MAS3202. Group theory

Sarah Rees,

Sarah.Rees@ncl.ac.uk http://www.mas.ncl.ac.uk/~nser/teaching/3202

© Sarah Rees, 2010, modified 2011,2012

Contents

Approximate schedule of lectures and coursework

L1	Introduction	(1.1)–(1.6)
L2	Permutations and	(2.1)–(2.6)
L3	permutation groups	(2.7)–(2.12)
L4		(2.13)–(2.16)
L5	Group axioms and examples	(3.1)–(3.4)
L6	Basics of group theory	(4.1)–(4.3)
L7		(4.4)–(4.5)
L8	Cyclic groups. Generating sets	(5),(6.1)
L9	and presentations	(6.2)
L10	Cosets and Lagrange's theorem	(7.1)

L11		(7.2)
L12	Normal subgroups and	(8.1),(8.2)
L13	quotient groups	(8.3),(8.4)
L14	Group actions	(9.1)–(9.3)
L15		(9.4)–(9.9)
L16		(9.10)–(9.11)
L17		(9.12)–(9.13)
L18		(9.14)–(9.15)
L19	Sylow theorems	(10.1)–(10.2)
L20		(10-2)ctd.–(10.3)

This approximate schedule uses 20 of the 22 lectures available; the two remaining lectures will be used as necessary, to spend additional time on some sections, or for review.

In 2012,13 the course meets on Mondays at 1300 in Herschel TR2, Tuesdays at 1100 in Herschel TR2, Wednesdays at 09.00 in Herschel TR3. In general the Monday and Tuesday meetings will be lectures, and the Wednesday meeting will be a problem class in even weeks, and a drop-in tutorial in odd weeks, but the meeting on Wednesday of week 1 will also be a lecture.

There will be no meeting on Wednesday November 7th, and so the meeting on November 6th will be used as a problem class rather than as a lecture.

All meetings in week 12 will be used for revision.

Homeworks will be set in the Monday lecture of weeks 2,4,6,8,10 and will be due by the end of Friday 11 days later (weeks 3,5,7,9,11).

In general my office hours will be on Tuesdays 1230-1400 and Thursdays 1130-130. But there will be no office hour on November 1st (and that week my Tuesday office hour will be extended until 1430). My office hour on October 24th will run 11-12, and my office hour on November 29th will start late and so run approx. 12-1 (I have a meeting before). Students who cannot manage those times may e-mail me for appointments.

Homework	Sections covered	Due date
Homework 1	(1),(2)	End of week 3
Homework 2	(3),(4)	End of week 5
Homework 3	(5)–(7.1)	End of week 7
Homework 4	(7.2)–(9.6)	End of week 9
Homework 5	(9.7)–(10.3)	End of week 11

1 Introduction

1.1 What is group theory?

Group theory is a branch of algebra with applications both within mathematics and in other sciences. Essentially groups are used as algebraic descriptions of symmetry.

Many structures can be best understood through space transformations that leave them unchanged, that is, via their **symmetry groups**.

Other, less symmetrical structures are easily understand via their **fundamental groups**, which allow them to be found as **quotients** of more symmetrical structures.

1.2 The platonic solids

The 5 platonic solids, tetrahedron, cube, octahedron, dodecahedron, and icosahedron. are the only convex polyhedra with identical regular polyhedral faces; see wikipedia for animation. All 5 solids have lots of rotational and reflective symmetry, so large symmetry groups:

$$\mathcal{S}_4, \quad \mathcal{S}_4 \times C_2, \quad \mathcal{S}_4 \times C_2, \quad \mathcal{A}_5 \times C_2, \quad \mathcal{A}_5 \times C_2.$$

Even without understanding the notation we can see that :-

● the groups for the cube and the octahedron match, so do those for the dodecahedron and the icosahedron,

● the group of the tetrahedron ($\mathcal{S}_4$) is related to the group of the cube and octahedron ($\mathcal{S}_4 \times C_2$).

1.3 Dualities between solids whose groups match

Take a cube. Put a vertex in the middle of each face, and join two such vertices if they are in adjacent faces. The resulting 6 vertex polyhedron is an octahedron. Do the same construction with an octahedron and you get a cube. The same construction with a dodecahedron gives an icosahedron, and vice versa. From a tetrahedron you get another tetrahedron.

There's a **duality** between the cube and the octahedron, and between the dodecahedron and the icosahedron; the tetrahedron is **self-dual**.

Two polyhedra related by a duality have to have the same symmetry group.

1.4 Tetrahedra within cube because groups are related

The 8 vertices of a cube can be coloured black and white alternately, so that every edge contains a black and a white vertex. The black vertices can be joined to give one tetrahedron, the white vertices another.

So there are two tetrahedron within a cube. That's why the group of the tetrahedron ($\mathcal{S}_4$) is a **subgroup** of the group of the cube ($\mathcal{S}_4 \times C_2$).

To find two tetrahedra outside an octahedron, colour the 8 faces of the octahedron alternately black and white. Then extend each face to a $4\times$bigger triangle, by adding a triangle outside each edge. The 2 sets of 4 faces form a black and a white tetrahedron.

1.5 The fundamental group of a torus

We can unwrap a torus (ring doughnut) to get a square. First cut the torus along a circle to get a tube. Then cut the tube along its length to get a square. Since 2-D space ($\mathbb{R}^2$) can be tiled with unit squares, we can understand the torus through the set of (translational) symmetries of $\mathbb{R}^2$ of the form $(x, y) \mapsto (x + i, y + j)$ (for $i, j \in \mathbb{Z}$) that preserve those tilings. This is the fundamental group of the torus.

We can unwrap a double torus (pretzel) too; we get an octagon. We can tile the Poincaré disc (hyperbolic plane, $\mathbb{H}^2$) with those. So we can understand the double torus through a group of symmetries of the hyperbolic plane.

1.6 Introducing permutation groups

All the groups we have introduced so far are permutation groups, that is, they are sets of bijections from a set to itself.

The symmetries of the Platonic solids are transformations of 3-D space ($\mathbb{R}^3$) that fix the solids, i.e. they are permutations of the points of $\mathbb{R}^3$.

The fundamental group of the torus consists of the permutations of $\mathbb{R}^2$ of the form $(x, y) \mapsto (x + i, y + j)$.

The fundamental group of the torus is a set of permutations of the points of the Poincaré disc.

Actually a famous theorem of Cayley tells us that every group can be represented as a permutation group; although since any given group can be seen in many different ways, we will also see groups in other disguises. Still, in this course, we will meet a lot of permutation groups. We'll be particularly interested in the symmetric groups $\mathcal{S}_n$, the alternating groups $\mathcal{A}_n$ and the dihedral groups D_{2n} (symmetry groups of regular n-gons), which between them provide us with a rich set of examples. So we'll start the course by looking at permutations, and getting to know these particular groups.

2 Permutations and permutation groups

2.1 The set of permutations, $\mathcal{S}(\Omega)$

Definition 2.1 *A* **permutation** *of Ω is a bijection from Ω to Ω.*

e.g.1: $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x + 1$. But NOT $f : \mathbb{N} \to \mathbb{N}$, with the same rule (it's not onto).

e.g.2: $f : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$ defined by the rule $f(x) = x + 1$ if $x = 1, 2, 3$ or 4, and $f(5) = 1$.

In group theory we usually label permutations with Greek letters like π, ρ, σ, rather than f, g, h. We write ι for the identity permutation.

We shall be interested not just in single permutations of a set Ω, but in the set of all permutations of Ω.

Notation 2.2 *We write $\mathcal{S}(\Omega)$ to denote the set of all permutations of a set Ω. Where $\Omega = \{1, 2, \ldots, n\}$, we may also write $\mathcal{S}_n$.*

Some authors use the notations $\Sigma(\Omega)$ or $Sym(\Omega)$, Σ_n or $Sym(n)$.

In this section we'll learn some techniques to work with $\mathcal{S}(\Omega)$. Usually Ω will be a finite set and usually $\Omega = \{1, 2, 3, \ldots n\}$, for some positive integer n. But much of what we say also makes sense for infinite sets.

2.2 Composing and inverting permutations

Standard results about bijections tell us that, for any set Ω,

- for $\pi, \rho \in \mathcal{S}(\Omega)$, $\rho \circ \pi$ is in $\mathcal{S}(\Omega)$,
- the identity map $\iota : \Omega \to \Omega$ is in $\mathcal{S}(\Omega)$,
- for $\pi \in \mathcal{S}(\Omega)$, π is invertible, with inverse $\pi^{-1} \in \mathcal{S}(\Omega)$.

So the set $\mathcal{S}(\Omega)$ of permutations is more than just a set. Composition and inversion give it extra structure, make it a **group**.

We shall often abbreviate $\rho \circ \pi$ as $\rho\pi$. We shall also write π^n to mean the composite of n copies of π, $\pi \circ \cdots \circ \pi$.

2.3 Two-line matrix notation for permutations

In the two-line matrix notation for a permutation of a finite set Ω, the top row contains the elements of Ω in some order, and the entry in the second row below the element x of Ω is its image $\pi(x)$.

It doesn't matter what order the elements of the top row are given in. So the matrices below both represent the same permutation of $\{1, 2, 3, 4, 5\}$:

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

But it's usual for a permutation of $\Omega = \{1, 2, 3, 4, \ldots n\}$ to write the elements of Ω in the top row in the natural order.

Computing composites and inverses

Using two-line notation it is quite easy to compute composites and inverses.

To compute the composite $\rho \circ \pi$ we reorder the columns of ρ so that the top row of ρ matches the bottom row of π. Then the matrix whose top row matches the top row of π and whose bottom row is the reordered bottom row of ρ represents $\rho \circ \pi$.

A matrix for π^{-1} is found by turning the matrix for π upside down (and then we probably need to reorder the columns).

Example 2.3

Suppose that $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$, $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix}$.

Then $\rho = \begin{pmatrix} 2 & 3 & 4 & 5 & 1 \\ & & & & \end{pmatrix}$, and so $\rho\pi = \begin{pmatrix} \quad & \quad \\ \quad & \quad \end{pmatrix}$,

and $\pi = \begin{pmatrix} 2 & 1 & 4 & 3 & 5 \\ & & & & \end{pmatrix}$, and so $\pi\rho = \begin{pmatrix} \quad & \quad \\ \quad & \quad \end{pmatrix}$,

$$\pi^{-1} = \begin{pmatrix} \quad & \quad \\ \quad & \quad \end{pmatrix} = \begin{pmatrix} \quad & \quad \\ \quad & \quad \end{pmatrix},$$

$$\rho^{-1} = \begin{pmatrix} \quad & \quad \\ \quad & \quad \end{pmatrix} = \begin{pmatrix} \quad & \quad \\ \quad & \quad \end{pmatrix}.$$

2.4 Counting permutations

Using matrix notation it is very easy to count the elements of $\mathcal{S}_n$.

