.

#### LEMMA 4

1. *The composition of two homomorphisms is a homomorphism;*
2. *The composition of two isomorphisms is a isomorphism;*
3. *The inverse of an isomorphism is an isomorphism.*

[while we are about it we may as well observe that the identity map from a group to itself is an isomorphism.]

*Proof:*

- (1) Suppose  $\theta_1 : (G_1, *_1) \rightarrow (G_2, *_2)$  and  $\theta_2 : (G_2, *_2) \rightarrow (G_3, *_3)$  are homomorphisms. Then  $\theta_2 \cdot \theta_1$  is a map  $G_1 \rightarrow G_3$ .

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



- (2) By lemma 2 composition of bijections is a bijection.
- (3) Suppose  $\theta : (G_1, *_1) \rightarrow (G_2, *_2)$  is an isomorphism. Then  $\theta$  is a bijection and accordingly has an inverse. This inverse is also an isomorphism, as follows.

Suppose  $y, z \in G_2$ . Then there are  $x, k \in G_1$  with  $\theta^{-1}(y) = x$  and  $\theta^{-1}(z) = k$ .

Then  $\theta(x) = y$  and  $\theta(k) = z$ .

$$y *_2 z = \theta(x) *_2 \theta(k) = \theta(x *_1 k)$$

■

#### DEFINITION 4

*Exponent notation:  $x^n$  is  $x$  starred with itself  $n$  times.  $x^0$  is  $e$ , and  $x^{-n}$  is the inverse of  $x^n$ .*

*A group  $(G, *)$  is cyclic if there is an element  $g$  of  $G$  such that every element of  $G$  is a power of  $g$ . Such a  $g$  is a generator.*

*Beware: there may be more than one such element!*

*The “order” of an element  $g$  in a group is a number, the same number as the size (which, too is called ‘order’) of the cyclic subgroup of powers of  $g$ . We will write it as ‘ $o(g)$ ’.*

This number might be infinite of course.

Examples:

- $(\mathbb{Z}, +)$  is cyclic, and it has generators 1 and  $-1$ . Both these generators have infinite order
- $\{1, -1\}$  with  $\times$  is cyclic with generator  $-1$ , which has order 2
- $\{0, 1, 2, 3\}$  with addition mod 4 is cyclic and has generator 1 (or 3), both of which have order 4.
- Example 10 earlier: The subgroup  $\{1, \sigma, \sigma^2\}$  is cyclic and has generator  $\sigma$ . Or  $\sigma^2$ ! Both generators have order 3.

It seems that whenever a cyclic group has more than one generator then the generators all have the same order ...

Cyclic groups are Abelian. (This is beco’s the group multiplication corresponds to addition on the exponents, and addition on  $\mathbb{Z}$  is abelian.)

The subgroup of  $G$  generated by an element  $g$  is the  $\subseteq$ -least subset of  $G$  containing  $g$  and closed under the group operations. (And then of course equipped with those operations, to make it a group not a mere set.)

The  $n$ th roots of unity with complex multiplication is (‘are’?) the same (abstract) group as the interval  $[0, n - 1]$  of  $\mathbb{N}$  (the square bracket notation means what you think it means) equipped with addition mod  $n$ . We call this [abstract] group ‘ $C_n$ ’ and we say that the two [concrete] groups i have just described are “realisations” of it.

[end of third lecture]

The “kernel”  $\ker(\theta)$  of a homomorphism  $\theta : G \rightarrow H$  is  $\{g \in G : \theta(g) = e_H\}$ , aka “the preimage of the singleton of the identity under  $\theta$ ”. I was brought up to write images with double apostrophes (see above) so i write this  $\theta^{-1}“\{e\}$ ”.

**REMARK 2** Let  $G$  be a group and  $g_1 \dots g_k$  elements of  $G$ . Then  $\langle g_1 \dots g_k \rangle$  is the “subgroup generated by  $g_1 \dots g_k$ ”. It’s  $\bigcap \{G' \leq G : \{g_1, \dots, g_k\} \subseteq G'\}$ , the intersection of all the subgroups of  $G$  that contains all the  $g_i$ .

Observe that the intersection of a hatful of groups is a group (see sheet 1 exercise 2) so this intersection really is a group.

### 3 Symmetric and Dihedral Groups

A bijection  $X \rightarrow X$  of a set  $X$  is a *permutation* of  $X$ . The collection of permutations of a fixed set  $X$ , equipped with composition, is a group, the symmetric group on  $X$ , aka  $Sym(X)$ . Check

- (i) Closure: a composition of two permutations is a permutation. (We showed in lemma 2 that a composition of two bijections is a bijection)
- (ii)  $e_{Sym(X)}$  is obviously going to be the identity relation on [the members of]  $X$ . This function is written variously:  $\mathbb{1}_X$ ,  $\Delta_X$  and God Knows what else.
- (iii) Associativity. Didn’t we show earlier that composition of relations is associative? [will supply more details if called upon]

We will write ‘ $S_n$ ’ for the abstract group corresponding to  $Sym(X)$  where  $X$  is a set with  $|X| = n$ .  $S_n$  is the “symmetry group of degree  $n$ ”. (NB: ‘degree’ ‘not order’! What is its order?)

We will use “double row notation”

If  $\sigma \in S_n$  think of it as a permutation of  $[1, n]$ , so we are thinking of  $S_n$  concretely as  $Sym([1, n])$ . We represent the information in  $\sigma$  in a table:

$$\left( \begin{array}{cccc} 1 & 2 & 3 & \dots n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots \sigma(n) \end{array} \right) \quad (1)$$

Let’s now have a look at some of the  $S_n$ , for small  $n$ .

$$(1) S_1 = \left\{ \left( \begin{array}{c} 1 \\ 1 \end{array} \right) \right\}$$

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

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

It is the triangle group we saw earlier.

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$  is  $\sigma$ ;  $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$  is  $\sigma^2$ ;  $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$  is  $\tau_1$ ;  $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$  is  $\tau_2$ ;

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$  is  $\tau_3$ .

$S_3$  is nonabelian: the rotation  $\sigma$  does not commute with  $\tau_1$  (nor with  $\tau_2$  or  $\tau_3$ ).

What are the subgroups of  $S_3$ ? Answer:  $\langle \sigma \rangle$  (which is of course the same as  $\langle \sigma^2 \rangle$ ) and the three subgroups  $\langle \tau_1 \rangle$ ,  $\langle \tau_2 \rangle$  and  $\langle \tau_3 \rangle$  generated by the three reflections, all of which are realisations of  $C_2$ —the cyclic group on two elements. They are also, of course, realisations of  $S_2$ , corresponding to the symmetric group on two-membered subsets of the vertex set.

Observe that, for  $n \geq 4$ ,  $S_n$  is nonabelian. Any group with a nonabelian subgroup is nonabelian, and  $S_3 \leq S_n$  for any  $n \geq 3$ :

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

and

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

clearly do not commute.

**DEFINITION 5** Suppose  $\{a_1, \dots, a_k\} \subseteq [1, n]$ , and  $\sigma$  sends each  $a_i$  to  $a_{(i+k)1}$  (addition mod  $k$  on the subscripts). We write  $\sigma$  as  $(a_1, \dots, a_k)$ . This object is also denoted by the expression  $(a_2 \dots a_k, a_1)$ . (The subscripts have a “circular” order).

... the point being that everything *not* mentioned inside the brackets is fixed.

When the things being permuted in a cycle come equipped with a natural order, we tend to write the “smallest” one first: thus “ $(a_1, a_2, a_3)$ ” rather than “ $(a_2, a_3, a_1)$ ”.

If  $\sigma = (a_1, \dots, a_k)$  we say that the cycle  $\sigma$  is a *rotation* of the  $a_i$ . What is  $\sigma^{-1}$ ? Obviously  $(a_k, \dots, a_1)$  with the subscripts decreasing. But we would tend to write it as  $(a_1, a_k, a_{k-1}, \dots, a_2)$

Cycles of order 2 are *transpositions*.

**DEFINITION 6** Two cycles are **disjoint** iff their supports are disjoint.

“Supports”? The *support* of a permutation  $\sigma$  is the set  $\{x : \sigma(x) \neq x\}$  of things moved by  $\sigma$ , often written ‘ $\text{supp}(\sigma)$ ’.

**LEMMA 5** *Disjoint cycles commute.*

*Proof:* Suppose  $\sigma$  and  $\tau$  are disjoint cycles. We will show that

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

There are three cases to consider:

- (i)  $x \in \text{supp}(\sigma) \setminus \text{supp}(\tau)$ ;
- (ii)  $x \in \text{supp}(\tau) \setminus \text{supp}(\sigma)$ ;
- (iii)  $x$  fixed by both  $\tau$  and  $\sigma$ .

(iii) is obvious. (i) and (ii) are analogous so i shall prove (i) only.

$$\sigma \circ \tau(x) = \sigma(x) \text{ beco's } \tau(x) = x.$$

$$\tau \circ \sigma(x) = \tau(\sigma(x)) = \sigma(x), \text{ the second equality holding beco's } \tau \text{ fixes everything in } \text{supp}(\sigma).$$

■

Observe that what we have actually just proved is that if  $\sigma$  and  $\tau$  are a pair of disjoint permutations then they commute. If the supports overlap then they mightn't commute: e.g  $(1, 2) \cdot (2, 3) = (2, 3, 1) \neq (2, 3) \cdot (1, 2) = (2, 1, 3)$ <sup>1</sup>.

[end of fourth lecture]

When we think of  $S_n$  concretely it is the group of all permutations of  $[1, n]$

**THEOREM 1** *Every permutation in  $S_n$  ( $n \geq 2$ ) can be written as a product of disjoint cycles, the product being unique up to order.*

*Proof:*

And the cycles themselves are unique up to rotation! Two levels of abstraction. It would be nice if we could write the cycles as spinning circles on the page, so they we didn't have this spurious reduplication of notation, but sadly pages are static objects. A .gif file perhaps ...

Let's just do an example, that should do the trick.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 5 & 7 & 6 & 3 & 1 & 9 & 8 \end{pmatrix}$$

$$1 \mapsto 2 \mapsto 4 \mapsto 7 \mapsto 1$$

$$3 \mapsto 5 \mapsto 6 \mapsto 3$$

$$8 \mapsto 9 \mapsto 8$$

---

<sup>1</sup>Actually we would leave out the ‘.’ and write ‘ $(1, 2)(2, 3) \neq (2, 3)(1, 2)$ ’.

So this permutation is represented by the product  $(1, 2, 4, 7)(3, 5, 6)(8, 9)$ . And—beco's these cycles are disjoint—it doesn't matter in what order we write them. [Given that the cycles can themselves be rotated, how many equivalent ways are there, Dear Reader, of writing this product? (just checking!!)]

One thing that might bother you, Dear Reader (it sort-of bothers me) is the way in which the standard notation— $(1, 2, 4, 7)(3, 5, 6)(8, 9)$  is our example in-hand—suggests that when we apply this permutation to an argument we first apply  $(8, 9)$  to the argument, then apply  $(3, 5, 6)$  to the result, and then apply  $(1, 2, 4, 7)$  to the output of that. But of course we don't. What we do is: look for the cycle in which our argument appears (if there is one, and if there isn't, do nothing) and apply *that* cycle. An ideal notation for this permutation would be one that displayed the three cycles in a way that had perfect threefold symmetry, so that none of them had a distinguished position but of course there is no way of doing that!

Let's write something snotty and official.

Suppose  $a \in \text{supp}(\sigma)$ . Consider the sequence  $a, \sigma(a), \sigma^2(a) \dots$ . The support of  $\sigma$  is finite, so this sequence is finite, and something must appear for a second time. Now  $\sigma$  is a bijection, so when the sequence rejoins it cannot rejoin in the middle (for o/w something in it would be  $\sigma$  of two different arguments) so it must go back to the beginning. So we have a cycle. ■

**LEMMA 6** *Let  $g$  be a group element. Then  $g^n = e$  iff  $o(g)|n$ .  
[the order of  $g$  divides  $n$ ].*

*Proof:*

$L \rightarrow R$ : easy!

$R \rightarrow L$ : Suppose  $g^n = e$  where  $n$  is not a multiple of  $o(g)$ . Then  $n = k \cdot (o(g)) + m$  for some  $m < n$ . Then

$$e = g^n = g^{k \cdot (o(g)) + m} = g^{k \cdot (o(g))} \cdot g^m = e^k \cdot g^m = g^m$$

so  $n|m$  contradicting  $m < n$ . ■

**LEMMA 7**

*Let  $\sigma, \tau$  be disjoint cycles in  $S_n$ . Then  $o(\sigma \cdot \tau) = LCM(o(\sigma), o(\tau))$*

Write ' $k$ ' for  $LCM(o(\sigma), o(\tau))$ . Then consider  $(\sigma \cdot \tau)^k = \sigma \cdot \tau \cdot \sigma \cdot \tau \cdot \sigma \cdot \tau \cdot \sigma \cdot \tau \dots$

Since  $\sigma$  and  $\tau$  commute [they are disjoint, after all] we can rearrange to get  $\sigma^k \tau^k = e \cdot e = e$ . Now we must show that  $k$  is minimal s.t.  $(\sigma \cdot \tau)^k = 1$ . So suppose  $(\sigma \tau)^n = e$ . Then, rearranging as before, we get  $\sigma^n \tau^n = 1$ . So  $\sigma^n$  and  $\tau^n$  are inverse. How can this be? They're disjoint! The answer must be that they are both  $e$ . So  $o(\sigma)|n$  and  $o(\tau)|n$ , whence  $k|n$ . ■

**PROPOSITION 1** *Any  $\sigma \in S_n$  can be written as a product of transpositions.*

*Proof:* .

It will suffice to show that any cycle can be written as a product of transpositions. So here's an illustration:

$(a_1, \dots, a_k)$  can be written as  $(a_1, a_2)(a_2, a_3)(a_3, a_4)(a_4, a_5) \cdots (a_{k-1}, a_k)$

You then have to go through this by hand to check that it works!

■

The order of the transpositions in the product matters (beco's transpositions that overlap don't commute, as we saw earlier) but are we applying this product left-to-right or right-to-left? I think we are doing it properly, applying the rightmost first. . . .

Now for the annoying bit! The representation as a product of transpositions is not unique! Grrr!

$(1, 2, 3, 4, 5) = (1, 2)(2, 3)(3, 4)(4, 5) = (1, 2)(1, 2)(1, 2)(2, 3)(3, 4)(4, 5)$  or even  $(1, 5)(1, 4)(1, 3)(1, 2)$

**DEFINITION 7** Suppose  $\sigma \in S_n$ ,  $n \geq 2$ . Let us say the **sign** of  $\sigma$  is  $(-1)^k$  where  $k$  is the number of factors in a representation of  $\sigma$  as a product of transpositions.

It remains to be shown that

**LEMMA 8**  $\text{sign}(\sigma)$  is well-defined.

. . . which is to say that  $\text{sign}(\sigma)$  does not depend on the choice of transpositions for  $\sigma$ .

*Proof:*

We start with a special case. Let  $\sigma$  be a permutation expressed as a product of cycles, and  $\tau$  the permutation  $(k, l)$ . We develop a representation of  $\sigma\tau$  as a product of cycles, given a representation of  $\sigma$  as a product of cycles.

There are two cases to consider, depending on whether or not  $k$  and  $l$  belong to the same  $\sigma$ -cycle.

Case (i)  $k$  and  $l$  belong to the same  $\sigma$ -cycle.

So  $\sigma$  has a cycle  $(k, a_1 \cdots a_n, l, b_1 \cdots b_m)$ . What happens if we do  $\tau$  and then  $\sigma$ ? We get  $(k, b_1 \cdots b_m)(l, a_1 \cdots a_n)$ . One more cycle!

check this calculation

Case (ii)  $k$  and  $l$  belong to different  $\sigma$ -cycles:  $(k, a_1 \cdots a_n)$  and  $(l, b_1 \cdots b_m)$ . What happens if we do  $\tau$  and then  $\sigma$ ?

In the product:

$$\begin{array}{llll} k & \mapsto^\tau & l & \mapsto^\sigma b_1; \\ b_1 & \mapsto^\tau & b_1 & \mapsto^\sigma b_2; \\ & & \vdots & \\ b_m & \mapsto^\tau & b_m & \mapsto^\sigma l \\ l & \mapsto^\tau & k & \mapsto^\sigma a_1 \end{array}$$

$$\begin{array}{ccccc}
a_1 & \mapsto^\tau & a_1 & \mapsto^\sigma & a_2 \\
& & \vdots & & \\
a_n & \mapsto^\tau & a_n & \mapsto^\sigma & k
\end{array}$$

The two cycles get spliced together:  $(k, b_1 \cdots b_m, l, a_1, \cdots a_n)$   
One fewer cycle!

To use this to prove that every permutation is either odd or even we need to think of the identity as the product of  $n$  trivial cycles. !?@!? Yes, i know, but trust me, i'm a doctor.

So suppose we have two decompositions of  $\sigma$  into products of transpositions.

$$\tau_1 \cdots \tau_a = \tau'_1 \cdots \tau'_b$$

We will show that  $(-1)^a = (-1)^b$ .

Think of  $\sigma$  both as  $\mathbf{1} \cdot \tau_1 \cdots \tau_a$  and  $\mathbf{1} \cdot \tau'_1 \cdots \tau'_b$ .

Multiply  $\mathbf{1}$  on the right by  $\tau_1$ . By the results earlier, this flips the parity of the number of cycles in our representation. Now multiply it on the the right by  $\tau_2$ . Flips it again. By the time we have done it  $a$  times the product is  $\sigma$  and its parity is  $(-1)^a$ .

Do the same with the other list of transpositions. In both cases you end with a representation of  $\sigma$  as a product of disjoint cycles. But the representation of  $\sigma$  as a product of disjoint cycles is unique! (up to rearrangement, so certainly up to the number of cycles and so certainly up to the parity of the number of cycles). Now the parity of the number of cycles in the two representation that we obtain of  $\sigma$  as a product of disjoint cycles is controlled precisely by the parity of the lengths of the two lists of transpositions. So the two lists must have the same parity! ■

**THEOREM 2** *Let  $n \geq 2$  be a natural number. Then*

*$\text{sign}: (S_n, \cdot) \twoheadrightarrow (\{1, -1\}, \times)$  is a [surjective] group homomorphism.*

Just check that it is indeed surjective and nontrivial:  $\text{sign}((1, 2)) = -1$  and  $\text{sign}(\mathbf{1}) = 1$ .

Check too that  $\text{sign}(\alpha) \times \text{sign}(\beta) = \text{sign}(\alpha \cdot \beta)$ . After all,  $\alpha$  and  $\beta$  are both products of transpositions.

Now  $\text{sign}$  is a homomorphism, and we showed earlier that the kernel of a homomorphism is always a group.

**DEFINITION 8**  $\sigma$  is even iff  $\text{sign}(\sigma) = 1$ , and odd otherwise.

Observe:  $\mathbf{1}$  is even beco's  $\mathbf{1} = (1, 2)(2, 1)$ . I prefer to think that  $\mathbf{1}$  is even beco's it's the product of the empty set of transpositions, and 0 is even.

The collection of even permutations is going to be the same group as the kernel of  $\text{sign}$ . [pretty obvious, really]. Check closure, inverse, assoc.

The inverse of a product of transpositions is just the same list written backwards. Product; easy. Associativity inherited as always.

The group of even permutations of  $n$  things is the **Alternating Group** on  $n$  things aka  $A_n$ .

$$A_4 = \{1, (123), (132), (124), (142), (234), (243), (134), (143), (12)(34), (13)(24), (14)(23)\}$$

I have written the cycles without commas. This is partly to save space, and also to make the point that it's OK to do so if the things being moved around are denoted by single characters so there is no need for delimiters!

**EXERCISE 1**  $|A_n| = |S_n|/2 = n!/2$

[Why is there the same number of odd permutations as even permutations?]

### 3.1 Dihedral Groups

Symmetry groups of regular polygons.

Can also think of them as distance-preserving maps from  $\mathbb{C}$  to  $\mathbb{C}$  that fix the  $n$ th roots of unity setwise. ("setwise"? ask your supervisor). So we will think of a dihedral group as acting on a polygon in the complex plane whose vertices are the  $n$ th roots of unity.

**DEFINITION 9** *The group of symmetries of a regular  $n$ -gon is the **dihedral group of order  $2n$**  and called ' $D_{2n}$ '*

Beware, some deviants think ' $D_n$ ' denotes the  $n$ th dihedral group, which is of course our  $D_{2n}$ .

There is an obvious embedding  $D_{2n} \hookrightarrow S_{2n}$  co's  $D_{2n}$  is moving  $2n$  things around.

Write a square in the plane and number its elements 1,2,3,4 clockwise.

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

[I hope i've copied these down properly: you should check, Dear Reader!]

**PROPOSITION 2** *Let  $n \geq 3$ . Then  $D_{2n}$  is a nonabelian group of order  $2n$  which naturally embeds into  $S_n$ . It is generated by  $\sigma$  of order  $n$  (a rotation) and  $\tau$  of order 2 (a reflection). Only one reflection needed!*

$$\{1, \sigma, \dots, \sigma^{n-1}, \tau, \sigma\tau, \sigma^2\tau, \dots, \sigma^{n-1}\tau\}$$



*Proof:*

Check that it really is a group ...

Composition of symmetries is another symmetry; inverse of a symmetry is another symmetry.

A choice of labelling (with  $[1, n]$ ) of the vertices of the regular  $n$ -gon [How many such labellings are there, Dear Reader?] defines an embedding from the group of symmetries of the regular  $n$ -gon into the symmetric group on  $[1, n]$  which of course is a realisation of  $S_n$ .

It's easy to find  $2n$  symmetries (rotations through  $(2\pi)/k$  for  $k \leq n$  plus  $n$  reflections—one in each vertex). Not immediately blindingly obvious that that is all there is. Must show that any symmetry is one of  $\{\mathbf{1}, \sigma, \dots, \sigma^{n-1}, \tau, \sigma\tau, \sigma^2\tau, \dots, \sigma^{n-1}\tau\}$ .

Let  $g$  be a symmetry. Suppose  $g$  moves vertex 1 to vertex  $j$ . Then  $g$  agrees with  $\sigma^{j-1}$  on the argument 1 at least. Now any symmetry must preserve adjacency of vertices, so  $g$  must move vertex 2 to vertex  $j-1$  and vertex  $n$  to vertex  $j+1$  or vertex 2 to vertex  $j+1$  and vertex  $n$  to vertex  $j-1$ . Using the fact that  $g$  must preserve adjacency we, in each case, can compute what  $g$  does to all the other vertices. In the first case  $g$  is a rotation and in the second case it's a rotation followed by a reflection. In this second case the reflection is in vertex  $j$  not vertex 1, and we are only allowed the rotation in vertex 1. However, the reflection in vertex  $i$  can be effected by rotating through  $-i$  and then reflecting in vertex 1. This composite is in the list above.

[end of fifth lecture]

Have i miscounted? Wasn't that the *sixth* lecture?

### 3.2 Group Presentations

Observe that if  $\sigma$  is a rotation and  $\tau$  a reflection in  $D_n$  then  $\sigma\tau$  is a reflection and is of order 2, which is to say  $\sigma\tau\sigma\tau = \mathbf{1}$  which is to say  $\tau\sigma\tau^{-1} = \sigma^{-1}$ .

We showed earlier (well, Dr Camina did, i am not happy with what i wrote down—might revise it later) that every symmetry of the regular  $n$ -gon is a product of rotations and reflections. We encapsulate this fact in the following impressive inscription

$$D_{2n} = \langle s, t : s^n = \mathbf{1}, t^2 = \mathbf{1}, tst = s^{-1} \rangle$$

What this says is that every element of the group  $D_{2n}$  can be obtained from the two elements  $s$  and  $t$  (that's them, to the left of the colon) by multiplying them together and making the identifications that follow the colon. These equations after the colon are the *relations*. *Prima facie* there could be infinitely many distinct products (there certainly are infinitely many *strings* of  $ss$ ,  $s^{-1}s$ ,  $t^{-1}s$  and  $ts$ ) but with luck they collapse down to finitely many (as they do in this case) once we make the identifications listed after the colon. And we do not identify two strings unless we are told to.

## 4 Cosets and Lagrange

**DEFINITION 10** *Left and right cosets:*

For  $G$  a group,  $H \leq G$  a subgroup of  $G$ , and  $g \in G$  we say  
 $gH := \{gh : h \in H\}$  is a left coset of  $H$ . It is a translation of  $H$  by  $g$ . (A left-translation.)

$Hg := \{hg : h \in H\}$  is a right coset of  $H$ . It, too, is a translation of  $H$  by  $g \dots$  a right-translation.

Think of  $S_3$  concretely as the symmetric group on  $[1, 3] = \{1, 2, 3\}$ . Consider  $H = \{\mathbf{1}, (123), (132)\}$ . then  $(12)H = \{(12), (23), (13)\}$ . This is the same as  $(13)H$ . Check it!

Observe that if  $g \in H$  then  $gH = H$ .

Observe that  $S_3 = H \cup (12)H$ . Observe also that  $H \cap (12)H$  is empty. People sometimes use the expression ‘disjoint union’ for this phenomenon, so beware! co’s the expression ‘disjoint union’ has another—distinct—usage, and you shouldn’t become confused.

Try  $K := \{\mathbf{1}, (12)\}$ . Then  $(123)K = \{(123), (13)\}$ ,  $(132)K = \{(132), (23)\}$ . Observe that  $S_3 = K \cup (123)K \cup (132)K$  and that, again, the union is disjoint. (The things-being-unioned are pairwise disjoint.)

Observe that typically cosets are not subgroups co’s they tend not to contain  $\mathbf{1}$ .

**LEMMA 9** *Suppose  $H \leq G$ . Then all the left cosets of  $H$  are the same size.*

And that size is the same as the size of  $H$  itself co’s  $H$  is the coset  $\mathbf{1}H$ . (This is basically beco’s group multiplication has inverses and is therefore injective, but let’s grind it out.)

We seek a bijection between  $aH$  and  $bH$ . Suppose  $x \in aH$ . Then  $x = ah$  for some (unique!)  $h \in H$ . Send  $x$  to  $ba^{-1}x$ . This is a member of  $bH$ . If we now try to send  $ba^{-1}x$  (which is in  $bH$ ) to something in  $aH$  by using the same idea to build a map  $bH \rightarrow aH$  we find that we have sent it back to  $x$ . So our construction actually constructed a *bijection* between  $aH$  and  $bH$ . Observe that in order to describe this bijection we needed to have an  $a$  and a  $b$  to compute with. It didn’t matter which  $a$  and  $b$  we used—co’s we’ll always get a bijection—but it might be different each time, and there is no way of finding a *distinguished* or *canonical* bijection. ■

(you can skip this bit if you like)

Let  $gH$  and  $g'H$  be two cosets of  $H$ . Send  $x$  in  $gH$  to  $g'g^{-1}x$ , which will clearly be in  $g'H$ . Is this function injective? If  $g'g^{-1}x = g'g^{-1}y$  then equally clearly  $x = y$ . Observe, however that the bijection  $x \mapsto g'g^{-1}x$  between the two cosets  $gH$  and  $g'H$  depends on our choice of  $g$  and  $g'$ , not purely on the cosets. Every coset of  $H$  is of the form  $gH$  for some  $g$ , but there may be lots of  $g$  that give rise to the same coset, and there is no canonical way to pick such a  $g$ . Thus, altho’ any two cosets of  $H$  in  $G$  have the same cardinality, there is no uniform way of assigning bijections.

**LEMMA 10** Suppose  $H \leq G$ .

Any two left cosets of  $H$  are either identical or disjoint, and the set  $\{gH : g \in G\}$  of left cosets of  $H$  forms a partition of  $G$ .

*Proof:*

For starters, the cosets cover the whole of  $G$  co's if  $g \in G$  then  $g \in gH$ !

We will show that if  $aH$  and  $bH$  overlap then they are identical.

Observe that  $aH = bH$  iff  $ab^{-1} \in H$ . This is beco's  $b \in bH = aH$  so  $b = ah$  for some  $h \in H$  which is of course  $a^{-1}b$  and the arrows can be reversed. Actually that wasn't what i claimed was it? I said ' $ab^{-1}$ ', but you can get that by permuting ' $a$ ' and ' $b$ '—the allegation is symmetric in ' $a$ ' and ' $b$ '.

Now suppose there is  $c \in aH \cap bH$ . So  $a^{-1}c \in H$  and  $b^{-1}c \in H$ . Now  $H$  is a group and is closed under inverses so  $(b^{-1}c)^{-1} = c^{-1}b \in H$ . Further,  $H$  is a group and is closed under  $\cdot$  so  $a^{-1}cc^{-1}b = a^{-1}b \in H$ , and this is the same as  $aH = bH$ . ■

Now  $aH = bH$  defines an equivalence relation on  $G$  (obviously!). Let's think about the partition corresponding to this equivalence relation. The pieces of the partition are the equivalence classes. [make sure you understand the correspondence between partitions and equivalence relations!! There is a natural bijection between the set of equivalence relations on a fixed set  $X$  and the set of partitions of  $X$ .] It is customary to use square brackets to denote equivalence classes, thus ' $[a]_{\sim}$ ' denotes the equivalence class of  $a$  under the equivalence relation  $\sim$ . If we know which equivalence relation we mean we can discard the subscript. So what is  $[a]$ ? Blindlingly cute fact:  $[a] = aH$ !! Why is this?

The equivalence relation  $a \sim_H b \iff aH = bH$  is the same as the relation  $a^{-1}b \in H$ . So so  $[a]_{\sim_H} = \{b : a^{-1}b \in H\}$ . But this object on the RHS is precisely  $aH$ !

This strikes your humble correspondent as a very cute fact.  $\sim_H$  is clearly an equivalence relation, and it must have as many equivalence classes as there are cosets, but it's very nice that the equivalence classes turn out to be precisely those cosets. I mean: for all we know they could have turned out to be the *right* cosets instead?



Which reminds us: all this stuff about *left* cosets ... we could have done exactly the same development with *right* cosets instead.

Observe that the left cosets and the right cosets all turn out to be the same if the group  $G$  is abelian.

Observe that the number of left cosets is the same as the number of right cosets. This is beco's in each case one can compute the number of cosets by observing that all cosets are the same size and are the same size as the subgroup, a bit of division does the rest and we get the same answer in both cases. Notice that there is no obvious way of describing a bijection between the set  $\{gH : g \in G\}$  of left cosets and the set  $\{Hg : g \in G\}$  of right cosets. The situation is bit like that earlier where i pointed out that there is no canonical bijection between two given left cosets of  $H$ . We can find

bijections but no canonical one. In this case we can't even point to any bijections at all, altho' we can prove that there must be such bijections—at least in the finite case. We have traded heavily on the assumption that the group  $G$  is finite.

Amid all this above chat there is a proof of:

**THEOREM 3** *Lagrange*

*Suppose  $H \leq G$ ,  $G$  finite. Then  $|H|$  divides  $|G|$ .*

**DEFINITION 11** *The index of a subgroup  $H \leq G$  is the cardinality of the set of left  $H$ -cosets, and this cardinality is written  $|G : H|$ .*

Remark: If  $G$  is finite then  $|G : H| = |G|/|H|$ . (Observe overloading of the vertical bar notation(!) Just to be really annoying i shall continue to use a single vertical bar for divisibility, as in Numbers and Sets.)

Further remark: we can have  $|G : H|$  finite even if both  $G$  and  $H$  are infinite: e.g, let  $G$  be the group of permutations of  $\mathbb{N}$  that move only finitely many things, and let  $H$  be the subgroup consisting of all the even permutations. Both these groups are countably infinite, but  $|G : H| = 2$ .

We will write ' $(G : H)$ ' for the set  $\{gH : g \in G\}$  of left cosets.

We should not expect a converse to Lagrange. Groups of order  $n$  do not reliably have subgroups of all orders that are divisors of  $n$ .  $A_4$  has no subgroups of order 6, and  $A_5$  has no subgroups of order 30. We will prove these later.

[end of sixth lecture]

**COROLLARY 1** *Lagrange's Corollary*

*If  $G$  is a finite group, and  $g \in G$  then  $o(g) \mid |G|$ . In particular  $g^{|G|} = \mathbf{1}_G$ .*

*Proof:*

Consider  $\langle g \rangle$ , the<sup>2</sup> cyclic [sub]group [of  $G$ ] generated by  $g$ . This is a subgroup of  $G$  so its order must divide the order of  $G$  ■

Overloading of vertical line!!

**COROLLARY 2** *If the order  $|G|$  of  $G$  is a prime,  $p$ , then every  $g \in G$  has order  $p$ .*

Indeed every group of order  $p$  is cyclic.

Now we are going to consider Euler's totient function.

$$\phi(n) = |\{m \in \mathbb{N} : (0 < m < n) \wedge (n, m) = 1\}|$$

[In case you were wondering, Dear Reader,  $(n, m)$  here is the highest common factor of  $n$  and  $m$  not the transposition swapping  $n$  and  $m$ . Nor is it the open interval in  $\mathbb{R}$  bounded by  $n$  and  $m$ . Life's like that.]

---

<sup>2</sup>Strictly speaking this notation has not yet been introduced, but i think you can guess what it means!

**THEOREM 4 Fermat-Euler**

Let  $n \in \mathbb{N}$ ,  $a \in \mathbb{Z}$  with  $(a, n) = 1$ . Then  $a^{\phi(n)} \equiv 1 \pmod{n}$ .

*Proof:*

This is a generalisation of *Fermat's little theorem*: If  $p \in \mathbb{N}$  is prime and  $a \in \mathbb{Z}$  is prime to  $p$ , then  $a^{p-1} \equiv 1 \pmod{p}$ .

Suppose  $n \in \mathbb{N}$ . Let  $R_n^*$  be  $\{0 < a < n : (a, n) = 1\}$ . Equip  $R_n^*$  with multiplication mod  $n$ . It's pretty obvious that the result is a group so in the interests of speed i might omit the proof for the moment.

closure

inverses

Associativity. Not totally blindingly obvious that multiplication mod  $n$  is associative. One needs to do a small amount of hand-calculation and that might be good for the soul.

Observe that  $|R_n^*| = \phi(n)$ .

Suppose  $a \in \mathbb{Z}$  with  $a$  prime to  $n$ . (Let us write  $a \text{ REM } n$  for the remainder of  $a$  on division by  $n$ , so that  $a \text{ REM } n$  is always a natural number  $< n$ .) Then  $a \text{ REM } n$  is in  $R_n^*$ . So, by Lagrange,  $(a \text{ REM } n)^{\phi(n)} = a^{|R_n^*|} = 1 \in R_n^*$ . So  $a^{\phi(n)} \equiv 1 \pmod{n}$ .

Proof needed here

insert hand-calculation here

You may be confused, Dear Reader—as was i—by the overloading of the exponential notation. In  $(a \text{ REM } n)^{\phi(n)}$ , we mean the group element  $a \text{ REM } n$  composed with itself  $\phi(n)$  times. This is of course the same as the number  $a \text{ REM } n$  raised to the power  $\phi(n)$ —mod  $n$  of course. Persist and it will all come right.

## 5 Normal Subgroups, Quotient Groups and Homomorphisms

Idea: given  $G$  and  $H \leq G$ , strive to define a group operation [which we will write ‘ $\circ$ ’] on the *quotient*, the set  $(G : H)$  of [left] cosets of  $H$  in  $G$ .

The obvious thing is . . . . Well, the elements of  $(G : H)$ , the cosets, are sets of group elements, and we have an operation on the group. It would be nice if we could obtain a third coset from two cosets  $C$  and  $C'$  by taking a  $c \in C$  and a  $c' \in C'$ , and seeing which coset the product lands in<sup>3</sup>.