Proposition 2.4 $|\mathcal{S}_n| = n!$

Proof: $|\mathcal{S}_n|$ is the number of matrices with top row $1\,2\,\ldots n$ and with the numbers $1, 2, \ldots, n$ in some order in the bottom row. So it's the number of ways of putting the numbers $1, 2, \ldots, n$ into order, that is, it's $n!$. □

2.5 Order of a permutation

Definition 2.5 *The* **order** *of a permutation $\pi \in \mathcal{S}_n$, written $|\pi|$, is defined to be the smallest integer N for which $\pi^N = \iota$*

Notice that

- if $\pi^m = \iota$ then m is a multiple of $|\pi|$;
- $|\pi|$ divides $n!$ (this follows from Lagrange's theorem, which we'll meet later in the course).

A permutation of an infinite set could have infinite order, i.e there need not exist an integer $N \neq 0$ with $\pi^N = \iota$. The permutation of $\mathbb{Z}$ which maps each x to $x + 1$ has infinite order.

For a permutation described by matrix notation, we can find its order by repeatedly computing powers of it until we reach the identity permutation.

e.g.

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

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

$$\begin{aligned}
\pi^2 &= \begin{pmatrix}1&2&3&4&5\\2&3&4&5&1\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\2&3&4&5&1\end{pmatrix} = \begin{pmatrix}\quad&\quad&\quad&\quad&\quad\\ & & & & \end{pmatrix}\\
\pi^3 &= \begin{pmatrix}\quad&\quad&\quad&\quad&\quad\\ & & & & \end{pmatrix}\begin{pmatrix}1&2&3&4&5\\2&3&4&5&1\end{pmatrix} = \begin{pmatrix}\quad&\quad&\quad&\quad&\quad\\ & & & & \end{pmatrix}\\
\pi^4 &= \begin{pmatrix}\quad&\quad&\quad&\quad&\quad\\ & & & & \end{pmatrix}\begin{pmatrix}\quad&\quad&\quad&\quad&\quad\\ & & & & \end{pmatrix} = \begin{pmatrix}\quad&\quad&\quad&\quad&\quad\\ & & & & \end{pmatrix}\\
\pi^5 &= \begin{pmatrix}\quad&\quad&\quad&\quad&\quad\\ & & & & \end{pmatrix}\begin{pmatrix}\quad&\quad&\quad&\quad&\quad\\ & & & & \end{pmatrix} = \begin{pmatrix}\quad&\quad&\quad&\quad&\quad\\ & & & & \end{pmatrix}
\end{aligned}$$

We’ll see soon that it’s much easier to find the order of a permutation which is described using cycle notation.

2.6 Cycle notation for permutations

Definition 2.6 (cycle) *A permutation π of a set Ω is called a* **cycle** *of length r (or r-cycle) if there are elements $x_1, \ldots x_r$ of Ω such that $\pi(x_1) = x_2$, $\pi(x_2) = x_3$, …, $\pi(x_r) = x_1$, and for all other $x \in \Omega$, $\pi(x) = x$. We write $\pi = (x_1, x_2, \ldots x_r)$.*
A cycle of length 2 is called a **transposition**.

E.g. If $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$, $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix}$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix}$,

then π is a 5-cycle on $\{1, 2, 3, 4, 5\}$, σ is a 3-cycle on $\{2, 3, 5\}$, ρ is not a cycle. We write $()$ or (1) or (2) etc. to represent ι.

Definition 2.7 (disjoint cycles) *Two cycles $\pi = (a_1, \ldots a_r)$ and $\sigma = (b_1, \ldots, b_s)$ are said to be disjoint if no a_i is equal to any b_j.*

e.g. $(1, 2, 3)$ and $(4, 5, 6, 7)$.

Proposition 2.8 *If π and σ are disjoint cycles then $\pi\sigma = \sigma\pi$.*

Proof: Where $\pi = (a_1, \ldots, a_r)$ and $\sigma = (b_1, \ldots, b_s)$,
we can check that $\pi\sigma(a_i) = \sigma\pi(a_i) = a_{i+1}$ (subscripts taken mod r),
that $\pi\sigma(b_j) = \sigma\pi(b_j) = b_{j+1}$ (subscripts taken mod s),
and that for all other x, $\pi\sigma(x) = \sigma\pi(x) = x$.

Hence $\pi\sigma = \sigma\pi$. □

Proposition 2.9 **(i)** *The cycle* $\sigma = (a_1, \ldots, a_r)$ *has order* r*.*

(ii) *A product* $\pi = \pi_1 \cdots \pi_k$ *of disjoint cycles, of lengths* $r_1, \ldots r_k$*, has order* $N = \mathrm{lcm(r_1, \ldots, r_k)}$*.*

(iii) *The inverse of the cycle* $\sigma = (a_1, \ldots, a_r)$ *is the cycle* $\sigma^{-1} = (a_r, \ldots, a_1)$

(iv) *The inverse* π^{-1} *of a product* $\pi = \pi_1 \cdots \pi_k$ *of disjoint cycles, can be written as the product of disjoint cycles* $\pi_1^{-1} \cdots \pi_k^{-1}$ *of disjoint cycles.*

Proof: Part (i) is immediate once we realise that for any m, σ^m maps a_1 to a_{m+1} (taking subscripts mod r).

To see part (ii), we see that since the π_is are disjoint, they commute, and so for any integer m, $\pi^m = \pi_1^m \pi_2^m \ldots \pi_k^m$. Since the powers of the π_i's move disjoint sets of elements of Ω, $\pi^m = \iota$ iff $\pi_i^m = \iota$ for each i, iff r_i divides m for each i (using (i)).

To see part (iii) we calculate the compositions $(a_1, \ldots, a_k)(a_k, \ldots, a_1)$ and $(a_k, \ldots, a_1)(a_1, \ldots, a_k)$.

Then part (iv) follows immediately from part (iii) together with the fact that the disjoint cycles $\pi_1, \ldots, \pi_k$ commute. □

2.7 Products of disjoint cycles

The above results suggest that it is easy to work with permutations that can be written as products of disjoint cycles. And luckily we have the following result.

Proposition 2.10 *Every permutation π of a finite set Ω can be written as a product of finitely many disjoint cycles. The decomposition is unique, apart from the order of the cycles in the product.*

Proof: If π is the identity then it is a product of zero cycles.

Otherwise we choose $x_1 \in \Omega$ with $\pi(x_1) \neq x_1$, and define our first cycle π_1 to be $(x_1, \pi(x_1), \pi^2(x_1), \ldots, \pi^{k_1-1}(x_1))$, where $\pi^{k_1}(x_1) = x_1$.

Assuming we can find x_2 outside the cycle π_1 with $\pi(x_2) \neq x_2$, we then define a second cycle π_2 to be $(x_2, \pi(x_2), \pi^2(x_2), \ldots, \pi^{k_2-1}(x_2))$, where $\pi^{k_2}(x_2) = x_2$, and so on, always choosing x_{r+1} outside the cycles $\pi_1, \ldots, \pi_r$, with $\pi(x_{r+1}) \neq x_{r+1}$ until no such x_{r+1} exists.

At that stage we have disjoint cycles $\pi_1, \ldots, \pi_r$, and for each $x \in \Omega$ either $\pi(x) = x$ or $\pi(x) = \pi_i(x)$ for some i. So $\pi = \pi_1 \cdots \pi_r$.

Now given π as a product of disjoint cycles, any element x can be in at most one cycle. And if x is in the cycle π_i, then that cycle must have the form $(x, \pi(x), \pi^2(x), \ldots, \pi^{k-1}(x))$ for some k. So it must be exactly as described above. Hence the decomposition is unique. $\square$

Example 2.11 *Write π and ρ (defined below) as products of disjoint cycles.*

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 1 & 3 & 5 & 7 & 9 & 11 & 13 & 2 & 4 & 6 & 8 & 10 & 12 & 14 \end{pmatrix},$$
$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 4 & 3 & 6 & 9 & 10 & 8 & 2 & 7 & 1 & 12 & 5 & 11 & 14 & 13 \end{pmatrix}$$

In both examples we compute the first cycle by computing the successive images of 1, the image of 1, the image of the image of 1, etc. until we get back to 1. Then we compute the second cycle by doing the same starting with the smallest number we have not yet seen, etc., etc.

First we compute the cycles of π.

$$1 \mapsto$$

$$2 \mapsto \qquad \mapsto \qquad \mapsto \qquad \mapsto$$

$$14 \mapsto$$

$$\text{So} \quad \pi \; =$$

Now we compute the cycles of ρ.

$$\begin{aligned} 1 &\mapsto \\ 2 &\mapsto \\ 5 &\mapsto \\ 13 &\mapsto \\ \text{So}\quad \rho &= \end{aligned}$$

2.8 Multiplying permutations given in cycle notation

To represent the product of two permutations given in cycle notation as a single product of disjoint cycles, we first concatenate the two products of cycles to get a single composite of cycles, then use the method above to write that composite function as a product of disjoint cycles.

Example 2.12

Let $\pi = (1, 2, 4, 5)$, $\sigma = (2, 4)(6, 7)$. Then $\sigma\pi = (2, 4)(6, 7)(1, 2, 4, 5)$, a product of cycles that are not yet disjoint. Now under $\sigma\pi$, $1 \mapsto 4 \mapsto 5 \mapsto 1$, and $6 \mapsto 7 \mapsto 6$. So $\sigma\pi = (1, 4, 5)(6, 7)$.

And $\pi\sigma =$

2.9 Listing the elements of $\mathcal{S}_n$

We can write down the sets of $n!$ elements of the first few groups $\mathcal{S}_n$, using disjoint cycle notation.

$$\begin{aligned}
\mathcal{S}_1 &= \{()\}\\
\mathcal{S}_2 &= \{(),\ (1,2)\}\\
\mathcal{S}_3 &= \{(),\ (1,2),\ (1,3),\ (2,3),\ (1,2,3),\ (1,3,2)\}\\
\mathcal{S}_4 &= \{(),\ (1,2),\ (1,3),\ (1,4),\ (2,3),\ (2,4),\ (3,4)\\
&\quad (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3),\quad (1,2,3),\ (1,3,2),\\
&\quad (1,2,4),\ (1,4,2), (1,3,4),\ (1,4,3),\ (2,3,4),\ (2,4,3),\\
&\quad (1,2,3,4),\ (1,4,3,2),\ (1,2,4,3),\ (1,3,4,2),\ (1,3,2,4),\ (1,4,2,3),\ \}
\end{aligned}$$

2.10 Products of transpositions; odd and even

It's usually convenient to write a permutation as a product of disjoint cycles, but there are also other meaningful ways to decompose a permutation.