Things are greatly simplified for us by the fact that the equivalence relation of belonging-to-the-same-coset is the same relations giving-rise-to-the-same coset, viz  $a$  is equivalent to  $b$  if  $aH = bH$ . So what we have to check is

$$aH \circ bH = (ab)H??$$

<sup>3</sup>This is a special case of a general situation where we have an operation  $\circ$  on a set  $x$  and we try to define an operation defined on the pieces of a partition of  $X$ . Another example:  $\mathbb{Z}$  with  $\times$ : can we define a  $\times$  operation on the equivalence classes of  $\mathbb{Z} \text{ mod } p$ ?

When does this happen?? There will now be an ad-break, i mean a definition break before we learn when. . .

**DEFINITION 12** *A subgroup  $H \leq G$  is a **normal** subgroup [of  $G$ ]<sup>4</sup>, written ‘ $H \trianglelefteq G$ ’ if  $(\forall g \in G)(gH = Hg)$ .*

Observe that this is saying more than just “every left coset is a right coset”; it’s saying that the left coset corresponding to  $g$  is the same set as the right coset corresponding to  $g$ . Must think a bit about what the weaker condition “every left coset is a right coset” does for us.

Try  $K = \{\mathbf{1}, (123), (132)\} \leq S_3$ .

Then

$$\begin{aligned}(12)K &= \{(12), (23), (13)\} = K(12) \\ (13)K &= \{(13), (23), (12)\} = K(13) \\ (23)K &= \{(23), (13), (12)\} = K(23)\end{aligned}$$

[check the stuff in the middle of each of these three lines, to confirm that these three cosets are the same—which they are. No time to copy it down off the board.]

So  $gK = Kg$  for every  $g \in S_3$  so  $K$  is a normal subgroup of (or “is normal in”)  $S_3$ .

In contrast  $\{\mathbf{1}, (12)\}$  is *not* a normal subgroup beco’s  $(13)\{\mathbf{1}, (12)\}$  and  $\{\mathbf{1}, (12)\}(13)$  are distinct sets.

**PROPOSITION 3** *the following are equivalent*

*For  $G$  a group, and  $K \leq G$*

1.  $(\forall g \in G)(gK = Kg)$ ;
2.  $(\forall g \in G)(gKg^{-1} = K)$ ;
3.  $(\forall g \in G)(\forall k \in K)(gkg^{-1} \in K)$ .

The notation in line 2 is a *teeny* bit naughty, beco’s we were told what  $gH$  and  $Hg$  are only when  $H$  is a subgroup. We haven’t been told what it means if  $H$  merely a coset. But this notation can be used even if  $H$  is any subset of  $G$  whatever, and it can even be used both sides, so that  $gHk := \{ghk : h \in H\}$ .

*Proof:*

We will show (1)  $\rightarrow$  (2); (2)  $\rightarrow$  (3); and (3)  $\rightarrow$  (1).

(1)  $\rightarrow$  (2)  $gKg^{-1} = \{gkg^{-1} : k \in K\}$ , and this must be

$$\begin{aligned}&\{(gk)g^{-1} : k \in K\} \text{ but, by (1), we can commute} \\ &= \{kgg^{-1} : k \in K\} \\ &= \{k : k \in K\} \\ &= K\end{aligned}$$

---

<sup>4</sup>‘normal’ is a two-place relation not a one-place predicate—like *abelian*. No such thing as a normal group, just a normal-**sub**group-of —

(2)  $\rightarrow$  (3) is a piece of cake

(3)  $\rightarrow$  (1) Suppose  $g \in G$ ,  $k \in K$ . Then  $gkg^{-1} = k'$  for some  $k' \in K$ .

So  $gk = k'g$ . But every member of  $gK$  has the form of the thing on the LHS of this equation, and anything of the form on the thing on the right is in  $Kg$ . So this is telling us that  $gK \subseteq Kg$ .

The inclusion in the other direction is analogous.

Write it out  
...

## 5.1 Examples of normal subgroups

The trivial subgroup and the improper subgroup;  
Every subgroup of every abelian group is normal;  
Kernels of group homomorphisms are normal subgroups (sheet 1 q 8);  
 $A_n \trianglelefteq S_n$  co's  $A_n$  is kernel(sign).

Recall the presentation of  $D_{2n}$  on page 16. The cyclic [sub]group generated by the rotation is a normal subgroup; the cyclic subgroup of order 2 generated by the reflection in vertex 1 is not a normal subgroup.

[end of eighth lecture]

**LEMMA 11** *If  $K \leq G$  is of index 2 then  $K \trianglelefteq G$ .*

*Proof:*

There are only two cosets (either on the left or the right). One of the two cosets is  $K$ , so the other (whichever side you are on!) is  $G \setminus K$ . So the left cosets are the same as the right cosets!! ■.

That gives us another reason why  $A_n \trianglelefteq S_n$ .

**THEOREM 5** *If  $K \trianglelefteq G$  the set  $(G : K)$  of left cosets is a group under the operation  $\circ$  of coset multiplication defined earlier.*

*Proof:*

The concept of normal subgroup was designed precisely to ensure that this happens, so this should not come as a great surprise.

You shouldn't really need a proof of this fact at this stage Dear Reader, but Dr Camina is soft-hearted and is going to give one anyway.

Suppose  $gK = g'K$  and  $hK = h'K$ . We want  $(gh)K = (g'h')K$ .

We use lemma 11.

$gK = g'K$  iff  $(g')^{-1}g \in K$ , and

$hK = h'K$  iff  $(h')^{-1}h \in K$ .

Now  $K$  is normal and therefore is closed under conjugation. So from  $(g')^{-1}g \in K$  we can infer  $h^{-1}(g')^{-1}gh \in K$ . Now  $h'$  and  $(h')^{-1}$  are both in  $K$  so we can multiply this last thing by  $(h')^{-1}h$  getting  $(h')^{-1}hh^{-1}(g')^{-1}gh \in K$ .

Must check  
this calculation  
again

We wanted  $(gh)K = (g'h')K$ , and for this it is suff that  $(g'h')^{-1}gh \in K$ —but this is what we have just proved. ■

The identity of  $G/K$  is of course the coset  $K$  itself.

Inverses? The inverse of  $gK$  is  $g^{-1}K$ .

Associativity? This is actually tricky, co's there are lots of things you could try.

$$\begin{aligned}(gK \circ hK) \circ lK &= \\ (ghK) \circ lK &= \\ (gh)lK\end{aligned}$$

Examples:

1.  $S_n/A_n = (\{A_n, (12)A_n\}, \circ) = C_2$ .
2.  $D_8 = \langle a, b | a^4 = 1 = b^2, bab = a^{-1} \rangle$  ( $a$  is the rotation,  $b$  a reflection). If  $K = \{1, a^2\}$  then  $K \trianglelefteq D_8$ . To check this, calculate  $(a^j b) a^2 (a^j b)^{-1}$

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

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

This is example 9 from lecture 1, aka  $C_2 \times C_2$ .

[We haven't actually defined group products yet. We will do this on p. 27.]

3. What are the quotient groups of  $(\mathbb{Z}, +)$ ?

First find all the subgroups. Clearly, for any  $n \in \mathbb{Z}$ , the set of all multiples of  $n$  will be a subgroup. Such subgroups are denoted ' $\mathbb{Z}_n$ '. We have to do a bit of work to establish the obvious fact that there are no other subgroups.

Suppose  $H \leq \mathbb{Z}$ . Let  $n$  be the smallest +ve integer in  $H$ . (If there isn't one then  $H$  is the trivial group.) Consider the (cyclic) subgroup of  $\mathbb{Z}$  generated by  $n$ . This must be a subgroup of  $H$ . If it isn't the whole of  $H$  then we can find  $m \in H \cap \mathbb{N}$  with  $m$  not a multiple of  $n$ . Use Euclid to express  $m$  as  $qn + r$  for some  $q$  and  $r < n$ . Then  $r = m - qn$ . But  $m \in H$



by assumption,  $qn \in H$  beco's  $n \in H$  so  $r \in H$ . But  $r < n$  contradicts minimality of  $n$ . ■

OK, so we know what the subgroups are. Since  $(\mathbb{Z}, +)$  is abelian all these subgroups are normal, so we have located all the quotient groups.

Let's work thru' an example. Take  $n = 5$ ; what are the cosets?

$5\mathbb{Z} = \{5z : z \in \mathbb{Z}\}$ ;  $1 + 5\mathbb{Z} = \{1 + 5z : z \in \mathbb{Z}\}$ ;  $2 + 5\mathbb{Z} = \{2 + 5z : z \in \mathbb{Z}\}$ ;  $3 + 5\mathbb{Z} = \{3 + 5z : z \in \mathbb{Z}\}$ ;  $4 + 5\mathbb{Z} = \{4 + 5z : z \in \mathbb{Z}\}$ . We get

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

and in general

$$(i + 5\mathbb{Z}) \circ (j + 5\mathbb{Z}) = (i + j \text{ REM } 5) + 5\mathbb{Z}$$

So the result is isomorphic to  $([1, 4], +_5)$  and the isomorphism is of course  $n + 5\mathbb{Z} \mapsto n$  (or perhaps  $\mapsto n \text{ REM } 5$  if you think  $n$  can be anything in  $\mathbb{Z}$ ).

In general  $\mathbb{Z}/n\mathbb{Z} \cong ([0, n-1], +_n)$

[end of ninth lecture]

4. Fix  $p$  a prime; then  $C_{p^\infty} = \{z \in \mathbb{C} : (\exists n \in \mathbb{N})(zp^n = 1)\}$ . This is the **Prüfer group**. Never heard of it. This is obviously a plot point. All its subgroups are finite. (This is in contrast to the additive group of the integers, all of whose subgroups are infinite).
5. To illustrate why normality is necessary... let  $H = \{1, b\} \leq D_8 = \langle a, b | a^4 = 1 = b^2, bab = a^{-1} \rangle$ . Observe  $b \in H$  but  $aba^{-1} \notin H$  so  $H$  is not closed under conjugation and is therefore not normal. So it is meet for our purposes. Consider the cosets

$$\begin{aligned} H &= \{1, b\}; \\ aH &= \{a, ab\} = abH; \\ a^2H &= \{a^2, a^2b\}; \\ a^3H &= \{a^3, ab\}. \end{aligned}$$

Now  $aH \circ aH$  ought to be  $a^2H$ . However  $aH = abH$  and  $abH \circ abH$  ought to be  $ababH$ , and we can rewrite the underlined bit as ' $a^{-1}$ ', so  $ababH = H$ . And  $H \neq a^2H$ .

We really shouldn't need this, beco's the definition of normal subgroup was cooked up precisely to make this true. However, no harm has been done.

#### **THEOREM 6** *The First Isomorphism Theorem*

Suppose  $\theta : G \rightarrow H$  is a homomorphism, and let us write ' $K$ ' for the kernel of  $\theta$ . Then  $K \trianglelefteq G$  and  $G/K \simeq \theta[G]$  (the "image" of  $G$  [in  $\theta$ , understood].)

I might have copied these down wrong. Couldn't see blackboard properly. Check them and get back to me this should be theorem 6, according to the blackboard

Illustrations before proof!!

1. sign:  $S_n \twoheadrightarrow (\{1, -1\}, \times)$ .

$\text{Ker}(\text{sign}) = A_n \trianglelefteq S_n$ , and  $S_n/A_n = C_2$ —of which  $(\{1, -1\}, \times)$  is a realisation.

2. Can define  $\theta : (\mathbb{R}, +) \rightarrow (\mathbb{C} \setminus \{0\}, \times)$  by  $\theta : r \mapsto e^{2\pi i r}$ . Check it's a homomorphism .... The image  $\theta^*\mathbb{R}$  is the unit circle in the complex plane.

$\text{Ker}(\theta) = \mathbb{Z}$  beco's 1 is the identity in the target group.

$(\mathbb{R}, +)/(\mathbb{Z}, +) \simeq (S^1, \times)$ , the unit circle.

Could probably say a bit more about this

3.  $\det: GL_2(\mathbb{R}) \rightarrow (\mathbb{R} \setminus \{0\}, \times)$ , by  $\det: M \mapsto \text{determinant}(M)$ . [Recall from 3 that  $GL_2(\mathbb{R})$  is the family of  $2 \times 2$  matrices with nonzero determinants.] Recall, too, that  $\det(AB) = \det(A) \cdot \det(B)$ . The image of the homomorphism is the whole of the target, beco's any  $\alpha \in \mathbb{R}$  is the determinant of

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

The kernel is  $SL_2(\mathbb{R}) = \{A \in GL_2(\mathbb{R}) : \det(A) = 1\}$

Nothing special here about either the '2' nor the ' $\mathbb{R}$ '. We can have  $n \times n$  matrices over any field we choose. Not that you know what is field is yet but you're about to find out. Integers mod  $p$ .

This is probably a definition of  $S^1$ .

Now for a proof.

We need an isomorphism between  $G/K$  and  $\theta^*G$ , the image of  $\theta$ . This isomorphism will be the gadget  $\phi$  defined by:

$$\phi(gK) = \theta(g)$$

This is well-defined beco's  $K \trianglelefteq G$ , as follows. Suppose  $gK = hK$ . Then  $h^{-1}g \in K$  (by normality of  $K$ , lemma 11) whence  $\theta(h^{-1}g) = e_H$ , giving  $\theta(h^{-1}) \cdot \theta(g) = e_H$  and finally  $\theta(h) = \theta(g)$ .

$\phi$  is a homomorphism beco's  $\theta(gK \circ hK) = \phi(ghK) = \theta(gh) = \theta(g)\theta(h) = \phi(gK)\phi(hK)$ .

$\phi$  is onto beco's  $\theta(g) \in \text{image of } \theta$  and  $\phi(gK) = \theta(g)$ .

To establish that  $\phi$  is 1-1 we need  $\phi(gK) = \phi(hK)$  iff  $\theta(g) = \theta(h)$ . Let's calculate:

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

■

A normal subgroup  $K \trianglelefteq G$  is the kernel of the quotient map  $G \twoheadrightarrow G/K$ .

**LEMMA 12** *A homomorphism  $\theta : \rightarrow H$  is injective iff the kernel is trivial.*

*Proof:*

Left-to-Right

Suppose  $\theta(g) = e_H = \theta(e_G)$ . Then  $g = e_G$  by injectivity.

Right-to-Left

Suppose  $\theta(g) = \theta(h)$ . Then  $(\theta(h))^{-1}\theta(g) = e_H$ .  $\theta$  is a homomorphism, so  $\theta(h^{-1}g) = e_H$ , so  $hg^{-1} \in \ker(\theta) = \{e_G\}$  so  $h = g$ . ■

An extra bit of notation. . . . For  $A, B$  subsets of  $G$ , write ' $AB$ ' for  $\{ab : a \in A \wedge b \in B\}$

**LEMMA 13** *Suppose  $N \trianglelefteq G$  and  $H \leq G$ .*

*Then  $NG \leq G$ .*

*Suppose further that  $H$ , too is normal.*

*Then  $NH \trianglelefteq G$ .*

I didn't know that!! And it's easy!

*Proof:*

All we have to do is show that  $NH$  is closed under  $G$ 's multiplication and inverse.

Multiplication:

So suppose  $nh$  and  $n'h'$  are two elements of  $NH$ .  $H \trianglelefteq G$  so  $hn' = n''h$  for some  $n'' \in N$ . This tells us that  $nhn'h'' = nn''hh'$ , and this is definitely in  $NH$ .

Inverse

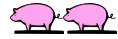
Suppose  $nh \in NH$ . We want  $h^{-1}n^{-1} \in NH$ . But, by normality of  $H$ , there is  $n \in N$  s.t.  $h^{-1}n^{-1} = n'h^{-1}$ , and the RHS of this last equation is obviously in  $NH$ . ■

Dr C hasn't proved the second part. Perhaps she'll do it in the next lecture, or perhaps she wants you to do it as an exercise.

[end of tenth lecture]

This should be lemma 13, according to Dr C

Should be lemma 14 by RDC's counting



An aside at the start of the lecture. How do you know that homomorphisms preserve inverses? The morally correct answer is that homomorphisms preserve all structure—that what you have to do if you aspire to be a homomorphism, it’s part of the definition. However, if you define a homomorphism to be something that preserves  $\mathbb{1}$  and multiplication, then if  $\theta$  is a homomorphism from a group to another group then you can prove that it also preserves inverses. What does it send  $g^{-1}$  to? Something that in the target cancels  $g$ . But then, by uniqueness of inverse in the target [wot is a group after all] the inverse that  $g^{-1}$  got sent to must be the unique inverse. You really don’t want to think about this. Just define a homomorphism to be something that preserves all structure. Don’t try to get clever.

## 6 Direct (cartesian) Products

Do not confuse this with  $NH$  earlier. That will crop up too!

If  $(G, \times)$  and  $(H, \times)$  are groups then consider the set  $G \times H$ , the set of all ordered pairs whose first components are in  $G$  and whose second components are in  $H$ . This set is commonly known as the *product* of  $G$  and  $H$ . Suppose you wanted to put a group structure on this set. How might you do it? The obvious answer [the one you have already tho’rt of] is the operation defined *coördinatewise*.

If  $(G, *)$  and  $(H, *)$  are groups then the set  $G \times H = \{(g, h) : g \in G \wedge h \in H\}$  of all ordered pairs whose first (“left”) components are in  $G$  and whose second (“right”) components are in  $H$  can be equipped with group gadgetry as follows

- The unit is the pair  $(\mathbb{1}_G, \mathbb{1}_H)$ ;
- $(g, h) * (g', h') = (gg', hh')$ ;
- The inverse of  $(g, h)$  is  $g^{-1}h^{-1}$ .

The group that is the set  $G \times H$  equipped with the coördinatewise operation is also called  $G \times H$ . Its size (order!) is clearly  $|G| \cdot |H|$ .

Observe that the operation that flips ordered pairs round—thus:  $(x, y) \mapsto (y, x)$ —is an isomorphism between  $G \times H$  and  $H \times G$ . By thinking about ordered pairs in this way you can explain why  $(G \times H) \times K \simeq G \times (H \times K)$ .

Observe further: the set  $G \times \{\mathbb{1}_H\}$  supports a group structure that is an exact copy of  $\times_H$ , and the set  $\{\mathbb{1}_G\} \times H$  supports a group structure that is an exact copy of  $\times_G$ . So both  $G$  and  $H$  inject isomorphically into  $G \times H$ .

Observe:  $G \times H$  is abelian iff  $G$  and  $H$  are both abelian.

Let’s have some examples

1.  $C_2 \times C_2$ . Two copies,  $\langle a | a^2 = \mathbf{1} \rangle$  and  $\langle b | b^2 = \mathbf{1} \rangle$ . The product of the two sets is  $\{(e, e), (e, b), (a, e), (a, b)\}$ . Let's have a multiplication table<sup>5</sup>

*	ee	ae	eb	ab
ee	ee	ae	eb	ab
ae	ae	ee	ab	eb
eb	eb	ab	ee	ae
ab	ab	eb	ae	ee

Here i have  
omitted com-  
mas and  
brackets.

This is example 9 from earlier. It's the *Klein 4 group*. Observe that all nonidentity elements have order 2

2.  $C_2 \times C_3$ . Two factors  $\langle a | a^2 = \mathbf{1} \rangle$  and  $\langle b | b^3 = \mathbf{1} \rangle$ , and the product is the following set of pairs:  $\{ee, eb, eb^2, ae, ab, ab^2\}$ .

Now consider the element  $ab$ .

$$\begin{aligned}(ab)^2 &= (a^2, b^2) = (e, b^2); \\(ab)^3 &= (a^3, b^3) = (a, e); \\(ab)^4 &= (a^4, b^4) = (e, b); \\(ab)^5 &= (a^5, b^5) = (a, b^2); \\(ab)^6 &= (a^6, b^6) = (e, e).\end{aligned}$$

They're all distinct. Thus the product is the cyclic group generated by  $(a, b)$ .

**LEMMA 14** *Let  $h \in H$  and  $k \in K$ , then the order of the pair  $(h, k)$  in the product  $H \times K$  is  $LCM(o(h), o(k))$ .*

*Proof:*

Let's write ' $m$ ' for the least common multiple of  $o(h)$  and  $o(k)$ . Then  $(h, k)^m = (h^m, k^m) = (\mathbf{1}_H, \mathbf{1}_K)$ , so  $m$  is a multiple of the order of  $(h, k)$ . And it's not a proper multiple beco's, if  $(h, k)^n = \mathbf{1}$ , then  $(h^n, k^n) = \mathbf{1}$ —whence  $o(h)|n$  and  $o(k)|n$  and  $m|n$ . ■

**COROLLARY 3**  $C_n \times C_m \simeq C_{nm}$  iff  $LCM(n, m) = 1$ .

By the preceding lemma, there is an element of  $C_n \times C_m$  of order  $mn$  iff  $(n, m) = 1$ .

**PROPOSITION 4** *Let  $G$  be a group with subgroups  $H$  and  $K$ . Then if*

<sup>5</sup>Initially i left out the brackets beco's it's probably safe to. But also beco's i cannot bring myself to write ' $(a, e)$ ' for the ordered pair of  $a$  and  $b$ , and my preferred notation—' $\langle a, b \rangle$ '—collides with the notation we are using for group presentations. And i'll try to write ' $LCM(x, y)$ ' instead of ' $(x, y)$ '. The possibility of confusion caused by all this overloading is potentially alarming. The commas in expressions like ' $(e, a)$ ' do not serve the same purpose as the [higher level] commas demarcating the pairs themselves as elements of the set.

$$1. (\forall g \in G)(\exists h \in H)(\exists k \in K)(g = hk);$$

$$2. H \cap K = \{1_G\};$$

$$3. (\forall h \in H)(\forall k \in K)(hk = kh);$$

then  $G \simeq H \times K$ .

[“Internal direct product”]. Notice that we really do mean  $H \times K$  not  $K \times H$ . They ain’t the same: item (1) is *not* the same as  $(\forall g \in G)(\exists h \in H)(\exists k \in K)(g = kh)$ ;

*Proof:*

Every  $g$  in  $G$  is  $hk$  for some  $h \in H$  and  $k \in K$ . The obvious thing to do is to send  $g$  to the ordered pair  $(h, k)$ . What problem could there possibly be? Well, there might be more than one way of representing  $g$  as a-member-of- $H$ -times-a-member-of- $K$ . So we want uniqueness of the representation. So suppose  $g = h_1k_1 = h_2k_2$ .

$$h_1k_1 = h_2k_2.$$

multiply both sides by  $k_1^{-1}$  on the right to get

$$h_1 = h_2k_2k_1^{-1}.$$

Now multiply both sides by  $h_2^{-1}$  on the left to get

$$h_2^{-1}h_1 = k_2k_1^{-1}.$$

Observe now that the LHS is an element of  $H$  and the RHS is an element of  $K$  so, by condition 2, we must have  $h_2^{-1}h_1$  and  $k_2k_1^{-1}$  both equal to  $1$ . But then  $h_1 = h_2$  and  $k_1 = k_2$ .

So in these circumstances we can legitimately define  $\theta : G \rightarrow G \times H$  by  $\theta : g \mapsto (h, k)$ . It now only remains to check that  $\theta$  is indeed a group homomorphism.

Preserves product:  $\theta(g_1 * g_2) = \theta(h_1k_1 * h_2k_2)$ . By clause (3) we have commutativity so this is  $\theta(h_1h_2k_1k_2)$  which is  $(h_1, k_1) \cdot (h_2, k_2) = \theta(g_1) \cdot \theta(g_2)$ .

It’s onto:  $(h, k) \in H \times K$  is  $\theta$  of  $hk \in G$ .

$C_6 = \langle a | a^6 = 1 \rangle$ . Try  $H = \langle a^2 \rangle$  and  $K = \langle a^3 \rangle$ . (Recall the notation ‘ $\langle x \rangle$ ’ for the cyclic [sub]group generated by the element  $x$ .)

Then  $C_6 \simeq H \times K$ . This is easy beco’s all these groups are abelian and so all subgroups are normal.

Worth noting that there are other (equivalent) definitions of internal direct product. Here’s one:

“ $G$  is the internal direct product of  $H$  and  $K$  if

$$1. H \trianglelefteq G, K \trianglelefteq G;$$

2.  $H \cap K = \{1\}$ ;
3.  $G = HK$  in the old (page 26) sense.”

We will show that these 1, 2, 3 are equivalent to the old 1, 2, 3 from proposition 4.

We first prove the left-to-right implication.

We want  $K \trianglelefteq G$ . Let  $k'$  be in  $K$  and  $g \in G$ . By (1) we can write  $g = hk$  for some  $h \in H$  and  $k \in K$ . so

$$gh'g^{-1} = (hk)k'(hk)^{-1} = \underline{hkk'k^{-1}}h^{-1}.$$

The underlined part is in  $K$ , and by (3) we can commute things in  $H$  with things in  $K$  so this is  $kk'k^{-1}$  which is in  $K$ .

Similarly  $H \trianglelefteq G$ . So  $HK \leq G$  by lemma 14 (her numbering). This makes sure that (1) is satisfied.

Right-to-left

We will use (3)' to prove (1). Consider the term  $h^{-1}k^{-1}hk$ . Terms like this are called “commutators”. (If everything commuted they would be  $1$ .) Write it as  $h^{-1}\underline{k^{-1}hk}$ . The underlined bit is in  $H$  beco’s  $H$  is normal, so the whole thing is in  $H$ . But we can also write it as  $\underline{h^{-1}k^{-1}h}k$ . This time the underlined bit is in  $K$  so the whole thing is in  $K$ . So it’s in both  $H$  and  $K$ . Therefore, by (3'),  $h^{-1}k^{-1}hk = 1$ , so  $h$  and  $k$  commute as desired.

## 7 Small groups

$$|G| = 1$$

$G$  must be the trivial group.

$$|G| = 2$$

2 is prime so we can use Lagrange (a taste of things to come) to argue that every nonidentity element is of order 2. (Pretty bloody obvious in this case, but ...). We must get  $C_2$ .

$$|G| = 3$$

3 is prime so all we get is  $C_3$ . In fact if  $G$  is of order a prime  $p$  then it can only be  $C_p$ .

$$|G| = 4$$

By Lagrange, if  $g \neq \mathbf{1}$  then  $o(g)|4$ . If there is a nonidentity element of order 4 then we are clearly looking at  $C_4$ . So suppose all nonidentity elements are of order 2. But then (this was a question on an example sheet) the group is abelian. It must be  $\langle a, b | a^2 = b^2 = 1 \rangle$ , which is  $\{\mathbf{1}, a, b, ab\}$  which is  $C_2 \times C_2$ .

$$|G| = 5$$

$C_5$  yawn.

$$|G| = 6$$

By Lagrange any nonidentity element must have order 2, 3 or 6. If every element of a group  $G$  is of order 2 then  $|G|$  is a power of 2.<sup>6</sup> But  $|G|$  is not a power of 2, so there are elements of order 3 or 6. If there is an element of order 6 then we are in  $C_6$ . But there must be an element of order 3 in any case, since if  $g^6 = \mathbf{1}$  then  $(g^2)^3 = \mathbf{1}$ . So let  $a$  be an element of order 3. Then the cyclic subgroup generated by  $a$  is of index 2 and is therefore normal by lemma 12 (her numbering). Choose  $b \in G \setminus \langle a \rangle$ . Then  $b^2 \in \langle a \rangle$  by sheet 2 q 11. So  $G$  is generated by  $a$  and  $b$ .

If  $b^2 = a$  or  $b^2 = a^2$  then  $o(b) = 6$  so  $G \simeq C_6 \simeq C_2 \times C_3$ .

If  $b^2 = \mathbf{1}$  we have  $\langle a \rangle$  is normal, so  $bab^{-1} \in \langle a \rangle$ . Which element of  $\langle a \rangle$  is it?

If  $bab^{-1} = \mathbf{1}$  then  $a = \mathbf{1} \dots$  No!

If  $bab^{-1} = a$  then  $a$  and  $b$  commute making  $G$  abelian (it's generated by two elements wot commute), so  $o(ab) = 6$  so  $G = C_6$ .

If  $bab^{-1} = a^2$  then  $G = \langle a, b | a^3 = \mathbf{1} = b^2, bab^{-1} = a^{-1} \rangle$  and this is  $D_6$  aka  $S_3$ .

$$|G| = 7$$

Yawn

$$|G| = 8$$

Apparently lots of groups of order  $2^n$ , according to Dr C. Perhaps this case will illustrate why.

We start off by brandishing Lagrange as before. Every nonidentity element has order 2, 4 or 8.

If there is even one element of order 8 then we are in  $C_8$ .

If all elements have order 2 then we are abelian and it's not hard to see we are in  $C_2 \times C_2 \times C_2$ .

---

<sup>6</sup>Apparently this is sheet 1 Q 11. Go away and do it now if you have not already done so. Presumably it's beco's all subgroups are normal by abelianness so the quotient over a copy of  $C_2$  gives you a quotient group whose order is  $|G|/2$ , and you keep on doing it ...



If there are elements of order 4, what then? Suppose  $a$  is an element of order 4. Then the cyclic subgroup  $\langle a \rangle$  has index 2 and must be normal.<sup>7</sup>

Let  $b$  be in  $G \setminus \langle a \rangle$ . Then  $G = \langle a, b \rangle$ . This is beco's  $G/\langle a \rangle \simeq C_2$  (the quotient has order two so it must be  $C_2$ ). So  $b^2 \in \langle a \rangle$ . [why?]

If  $b^2$  is  $a$  or  $a^3$  then  $o(b) = 8$  and we are in  $C_8$ .

If  $b^2$  is  $\mathbf{1}$  or  $a^2$  there is still life in the old dog. Let's see what can happen.

Either way,  $\langle a \rangle \trianglelefteq G$  so  $bab^{-1} \in \langle a \rangle$ . So  $bab^{-1} = a^i$  for some  $i$ . Also  $b^2 \in \langle a \rangle$ . So  $a = b^2ab^{-2} = \underline{bbab^{-1}}b^{-1}$  and the underlined bit is  $a^i$  so it becomes  $ba^ib^{-1} = a^{i^2}$ . So  $a = a^{i^2}$  so  $\mathbf{1} = a^{i^2-1}$  so  $i^2 \equiv 1 \pmod{4}$ , so  $i \equiv 1$  or  $-1 \pmod{4}$ .

There are two cases:

- $i \equiv 1 \pmod{4}$ . Then  $G$  is abelian, beco's

**either**

$b^2 = \mathbf{1}$  so  $a$  and  $b$  commute so  $G$  is generated by things that commute [and in this case  $G$  is  $C_4 \times C_2$ ]

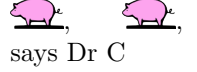
**or**

$b^2 = a^2$  in which case  $(ba^{-1})^2 = \mathbf{1}$ , so  $G = \langle a, b \rangle = \langle a, ba^{-1} \rangle = \langle a \rangle \times \langle ba^{-1} \rangle = C_4 \times C_2$ .

- $i \equiv -1 \pmod{4}$ . Suppose  $bab^{-1} = a^{-1}$ .

If  $b^2 = \mathbf{1}$  then  $G = \langle a, b | a^4 = \mathbf{1} = b^2, bab^{-1} = a^{-1} \rangle$  which is to say that  $G$  is  $D_8$ .

If  $b^2 = a^2$  we get a new group, called  $Q_8$ .



## 7.1 Realisations of $Q_8$

$Q = \{1, -1, +i, -i, +j, -j, +k, -k\}$ . As you can see, the elements have special names.  $1$  is  $\mathbf{1}_{Q_8}$ . I don't think the '+' and the '-' allude to group operations, at least not directly:  $-j$  is not the inverse of  $j$  in  $Q_8$ . It's  $(-1) \cdot j$  where the dot is multiplication-in- $Q_8$ . This notation works beco's  $(-1)$  commutes with each of  $i, j$  and  $k$ . (And presumably it's an involution, a chap of order 2). Thus when you  $Q_8$ -multiply two things the minus signs cancel.

We have the following bits of info about the group operation.

$$\begin{aligned} ij &= k; jk = i; ki = j; ji = -k; kj = -i; ik = -j; i^2 = j^2 = k^2 = -1; \\ (-1)^2 &= \mathbf{1}. \\ o(i) &= o(j) = o(k) = 4. \end{aligned}$$

I think we are supposed to infer from  $jk = i$  that  $(-j)k = -i$ ,  $j(-k) = -i$  and  $(-j)(-k) = i$ . I have used inferences like that in my attempt to fill in

<sup>7</sup>The point here is that, in general, if  $N \trianglelefteq G$  and  $G/N$  is cyclic of prime order then, if  $g \in G \setminus N$ , we find that the coset  $gN$  generates a subgroup isomorphic to the quotient  $G/N$ . This is beco's, if  $h$  is any element of  $G$ ,  $h$  belongs to some coset  $g^iN$  so  $h = g^i n$  for some  $n \in N$ .

the multiplication table below. In fact  $-j$  (and  $-k$ ,  $-i$  *mutatis mutandis*) is a seductive cheating notation for  $(-1) \cdot j$ . If you grasp that then everything follows.

[What is  $o(-1)$ ? I think we are suppose to be guided by the notation into thinking that  $(-1)^2 = 1 = \mathbf{1}$  so  $o(-1) = 2$ ]

$\times$	1	-1	$i$	$-i$	$j$	$-j$	$k$	$-k$
1	1	-1	$i$	$-i$	$j$	$-j$	$k$	$-k$
-1	-1	1	$-i$	$i$	$-j$	$j$	$-k$	$k$
$i$	$i$	$-i$	-1	1	$k$	$-k$	$-j$	$j$
$-i$	$-i$	$i$	1	-1	$-k$	$k$	$j$	$-j$
$j$	$j$	$-j$	$-k$	$k$	-1	1	$i$	$-i$
$-j$	$-j$	$j$	$k$	$-k$	1	-1	$-i$	$i$
$k$	$k$	$-k$	$j$	$-j$	$-i$	$i$	-1	1
$-k$	$-k$	$k$	$-j$	$j$	$i$	$-i$	1	-1

This multiplication is a construction site. Hard hats needed. There is no guarantee that the calculations are correct!!

We can think of  $Q_8$  as a group of matrices.

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \quad i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}; \quad j = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}; \quad k = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix};$$

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

These eight matrices all have determinant 1, so  $Q_8$  is a subgroup of  $SL_2(\mathbb{C})$ .

$Q_8 = \langle a, b | a^4 = \mathbf{1}, b^2 = a^2, bab^{-1} = a^{-1} \rangle$ , and we can make the following identifications:

$$a = i; \quad b = j; \quad j i j^{-1} = j i (-j) = -j k = -i.$$

So! There are five groups of order 8:  $C_8$ ,  $C_4 \times C_2$  and  $C_2 \times C_2 \times C_2$  (which are abelian) and  $D_8$  and  $Q_8$  which are not.

[end of eleventh lecture]

$$|G| = 9$$

Either there is an element of order 9, in which case we are in  $C_9$ , or there isn't in which case every nonidentity element has order 3. Pick one, and consider the cyclic subgroup it generates. Then consider something not in that subgroup. Easy to see that we get  $C_3 \times C_3$ . Observe [a very mathematical move, this] that all we were using is that 9 is the square of a prime. The moral is that any group of order  $p^2$  is a product of cyclic groups and is therefore abelian. And, yes, a product of abelian groups is abelian. Think about it a bit.

$$|G| = 10$$

We didn't go through this case in lectures, but we get  $C_{10}$ ,  $C_5 \times C_2$  or  $D_{10}$ . [look at sheet 2 q 12]. Might have to do a bit of work to check that that is all you get. Oops!!  $C_5 \times C_2$  is  $C_{10}$ ! That's beco's 2 and 5 are coprime. (Corollary 3).

$$|G| > 16$$

10 groups of order 16. Something like  $10^{11}$  of order 1024.

## 8 Group Actions



The groups  $D_{2n}$  and  $S_n$  arise beco's they *do* something. They *act*<sup>8</sup>!  $D_{2n}$  *acts* on the  $n$ -gon;  $S_n$  *acts* on  $[1, n]$ .

Remember the distinction between abstract groups and concrete groups. A concrete group is a *realisation* (p 9) of an abstract group. If you equip an *abstract* group with an *action* it becomes a *concrete* group.