Theorem 2.13 *Every permutation π of a finite set Ω can be written as a product of transpositions.*

Proof: Write π as a product $\pi_1, \ldots \pi_k$ of disjoint cycles. We prove the theorem by showing that each one of those cycles can be written as a product of transpositions. Then π is equal to the product of those products.

To see that any cycle can be written as a product of transpositions, note that

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

□

In particular, notice that

$$(1, n)(1, n-1) \ldots (1, 2) = (1, 2, 3, 4, \ldots n)$$

Notice that if $\pi = \pi_1 \cdots \pi_k$ is written as a product of cycles that are **not** disjoint then the inverse of π must be computed as $\pi_k^{-1} \cdots \pi_1^{-1}$. That product is only equal to $\pi_1^{-1} \cdots \pi_k^{-1}$ when the cycles are disjoint.

A given permutation can be written as a product of transpositions in many different ways, and different products may well involve different numbers of transpositions. For instance, notice that

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

What is remarkable is the following:-

Theorem 2.14 *For any given permutation π, the number of transpositions in any product of transpositions representing π has the same value modulo 2.*

This is non-trivial to prove, and we shall not prove it in this course. But the result allows us to divide permutations into two types, odd and even.

Definition 2.15 *We define a permutation to be* **even** *if it can be written as a product of an even number of transpositions, and* **odd** *if it can be written as a product of an odd number of transpositions. We call the value 'even' or 'odd' the* **parity** *of the permutation.*

Since an r-cycle can be written as a product of $r - 1$ transpositions, we see that cycles of odd length represent even permutations, while cycles of even length represent odd permutations.

It follows from theorem 2.14 that the product of two odd permutations or of two even permutations is always even, and that the product of an odd and an even permutation is always odd.

Where $\pi = \pi_1 \cdots \pi_k$ is written as a product of cycles (disjoint or otherwise), π represents an even permutation if an even number of the cycles have even length, and an odd permutation if an odd number of the cycles have even length.

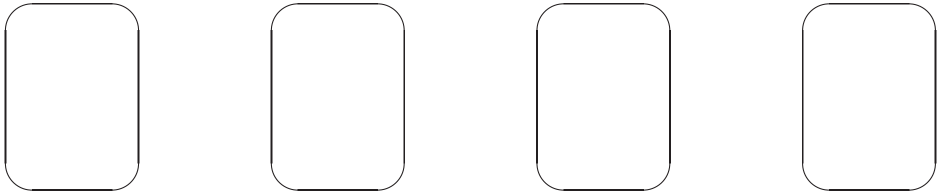
2.11 The alternating groups

We already defined the alternating group $\mathcal{A}_n$ to be the group of all even permutations of $\{1, 2, \ldots, n\}$. Note that we haven't actually defined a group yet, but in essence the group is the set of even permutations, together with the extra structure on that set provided by function composition. Then

$$\begin{aligned}
\mathcal{A}_1 &= \{()\} \\
\mathcal{A}_2 &= \{()\} \\
\mathcal{A}_3 &= \{(),\ (1,2,3),\ (1,3,2)\} \\
\mathcal{A}_4 &= \{(),\ (1,2,3),\ (1,3,2),\ (1,2,4),\ (1,4,2),\ (1,3,4),\ (1,4,3), \\
&\qquad (2,3,4),\ (2,4,3),\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3)\}
\end{aligned}$$

2.12 A useful card trick

The first player deals out 4 playing cards onto a table, left to right.

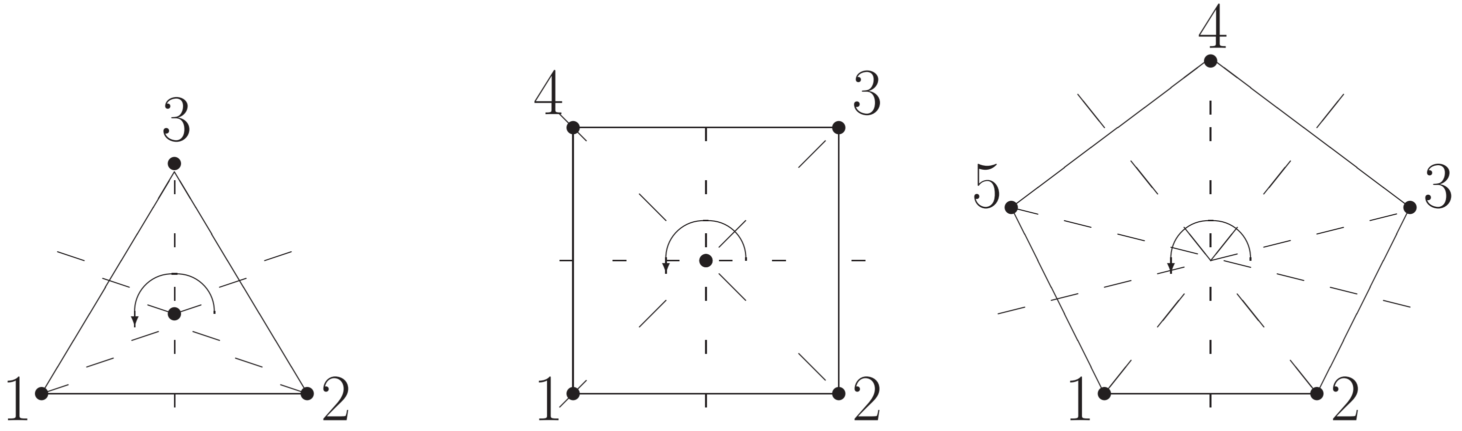


The second player is allowed to swap cards in pairs, for as long as he likes, except that in each move he must always perform two swaps.

The second player wins if he can put the cards into the ascending order defined by $\mathtt{A} < 2 < 3 \cdots < \mathtt{J} < \mathtt{Q} < \mathtt{K}$ within each suit, with all $\heartsuit$s preceding all $\spadesuit$s, then all $\diamondsuit$s, then all $\clubsuit$s. Otherwise he loses.

How must the first player deal to ensure that he always wins?

2.13 The dihedral groups



We can describe the symmetries of a regular n-gon in terms of their effects on the n-vertices of the polygon, that is as permutations of n-points, and so as elements of $\mathcal{S}_n$. In fact the set of symmetries of a regular n-gon forms a group, called the **dihedral group** D_{2n}; it contains $2n$ elements.

$D_6 = \{(), (1,2,3), (1,3,2), (1,2), (1,3), (2,3)\}$ is the group of symmetries of the equilateral triangle with vertices $1,2,3$. It contains two non-trivial rotations, and three reflections. In fact it's the whole of $\mathcal{S}_3$.

$$\begin{aligned} D_8 = \{&(), (1,2,3,4), (1,3)(2,4), (1,4,3,2), \\ &(1,3), (1,2)(3,4), (2,4), (1,4)(2,3)\} \end{aligned}$$

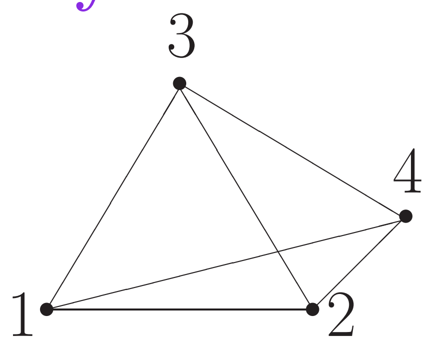
is the group of symmetries of the square with vertices $1,2,3,4$. It contains three non-trivial rotations, and four reflections.

In general, D_{2n} contains $n-1$ non-trivial rotations and n reflections.

2.14 Platonic solids

We can describe the symmetry groups of the 5 platonic solids as groups of permutations of their vertices (or alternatively of their edges, or faces). So we can find the symmetry group of the tetrahedron within $\mathcal{S}_4$, the groups of the cube, octahedron, dodecahedron, icosahedron within $\mathcal{S}_8$, $\mathcal{S}_6$, $\mathcal{S}_{20}$, $\mathcal{S}_{12}$. We'll find other, more compact descriptions of these groups later in the course.

2.15 Symmetries of the tetrahedron



We can write down the permutations in $\mathcal{S}_4$ that represent the symmetries of the tetrahedron as follows.

The tetrahedron is fixed by the identity permutation $()$.

There are 8 rotations through $\pm 2\pi/3$ about axes that join a vertex to the centre of the triangular face opposite it:
$(2,3,4)$ and $(2,4,3)$ about the axis joining 1 to the centre of 234,
$(1,3,4)$ and $(1,4,3)$ about the axis joining 2 to the centre of 134,

$(1,2,4)$ and $(1,4,2)$ about the axis joining 3 to the centre of 124,
$(1,2,3)$ and $(1,3,2)$ about the axis joining 4 to the centre of 123.

There are three rotations through π about axes that join the midpoints of two edges:
$(1,2)(3,4)$ about the axis joining the midpoints of 12 and 34,
$(1,3)(2,4)$ about the axis joining the midpoints of 13 and 24,
$(1,4)(2,3)$ about the axis joining the midpoints of 14 and 23.

We can see that these are the elements of $\mathcal{A}_4$.

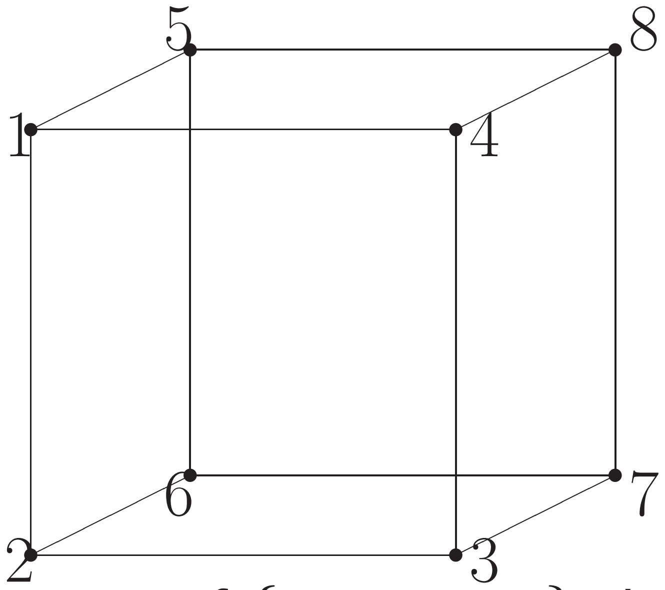
The 12 remaining elements are found as reflections and products of 3 reflections (the product of any two reflections is a rotation).

There are 6 reflections through planes each of which are passes through one edge and bisects two faces:
$(1, 2)$, which reflects in a plane through the edge 34,
and then similarly $(1, 3)$, $(1, 4)$, $(2, 3)$, $(2, 4)$ and $(3, 4)$.

The 6 other elements, each a product of 3 reflections, each permute the 4 elements in a 4-cycle. They are

$$(1, 2, 3, 4),\ (1, 2, 4, 3),\ (1, 3, 2, 4),\ (1, 3, 4, 2),\ (1, 4, 2, 3),\ (1, 4, 3, 2)$$

2.16 Symmetries of the cube



Similarly we can write down the permutations of $\{1, 2, \ldots, 8\}$ that represent the symmetries of the cube, e.g. the reflection in the vertical plan containing the vertices 1,8,7,2 is represented by the permutation $\pi_1 = (3, 6)(4, 5)$, and the reflection in the horizontal plane that bisects each of the lines 12, 34, 56, 78 is represented by the permutation

$$\pi_2 = (1,2)(3,4)(5,6)(7,8).$$

The product

$$\pi_2\pi_1 = (1,2)(3,4)(5,6)(7,8)(3,6)(4,5) = (1,2)(3,5)(4,6)(7,8)$$

represents a rotation through π about an axis that joins the midpoints of 12 and 78.

3 Group axioms and examples

3.1 The axioms

We've met some examples of groups; it's time for a proper definition.

Basically a group is a set G with additional structure. A rule known as a 'binary operation' allows pairs of elements to be multiplied together. 3 group axioms govern the behaviour of this multiplication rule.

By definition, a binary operation $\circ$ on G is a rule that defines a unique element $x \circ y$ of G, given any ordered pair of elements $x, y \in G$, $x \circ y$ needs to be unambiguously defined, and to be an element of G (neither of this properties is necessarily obvious).

Definition 3.1 *A set G, equipped with a binary operation $\circ$, is a group, provided that is satisfies the following three basic axioms.*

associativity *For all elements x, y, z of G,*

$$(x \circ y) \circ z = x \circ (y \circ z).$$

$\exists$ **identity** *G contains an element e, the* **identity element**, *s.t. for all $x \in G$,*

$$x \circ e = e \circ x = x.$$

$\exists$ **inverses** *For each element x of G, there is an element x', the* **inverse** *of x, s.t.*

$$x \circ x' = x' \circ x = e.$$

To verify that a pair $(G, \circ)$ forms a group we simply need to verify

- that $\circ$ is a binary operation,
- that the three axioms hold.

It is in fact a consequence of the axioms that a group can contain only **one** identity element, and that each element has **just one** inverse.

Very often we write just xy rather than $x \circ y$, that is, no symbol is used for the binary operation, just juxtaposition. And we write x^n for $x \circ x \cdots \circ x$ (a product of n copies of x).

3.2 Groups of permutations

So far we have met 3 families of permutation groups as examples: the symmetric groups $\mathcal{S}_n$, the alternating groups $\mathcal{A}_n$ and the dihedral groups D_{2n}.

That these are groups under the operation of function composition (well known to be associative) is clear from the fact that each contains the identity permutation, the inverse of any one of its elements, and the product of any two of them.

It is easy to find other examples of permutation groups.

And it turns out that we can find group structures also on many other sets, e.g. of matrices, of numbers, and of strings.

3.3 Groups of matrices

We can find many examples of groups of square matrices. For any n, a set of $n \times n$ matrices forms a group under matrix multiplication (well known to be associative) provided that it contains the identity matrix I_n, the inverse of any one of its elements, and the product of any two of them.

Examples 3.2

E.g.1 the group of all invertible $n \times n$ matrices over $\mathbb{R}$, called the **general linear group** $\mathsf{GL}_n(\mathbb{R})$. Similarly we define $\mathsf{GL}_n(\mathbb{C})$ over $\mathbb{C}$.

E.g.2 The symmetry group D_8 of the square can be described as the group of 8 matrices:

$$\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad \begin{pmatrix}0&-1\\1&0\end{pmatrix},\quad \begin{pmatrix}-1&0\\0&-1\end{pmatrix},\quad \begin{pmatrix}0&1\\-1&0\end{pmatrix},\right.$$
$$\left.\begin{pmatrix}-1&0\\0&1\end{pmatrix},\quad \begin{pmatrix}1&0\\0&-1\end{pmatrix},\quad \begin{pmatrix}0&1\\1&0\end{pmatrix},\quad \begin{pmatrix}0&-1\\-1&0\end{pmatrix}\right\}$$

E.g.3 The quaternion group Q_8 consists of the 8 matrices:

$$\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad \begin{pmatrix}-1&0\\0&-1\end{pmatrix},\quad \begin{pmatrix}0&i\\i&0\end{pmatrix},\quad \begin{pmatrix}0&-i\\-i&0\end{pmatrix},\right.$$
$$\left.\begin{pmatrix}i&0\\0&-i\end{pmatrix},\quad \begin{pmatrix}-i&0\\0&i\end{pmatrix},\quad \begin{pmatrix}0&1\\-1&0\end{pmatrix},\quad \begin{pmatrix}0&-1\\1&0\end{pmatrix}\right\}$$

3.4 Groups of numbers

We can make plenty of examples of groups using standard addition and multiplication of numbers in familiar sets.

E.g.1 Any one of the sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ (and indeed many other sets of numbers) forms a group under addition.

For it is clear that for each of those sets the sum of any two elements is an element of the set, and addition is associative.

In each group,0 is the identity element, and a has inverse $-a$.

We can write $(\mathbb{Z}, +)$ rather than $\mathbb{Z}$, etc. if we need to distinguish between the groups and the underlying sets.

E.g.2 Each of the sets $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$ and $\mathbb{C} \setminus \{0\}$ forms a group under multiplication. We call the groups $(Q \setminus \{0\}, \times)$, $(\mathbb{R} \setminus \{0\}, \times)$, $(\mathbb{C} \setminus \{0\}, \times)$.

Again it is clear that for each of those sets the product of any two elements is an element of the set, and multiplication on each of those sets is associative.

In each group, 1 is the identity element, and a has inverse $1/a$.

The multiplicative groups have to exclude 0, since $1/0$ is not defined, and we can't make a multiplicative group out of $\mathbb{Z}$, since in general $1/a$ is not an integer, for $a \in \mathbb{Z}$.

E.g.3 The integers in the set $\mathbb{Z}_m = \{0, 1, \cdots, m-1\}$ form a group under addition mod m, in which 0 is the identity and the inverse of a is $m - a$. We call this the additive group of the integers mod m, $(\mathbb{Z}_m, +_m)$ (or C_m, as will be explained later).

For a prime p, the integers in the set $\{1, 2, 3, \cdots, p-1\}$ form a group under multiplication mod p, in which 1 is the identity and the inverse of a is the unique integer b that satisfies $ab = 1 \bmod p$.

For a non-prime m, the equation $ab = 1 \bmod m$ does not have a solution b if a divides m. But in that case, the set of integers a with $1 \leq a \leq m - 1$, and a coprime to m forms a group in the same way.

3.5 Groups of strings

Given any set of symbols $X = \{a, b, c, \cdots\}$, we can define groups of strings over X.

E.g.1 The simplest example of these groups are the **free groups**.

The elements of the free group F_2 on $\{a, b\}$ are all the strings involving the symbols a, a^{-1}, b, b^{-1}, in which a and its inverse a^{-1} are never adjacent, and nor are b and b^{-1}. We call these freely reduced strings.

The product of two freely reduced strings is formed by concatenating them, then cancelling any two inverse symbols that become adjacent.

e.g. the product of $ababab$ and $b^{-1}ab$ is $ababaab$, which we can write as $ababa^2b$.

In this group the empty string (written e) is the identity, a^{-1} is the inverse of a (and vice versa), b^{-1} is the inverse of b (and vice versa), and for any string of symbols $x_1 \cdots x_k$, the string $x_k^{-1} \cdots x_1^{-1}$ is the inverse of $x_1 \cdots x_k$.

We can compute a few products in this group as an exercise:

$$\begin{aligned} aba^{-1} \circ ab^{-1}aba^2 &= \\ ab^2a^{-1}ba \circ a^{-1}b^{-2}ab^{-1}a^{-1} &= \\ ab^2a^{-1}ba \circ a^{-1}b^{-1}ab^{-2}a^{-1} &= \end{aligned}$$

We can define a free group over any set of symbols.

We can modify the definition of a free group to get further groups. Basically we add some rules or equations in the group, that makes several freely reduced strings represent the same element.

E.g.2 We define the **free abelian group** $\mathbb{Z}^2$ on $\{a, b\}$ by adding the rule $ab = ba$ to the definition of the free group. From $ab = ba$ we can deduce the rules

$$b^{-1}a = ab^{-1}, \quad ba^{-1} = a^{-1}b, \quad a^{-1}b^{-1} = b^{-1}a^{-1}.$$

since, for example,

$$ab = ba \Rightarrow b^{-1}(ab)b^{-1} = b^{-1}(ba)b^{-1} \Rightarrow b^{-1}a = ab^{-1}.$$

And using these rules we deduce that any string is equal to one of the form $a^i b^j$, for integers i, j.

In this group the product of two strings of the form $a^i b^j$ is formed by concatenating them and then swapping the order of the terms until the product string has the form $a^i b^j$. e.g.

$$a^3 b^5 \circ a^{-2} b^3 =$$

As before the empty string e is the identity element. The inverse of $a^i b^j$ is $a^{-i} b^{-j}$.

We can define a free abelian group on any set of symbols.

3.6 Abelian groups

Definition 3.3 *A group G with binary operation $\circ$ is called abelian if, for all elements x, y of G,*

$$x \circ y = y \circ x.$$

Examples 3.4

E.g.1 All the groups of numbers we have seen are abelian; for addition and multiplication of numbers is certainly commutative.

E.g.2 The free abelian group over any set is abelian, but the free group is not.

The groups of permutations and matrices we have met so far are not abelian; function composition and matrix multiplication is not in general a commutative operation. However there **are** abelian matrix and permutation groups; we just haven't met any so far.

E.g.3 The set of 4 permutations

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

forms an abelian group under function composition.

E.g.4 The set of matrices

$$\left\{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{Z}\right\}$$

forms an abelian group under matrix multiplication.