**DEFINITION 13** Let  $G$  be a group and  $X$  a nonempty<sup>9</sup> set. An **action** of  $G$  on  $X$  is a function  $\rho : G \times X \rightarrow X$  satisfying

(0)  $\rho^{\text{“}}(G \times X) \subseteq X$ . (Actually this is enforced by the conventions underlying the use of the above syntax, but it is something that has to be checked when you encounter a  $\rho$  that might be an action.)

$$(1) (\forall g, h \in G)(\forall x \in X)(\rho(gh, x) = \rho(g, \rho(h, x)))$$

$$(2) (\forall x \in X)(\rho(1, x) = x)$$

Let's have some examples.

1. Trivial action:  $(\forall x)(\rho(g, x) = x)$ .
2.  $S_n$  acts on  $[1, n]$  by permutation.<sup>10</sup>
3.  $D_8$ . We know where the dihedral groups come from. Let's not forget that the elements of the dihedral group can be taken to be permuting not edges but (if we choose) *vertices*.

Suppose we have a square with four sides  $a, b, c$  and  $d$ , reading clockwise from the horizontal chap  $a$  at the top.  $\tau(a) = a, \tau(b) = d, \tau(c) = c$ .

need a picture!!

<sup>8</sup>

In Modern Thought, if not in fact  
Nothing is which does not act.  
Thus that is counted *wisdom* which  
Describes the *scratch* but not the *itch*.

<sup>9</sup>

Not sure why it has to be nonempty but never mind.

<sup>10</sup>Of course it does: that's where it came from. However there are some things to worry about here—at any rate they worried *me*. What is the abstract group  $S_3$  anyway? It's a multiplication table. To get it to act we have to decide which row (column) corresponds to which actual physical permutation. The group elements of order 2 had better correspond to transpositions? I don't suppose for a moment that the answer is interesting (my guess is that it's *n!*) but one should understand this situation well enuff to be able to perform the calculation. Of course one can think of a group as a group presentation, so that  $S_3 = \langle a, b, c | a^2 = b^2 = c^2 = 1, (ab)^3 = (bc)^3 = (ac)^3 = 1 \rangle$ —at least i think that is correct—and then one has to identify  $a, b$  and  $c$  with the three transpositions, and this can be done in  $3!$  ways.

$\sigma(a) = b$  and so on.

If we have a square with vertices 1, 2, 3 and 4, reading clockwise from the top left corner. [need a picture!!]  $\tau(1) = 2, \tau(2) = 1, \tau(3) = 4$  and so on.

Of course  $G$  can act on itself! And in more than one way...!

- Left-multiplication:  $\rho(a, b) = ab$ . Let's just check that this really is a group action in the meaning of the act.

$$(0) \rho(a, b) = ab \in G$$

$$(1) \rho(g, \rho(h, k)) = \rho(g, hk) = ghk.$$

$\rho(gh, k) = ghk$ , so we get associativity (in case anyone was wondering).

This is often known as the **left regular action**. There is also [of course] the

- **right regular action**

The reader can fill in the details by themselves

- $G$  can act on itself by **conjugation**

$$\rho(g, h) = ghg^{-1}.$$

Let's check the conditions

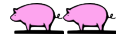
$$(0) k \in G \rightarrow gkg^{-1} \in G$$

$$(1) \rho(gh, k) = ghk(gh)^{-1} = ghkh^{-1}g^{-1};$$

$$\rho(g, \rho(h, k)) = g\rho(h, k)g^{-1} = ghkh^{-1}g^{-1}.$$

so it really is an action.

But  $G$  acting on itself gives a map  $G \times G \rightarrow G$ . Is this map a group homomorphism? What is the kernel?? Do not miss next week's thrilling installment! Subscribe now!



[end of twelfth lecture]

- $G$  can also act by conjugation on any normal subgroup. The point is that you need the subgroup to be normal-in- $G$  in order for condition (0) to be satisfied.
- $G$  acts on the set of left-cosets by [wait for it!] left-multiplication. This is the **left coset** action.

$$(0) \rho(g, kH) = (gk)H;$$

$$(2) \rho(g, \rho(l, kH)) = \rho(g, lkH) = glkH;$$

$$(3) \rho(\mathbf{1}, kH) = \mathbf{1}kH = kH.$$

- There is also of course the action on *right* cosets by multiplication on the right.

[end of thirteenth lecture]

Every action  $\rho(G \times X) \rightarrow X$  gives rise to a homomorphism  $G \rightarrow \text{Symm}(X)$ .  
[Think about it for a bit]

To what element of  $\text{Symm}(X)$  do we send  $g \in G$ ? Obviously to that element of  $\text{Symm}(X)$  that, when we give it  $x$ , gives us  $\rho(g, x)$ . I am going to write this using lambda notation, as  $\lambda x. \rho(g, x)$ .

We'd better check that this  $\lambda x. \rho(g, x)$  really is a permutation of  $X$ . Here we get clever and use the fact proved earlier (plot point!) that a function is a bijection iff it has a two-sided inverse. You can have a one-sided inverse and not be a bijection. Consider  $\lambda n. 2n : \mathbb{Z} \rightarrow \mathbb{Z}$ . It has a left-sided inverse but no right-sided inverse. Now  $\lambda x. \rho(g, x)$  has a two-sided inverse, namely  $\lambda x. \rho(g^{-1}, x)$ —which is of course an inverse by the definition of group action—so it is indeed a bijection.

This is lemma 16. The homomorphism  $G \rightarrow \text{Symm}(X)$  induced by the action  $\rho$  of  $G$  on  $X$  is of course  $\lambda g. \lambda x. \rho(g, x)$ . Dr Camina is going to write the with a capital phi: ' $\Phi$ '. I don't know if this is the letter always used for this homomorphism induced by a group action. We shall see.

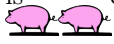
**PROPOSITION 5** *Check for yourself that  $\Phi : G \rightarrow \text{Symm}(X)$  is not only a function from  $G$  to  $\text{Symm}(X)$  (all its values are in  $\text{Symm}(X)$ ) but is actually a group homomorphism. I shall write out a proof if suitably threatened but not otherwise.*

Things in the kernel of  $\Phi$  are things that “act trivially”. If the kernel is  $\{1_G\}$  we say that the action is **faithful**.

Something in me wants to write this capital  $\Phi$  with a  $\rho$  subscript. . .

OK, so group actions correspond to homomorphisms, and where we have homomorphisms we have normal subgroups and homomorphic images and so on. Let's have some examples, and dig up the first isomorphism theorem.

1. The trivial action.  $\ker(\Phi) = G$ . Not faithful!
2.  $S_n$  acting on  $[1, n]$  [in the obvious way] is faithful. What about  $S_n$  acting on  $[1, n + 1]$ ? Well, it could act on it in various ways, but i think what Dr C had in mind was an action that moved  $1, \dots, n$  around and fixed  $n + 1$ , and the point of this example is that it is *not* faithful. Is there an action of  $S_n$  on  $[1, n + 1]$  where only the identity element of  $S_n$  fixes everything? I don't know!
3.  $D_8$  acting on the edges of a square: faithful.
4. Left regular action: faithful.

$\lambda$  notation  
is coool!  


This is proposition 6 in Dr Camina's numbering

5.  $G$  acting on itself by conjugation. The kernel is  $\{g \in G : (\forall h \in G)(ghg^{-1} = h)\}$ . The kernel contains precisely those elements that commute with everything in  $G$ . It is called the **centre** of the group  $G$  and it is notated ' $\mathbb{Z}(G)$ '. Whether or not this action is faithful depends on whether or not the kernel is trivial. It might be. But if  $G$  is abelian the kernel is the whole group. Examples:  $\mathbb{Z}(D_8) = \langle \sigma^2 \rangle$ ;  $\mathbb{Z}(A_5) = \{1\}$ .
6.  $G$  acting by conjugation on a normal subgroup  $N$  of itself. The kernel is written in the following style

$$C_G(N) = \{g \in G : (\forall n \in N)(gng^{-1} = n)\}$$

and it is called the **centraliser** (of  $N$  in  $G$ ).

Actually we talk of centralisers of arbitrary subsets of  $G$ , not merely centralisers of normal subgroups.

7. Left coset action. [Remember, we have fixed a subgroup  $H$ , and we are moving its cosets around with this action.] The kernel is

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

which is the  $\subseteq$ -biggest normal subgroup of  $G$  that is included in  $H$ . [Need to think a bit about this.] This called the **core** of  $H$  (in  $G$ ). Thinking aloud... by lemma 13 you can “multiply” two normal subgroups together, so i suppose as long as the group is finite you can “multiply” together all the normal subgroups, and even—specifically—all the normal subgroups that happen to be included in a given subgroup  $H$ . (Is the result included in  $H$ ?) What we have just learnt is that you can multiply them all together even if the group is infinite.

(Observe that if  $|G| > |\text{Symm}(X)|$ , then the action is not faithful.)

So we have proved:

**THEOREM 7** *Cayley's theorem*

*If  $\ker(\Phi_\rho)$  is  $\{1\}$  (so the action is faithful) then  $G \simeq$  some subgroup of  $\text{Symm}(X)$ . The left-regular action of  $G$  on itself is faithful, so every group  $G$  is isomorphic to a subgroup of  $\text{Symm}(G)$ .*

*Proof:*

■

Given an action  $\rho$  of  $G$  on a set  $X$  we will often write ' $g(x)$ ' for ' $\rho(g, x)$ ', of course only if  $\rho$  is fixed and understood.

**DEFINITION 14** *The orbit of  $x$  [under  $\rho$  and  $G$ ] is  $\{x' \in X : (\exists g \in G)(gx = x')\}$  (also written  $\{g(x) : g \in G\}$ ) and  $\text{Orb}_G(x)$  for short. Sometimes written ' $G(x)$ '.*

Let's go back to our portfolio of standard examples.

1. The trivial action.  $\text{Orb}(x) = \{x\}$ . (I've omitted the subscript as Dr C did.)
2.  $S_n$  acting on  $[1, n]$ .  $\text{Orb}_{S_n}(x) = [1, n]$ . Suppose  $H \leq S_5$  is  $\langle (1, 2)(3, 4, 5) \rangle$  acting on  $[1, 5]$  then  $H$  has two orbits, namely:  $\text{Orb}_H(1) = \{1, 2\}$  and  $\text{Orb}_H(3) = \{3, 4, 5\}$ .
3.  $D_8$  acting on the edges of the square with edges  $a, b, c, d$  labelled clockwise from the top horizontal [need a picture!].  $\text{Orb}_{D_8}(a) = \{a, b, c, d\}$ .
4. Left regular action.  $\text{Orb}_G(h) = G$  for all elements  $h \in G$ .
5. Conjugation action.  $\text{Orb}_G(h) = \{ghg^{-1} : g \in G\}$ . We write ' $\text{ccl}(h)$ ' for this object.

**DEFINITION 15**  *$G$  acts transitively on  $X$  iff  $(\forall x \in X)(\text{Orb}_G(x) = G)$ . ( $G$  has only one orbit ... moves everything to everything). Equivalently  $(\forall x_1 x_2 \in X)(\exists g \in G)(\rho(g, x_1) = x_2)$*

Definition 18 according to Dr C but my L<sup>A</sup>T<sub>E</sub>X has its own views

Orbits [unlike cosets] can emphatically be of different sizes (like the ears of the old man of Devizes) as is illustrated by example 2 above, where  $\text{Orb}_H(1) = \{1, 2\}$  and  $\text{Orb}_H(3) = \{3, 4, 5\}$ .

**LEMMA 15** *The orbits form a partition.*

*Proof:*

It will sufficient to show that the binary relation of belonging-to-the-same-orbit is an equivalence relation. To this end the best definition of  $\text{Orb}_G(x)$  is  $\{x' \in X : (\exists g \in G)(gx = x')\}$ .

- It's reflexive. Take  $g$  to be  $\mathbf{1}_G$ .
- It's transitive. If  $y \in \text{Orb}_G(x)$  that's beco's there is  $g \in G$  s.t.  $\rho(g, x) = y$ ; if  $z \in \text{Orb}_G(y)$  that's beco's there is  $h \in G$  s.t.  $\rho(h, y) = z$ . But then  $z \in \text{Orb}_G(x)$  beco's there is  $hg \in G$  and  $\rho(hg, x) = z$ . ("if  $g$  takes me from  $x$  to  $y$  and  $h$  takes me from  $y$  to  $z$  then  $hg$  takes me from  $x$  to  $z$ ".)
- It's symmetrical: ("if  $g$  takes me from  $x$  to  $y$  then  $g^{-1}$  takes me from  $y$  to  $x$ ".)

■

Brief reality check. Fix your action. Then  $G$  acts transitively on each orbit. We say " $\text{Orb}_G(x)$  is  $G$ -invariant".  $G$  acts *trivially* on the set of orbits—co's it fixes each orbit (as a set).

**DEFINITION 16** The **stabiliser** of  $x \in X$ , written ' $\text{stab}_G(x)$ ' is  $\{g \in G : g(x) = x\}$ <sup>11</sup>

Think of the automorphisms of a *cube* (not a mere flatland square as hitherto), and think about the stabiliser of a vertex. It's the copy of  $C_3$  consisting of the rotations thru'  $2\pi/3$  radians about an axis thru' your vertex and the vertex diagonally opposite at a distance of  $\sqrt{3}$ .

$\text{Stab}_G(x)$  sometimes written ' $G_x$ ' as, indeed, in sheet 3 q 8.

Observe that  $\text{stab}_G(x)$  is always a group, and a subgroup of  $G$  at that.

Some examples

1. Trivial action on  $X$ .  $\text{Stab}_G(x) = G$  for all  $x \in X$ ;
2.  $S_n$  acting on  $[1, n]$  in the obvious way:  $\text{stab}_{S_n}(1) = S_{n-1}$ ; try  $H = \langle (1, 2)(3, 4, 5) \rangle$  acting on  $[1, 5]$  in the obvious way.  $\text{Stab}_H(1) = \langle (3, 4, 5) \rangle$ . ("even powers of  $H$ ")<sup>12</sup>
3.  $D_8$  acting on the edges of a square.  $\text{Stab}_{D_8}(a) = \{1, \tau\}$ . (Remember:  $\tau$  was the reflection about the perpendicular bisector of the two horizontal edges.)
4. Left regular action of  $G$  on  $G$ .  $\text{Stab}_G(h) = \{1\}$ .
5. Conjugation action of  $G$  on  $G$ .  $\text{Stab}_G(h) = \{g \in G : g(h) = h\} = \{g \in G : ghg^{-1} = h\} =$  the centraliser  $C_G(h)$  of  $h$  in  $G$ .

**LEMMA 16** Stabilisers are always subgroups.

*Proof:*

Every stabiliser contains  $1$ . If  $g(x) = x$  then  $g^{-1}(x) = g^{-1}(g(x)) = x$  so  $g^{-1}$  fixes  $x$  too. Composition is easy. ■

**REMARK 3**  $\ker(\Phi) = \bigcap_{x \in X} \text{stab}_G(x)$

**THEOREM 8** The orbit-stabiliser theorem

Let  $G$  be a finite group acting on a set  $X$ , and  $x \in X$ . Then

$$\text{stab}_G(x) \leq G \text{ and } |G| = |\text{stab}_G(x)| \cdot |\text{orb}_G(x)|.$$

[end of fourteenth lecture]

<sup>11</sup>Remember that this, strictly, is  $\{g \in G : \rho(g, x) = x\}$ .

<sup>12</sup>what did she mean?



Fix  $x \in X$ , and consider  $(G : \text{stab}_G(x))$ , the set of left-cosets in  $G$  of the subgroup  $\text{stab}_G(x)$ . We will show that it is the same size as  $\text{Orb}_G(x)$ . This proof [unlike the proof of Lagrange] does not depend on  $G$  being finite. What do we mean when we say that two sets are the same size? We mean there is a bijection between them. So let's explicitly exhibit such a bijection.

Let  $g\text{stab}_G(x)$  be a left coset. To which element of the orbit do we send it? What operations can we do to the things mentioned in  $g\text{stab}_G(x)$  to obtain an element of  $\text{Orb}_G(x)$ . Well, you can apply  $g$  to  $x$ . Let's try that!

$$g\text{stab}_G(x) \mapsto g(x)$$

There is some checking we have to do. Remember that a coset can be obtained from the subgroup by multiplication on the left in potentially more than one way, so we have to establish that it doesn't matter whether we are thinking of our coset as  $g\text{stab}_G(x)$  or  $h\text{stab}_G(x)$ . Observe that by lemma 11,  $g\text{stab}_G(x) = h\text{stab}_G(x)$  iff  $hg^{-1} \in \text{stab}_G(x)$ , which is to say  $hg^{-1}(x) = x$  which is to say  $h(x) = g(x)$ .

So the definition is legitimate.

Now we have to show that this function (Dr Camina write it ' $\theta$ ' but i am wondering if there is an official name for it. There is of course a lambda notation for it, but it's a bit messy) is 1-1.

To show it's 1-1, suppose it sends  $g\text{stab}_G(x)$  and  $h\text{stab}_G(x)$  to the same element of  $\text{Orb}_G(x)$ . But then  $g(x) = h(x)$ , but (and this is like a backwards version of the proof in the last para that the function was legitimate) we have  $g(x) = h(x)$  whence  $h^{-1}g(x) = x$  whence  $h^{-1}g \in \text{stab}_G(x)$  whence—by lemma 11 as always—the two cosets  $g\text{stab}_G(x)$  and  $h\text{stab}_G(x)$  are one and the same. ■

## 9 Symmetries of Regular Solids

Distance-preserving permutations (“isometries”) of  $\mathbb{R}^3$  that fix the vertex set. (That fix the vertex set *setwise*, not *pointwise*).

We need the notion of the *dual* of a polyhedron. Put a vertex in the middle of each face of a regular polyhedron. Join up the vertices to obtain a new regular polyhedron. If you do this to a tetrahedron you get a tetrahedron. If you do it to a cube you get an octahedron and *vice versa*. If you do it to a dodecahedron you get an icosahedron and *vice versa*. I think the Greeks knew this.

### 9.1 The Tetrahedron

Let  $G$  be the symmetry group, the group of all isometries of  $\mathbb{R}^3$  that move the vertices around. Evidently there is a homomorphism  $\rightarrow S_4$ . Let  $G^+$  be the subgroup consisting of *rotations*.

Join each vertex to the centre of the opposite triangle, and rotate about this vertex. If you rotate about this axis by  $2\pi/3$  radians you fix the vertices setwise. Thus through vertex 1 you have the rotation  $(2, 3, 4)$  of order 3, which we will

call ‘ $\sigma$ ’. You have its square  $(3, 4, 2)$ . You can do this for each vertex, so you have  $4 \times 2$  rotations thru’  $2\pi/3$  each of order 2.

Now join the midpoints of opposite edges, and rotate about these axes by  $\pi$  radians. This gives (for example)  $(1, 4)(2, 3)$ . There are three pairs of opposite edges so three such elements.

There are no other rotations. This is  $A_4$ .  $\text{Orb}_{G^+}(1) = \{1, 2, 3, 4\}$ ;  $\text{stab}_{G^+}(1) = \langle \sigma \rangle$ . No more: we’ve considered rotations that fix one vertex, that fix two, and if three vertices are fixed the whole figure is fixed.

Now consider  $G$ , the group of all symmetries of the tetrahedron.  $\text{Orb}_G(1) = \{1, 2, 3, 4\}$ . But now we have reflections to consider. Each edge  $e$  belongs to a unique plane which cuts the opposite edge thru’ its midpoint. We can reflect in this plane. The reflection fixes the two vertices joined by  $e$  and swaps the other two vertices. Let us use the letter ‘ $\tau$ ’ to denote the reflection that fixes vertices 1 and 2. So  $\text{stab}_G(1) = \langle \sigma, \tau \rangle = D_6$ . You need only *one* reflection when trying to generate the whole group, beco’s the other reflections are conjugates of it.

So by theorem 8 we have  $|G| = 4 \cdot 6 = 24$ .  $G = S_4$ .

$(1234) = (12)(234)$  is a composition of a rotation and a reflection but is itself neither.

This is ringing bells with me concerning organic chemistry. It is known that the four valences of a carbon atom are directed outwards from the centre of the tetrahedron to the four vertices. A molecule that consists of a carbon joined to four different chaps exists in two forms. (The fact that it’s only two was one way in which the chemists were able to determine that the arms were directed to the corners of a tetrahedron.) Presumably this is something to do with the fact that the rotations of a tetrahedron are  $S_4$  and the group of all isometries is  $A_4$  and that  $A_4$  is of index 2 in  $S_4$ .

## 9.2 The Cube

The cube is dual to the octahedron.

Think of the group of symmetries of the cube as acting on the long ( $\sqrt{3}$ ) diagonals. Let’s call them  $\{d_1, d_2, d_3, d_4\}$ . (We have numbered the vertices so that 1,2,3,4 go round the top clockwise and the  $\sqrt{3}$  diagonals join 1 to 1’, 2 to 2’, 3 to 3’ and 4 to 4’, with the dashed numbers living on the bottom storey.)

Let  $G^+$  be the group of rotations. Only the identity rotation fixes all the long diagonals. This means that the obvious map  $G^+ \rightarrow S_4$  is injective.

Rotations  
about what?

Let  $\sigma$  be a rotation thru’  $\pi/2$  about an axis joining the centres of the top and bottom faces.  $\sigma$  is of order 4, so there are three rotations about that axis.  $\sigma = (1234)$  (order 4);  $\sigma^2 = (13)(24)$  (order 2);  $\sigma^3 = (1432)$  (order 4). There are three pairs of opposite-faces, so three such axes, giving 6 elements of order 4 plus three elements of order 2. (“double transpositions”).

There are also 4 long diagonals to rotate round, thru’  $2\pi/3$  in the first instance. Use the letter rho for these. Then  $\rho^3 = \mathbf{1}$  so each long diagonal contributes two elements of order three  $\rightarrow$  8 elements of order 3.

Next we consider axes joining midpoints of opposite *edges*, what one might call the  $\sqrt{2}$  diagonals-within-the-body. Let  $\tau$  be the rotation thru'  $\pi$  radians about the axis through the midpoint of the edge joining 1 to 4 with the midpoint of the edge joining 1' to 2'.

Six such axes with rotations of order 2. So six more elements of order 2. So we get  $G^+ = S_4$ .

$$\text{Orb}_{G^+}(d_1) = \{d_1, d_2, d_3, d_4\}$$

$$\text{Stab}_{G^+}(d_1) = \langle \rho, \tau \rangle$$

(not necessarily the same  $\tau$  but at any rate one of the rotations thru' opposite midpoints)

[end of fifteenth lecture]

Now let  $G$  be the full symmetry group of the cube. Consider the action of  $G$  on the six faces. The action is faithful—anything that fixes the six faces fixes the whole cube (i.e., fixes the eight vertices). This gives an injection  $G \hookrightarrow S_6$ . Clearly  $G$  acts transitively on the faces. Let  $F$  be a face. Thus  $|\text{orb}_G(F)| = 6$ .  $\text{Stab}_G(F) = D_8$  (why? what about the reflections that we find in  $D_8$ ? Don't they reflect the cube “out of the paper”?) Now  $D_8 = 8$  so, by the orbit-stabiliser theorem,  $|G| = 6 \cdot 8 = 24$ . So the action of  $G$  on diagonals is not faithful. So there is  $g \in G$  with  $g \neq 1$  but  $g$  fixes all diagonals. Let's think about what such a  $g$  might do. Label the vertices of the cube with the 8 elements in  $\{+1, -1\}^3$  (which is in any case naturally tho'rt of as a cube in  $\mathbb{R}^3$ ) and consider the function  $g(x, y, z) = (-x, -y, -z)$ . “swap opposite faces”. The numbers on opposite faces of a gambler's die add up to 7, so use the numbers on the faces of the die and then we can think of  $g$  as  $(1, 6)(2, 5)(3, 4)$ . [am i right in thinking that this operation transforms a die into a different die which is its mirror image and the two are not superimposable...?] Then  $G \simeq S_4 \times \langle g \rangle$ .  $\langle g \rangle$  is  $C_2$ .

Remember that subgroups of order 2 are always normal. So  $S_4 \trianglelefteq G$ . As it happens  $\langle g \rangle \trianglelefteq G$  too. Is this a case of internal direct product?

### 9.3 The Dodecahedron

Dual to the icosahedron. Let's call it ' $\mathcal{D}$ '. Twelve faces, each a regular pentagon. 30 edges 20 vertices.

As before, let  $G^+$  be the group of rotation. Clearly  $G$  has transitively on the faces. (How many orbits on pairs of faces?)  $|\text{Orb}_{G^+}(F)| = 12$ ;  $|\text{stab}_{G^+}(F)| = 5$ .

We can embed five cubes in the icosahedron



This view of a complete edge is supposed to be a face of an embedded cube.

Now  $G^+$  acts faithfully on the five cubes, whence  $G^+ \hookrightarrow S_5$ .  $|G^+| = 60$ . The only subgroup of  $S_5$  of order 60 is  $A_5$ . (We aren't expected to know why this is true!)  $A_5$  is the group of even permutations, so there should be a way of thinking of a symmetry of  $\mathcal{D}$  as an even permutation. A five-cycle is an even permutation (check it!) and each face is a pentagon so there might be a good fit there. Think of a pair of opposite faces; join their centres and consider rotations around that axis. (The opposite faces are staggered not eclipsed but i'm persuading myself that that doesn't matter) Six such opposite pairs, and each gives a 5-cycle. There are 10 pairs of opposite vertices and each of those gives rise to a 3-cycle (the vertices "have degree 3")  $\rightarrow 20$  elements of order 3.

$A_5$  also contains the "double transpositions"—a product of two disjoint transpositions. These correspond to rotations about axes through pairs of opposite edges.

Now we proceed to another application of orbit-stabiliser.

### THEOREM 9 *Cauchy*

Let  $G$  be a finite group and  $p$  a prime dividing  $|G|$ . Then  $G$  has an element of order  $p$ .

*Proof:*

Fix  $G$  and  $p$ .  $G^p$  is the set of  $p$ -tuples of elements of  $G$ . (This is pretty standard notation.). Then let  $X$  be  $\{s \in G^p : s \text{ multiplies out to } \mathbf{1}\}$ . In particular if  $o(x) = p$  then

$$\overbrace{x, x, x \dots x}^{p \text{ times}} = \mathbf{1} \text{ so}$$

$$\overbrace{x, x, x \dots x}^{p \text{ times}} \in X.$$

Now let  $H$  be a realisation of  $C_p$ .  $H$  is cyclic and so is  $\langle h \rangle$  for any  $h \in H$ . Fix one such and call it  $h$ .


Consider now the following action of  $H$  on  $X$ .

$$(h, \bar{x}) = (x_2, x_3, x_4 \dots x_p, x_1)$$

So far i've only said what the generator  $h$  does to a tuple in  $X$ , and even that not clearly! What it does is what used to be called in old assembler languages ROTATE-LEFT.  $\bar{x} \in X$  is a string of length  $p$ , and we can whack it with commands like ROTATE-LEFT.

OK, so what do other elements of  $H$  do to strings from  $X$ ? We can deduce what they do from two facts. (i) This is a group action, and (ii) every element of  $H$  is a power of  $h$ . Thus (using the fact that this is an action)  $h^2$  must ROTATE-LEFT twice, and so on. Since everything in  $H$  is a power of  $h$  this defines the action completely.

We have to check that if we ROTATE-LEFT a string in  $X$  then we obtain another string in  $X$ . Of course this is blindingly obvious if  $G$  is abelian but it

 says  
Dr C

mightn't be. So let  $\bar{x} = (x_1 \underline{x_2} \dots x_p)$  be a string in  $X$ . ROTATE-LEFT to obtain  $(\underline{x_2} \dots x_p, x_1)$ . Now observe that the underlined bit is simply  $x_1^{-1}$  (beco's  $\bar{x} \in X$ ) so  $\underline{x_2} \dots x_p, x_1$  evaluates to  $\mathbf{1}$  as well.

So we do really have a group action.

Sum the sizes of the orbits to get  $|X|$ . What is  $|X|$ ? Actually this can be easily computed. We want to build a string of length  $p$  whose product will be  $\mathbf{1}$ . We can choose the first  $p-1$  elements  $x_1 \dots x_{p-1}$  however we like, beco's we can then set  $x_p$  to be  $(x_1 \dots x_{p-1})^{-1}$ ! So we have  $p-1$  choices from  $G$ , so the answer is  $|G|^{(p-1)}$ . Now, *ex hypothesi*,  $p$  divides  $|G|$ , so  $p$  divides  $|G|^{(p-1)} = |X|$ . By the orbit-stabiliser theorem we have  $|\text{Orb}_H(\bar{x})| \cdot |\text{stab}_H(\bar{x})| = |H| = p$ .

So  $|\text{Orb}_H(\bar{x})| = 1$  or  $p$ —co's its order divides  $p$ .

There is an orbit of size 1, name the orbit of

$$\overbrace{\mathbf{1}, \mathbf{1}, \dots, \mathbf{1}}^{p \text{ times}}$$

How many such orbits are there? Every orbit has a size that is 1 or a multiple of  $p$ , so if there are any orbits of size 1 (and there are) there must be enuff of them so that the number of singleton-orbits as a multiple of  $p$ . So there must be at least one other singleton orbit.

Orbits of length 1 correspond to elements of order  $p$ , as follows. An element  $\bar{x}$  whose orbit is a singleton is of the form  $\overbrace{\{x, x, \dots, x\}}^{p \text{ times}}$ . But then  $x$  is an element of order  $p$ .

[end of seventeenth lecture]

We need to revise our definition of a *symmetry* of a figure. Isometry of  $\mathbb{R}^n$  that preserves the figure not just the vertices. Need a picture here, and i can't do it in L<sup>A</sup>T<sub>E</sub>X).

## 9.4 Conjugacy Action

Some remarks

(i) The conjugacy classes partition  $G$ .

(ii) By orbit-stabiliser thm we have  $(\forall x \in G)(|G| = |C_G(x)| \cdot |ccl(x)|)$ .

(iii) Elements that are conjugate have the same order. The key move is to consider what happens when one write out  $(ghg^{-1})^{o(h)}$  in full. All the “inner” occurrences of ‘ $g$ ’ and ‘ $g^{-1}$ ’ cancel, so we are left with  $gh^{o(h)}g^{-1}$  which is of course  $\mathbf{1}$ . Can this happen for any smaller exponent?  $(ghg^{-1})^j$  is  $gh^jg^{-1}$ . Can this be  $\mathbf{1}$ ? Not unless  $h^j = \mathbf{1}$ , co's anything conjugate to  $\mathbf{1}$  is  $\mathbf{1}$ .

(iv)  $\mathbb{Z}(G) = \{g \in G : (\forall h \in G)(ghg^{-1} = h)\} \trianglelefteq G$ . It's the intersection  $\bigcap_{g \in G} C_G(g)$  of all the centralisers.

N.B:  $z \in \mathbb{Z}(G)$  iff  $|ccl_G(z)| = 1$  (i.e., the conjugacy class of  $z$  is  $\{z\}$ ) beco's  $z$  commutes with everything so any conjugate  $gzg^{-1}$  of  $z$  must be  $z$ .

(v) A subgroup is normal iff it is a union of conjugacy classes. (Sheet 3 Q 2).

(vi)  $G$  is abelian iff  $\mathbb{Z}(G) = G$ .

**PROPOSITION 6** Let  $G$  be a finite group with  $G/\mathbb{Z}(G)$  cyclic. Then  $G$  is abelian.

$G/\mathbb{Z}(G)$  so it is  $\langle y(\mathbb{Z}(G)) \rangle$  for some  $\mathbb{Z}(G)$  coset  $y(\mathbb{Z}(G))$ . We have to show that any two  $g, h \in G$  commute.


We have  $g(\mathbb{Z}(G)) = y^i(\mathbb{Z}(G))$  for some  $i$  beco's the quotient is cyclic.

So  $g = y^i z_1$  for some  $z_1 \in \mathbb{Z}(G)$ .

Similarly So  $h = y^j z_2$  for some  $z_2 \in \mathbb{Z}(G)$ .

So  $gh = y^i z_1 y^j z_2$ .

The point now is that  $z_1$  and  $z_2$  are in the centre and commute with everything, so  $z_1$  can be pushed to the end, giving  $gh = y^i y^j z_2 z_1$ .  $y^i$  commutes with  $y^j$  and with  $z_2$  so we can push it to the right as well, getting  $gh = y^j z_2 y^i z_1 = hg$ . ■

I think that's worth a .

**COROLLARY 4** Suppose  $|G| = p^2$  with  $p$  prime. Then  $G$  is abelian, and in fact is either  $C_{p^2}$  or  $C_p \times C_p$ .

(Think about why  $C_{p^2}$  and  $C_p \times C_p$  are distinct: see  $C_5$  and  $C_2$  on p. 33.) Sheet 3 Q 10.

Remarks

1. A group of order  $p^n$  with  $p$  prime is a *finite  $p$ -group*.
2. If all elements of  $G$  are of  $p$ -power order we say the group is a  $p$ -group Eg, the Prüfer group on p. 24.

## 9.5 Conjugation in $S_n$

**DEFINITION 17** The **cycle type** of a permutation is a tuple that tells you how many cycles it has of which length. Thus  $(1, 2, 3)(4, 5, 6, 7)(8)$  has cycle type  $(4, 3, 1)$ . basic observation: the numbers in the cycle-type of an element of  $S_n$  must add up to  $n$ .

**THEOREM 10** In  $S_n$  two permutations are conjugate iff they have the same cycle type.

*Proof:*

Think of a permutation as a product of disjoint cycles. Think of each cycle as a polygon, with directed edges and each vertex labelled. Thus a permutation in  $S_n$  is a bundle of polygons (one for each cycle) with the vertices of the polygons labelled in such a way that each number  $\leq n$  is used precisely once.

This should be proposition 7 when i've persuaded LaTeX to number things properly.

Will be coroll 5 when LaTeX numbers things properly

theorem 9 according to Dr C

Such a picture represents a unique permutation  $\pi$  of  $[1, n]$ . What does  $\pi$  send  $k$  to? Find the vertex labelled ' $k$ '. There is a directed edge [precisely one!] going from that vertex to another vertex. The label on that vertex is your  $\pi(k)$ .

OK. Suppose we have two permutations  $\sigma$  in  $\tau$  with the same cycle type. They have the same number of  $k$ -cycles for each  $k$ , so pair them off, somehow. So each (as it might be)  $k$ -cycle  $s$  (written with pink edges) in  $\sigma$  has been assigned to a  $k$ -cycle  $t$  (written in blue edges) in  $\tau$ . We now have to map  $s$  onto  $t$  in an "adjacency-preserving" way, and there are clearly  $k$  ways to do this. Pick one such map  $s \rightarrow t$  for each married couple  $s$  and  $t$ , and write the edges joining  $s$ -vertices to  $t$ -vertices in green, with arrows pointing from  $s$  to  $t$ . What have we got? The green edges are a graphical representation of a new permutation  $\pi$  of  $[1, n]$ . And  $\pi$  conjugates  $\sigma$  and  $\tau$ . Start your odyssey on a vertex in a pink polygon. Fly over to a blue polygon using  $\pi$ . Move along a blue  $\tau$  edge; then fly back along a green  $(\pi^{-1})$  edge. What have you done? You've in effect travelled one step along a pink edge! ■

Observe that this construction tells you nothing about the cycle type of the green edges, the  $\pi$  that conjugates  $\sigma$  and  $\tau$ ...but then we were never promised that.