4 Basics of group theory

4.1 Order

Definition 4.1 *We define the* **order** *of a group G, usually written $|G|$, to be the number of elements in G. If G has infinitely many elements, we say that G has infinite order.*

The order of an element x, usually written $|x|$ or $o(x)$, is the smallest positive integer n such that $x^n = e$. If there is no such integer, we say that x has infinite order. An element of order 2 is called an **involution**

Of course this matches the definition of order we have already given for permutation groups.

Proposition 4.2 $x^k = e \iff |x|$ *divides* k.

Proof: The proof of $\Leftarrow$ should be obvious, since if $k = qn$ where $n = |x|$, then $x^k = x^{qn} = (x^n)^q = e^q = e$.

To see that $\Rightarrow$ holds, note that the division algorithm for integers tells us that $k = qn + r$ for some integers q, r where $0 \leq r < n$. Hence $x^k = e \Rightarrow x^{qn+r} = e \Rightarrow (x^n)^q x^r = e \Rightarrow e^q x^r = e \Rightarrow x^r = e$. But since $0 \leq r < n$ and n, as the order of x is the smallest positive power to which x can be raised to get e, we must have $r = 0$. So $k = qn$, and the result is proved. □

4.2 Conjugates

Definition 4.3 *For $x \in G$, $g \in G$, we write x^g to mean gxg^{-1} of G and call this the* **conjugate of x by g**, *and we write X^g for the set $\{x^g : x \in X\}$, for any subset X of G.*

(warning: some textbooks write x^g to mean $g^{-1}xg$ instead)

Proposition 4.4 *x^g has the same order as x.*

Proof: Exercise □

4.3 Subgroups and normal subgroups

Definition 4.5 *A subset H of a group G is called a* **subgroup** *of G if H (under the same binary operation) is also a group, that is, if*

- *$e \in H$, where e is the identity of G,*
- *for all $x, y \in H$, $xy \in H$*
- *for all $x \in H$, $x^{-1} \in H$*

We write $H \subset G$ or $H \subseteq G$ (or $H < G$, $H \leq G$). A subgroup H with $H \neq G$, is called a **proper subgroup***; we write $H \subsetneq G$.*

A subgroup N of G is called **normal** *if for all $g \in G$, $N^g \subseteq N$, that is if $n^g \in N, \forall n \in N, g \in G$. We write $N \trianglelefteq G$ or $N \lhd G$.*

Examples 4.6

E.g.1 For any integer n, $\mathcal{A}_n$, D_{2n} are subgroups of $\mathcal{S}_n$. That's because A_n, D_{2n} and $\mathcal{S}_n$ are all groups under function composition, and $\mathcal{A}_n$ and D_{2n} are both subsets of $\mathcal{S}_n$.

$\mathcal{A}_n \lhd \mathcal{S}_n$. This follows from the fact that if ϕ, ρ are two permutations, then $\pi^\rho = \rho\pi\rho^{-1}$ has the same parity as π.

But $D_{2n} \ntriangleleft \mathcal{S}_n$, except when $n = 3$. It's easy to see this when $n = 4$, i.e. that $D_8 \ntriangleleft S_4$. We choose $x = (1,2,3,4) \in D_8$ and $g = (1,2) \in \mathcal{S}_4$. Then $x^g = (1,2)(1,2,3,4)(1,2) = (1,3,4,2) \notin D_8$.

The set of odd permutations in $\mathcal{S}_n$ is not a subgroup of $\mathcal{S}_n$, because it's not a group. The product of two odd permutations is even.

E.g.2 The dihedral group D_8 is a subgroup of group $\mathsf{GL}_2(\mathbb{R})$ of invertible 2×2 matrices, and quaternion group Q_8 a subgroup of the group $\mathsf{GL}_2(\mathbb{C})$. For all are groups under matrix multiplication and clearly D_8 is a subset of $GL_2(\mathbb{R})$, Q_8 is a subset of $GL_2(\mathbb{C})$. Neither subgroup is normal, e.g. where

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ B = \frac{1}{2}\begin{pmatrix} 1 & \sqrt{3} \\ \sqrt{3} & -1 \end{pmatrix},$$

A is within D_8, but BAB^{-1} is not.

E.g.3 For any integer m, $m\mathbb{Z} = \{mx : x \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$. For $m\mathbb{Z} \subseteq \mathbb{Z}$ and both are groups under addition of integers. Then since $\mathbb{Z}$ is an abelian group, for any $x, g \in \mathbb{Z}$, $x^g = x$. So certainly $m\mathbb{Z} \lhd \mathbb{Z}$.

Note that subgroups are always normal in an abelian group.

E.g.4 For any group G, $\{e\}$ (which we may call either the **trivial** or the **identity** subgroup) and G are always normal subgroups.

E.g.5 For any subset X of G, the smallest subgroup of G containing X is the set of all products of powers of elements of X and their inverse. It's called the **subgroup generated by X**, and is written $\langle X \rangle$.

e.g. In $\mathcal{S}_4$,

$$\begin{aligned}
\langle (1,2,3) \rangle &= \{(),\ (1,2,3),\ (1,3,2),\} \\
\langle (1,2),(3,4) \rangle &= \{(),\ (1,2),\ (3,4),\ (1,2)(3,4)\} \\
\langle (1,2),(2,3) \rangle &= \{(),\ (1,2),\ (2,3),\ (1,2,3),\ (1,3,2)\}
\end{aligned}$$

Definition 4.7 *Where G is a group, the centre of G is defined to be*

$$Z(G) = \{g \in G : gx = xg, \forall x \in G\}$$

Proposition 4.8 *$Z(G)$ is a normal subgroup of G.*

Proof: We need to check 4 things.

(a) that $e \in Z$, i.e. that $ex = xe$ for all $x \in G$. This is immediate

(b) that if $g \in Z$ then $g^{-1} \in Z$, This is clear, since

$$gx = xg \iff g^{-1}(gx)g^{-1} = g^{-1}(xg)g^{-1} \iff xg^{-1} = g^{-1}x$$

(c) that if $g_1, g_2 \in Z$ then $g_1g_2 \in Z$. This is clear, since

$$g_1x = xg_1 \quad \text{and} \quad g_2x = xg_2 \Rightarrow g_1g_2x = g_1xg_2 = xg_1g_2$$

(d) that if $g \in Z$ and $y \in G$ then $ygy^{-1} \in Z$. This follows immediately from the fact that $ygy^{-1} = gyy^{-1} = ge = g$.

□

Examples 4.9

For all n, $Z(\mathcal{S}_n) = Z(\mathcal{A}_n) = \{()\}$.

$Z(D_8) = \{(), \ (1,3)(2,4)\}$. In general $|Z(D_{2n})| = 1$ or 2.

The centre of GL$(n, \mathbb{R})$ is the subgroup of so called **scalar** matrices, i.e., the diagonal matrices with all diagonal entries equal.

Any free group has trivial centre.

For any abelian group G we have $Z(G) = G$.

4.4 Homomorphisms and isomorphisms

Definition 4.10 *Given groups G, H, with binary operations $\circ, *$, a map ϕ from G to H is called a* **homomorphism** *if,*

$$\forall x, y \in G,\ \phi(x \circ y) = \phi(x) * \phi(y). \quad (*)$$

The set $\phi(G) = \{\phi(g) : g \in G\}$ is called the **homomorphic image** *of G under ϕ.*

A homomorphism which is bijective is called an **isomorphism**. *When there is an isomorphism from G to H, G and H are said to be* **isomorphic**, *and we write $G \cong H$.*

We call the defining rule (*) for a homomorphism the **product rule**.

NB.1 Where juxtaposition is used to denote both binary operations (as is usual), the product rule for a homomorphism simply reads

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

NB.2 It follows from the fact that every bijection has an inverse that whenever G is isomorphic to H then H is isomorphic to G.

It is elementary to show that,

(a) Where e_G, e_H are the identities of G, H, $\phi(e_G) = e_H$,

(b) for all $x \in G$, $\phi(x^{-1}) = \phi(x)^{-1}$.

Examples 4.11

E.g.1 The determinant map on $\mathrm{GL}_n(\mathbb{R})$, that maps every matrix to its determinant, is a homomorphism from $\mathrm{GL}_n(\mathbb{R})$ to $(\mathbb{R} \setminus \{0\}, \times)$. It is well known that the determinant map satisfies the product rule

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

E.g.2

$$\text{Where } G_1 = \left\{ \begin{pmatrix} b & a \\ 0 & b \end{pmatrix} : a, b \in \mathbb{R}, b \neq 0 \right\}, G_2 = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a, b \in \mathbb{R} \right\},$$

the map $\phi : G_1 \to (\mathbb{R}, +)$ defined by

$$\phi\left(\begin{pmatrix} b & a \\ 0 & b \end{pmatrix}\right) = a/b$$

is a homomorphism, and its restriction to G_2 is an isomorphism.

To verify that ϕ is a homomorphism, we need to verify the product rule.

$$\phi\left(\begin{pmatrix} b & a \\ 0 & b \end{pmatrix}\begin{pmatrix} d & c \\ 0 & d \end{pmatrix}\right) =$$

$$\phi\left(\begin{pmatrix} b & a \\ 0 & b \end{pmatrix}\right) + \phi\left(\begin{pmatrix} d & c \\ 0 & d \end{pmatrix}\right) =$$

It's elementary to see from the definition of $\phi|_{G_2}$ that it is both surjective and injective, and hence an isomorphism.

4.5 The kernel and image of a homorphism

Definition 4.12 *Where $\phi : G \to H$ is a homomorphism between groups, we define the* **kernel** *of ϕ,* ker(ϕ), *to be the set of elements of G mapped by ϕ to the identity, that is,* ker$(\phi) = \{g \in G : \phi(g) = e_H\}$

Examining the kernel of a homomorphism helps us to identify isomorphisms.

Proposition 4.13 *A homomorphism $\phi : G \to H$ is injective $\iff$* ker$(\phi) = \{e\}$

Proof: $\phi(x) = \phi(y) \iff \phi(xy^{-1}) = \phi(e) \iff xy^{-1} \in$ ker(ϕ).
□

Examples **4.14**

We look at the examples from 4.11.

E.g.1 The kernel of the determinant map

$$\det : \mathsf{GL}_n(\mathbb{R}) \to (\mathbb{R} \setminus \{0\}, \times)$$

is the subgroup $\mathsf{SL}_n(\mathbb{R})$ of matrices of determinant 1, known as the **special linear group**.