Consider specifically  $S_4$ . Build a table

[seventeenth lecture ends in the middle of this table]

	Cycle Type	Size of $S_4$ conj' class	Sign	Size of centraliser	$C_{S_4}(x)$
<b>1</b>	(1,1,1,1)	1	+1	24	$S_4$
(1, 2)	(2,1,1)	6	-1	4	$\langle(1, 2), (3, 4)\rangle$
(1, 2, 3)	(3,1)	8	+1	3	$\langle(1, 2, 3)\rangle$
(1, 2, 3, 4)	(4)	6	-1	4	$\langle(1, 2, 3, 4)\rangle$
(1, 2)(3, 4)	(2,2)	3	+1	8	$\langle(1, 3, 2, 4), (1, 2)\rangle = D_8$

**COROLLARY 5** *The number of distinct conjugacy classes in  $S_n$  is given by the function often written ' $p(n)$ ' aka the number of partitions of  $n$ , to wit: the number of ways in which  $n$  can be expressed as the sum of a multiset of smaller (nonzero) numbers.*

This will be Corollary 6 when L<sup>A</sup>T<sub>E</sub>X gets the numbering right

*Proof:* Each such "partition" corresponds to a conjugacy class!

Conjugacy class in  $A_n$  is a lot less clear. If we are thinking of  $A_n$  fairly concretely as the set of even permutations of a set of size  $n$  (say  $[1, n]$  if we want to be specific) then clearly two permutations that are conjugate in  $A_n$  are conjugate in  $S_n$ . Not obvious that the converse holds. In fact it's easy to see that it won't. Suppose i have two disjoint 3-cycles. They're both even, so they're in  $A_n$ . What conjugates them? Obviously a product of three disjoint transpositions, and that ain't in  $A_n$ . Dr C's example is even easier. What conjugates (1, 2, 3) and (1, 3, 2)? A single transposition! In both these case the

things are also conjugated by permutations that move other stuff around, but there might not be enough other stuff around to move.

Let's use her example, and work in  $A_4$  (where indeed there isn't room to move other stuff around) and consider  $C_{A_4}((1, 2, 3)) = C_{S_4}((1, 2, 3)) \cap A_4$ .

$$C_{A_4}((1, 2, 3)) = \langle (1, 2, 3) \rangle \subseteq A_4 \text{ so } C_{A_4}((1, 2, 3)) = C_{S_4}((1, 2, 3)).$$

So  $|ccl_{A_4}((1, 2, 3))| = |A_4|/|C_{A_4}((1, 2, 3))|$  by the orbit-stabiliser theorem.  
 $= (|S_4|/2)/|C_{S_4}((1, 2, 3))| = |ccl_{S_4}((1, 2, 3))|/2$ .

So the conjugacy class of a 3-cycle in  $A_4$  splits into two conjugacy classes in  $A_4$ . [Presumably this is because 3 is odd].

Dr C says: **key point!**

If  $C_{A_n}(x) = C_{A_n}(x)$  (which is to say that  $x$  doesn't commute with any odd element) then  $|ccl_{A_n}(x)| = |ccl_{S_n}(x)|/2$

On the other hand, if  $C_{A_n}(x) < C_{A_n}(x)$  (so  $C_{A_n}(x)$  contains an odd permutation) then

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

(see sheet 2 q 6) and  $|ccl_{A_n}(x)| = |ccl_{S_n}(x)|$ .

Let's have another table, for  $A_4$ .

	Cycle Type	Size of conj' class	Size of $C_{A_4}(x)$	$C_{S_4}(x)$
<b>1</b>	(1,1,1,1)	1	24	$A_4$
(1, 2, 3)	(3,1)	4	3	$\langle (1, 2, 3) \rangle$
(2, 1, 3)	(3,1)	4	3	$\langle (2, 1, 3) \rangle$
(1, 2)(3, 4)	(2,2)	3	8	$\langle (1, 3)(2, 4), (1, 2)(3, 4) \rangle \simeq C_2 \times C_2$

Now a table for  $S_5$

	Cycle Type	Size of conj' class	Sign	Size of centraliser	$C_{S_5}(x)$
<b>1</b>	(1,1,1,1,1)	1	+1	120	$S_5$
(1, 2)	(2,1,1,1)	10	-1	12	$\langle (1, 2) \rangle \times \text{Sym}([3, 5])$
(1, 2, 3)	(3,1,1)	20	+1	6	$\langle (1, 2, 3), (4, 5) \rangle \simeq C_6$
(1, 2, 3, 4)	(4,1)	30	-1	4	$\langle (1, 2, 3, 4) \rangle \simeq C_4$
(1, 2, 3, 4, 5)	(5)	24	+1	5	$\langle (1, 2, 3, 4, 5) \rangle \simeq C_5$
(1, 2)(3, 4)	(2,2,1)	15	+1	8	$\langle (1, 3, 2, 4) \rangle$
(1, 2, 3)(4, 5)	(3,2)	20	-1	6	$\langle (1, 2, 3), (4, 5) \rangle \simeq C_6$

	Cycle Type	Size of $A_5$ conj' class	$C_{A_5}(x)$
<b>1</b>	(1,1,1,1,1)	1	$A_5$
(1, 2, 3)	(3,1)	20	$\langle (1, 2, 3) \rangle$
(1, 2, 3, 4, 5)	(5)	12	same as in $S_5$
(2, 1, 3, 4, 5)	(5)	12	$\langle (2, 1, 3, 4, 5) \rangle$
(1, 2)(3, 4)	(2,2,1)	15	$\langle (1, 3)(2, 4), (1, 2)(3, 4) \rangle \simeq C_2 \times C_2$



*Message to myself:* Here's how to see that an orbit of an element of  $S_n$  might split into two orbits in  $A_n$ . (And *only* two orbits.) Let  $\pi$  be an even permutation in  $S_n$ . All the things conjugate to  $\pi$  are also even permutations, so how might they come in two flavours? Let  $\tau$  be something conjugate to  $\pi$ . There are things that conjugate  $\pi$  to  $\tau$ . It may be that there are even things that conjugate  $\pi$  to  $\tau$ , or it might be that there are only odd things. If the first, then  $\pi$  and  $\tau$  remain conjugate in  $A_n$ . If the latter, then evidently  $\pi$  and  $\tau$  will not be conjugate in  $A_n$ . Now suppose  $\tau$  and  $\sigma$  are two things which are conjugated to  $\pi$  in  $S_n$  only by odd things. Start with  $\tau$ ; conjugate it by an odd thing to obtain  $\pi$ ; now conjugate by another odd thing to obtain  $\sigma$ . What have you done? You have conjugated  $\tau$  to  $\sigma$  by an even permutation! So  $\tau$  and  $\sigma$  are conjugate in  $A_n$ . So any two things which are conjugate-to- $\pi$ -in- $S_n$ -but-not-in- $A_n$  are conjugate-to-each-other-in- $A_n$ . So the  $S_n$  orbit of an even permutation either splits into precisely two bits or remains in one piece.

What's all the fuss about? A conjugacy class of an even permutation might split into two or it mightn't. Is this a plot point? No. Apparently the reason for all this detail is merely that, once students get into their heads the idea that having-the-same-cycle-type might be a sufficient condition for being-conjugate, they assume that it is always sufficient. It ain't, and they have to be broken of the habit.

[end of eighteenth lecture]

## 10 Matrix Groups

$M_n(\mathbb{F})$  is the set of  $n \times n$  matrices with entries in the field  $\mathbb{F}$ .

section 7 in Dr C's numbering

$GL_n(\mathbb{F})$  is the general linear group—of invertible members of  $M_n(\mathbb{F})$ , equipped with matrix multiplication.

**PROPOSITION 7**  $GL_n(\mathbb{R})$  is a group under matrix multiplication.

proposition 8 in Dr C's numbering

*Proof:* Some trivial checking to be done. Clearly the matrix product of two invertible  $n \times n$  matrices with real entries is another such. The unit of  $GL_n(\mathbb{R})$  is the diagonal matrix with all 1's. Inverse? These matrices are *invertible*—duh! You know from V&M that matrix multiplication is associative. ■

**PROPOSITION 8**  $\det: GL_n(\mathbb{R}) \rightarrow \mathbb{R} \setminus \{0\}$  is a surjective group homomorphism.

proposition 9 in Dr C's numbering

Here we equip  $GL_n(\mathbb{R})$  with matrix multiplication and  $\mathbb{R} \setminus \{0\}$  with real multiplication to make both things into groups.

*Proof:*

This all follows from standard V&M stuff. The determinant of the product of two matrices is the product of the determinants, and other such standard facts. It's surjective beco's, for any real  $r$ , we can find a (diagonal)  $n \times n$  matrix whose determinant is  $r$ . ■

Observe that the proof of proposition 8 does not depend on anything very specific about the field  $\mathbb{R}$ . You could replace the set  $\mathbb{R} \setminus \{0\}$  with the nonzero elements of any field whatever and it would still work. This is important!

Clearly the kernel of the determinant map  $\det: GL_n(\mathbb{R}) \rightarrow \mathbb{R} \setminus \{0\}$  is going to be that subgroup of  $\det: GL_n(\mathbb{R})$  consisting of matrices of determinant 1. This subgroup is  $SL_n(\mathbb{R})$ , the special linear group, and it is clearly a normal subgroup of  $GL_n(\mathbb{R})$ .

What other fields are there? There is  $\mathbb{R}$  of course,  $\mathbb{Q}$  and  $\mathbb{C}$ . Also the field of rational functions, and, for every prime  $p \in \mathbb{N}$ , the field  $\mathbb{F}_p$  of integers mod  $p$ . Dr C wants us to think about the sizes of  $GL_n(\mathbb{F}_p)$  and  $SL_n(\mathbb{F}_p)$ .

### Now let's think about the actions of $GL_n(\mathbb{C})$

$GL_n(\mathbb{C})$  acts on  $\mathbb{C}^n$  in by the usual multiply-a-vector-on-the-left-by-a-matrix. (The vector has to be the right length of course). This is a faithful action: consider the basic vectors (every entry but one is 0) if it fixes all of those it's the identity matrix. This action has precisely two orbits on  $\mathbb{C}^n$ : one orbit for the null vector and one for all the others: if  $v, w \in \mathbb{C}^n$  neither of them null, then there is  $A \in GL_n(\mathbb{C})$  s.t.  $Av = w$ .

$GL_n(\mathbb{C})$  acts on  $\mathbb{C}^n$  by conjugation. This is much more fun. Two matrices  $A$  and  $B$  are conjugate iff they represent the same linear map  $\mathbb{C}^n \rightarrow \mathbb{C}^n$ . If  $A$  and  $B$  are conjugated by  $P$  then  $P$  represents a change of basis.

$$\begin{aligned} e_1 &= \begin{pmatrix} 1 \\ 0 \end{pmatrix}; \quad e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ A : e_1 &\mapsto 2e_1; \quad e_2 \mapsto 3e_2. \quad A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \\ P : e_1 &\mapsto e_2; \quad e_2 \mapsto e_1. \quad P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = P^{-1} \\ PAP^{-1} &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix} \\ \text{i.e., } e_2 &\mapsto 3e_2; \quad e_1 \mapsto 2e_1. \end{aligned}$$

When considering Möbius groups we will appeal to the following fact from V&M.

Suppose  $A \in M_2(\mathbb{C})$  and consider the conjugation action of  $GL_2(\mathbb{C})$  on  $M_c(\mathbb{C})$ . Then precisely one of the following happens

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  $A$  contains a diagonal matrix  $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ ;
3. The orbit of  $A$  contains a matrix  $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ .

Which is to say that  $A$  is conjugate to a matrix of one of those three forms. Apparently this cannot be relied upon to work for *all* fields (Dr C sez it doesn't work for  $\mathbb{R}$ , for example) but it does work for  $\mathbb{C}$ .

*Proof:*

1. In this case  $A$  has two distinct eigenvalues,  $\lambda \neq \mu$ . Take a basis consisting of eigenvectors. Distinct pairs  $\{\lambda, \mu\}$  give distinct orbits.
2. Eigenvalues  $\lambda, \lambda$ . Two linear independent eigenvectors.
3. Every maximal independent set of eigenvectors is a singleton.

■

### 10.0.1 some remarks

1.  $A^T$  is  $A_{ij}^T = A_{ji}$ . (“Reflect in the diagonal”).  
 $(AB)^T = B^T A^T$ . This is beco’s  
 $(AB)_{ij}^T = (AB)_{ji} = A_{jk} B_{ki}$  while  
 $(B^T A^T)_{ij} = B_{ik}^T A_{kj}^T = B_{ki} A_{jk}$


[end of nineteenth lecture]

2.  $AA^T = I_n$  iff  $A^T A = I_n$ <sup>13</sup>
3.  $(A^T)^{-1} = (A^{-1})^T$
4.  $\det(A^T) = \det(A)$ .

All this is standard from V& M.

**DEFINITION 18**  $O_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : A^T A = I_n\}$  is the orthogonal group

The rows of such an  $A$  form an ortho<sup>(\*)</sup>normal<sup>(\*\*)</sup> basis of  $\mathbb{R}^n$ . <sup>(\*)</sup> *ortho* for *orthogonal*; <sup>(\*\*)</sup> *normal* for the entries being units.

**PROPOSITION 9**  $O_n(\mathbb{R})$  is a [very nice ] subgroup of  $GL_n(\mathbb{R})$

proposition 10  
according to  
Dr C

*Proof:*

Note that  $1_{\mathbb{R}} = \det(I_n) = \det(A^T A) = \det(A^2)$  whence  $\det(A) \neq 0$ , so  $A$  is in  $GL_n(\mathbb{R})$  as claimed.<sup>14</sup>

Obviously  $I_n$  is the identity element of  $GL_n(\mathbb{R})$ .

Must check that ta product of two elements of  $O_n(\mathbb{R})$  is another element of  $O_n(\mathbb{R})$ .

$$(AB)^T(AB) = B^T \underline{A^T A} B = B^T B = I_n$$

(the underlined bit cancels).

<sup>13</sup> $I_n$  is the identity  $n \times n$  matrix.

<sup>14</sup>Sometimes i write ‘ $1_{\mathbb{R}}$ ’ when i want to emphasise that 1 is a real number. It can make formulae easier to read.

$A^T$  is the inverse of  $A$  in this group. (Yes,  $A^T$  is in the group if  $A$  is) ■

Remark:  $1 = \det(AA)$  so  $\det(A)$  is 1 or  $-1$  (we're in  $\mathbb{R}$ ). So  $\det: O_n(\mathbb{R}) \rightarrow \rightarrow (\{+1, -1\}, \times_{\mathbb{R}})$  is a surjective homomorphism. Must find  $A \in O_n(\mathbb{R})$  with determinant  $-1$  to be sure it's surjective. But the diagonal matrix with a  $-1$  in the top left is one such.

Now the kernel of this determinant homomorphism is  $\{A \in O_n(\mathbb{R}) : \det(A) = 1\}$ . This is called " $SO_n(\mathbb{R})$ " the special orthogonal group. By the first isomorphism theorem we have  $O_n(\mathbb{R})/SO_n(\mathbb{R}) = (\{+1, -1\}, \times_{\mathbb{R}})$

memo to self:  
draw this matrix properly when you have time  
lemma 20 according to Dr. C

**LEMMA 17** Let  $A \in O_n(\mathbb{R})$  and suppose  $\vec{x}, \vec{y} \in \mathbb{R}^n$ . Then

1.  $A\vec{x} \cdot A\vec{y} = \vec{x} \cdot \vec{y}$  (preserves dot-product);
2.  $|A\vec{x}| = |\vec{x}|$ ,<sup>15</sup>

*Proof:*

1.  $A\vec{x} \cdot A\vec{y} = (A\vec{x})^T (A\vec{y}) = \vec{x}^T \cdot A^T A \vec{y} = \vec{x}^T \vec{y} = \vec{x} \cdot \vec{y}$ ;
2.  $|A\vec{x}|^2 = A\vec{x} A\vec{x} = \vec{x} \vec{x} = |\vec{x}|^2$

So  $A$  is an isometry of  $\mathbb{R}^n$  ■

Let's analyse the  $2 \times 2$  case.

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}; I = AA^T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a^2+b^2 & ac+bd \\ ac+bd & c^2+d^2 \end{pmatrix}.$$

$$A^T A = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2+c^2 & ab+cd \\ ab+cd & b^2+d^2 \end{pmatrix}.$$

So we deduce

$$1 = a^2 + b^2 = c^2 + d^2 = a^2 + c^2 = b^2 + d^2$$

$$0 = ab + cd = ac + bd$$

Trig functions anyone?

So assume  $a = \cos\theta$  for some  $\theta$ . So  $c = \sin\theta$ .  $b$  and  $d$ ?

$$\begin{pmatrix} b \\ d \end{pmatrix} = \begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix} \text{ or } \begin{pmatrix} b \\ d \end{pmatrix} = \begin{pmatrix} \sin\theta \\ -\cos\theta \end{pmatrix}.$$

---

<sup>15</sup>The vertical bars are not cardinality this time!

### 10.0.2 Case 1

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

Then  $A\begin{pmatrix} x \\ y \end{pmatrix}$  is the vector  $\begin{pmatrix} \cos\theta x - \sin\theta y \\ \sin\theta x + \cos\theta y \end{pmatrix}$ .

So let's set  $z = x + iy$ , so that

$$e^{i\theta}z = (\cos\theta x - \sin\theta y) + i(\sin\theta x + \cos\theta y)$$

and  $A$  represents a rotation, and  $\det(A) = 1$ .

All elements of  $SO_2(\mathbb{R})$  are of this form.

### 10.0.3 Case 2

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

Then  $A\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cos\theta x + \sin\theta y \\ \sin\theta x - \cos\theta y \end{pmatrix}$ .

Let  $z = x + iy$  as in case 1,

$$e^{i\theta}\bar{z} = (\cos\theta x + \sin\theta y) + i(-\cos\theta y + \sin\theta x).$$

What are the fixed points of this map?

$e^{i\theta/2}z$  is a real, call it  $r$ . So  $A$  represents a reflection in the line  $re^{i\theta/2}$ .  $\det(A) = -1$ , and all such  $A$  are reflections. So

$O_2(\mathbb{R})$  is the union of the subgroup  $SO_2(\mathbb{R})$  and its coset  $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}SO_2(\mathbb{R})$ . The two are disjoint.

## 10.1 Now consider the three-dimensional case

**PROPOSITION 10** Any  $A \in SO_3(\mathbb{R})$  has an eigenvector with eigenvalue 1.

proposition 11  
in Dr C's num-  
bering

*Proof:*

Let  $\chi_A$  be the characteristic polynomial of  $A$ . It will be a cubic with coefficients in  $\mathbb{R}$ . It has at least one real root. (One or three).  $A$  is distance preserving [beco's the determinant is 1...?]