E.g.2 ker(ϕ) is the subgroup of scalar matrices,
while ker$(\phi|_{G_2}) = \{I_2\}$, verifying our claim that $\phi|_{G_2}$ is injective.

Proposition 4.15 *For any homomorphism ϕ from a group G to a group H,*

(a) ker(ϕ) *is a normal subgroup of G,*

(b) $\phi(G)$ *is a subgroup of H.*

Proof:

(a) Since $\phi(e_G) = e_H$, by definition $e_G \in \text{ker}(\phi)$

$$\begin{aligned} \text{Since} \quad \phi(x^{-1}) &= \phi(x)^{-1}, \\ x \in \text{ker}(\phi) &\Rightarrow \phi(x) = e_H \Rightarrow \phi(x^{-1}) = e_H \Rightarrow x^{-1} \in \text{ker}(\phi). \\ \text{And} \quad x, y \in \text{ker}(\phi) &\Rightarrow \phi(x) = \phi(y) = e_H \\ &\Rightarrow \phi(xy) = \phi(x)\phi(y) = e_H \Rightarrow xy \in \text{ker}(\phi). \end{aligned}$$

For $x \in \text{ker}(\phi)$ and $g \in G$,

$\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g)^{-1} = \phi(g)e_H\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = e_H$

So $gxg^{-1} \in \text{ker}(\phi)$.

(b) $e_H = \phi(e_G)$ is certainly in $\phi(G)$.

For $x \in \phi(G)$, we see that $x = \phi(g)$ for some $g \in G$, and then $x^{-1} = \phi(g^{-1}) \in \phi(G)$.

For $x, y \in \phi(G)$. we see that $x = \phi(g_1)$, and $y = \phi(g_2)$, for some $g_1, g_2 \in G$. And then $xy = \phi(g_1g_2) \in \phi(G)$.

□

5 Cyclic groups

Most groups have a lot of cyclic subgroups.

Definition 5.1 *Let G be a group with identity element e, and let x be an element of G. Then the (cyclic) group $\langle x \rangle$ generated by x is the set $\{x^n : n \in \mathbb{Z}\}$ of all positive and negative powers of x.*

Definition 5.2 *A group G is cyclic if $G = \langle x \rangle$ for some x.*

Examples 5.3

E.g.1 The permutation group $\{(), (1,2,3,4), (1,3)(2,4), (1,4,3,2)\}$ is a cyclic subgroup of $\mathcal{S}_4$, generated by $(1,2,3,4)$ or by $(1,4,3,2)$.

E.g.2 The additive group of the integers $(\mathbb{Z}, +)$ is cyclic, generated by 1, also by its inverse -1.
E.g,3 The additive group of the integers mod m is cyclic, generated by 1, also by its inverse, $m - 1$.

In fact there aren't very many different cyclic groups.

Proposition 5.4 *Let G be a cyclic group $\langle x \rangle$. If $|x|$ is infinite then G is isomorphic to $(\mathbb{Z}, +)$. Otherwise, where $|x| = m$, G is isomorphic to the additive group of the integers modulo m, and so has order m.*

From now on we'll call the unique cyclic group of order m C_m, and the infinite cyclic group C_∞ or $\mathbb{Z}$.

Proof: If x has infinite order. we define $\phi : \mathbb{Z} \to \langle x \rangle$ by $\phi(k) = x^k$, which is clearly well defined and surjective. To see that ϕ is injective, observe that

$$\begin{aligned} \phi(r) = \phi(s) &\Rightarrow \\ &\Rightarrow \\ &\Rightarrow \\ \text{Then since} \quad \phi(r+s) &= \\ &= \end{aligned}$$

ϕ is an isomorphism.

If x has finite order m, we define $\phi : \mathbb{Z}_m \to \langle x \rangle$ by $\phi(a) = x^a$. This is clearly well defined and surjective. That ϕ is an injection follows from

$$\begin{aligned} \phi(a) = \phi(b) &\Rightarrow \\ &\Rightarrow \\ &\Rightarrow \end{aligned}$$

Finally we need to verify that ϕ satisfies the multiplication rule. This follows from the observation that for $a, b \in \mathbb{Z}_m$, $a +_m b = a + b - \epsilon m$ (for $\epsilon = 0$ or 1). Hence

$$\begin{aligned} \phi(a +_m b) &= \\ &= \end{aligned}$$

and so ϕ is an isomorphism. □

6 Generating sets and presentations

6.1 Generating sets

Definition **6.1** *Where G is a group, and X is a subset of G, the subgroup $\langle X\rangle$* **generated** *by X is the set of all products of elements of X and their inverses.*

If $G = \langle X\rangle$, then we say that X is a **generating set** *for G. If $G = \langle X\rangle$ for some finite set X, we say that G is* **finitely generated**.

Examples 6.2

E.g.1 Every cyclic group is finitely generated, by 1 element.

E,g,2 None of $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ is finitely generated. Nor is $(\mathbb{Q}\setminus\{0\},\times)$, $(\mathbb{R}\setminus\{0\},\times)$, $(\mathbb{C}\setminus\{0\},\times)$.

E.g.3 Any finite group is finitely generated - the set of all elements is a generating set.

E.g.4 The symmetry group of the square with vertices at $(\pm 1, \pm 1)$ is finitely generated by the set of 2 elements consisting of

- rotation anticlockwise through $\pi/2$ (call this element α)
- reflection in the x-axis (call this element β).

It's not hard to see that the elements of the group are all found in the set

$$\{e, \alpha, \alpha^2, \alpha^3, \beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta\}$$

E.g.5 The group of all rotations about the origin in 2-dimensions is not finitely generated.

E.g.6 The symmetric group $\mathcal{S}_n$ is generated by any one of the following sets:

$$\begin{array}{l}
\{(1,2),(1,3),(1,4),\ \ldots,(1,n)\} \\
\{(1,2),(2,3),(3,4),\ \ldots,(n-1,n)\} \\
\{(1,2),\ (1,2,\ldots,n)\} \\
\{(1,n),\ (1,2,\ldots,n)\}
\end{array}$$

So in particular $\mathcal{S}_3$ is generated by $\{1,2),\ (1,3)\}$ or by $\{(1,2),\ (1,2,3)\}$, and $\mathcal{S}_4$ is generated by $\{(1,2),\ (2,3),\ (3,4)\}$ or by $\{(1,4),\ (1,2,3,4)\}$.

6.2 Presentations

When we try and write down the elements of a finitely generated group, in general we see that some elements can be written in more than one way as a product of the generators and their inverses.

For instance, in the symmetry group of the square, given as an example above, it's obvious that $\alpha\alpha^{-1} = \alpha^{-1}\alpha = e$, $\beta\beta^{-1} = \beta^{-1}\beta = e$, so certainly $\alpha = \alpha\alpha^{-1}\alpha = \alpha\beta\beta^{-1} \ldots$.

Also it's rather easy to see that $\alpha^4 = e, \beta^2 = e$, so $\alpha = \alpha^5 = \alpha\beta^2 \ldots$.

And it's not hard to show that $\alpha^3\beta = \beta\alpha$, $\alpha\beta = \beta\alpha^3$, $\alpha^2\beta = \beta\alpha^2$.

Exercise 6.3 *Suppose that $\{a, b\}$ generates a group G, in which the equations $a^4 = e$, $b^2 = e$, and $a^3b = ba$ hold. Then every element of G is equal to an element of the set $\{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$.*

Solution: Since G is generated by $\{a, b\}$, every element of G can be written as a product of integer powers of a and b.
Since $a^4 = e$, and $b^2 = e$, we have $a^{-1} = a^3$, $b^{-1} = b$, and so every element of G is equal to a product of non-negative powers of a and b.
Since $ba = ab^3$ any product of non-negative powers of a and b is equal to a product of the form a^ib^j, with $i \geq 0, j \geq 0$.
Since $a^4 = e$ and $b^2 = e$, any product of the form a^ib^j with $i \geq 0$, $j \geq 0$ is equal to such a product with $0 \leq i \leq 3$ and $j = 1$ or 0. □

Of course the symmetry group of the square is an example of a group G as above, for which $a = \alpha, b = \beta$. But it is not the only example.

For set $a = \alpha^2$, $b = \beta$. Then $a^4 = \alpha^8 = e$, $b^2 = \beta^2 = e$, and $a^3b = \alpha^6\beta = \alpha^2\beta = \beta\alpha^2 = ba$.

But $\langle\alpha^2, \beta\rangle$ is a subgroup of just 4 elements of D_8.

In fact the symmetry group of the square is the biggest example satisfying the given conditions. In all other examples, there are fewer than 8 elements, and there are equations holding between products of elements that are not deducible from the given 3.

We say that the equations $a^4 = e, b^2 = e, a^3b = ba$ define the symmetry group of the square.

Definition 6.4 *Where X is a finite set, and R be a finite set of equations relating pairs of products of powers of elements of X, there is a group G with generating set X in which the only equations which hold between products of powers of elements of X are deducible from the equations in R. We write*

$$G = \langle X \mid R \rangle,$$

and say that the pair (X, R) is a **finite presentation** *for G.*

A group which is defined in this way is called **finitely presented***. The set R is called its set of* **defining relations***. Its elements are called* **relations***, and if $w = e$ is a relation in R, then w is called a* **relator***.*

NB. I haven't actually proved that every pair (X, R) really does define a group. The proof is too hard for this course.

Examples 6.5

E.g.1 The symmetry group of the square is isomorphic to the finitely presented group

$$\langle a, b \mid a^4 = e, b^2 = e, a^3 b = ba \rangle .$$

E.g.2 The cyclic group C_m is isomorphic to the finitely presented group

$$\langle a \mid a^m = e \rangle$$

The infinite cyclic group $\mathbb{Z}$ has presentation $\langle a \mid \rangle$.

E.g.3 The free group F_2 on $\{a, b\}$ has presentation $\langle a, b \mid \rangle$ and the free abelian group $\mathbb{Z}^2$ on $\{a, b\}$ has presentation $\langle a, b \mid ab = ba\rangle$.

E.g.4 $\mathcal{S}_3$ has presentation

$$\langle a, b \mid a^3 = b^2 = e, ba = a^2b\rangle,$$

on generators $a = (1, 2, 3)$, $b = (1, 2)$. Alternatively, it has presentation

$$\langle x, y \mid x^2 = y^2 = (xy)^3 = e\rangle,$$

on generators $x = (1, 2)$, $y = (2, 3)$.

$\mathcal{S}_4$ has presentation

$$\langle x, y, z \mid x^2 = y^2 = z^2 = (xy)^3 = (yz)^3 = (xz)^2 = e\rangle,$$

on generators $x = (1, 2)$, $y = (2, 3)$, $z = (3, 4)$.