Let  $\lambda$  be a (possibly *the*) real root, and  $\vec{v}$  the corresponding eigenvector.  $|\vec{v}| = |A\vec{v}| = |\lambda\vec{v}| = |\lambda| \cdot |\vec{v}|$  so  $\lambda$  is 1 or  $-1$  by lemma 17.

What are the other eigenvalues of  $A$ ? Bear in mind that the product of the eigenvalues is equal to the determinant.

(i) or (ii):

(i) Suppose the other two roots are a complex pair  $\alpha$  and  $\bar{\alpha}$ . Then we have

$$1 = \det(A) = \lambda\alpha\bar{\alpha} = \lambda|\alpha|^2 \rightarrow \lambda = 1_{\mathbb{R}};$$

(ii) All roots are real. They must be 1, -1 and -1, or 1, 1 and 1. But at any rate at least one eigenvalue must be  $1_{\mathbb{R}}$ .

■

**THEOREM 11** Suppose  $A \in SO_3(\mathbb{R})$ . Then  $A$  is conjugate to a matrix of the form

theorem 11 according to Dr C

$$\begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad ()$$

for some  $\theta \in [0, 2\pi]$

In particular,  $A$  is a rotation about an axis thru' the origin.

*Proof:*

We have to find the right basis. By proposition 11,  $(\exists \vec{v})(A\vec{v} = \vec{v})$ , and we can assume  $|\vec{v}| = 1_{\mathbb{R}}$ . Let  $\{e_1, e_2, e_3\}$  be the standard orthonormal basis for  $\mathbb{R}^3$ . There must be  $P \in SO_3(\mathbb{R})$  s.t.  $P\vec{v} = e_3$ . NB:  $PAP^{-1}(e_3) = e_3$ . (This will turn the problem into a 2-dimensional one, and these we know how to solve.) Let  $\Pi$  be the plane orthogonal to  $e_3$  (so  $\Pi = \langle e_1, e_2 \rangle$ ). Then  $PAP^{-1}$  is

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

$Q$  is the action of  $PAP^{-1}$  on  $\Pi$ . So  $Q^T Q = I_3$  and  $\det(Q) = 1$  so

$$Q = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \text{ for some } \theta.$$

[end of twentieth lecture]

Every element of  $SO_3(\mathbb{R})$  is a product of reflections.<sup>16</sup> Suppose  $r$  is a reflection in a plane through the origin  $0_{\mathbb{R}}$ . Then let  $\underline{n}$  be the unit vector normal to this plane. Then  $r(\underline{x}) = \underline{x} - 2(\underline{x} \cdot \underline{n}) \cdot \underline{n}$  so  $r$  is conjugate to the matrix

Not sure about all these underlinings ... can't always see board properly

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (C)$$

which is in  $O_3(\mathbb{R})$ . So  $O_3(\mathbb{R})$  is  $SO_3(\mathbb{R})$  [which contains rotations] unioned with the left  $SO_3(\mathbb{R})$  coset given by the matrix  $C$  above [which contains reflections plus other stuff].

**THEOREM 12** Every element of  $O_3(\mathbb{R})$  is a product of at most three reflections.

13 according to Dr C

<sup>16</sup>this reminds me of a fact about  $S_n$  that i've always known: every permutation is a product of two involutions (elements of order two). Think of the permutation  $\pi$  as a whole lot of polygons written on the plane (with directed edges). Then the effect of  $\pi$  on each polygon can be tho'rt of a product of two reflections. On a  $\mathbb{Z}$ -cycle fix one element to be 1, and then consider the two involutions  $x \mapsto -x$  and  $x \mapsto 1 - x$ . Their composition moves each point along one edge...

*Proof:*

Let  $\{e_1, e_2, e_3\}$  be the standard orthonormal basis for  $\mathbb{R}^3$ . Let  $A$  be an element of  $O_3(\mathbb{R})$ . We will find three reflections  $r_1, r_2$  and  $r_3$  s.t.  $A = r_1 r_2 r_3$ .

$|Ae_3| = |e_3| = 1_{\mathbb{R}}$  since  $A$  is an isometry. Next we find a reflection  $r_1$  sending  $Ae_3$  to  $e_3$ . Let  $\Pi\langle e_1, e_2 \rangle$  be the plane  $\perp$  to  $e_3$ .<sup>17</sup> We must have  $r_1 \cdot A\Pi = \Pi$ .<sup>18</sup> So we choose a reflection  $r_2$  such that  $r_2(e_3) = e_3$  and  $r_2 r_1 A(e_2) = e_2$ , with the effect that  $r_2 \cdot r_1$  fixes both  $e_3$  and  $e_2$ . Further  $r_2 r_1 A(e_1) = e_1$  or  $r_2 r_1 A(e_1) = -e_1$ . If  $r_2 r_1 A(e_1) = e_1$  then we set  $r_3$  to be the identity; if  $r_2 r_1 A(e_1) = -e_1$  then we set  $r_3$  to be a reflection in a plane  $\perp$  to  $e_1$ .

Then  $r_1 r_2 r_3 A$  fixes everything! So  $A = r_1 r_2 r_3$ . ■

## 11 The Möbius Group

**DEFINITION 19** A Möbius Transformation is a map  $f : \mathbb{C} \rightarrow \mathbb{C}$  of the form

$$z \mapsto \frac{az + b}{cz + d}$$

subject to  $ad - bc \neq 0$ , and  $a, b, c, d$  all in  $\mathbb{C}$

Why  $ad - bc \neq 0$ ? Well, if  $ad = bc$  then  $f$  is constant, which is sooooo boring. Pleasingly, if  $ac \neq bd$  then  $f$  is actually injective:

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

Another tho'rt:  $f(-d/c)$  crashes... and we want  $f$  to be defined at the “point at infinity”. Only one point at infinity? Yes. **stereographic projection** and **Riemann Sphere**. Place a sphere on the complex plane, with the tangent at the origin. Place a light source at the top of the sphere, and project light thence downwards thru’ the sphere. All such downward rays go down thru’ the sphere, then they come out the other side and eventually reach the plane. This defines a bijection between the plane and the surface of the sphere. This is the **stereographic projection**. To what point in the complex plane does the point at the top of the sphere correspond? The point at infinity! That’s how there manages to be only *one* point at infinity!

The complex plane equipped with this extra point is called **the extended complex plane** and notated  $\mathbb{C} \cup \{\infty\}$  or (i think)  $\mathbb{C}_{\infty}$ . It is known as the *one-point compactification* of  $\mathbb{C}$ , the point being that the space with the added point is compact.

Armed with this new gadget we can redefine Möbius transformations by adding the following clauses:

<sup>17</sup>The symbol ‘ $\perp$ ’ means ‘perpendicular to’.

<sup>18</sup>Okay, Okay, you’ll probably be socialised into writing this as “ $r_1 \cdot A(\Pi) = \Pi$ .” My notation is easier to read.

section 8 in Dr  
C’s numbering  
dfn 22 in Dr  
C’s numbering

**DEFINITION 20**

if  $c \neq 0$  then  $f(-d/c) = \infty$  and  $f(\infty) = a/c$ ;  
if  $c = 0$  then  $f(\infty) = \infty$ .

definition 23  
according to  
Dr C  
proposition 12  
according to  
Dr C

**PROPOSITION 11** Suppose there are at least three  $z \in \mathbb{C}$  satisfying<sup>19</sup>

$$\frac{az+b}{cz+d} = \frac{\alpha z + \beta}{\gamma z + \delta}$$

(with  $ab - bc \neq 0$  and  $\alpha\delta - \beta\gamma \neq 0$ ). Then  $\exists \lambda \neq 0$  s.t.

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

i.e., these two Möbius transformations agree on all of  $\mathbb{C}$ .

*Proof:*

Suppose  $z$  is one of the three guilty parties. Then

$$(az+b)(\gamma z + \delta) = (\alpha z + \beta)(cz+d)$$

so these two quadratics in ‘ $z$ ’ are equal. Identify coefficients to obtain

$$a\gamma = \alpha c, \quad b\delta = \beta d \text{ and } b\gamma + a\delta = \alpha d + \beta c.$$

Now  $a\delta - \beta c = \alpha d - b\gamma$ , so abbreviate these two strings to ‘ $\mu$ ’.  
Then  $\mu^2 = (ad - bc)(\alpha\delta - \beta\gamma) \neq 0$ .  
Then

$$\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} \alpha \\ \gamma \end{pmatrix} = \begin{pmatrix} \mu \\ 0 \end{pmatrix}$$

So

$$\begin{pmatrix} \alpha \\ \gamma \end{pmatrix} = \frac{\mu}{ad-bc} \begin{pmatrix} ab \\ cd \end{pmatrix}$$

**THEOREM 13** The set  $M$  of Möbius maps  $\mathbb{C}_\infty \rightarrow \mathbb{C}_\infty$  is a group under composition of functions.

i don't trust  
my copy-  
ing skills—  
blackboard a  
long way away

theorem 14 ac-  
cording to Dr  
C

*Proof:*

- The identity map is a Möbius map. (set  $a := 1$ ,  $b := c := 0$  and  $d := 1$ ).
- Composition of two Möbius maps is a Möbius map? Suppose

$$f(z) = \frac{az+b}{cz+d} \text{ and } g(z) = \frac{\alpha z + \beta}{\gamma z + \delta}.$$

---

<sup>19</sup>we do mean  $\mathbb{C}$  not  $\mathbb{C}_\infty$ ?



There are several cases to consider. Let's start with a nondegenerate case, where  $c \neq 0$  and  $\gamma \neq 0$  and suppose  $z \in \mathbb{C}_\infty \setminus \{(-\delta)/\gamma\}$ . Then

$$f(g(z)) = \frac{a(\frac{\alpha z + \beta}{\gamma z + \delta}) + b}{c(\frac{\alpha z + \beta}{\gamma z + \delta}) + d} = \frac{(\alpha a + b\gamma)z + (\alpha\beta + \delta b)}{(c\alpha + \delta\gamma)z + (c\beta + \delta d)}$$

We claim that this is in  $M$ . The justification is that

$$(a\alpha + b\gamma)(c\beta + \delta d) - (a\beta + b\delta)(c\alpha + d\gamma) = (ad - bc)(\alpha\delta - \beta\gamma)$$

and neither factor on the RHS is 0, so the RHS isn't 0 either.

Now for the degenerate cases.

$$f(g(-\delta/\gamma)) = f(\infty) = a/c$$

and

$$\frac{(a\alpha + b\gamma)(-\delta/\gamma) + (\alpha\beta + b\delta)}{(c\alpha + \delta\gamma)(-\delta/\gamma) + (c\beta + \delta d)} = \frac{a(\alpha \cdot (-\delta/\gamma) + \beta)}{c \cdot (\alpha(-\delta/\gamma) + \beta)} = a/c.$$

(Need to check  $c = 0, \gamma = 0$ ).

- Inverses

If  $f \in M$  then  $f^{-1}(z)$  is  $\frac{dz-b}{-cz+a}$ .

**THEOREM 14**

$$GL_2(\mathbb{C})/Z \simeq M.$$

where  $Z$  is the centre of  $GL_2(\mathbb{C})$  and  $M$  is the Möbius group.

*Proof:*

$Z$  is actually  $\{(\lambda^0_0) \in GL_2(\mathbb{C}) : \lambda \neq 0\}$ .

We define a map  $\phi$  by:  $\phi: \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto f((az+b)/(cz+d))$ . We want  $\phi$  to be an isomorphism.

$$f = \phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) \text{ and } g = \phi\left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\right)$$

$$\phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) \cdot \phi\left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\right)(z) = \frac{(a\alpha + b\gamma)z + (a\beta + b\delta)}{(c\alpha + d\gamma)z + (c\beta + d\delta)}$$

(from proof of theorem 13)

$$f = \phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\right)$$

It's obvious that  $\phi$  is surjective

The identity  $\mathbf{1}_\mathbb{C} : \mathbb{C} \rightarrow \mathbb{C}$  is  $\phi\left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\right)$

**COROLLARY 6**  $SL_2(\mathbb{C})/\{I, -I\} \simeq M$

thm 15 according to Dr C

coroll 7 according to Dr C

*Proof:* We restrict  $\phi$  to  $SL_2(\mathbb{C})$ . The restriction  $\phi|_{SL_2(\mathbb{C})}$  is surjective and the kernel is  $\{I, -I\}$  with matrix multiplication.

**PROPOSITION 12** *Every Möbius map can be written as a composition of maps of the form*

proposition 13  
according to  
Dr C

- (i)  $f(z) = az$ , with  $a \neq 0$       *dilations or rotations*
- (ii)  $f(z) = z + b$       *translations*
- (iii)  $f(z) = 1/z$       *inversion*

*Proof*

Let  $g(z) = \frac{az+b}{cz+d}$  be a Möbius map.

If  $c = 0$  we do:

$z \mapsto (a/d)z \mapsto (a/d)z + (b/a)$  so  $g$  is a composition of a dilator and a translation.

If  $c \neq 0$  then  $g(z) = \frac{(a/c)z + (b/c)}{z + (d/c)} = a/c + \frac{(-ad+bc)}{z + (d/c)}$

so do:

$$z \mapsto z + (d/c) \mapsto \frac{1}{z + d/c} \mapsto a/c + \frac{(-ad+bc)}{z + (d/c)}$$

which is to say translation then inversion then multiplication then translation.

In definition 15 we defined what it is for a group  $G$  to act transitively on a set. We say now that

**DEFINITION 21** *An action of a group  $G$  is transitive on triples if for any three distinct  $x_1, x_2, x_3$  and distinct  $y_1, y_2, y_3$  there is  $g \in G$  s.t.  $g(x_1) = y_1$ ,  $g(x_2) = y_2$ ,  $g(x_3) = y_3$ . We say the action is **sharply** transitive if the  $g$  is unique:*

$$(\forall x_1 x_2 x_3, y_1 y_2 y_3)((\bigwedge_{0 < i \neq j \leq 3} x_i \neq x_j \wedge \bigwedge_{0 < i \neq j \leq 3} y_i \neq y_j) \rightarrow (\exists! g \in G)(\bigwedge_{0 < i \leq 3} g(x_i) = y_i))$$

We will show

that  $M$  acts sharply transitively on triples in  $\mathbb{C}_\infty$ .

*Proof:*

Suppose we want to send the triple  $x_1, x_2, x_3$  to  $w_1, w_2, w_3$ . The key move is to send  $x_1, x_2, x_3$  to  $0, 1, \infty$ . This is of course sufficient, co's if i can do this for every triple then i can get from any triple to any other triple via  $0, 1, \infty$ . To this end we will reletter the three variables ' $x_1$ ', ' $x_2$ ' and ' $x_3$ ' as ' $z_0$ ', ' $z_1$ ' and ' $z_\infty$ ' to remind those of us with short attention spans that the values of these three variables will be sent to  $0, 1$  and  $\infty$  respectively.

We will construct a function that does it.

First case, in which none of the  $z$  are 0.

Is this a theorem? A proposition ...?

$$g(z) := \frac{(z - z_0)(z_1 - z_\infty)}{(z - z_\infty)(z_1 - z_0)}$$

will do<sup>20</sup>

Let's now deal with some special cases:

$$\text{If } z_\infty = \infty \text{ set } g(z) := \frac{z - z_0}{z_1 - z_0}$$

$$\text{If } z_1 = \infty \text{ set } g(z) := \frac{z - z_0}{z - z_\infty}$$

$$\text{If } z_0 = \infty \text{ set } g(z) := \frac{z_1 - z_\infty}{z - z_\infty}$$

In exactly the same way we can construct a map  $h$  to send the  $\vec{w}$  to  $0, 1, \infty$ .

Now set  $f := h^{-1}g$ . That does the trick. Now we have to show that  $f$  is unique. Suppose  $f'$  is competition. Consider  $g \cdot (f')^{-1} \cdot f \cdot g^{-1}$ . It sends  $0 \mapsto 0$ ,  $1 \mapsto 1$  and  $\infty \mapsto \infty$

It fixes three points and so must be the identity.<sup>21</sup>

But then  $f = f'$ .

You can reconstruct a Möbius function from three ordered pairs in its graph!

### 11.0.1 Conjugacy classes in $M$

$M$  is a surjective image of  $GL_2(\mathbb{C})$  so information about conjugacy classes in  $M$  can be obtained from information about conjugacy classes in  $GL_2(\mathbb{C})$ . If  $A$  and  $B$  are conjugated by  $P$  in  $GL_2(\mathbb{C})$  then  $\phi(A)$  and  $\phi(B)$  are conjugated by  $\phi(P)$  in  $M$ .

Recall from V&M...

$$1. \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}; \lambda \neq 0 \neq \mu \neq \lambda$$

This goes to  $f$  defined by  $f(z) = (\lambda/\mu)z = \nu z$  with  $\nu \neq 0$

$$2. \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix};$$

This goes to  $f$  defined by  $f(z) = z$ .

$$3. \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \text{ with } \lambda \neq 0 \dots \text{goes to } f(z) = z + (1/\lambda)$$

But note that  $\begin{pmatrix} 1 & 1/\lambda \\ 0 & 1 \end{pmatrix}$  is conjugate to  $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ , as follows

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

so  $f$  is conjugate to  $g(z) = z + 1$ .

<sup>20</sup>You might be confused, as I was, by the fact that the 'z' without a subscript is a *variable* while the other zs are *constants*.

<sup>21</sup>A Möbius function has three degrees of freedom. You can always divide numerator and denominator by  $a$  to get the coefficient of 'z' in the numerator to be 1, leaving three choices for  $b, c$  and  $d$ . This isn't a *proof* that three ordered pairs from the graph of a Möbius function determine the whole thing but it's suggestive and can probably be turned into one.

theorem 17 in  
Dr C's counting

**THEOREM 15** *Any nonidentity Möbius function is conjugate to either  $f(z) = \nu z$  or  $f(z) = z + 1$*

*end of twenty-fourth lecture*

lectures wrong!