$\mathcal{S}_4$ also has presentation

$$\langle p, q, r \mid p^4 = q^3 = r^2 = pqr = e \rangle$$

on generators $p = (1, 2, 3, 4)$, $q = (3, 2, 1)$, $r = (1, 4)$.

7 Cosets and Lagrange's theorem

7.1 Cosets. The proof

The aim of this section is to prove the following theorem.

Theorem **7.1 (Lagrange's theorem)** *If G is a finite group and H is a subgroup of G, then the order of H divides the order of G.*

The theorem will be proved by showing that G can be cut up into disjoint pieces each of size $|H|$, called **cosets**. If there are k of these, then

$$|G| = k|H|.$$

Definition 7.2 *If G, H are groups, with $H \subseteq G$, and $g \in G$, the* **left coset** *gH and* **right coset** *Hg are defined to be the sets*

$$\begin{aligned} gH &= \{gh : h \in H\} \\ Hg &= \{hg : h \in H\} \end{aligned}$$

We write G/H for the set of left cosets of H in G, and $H \backslash G$ for the set of right cosets of H in G.

Examples 7.3

E.g.1 Where $\mathcal{S}_4 = G \supseteq H$ (isomorphic to D_8) given by

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

then $H(1,2,3,4) =$

$$1,2,3,4)H =$$

$$H(1,2) =$$

$$(1,2)H =$$

$$H(1,2,4) =$$

$$(1,2,4)H =$$

E.g.2 Let $G = \mathsf{GL}_n(\mathbb{R})$ the group of all $n \times n$ matrices with non-zero determinant, and $H = \mathsf{SL}_n(\mathbb{R})$, the subgroup of all $n \times n$ matrices of determinant 1.

Then for any $g \in \mathsf{GL}_n(\mathbb{R})$, gH is the set of all $n \times n$ matrices with the same determinant as g. And so is Hg.

In the examples, we can observe the following facts about cosets, which are straightforward to prove.

Proposition 7.4 *Let G be a group, and H a subgroup of G. Then, for all $g, g' \in G$, $h \in H$,*

(a) $g' \in gH \iff g^{-1}g' \in H$.

(b) $g \in gH$.

(c) *If $h \in H$, then $hH = H$.*

(d) *If $g' \in gH$, then $gH = g'H$.*

(e) *If $gH \cap g'H \neq \emptyset$, then $gH = g'H$.*

(f) *If $|H|$ is finite, then $|H| = |gH|$.*

Proof: (a),(b),(c),(d) follow immediately from the definition of gH.

(e) follows from (d). For if $g'' \in gH \cap g'H$, then by (d), $gH = g''H$ and $g''H = g'H$.

To prove (f) we observe that the rule $h \mapsto gh$ defines a bijection from H to gH.

□ A parallel result is true for right cosets.

Proof: (of Lagrange's theorem).

Since $g \in gH$, G is a union of the left cosets of H. And since two cosets that intersect must be equal, this union is a disjoint union.

Since every coset has $|H|$ elements, $|G| = k|H|$, where k is the number of distinct left cosets of H in G. $\square$

NB This proof would work just as well with right cosets. Hence it is clear that for $|G| < \infty$, the numbers of left and right cosets are both equal to $|G|/|H|$. Even when G is infinite, the map $gH \mapsto Hg^{-1}$ provides a bijection from G/H to $H\backslash G$, providing further proof that the two sets must have the same size. They might be finite even when G and H are infinite.

Definition 7.5 *For G, H groups and $H \subseteq G$, we call the number of distinct left cosets of H in G the* **index** *of H in G, and denote it by the symbol $|G : H|$.*

Examples 7.6

E.g.1 $|\mathcal{S}_4 : D_8| = 3.$

E.g.2 $|\mathsf{GL}_n(\mathbb{R}) : \mathsf{SL}_n(\mathbb{R})|$ is infinite. For every real number is the determinant of some matrix in $GL_n(\mathbb{R})$.

Corollary 7.7 *If G is a finite group and $x \in G$, then $|x|$ divides $|G|$.*

Proof: $\langle x \rangle$ is a cyclic subgroup of G or order $|x|$. The result now follows from Lagrange's theorem. □

7.2 The converse of Lagrange's theorem

The converses of Lagrange's theorem and its corollary are not in general true. They hold in finite cyclic and abelian groups. But in general, where G is a finite group, with m dividing $|G|$, G need not have a subgroup of order m, and even if it does, it need not have an element of order m.

Examples 7.8

E.g.1

$$\begin{aligned}\mathcal{A}_4 = \{&(), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3), (1,2,3),\\ &(1,3,2), (1,2,4), (1,4,2), (1,3,4), (1,4,3), (2,3,4), (2,4,3)\}\end{aligned}$$

has no subgroup of order 6.

For suppose that H is a subgroup of order 6. Certainly $() \in H$. Since H contains 6 elements, and the group $\mathcal{A}_4$ contains only 3 elements of order 2, H must contain an element of order 3. WLOG, we may assume that $(1,2,3) \in H$. Then $(1,3,2) = (1,2,3)^2 \in H$.

Suppose that H contains another element y of order 3. Then it also contains its inverse, and by the symmetry of the set $\mathcal{A}_4$, we can assume that those two elements are $(1,2,4)$ and $(1,4,2)$. But then H must contain both $(1,2,3)(1,4,2) = (1,4,3)$ and its inverse $(1,3,4)$, and hence $|H| \geq 7 > 6$,

So H cannot contain a third element of order 3, and so must contain all 3 elements of order 2. In particular $(1,2)(3,4) \in H$, and so $(1,3,4) = (1,2,3)(1,2)(3,4) \in H$; we have a contradiction.

E.g.2 $\mathcal{S}_4$ has a subgroup ($\mathcal{S}_3$) of order 6, but no element of order 6.

An element π of order 6 in $\mathcal{S}_4$ could not involve only 2-cycles or only 3-cycles, but would have to involve either 6-cycles (possibly with other cycles) or a mixture of 2-cycles and 3-cycles.

In that case the disjoint cycles of π would have to involve at least 5 elements of $\{1, 2, 3, 4\}$.

8 Normal subgroups and quotient groups

8.1 Recognising normal subgroups

The following gives new ways to recognise normal subgroups.

Note that (3) is the definition for a normal subgroup from 4.5.

Proposition 8.1 *Given groups $G \supseteq H$, the following are equivalent.*

(1) $\forall g \in G,\ Hg = gH.$

(2) *Every left coset of H in G is a right coset of H in G.*

(3) $\forall g \in G,\ H^g \subseteq H.$

(4) $\forall g \in G,\ H^g = H.$

Proof: (1) $\Rightarrow$ (2) and $4 \Rightarrow 3$ are immediate. To complete the proof we verify (2)$\Rightarrow$ (1) (1)$\Rightarrow$(4) and (3)$\Rightarrow$ (1), in that order.

Suppose that gH is a right coset Hg'. Since gH intersects Hg (in a set containing g), and distinct right cosets are disjoint, we must have $Hg = Hg' = gH$. Hence (2) $\Rightarrow$ (1).

We can deduce $H^g = H$ from $gH = Hg$ by multiplying that equation on the right by g^{-1}: $H^g = gHg^{-1} =$

So (1) $\Rightarrow$ (4).

We can deduce $gH \subseteq Hg$ from $gHg^{-1} \subseteq H$, by multiplying on the right by g, and similarly $Hg \subseteq gH$ from $g^{-1}Hg \subseteq H$. So (3) $\Rightarrow$ (1), □

We'll check normality in some examples.

Examples 8.2

E.g.1 $H = \{(), (1,2,3), (1,3,2)\}$ is a normal subgroup of $\mathcal{S}_3$. For since $|\mathcal{S}_3|/|H| = 2$, there are 2 right cosets, 2 left cosets, H and one other. In each case the second coset must be the complement $\mathcal{S}_3 \setminus H$. Hence this is both a left and a right coset, (1) holds, and H is normal.

E.g.2

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

is not normal in $\mathcal{S}_4$. We computed the right and left cosets in Examples 7.3, and can see that they don't match up.

E.g.3 $\mathsf{SL}_n(\mathbb{R}) \lhd \mathsf{GL}_n(\mathbb{R})$. We already observed that two matrices in $\mathsf{GL}_n(\mathbb{R})$ are in the same (right or left) coset of $\mathsf{SL}_n(\mathbb{R})$ if they have the same determinant. So certainly the right and left cosets match up.

E.g.4 $V = \{(), \ (1,2)(3,4), \ (1,3)(2,4), \ (1,4)(2,3)\}$ is normal in $\mathcal{S}_4$. We could compute and compare the 6 right and 6 left cosets. But we can check this much more quickly, once we realise that the conjugate of a k-cycle $(i_1, \cdots, i_k)$ by a permutation π is $(\pi(i_1), \cdots, \pi(i_k))$, hence a k-cycle. Hence any conjugate of any one of the elements of the set

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

is also in that set.

The first example points to a more general result,

Corollary 8.3 (of Proposition 8.1) *If G, H are groups with H a subgroup of index 2 in G, then $H \lhd G$.*

Proof: just in the first example of 8.2 □

Example 8.4

$\mathcal{A}_n$ is normal in $\mathcal{S}_n$.

8.2 Constructing quotient groups

The special properties that normal subgroups have allow us to factor them out and build quotient groups.

Theorem 8.5 *For groups G, N with $N \lhd G$, the rule*

$$xN \bullet yN = xyN$$

defines a binary operation on G/N that makes it a group.

Proof: We check first that we have a binary operation.

$xN = uN,\ yN = vN \Rightarrow \exists m, n \in N,\ \ u = xm,\ v = yn.$

So $uv = xmyn = xyy^{-1}myn = xym^{y^{-1}}n \in xyN;$ and $uvN = xyN$.

Next we have to verify that the three group operations hold.

We inherit associativity of $\bullet$ from G, for

$$\begin{aligned}(xN \bullet yN) \bullet zN &= (xyN) \bullet zN = (xy)zN = x(yz)N \\ &= xN \bullet yzN = xN \bullet (yN \bullet zN).\end{aligned}$$

We see that $N = eN$ is an identity, since

$$eN \bullet xN = exN = xN = xeN = xN \bullet eN.$$

And we see that $x^{-1}N$ is an inverse for xN, since

$$xN \bullet x^{-1}N = xx^{-1}N = eN = x^{-1}xN = x^{-1}NxN.$$

$\square$

Examples 8.6

E.g.1

$$G = \{(), (1,2,3,4), (1,4,3,2), (1,3)(2,4), (1,4)(2,3), (1,2)(3,4), \\ (1,3), (2,4)\}, \qquad N = \{(), (1,3)(2,4)\}$$

We met this pair of groups as an example in 4.9, where we observed that N is the centre of G; so it is certainly normal in G.

Now the left cosets of N in G are

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

Clearly G/N is a group of order 4. We observe the following.

$$\begin{aligned}
A^2 &= (1,3)N(1,3)N = (1,3)^2N = ()N = N \\
B^2 &= (1,2,3,4)N(1,2,3,4)N = (1,2,3,4)^2N = (1,3)(2,4)N = N \\
C^2 &= (1,2)(3,4)N(1,2)(3,4)N = ((1,2)(3,4))^2N = ()N = N \\
AB &= (1,3)N(1,2,3,4)N = (1,2)(3,4)N = C \\
BA &= (1,2,3,4)N(1,3)N = (1,4)(2,3)N = C = AB
\end{aligned}$$

So

$$G/N = \{N, A, B, AB\}$$

where N is the identity, $AB = BA$, and $A^2 = B^2 = (AB)^2 = N$.

In fact G/N is isomorphic to the subgroup

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

of G. For define ϕ by

$\phi(N) = ()$, $\phi(A) = (1,2)(3,4)$, $\phi(B) = (1,3)(2,4)$, $\phi(AB) = (1,4)(2,3)$

ϕ is clearly a bijection between the two groups. To verify that it's an isomorphism we simply have to check that

$$\phi(A^2) = \phi(A)^2,\ \phi(B^2) = \phi(B)^2,$$
$$\phi(AB) = \phi(A)\phi(B),\ \phi(BA) = \phi(B)\phi(A)$$

These are easy to check.

E.g.2 The quotient of $(\mathbb{Z}, +)$ by the normal subgroup $m\mathbb{Z}$ (defined as $m\mathbb{Z} = \{mx : x \in \mathbb{Z}\}$) is isomorphic to the additive group of the integers mod m. And in fact the quotient construction gives a rather more natural definition of that group than the one we gave in Subsection 3.4.

Of course the elements of the quotient are sets of integers, the cosets $a + m\mathbb{Z}$, and the binary operation is defined by the rule

$$(a + m\mathbb{Z}) + (b + m\mathbb{Z}) = (a + b) + m\mathbb{Z}.$$

It is standard to call $a + m\mathbb{Z}$ the **congruence class** of a mod m, and write it as $(a)_m$.

8.3 The first isomorphism theorem

In fact we get a normal subgroup and a quotient group whenever we have a homomorphism $\phi : G \to H$.

We recall from Proposition 4.15 that in this situation $\ker(\phi)$ is a normal subgroup of G, and $\phi(G)$ is a subgroup of H. In fact, we have more than this.

Theorem 8.7 (First isomorphism theorem) *Given groups G, H and a homomorphism $\phi : G \to H$, we have*

$$G/\ker(\phi) \cong \phi(G).$$

Proof: Let $N = \mathrm{ker}(\phi)$, for notational convenience.

$$\begin{aligned} \text{Now for} \quad & x, y \in G, xN = yN \Rightarrow y^{-1}x \in N = \mathrm{ker}(\phi), \\ \text{and so} \quad & \phi(x) = \phi(y(y^{-1}x)) = \phi(y)\phi(y^{-1}x) = \phi(y). \end{aligned}$$

So we can define a map $\theta : G/N \to \phi(G)$ by $\theta(xN) = \phi(x)$.

It's clear from the definition that θ is surjective. And θ is injective, since

$$\begin{aligned} \theta(xN) = \theta(yN) & \Rightarrow \phi(x) = \phi(y) \Rightarrow \phi(y^{-1}x) = e_H \\ & \Rightarrow y^{-1}x \in ker(\phi) = N \Rightarrow xN = yN. \end{aligned}$$

We see that θ is a homomorphism by verifying the product rule, making use of the fact that ϕ is a homomorphism:

$$\theta(xN \bullet yN) = \theta(xyN) = \phi(xy) = \phi(x)\phi(y) = \theta(xN)\theta(yN).$$

Therefore θ is an isomorphism from G/N to $\phi(G)$. $\square$

Example 8.8

Let ϕ be the determinant map from $G = \mathsf{GL}_n(\mathbb{R})$ to $(\mathbb{R} \setminus \{0\}, \times)$. Then $\phi(G)$ is the whole of $(\mathbb{R} \setminus \{0\})$. And $\ker(\phi)$ is $\mathsf{SL}_n(\mathbb{R})$. So we see that $\mathsf{GL}_n(\mathbb{R})/\mathsf{SL}_n(\mathbb{R}) \cong (\mathbb{R} \setminus \{0\}, \times)$.

8.4 Lifting subgroups from a quotient

The quotient of G by a normal subgroup N is in some sense just the top part of G. Everything in the quotient group is also to be found in G. Hence the following result (which we won't prove) should not be surprising.

Proposition 8.9 *Where G is a group and N a normal subgroup of G, then the set of subgroups of G/N can be described as*

$$\{H/N : H \leq G, N \leq H\}$$

Further, where H is a subgroup of G containing N, H is a normal subgroup of G if and only if H/N is a normal subgroup of G/N.

This result can sometimes help us to find subgroups of a group, using information about subgroups of a factor group.

Example **8.10 (Subgroups of $\mathcal{S}_4$)**

Elements of order $2, 3$ and 4 generate cyclic subgroups, as follows:-

- 6 subgroups such as $\langle(1,2)\rangle = \{(),\ (1,2)\}$,
- 3 subgroups such as $\langle(1,2)(3,4)\rangle = \{(), (1,2)(3,4)\}$
- 4 cyclic subgroups such as $\langle(1,2,3)\rangle = \{(),\ (1,2,3),\ (1,3,2)\}$,
- 3 cyclic subgroups such as

$$\langle(1,2,3,4)\rangle = \{(),\ (1,2,3,4),\ (1,3)(2,4),\ (1,4,3,2)\}.$$

Pairs of involutions generate three kinds of subgroups.

Any 2 disjoint 2-cycles generate an abelian subgroup of order 4, e.g.

$$\langle (1,2),\, (3,4) \rangle = \{(),\, (1,2),\, (3,4),\, (1,2)(3,4)\}.$$

Any 2 intersecting 2-cycles generate a subgroup isomorphic to $\mathcal{S}_3$, e.g.

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

Any 2 products of two disjoint 2-cycles generate the Klein 4-group

$$\begin{aligned} V &= \langle (1,2)(3,4),\, (1,3)(2,4) \rangle \\ &= \{(),\, (1,2)(3,4),\, (1,3)(2,4),\, (1,4)(2,3),\},\end{aligned}$$

which is normal.

The subgroups containing V, can be found by considering the quotient $\mathcal{S}_4/V$, which is isomorphic to $\mathcal{S}_3$.

Since $\mathcal{S}_3$ has 3 subgroups of order 2 and one of order 3, $\mathcal{S}_4$ must have 3 subgroups of order 8 that contain V and one of order 12 that contains V. These turn out to be 3 subgroups isomorphic to D_8 and the alternating group $\mathcal{A}_4$.

We have not proved it, but in fact, these subgroups, together with $\mathcal{S}_4$ itself and the identity subgroup, form the full collection of subgroups of $\mathcal{S}_4$.

9 Group actions

9.1 Introducing actions

Frequently groups are studied in mathematics because of their actions on other mathematical objects. The actions of groups on themselves are also important, provide some powerful tools in group theory.

Definition 9.1 *An* **action** *of a group G on a set Ω is defined to be a homomorphism from G to $\mathcal{S}(\Omega)$. G is said to* **act on** *Ω.*

In this context, the product rule for a homomorphism θ, $\theta(g_1g_2) = \theta(g_1)\theta(g_2)$, means that the image of the product g_1g_2 has the same effect on Ω as the composite of the images of g_1 and g_2, that is,

$$\theta(g_1g_2)(\alpha) = \theta(g_1)(\theta(g_2)(\alpha))\,\forall\alpha \in \Omega.$$

In order to avoid cumbersome notation, we prefer to represent the image of an element $g \in G$ in $\mathcal{S}(\Omega)$ not by $\theta(g)$ but by g itself. And we'll often write $g[\alpha]$ rather than $g(\alpha)$ (or $\theta(g)(\alpha)$), to avoid confusion with other uses of parentheses.

Then we define an action by specifying a rule $\alpha \mapsto^g g[\alpha]$ for each element $g \in G$. Using this notation, the product rule for a homomorphism now translates as

$$(g_1g_2)[\alpha] = g_1[g_2[\alpha]]\,\forall\alpha. \quad (**)$$

Given a set of rules $\alpha \mapsto^{g} g[\alpha]$, in order to verify that we have an action we need to check first that each such rule defines a permutation of Ω, second that we have a homomorphism.

If G is finitely generated then specify an action we only need to specify a rule for each of the generators. The rule for a product of generators can then be deduced as a composite using the product rule (**).

But to ensure that we really have an action, we still need to check that the image of each generator acts as a permutation of Ω and that different products of generators that represent the same element of G are defined by the rule to act in the same way.

9.2 The natural action of $\mathcal{S}_n$ and its subgroups.

Where G is $\mathcal{S}_n$ or one of its subgroups, the identity map provides an isomorphism from G to itself, and hence an injective homomorphism from G to a subgroup of $\mathcal{S}_n$. So every subgroup of $\mathcal{S}_n$ has an action on $\Omega = \{1, 2, \ldots, n\}$, which we call its **natural action**.

Various other actions can be inherited from the natural action, e.g. $\mathcal{S}_n$ and its subgroups also permute the set $\begin{pmatrix} \Omega \\ 2 \end{pmatrix}$ of unordered pairs of distinct elements from Ω.

9.3 The actions of $\mathcal{S}_4$ on the tetrahedron and the cube

Given a tetrahedron with vertices labelled $1, 2, 3, 4$, it is clear that the natural action of $\mathcal{S}_4$ defines an action on the vertices of the tetrahedron that preserves its structure, and from this actions of $\mathcal{S}_4$ on the edges and faces of the tetrahedron are inherited.

We write the edges and faces as sets of pairs and triples from $\{1, 2, 3, 4\}$

Then given generators $a = (1, 2)$, $b = (2, 3)$, $c = (3, 4)$ for $\mathcal{S}_4$, the actions of $\mathcal{S}_4$ on the edges and faces are defined as follows:-

$$\{1,2\} \mapsto^a \{1,2\}, \{1,3\} \mapsto^a \{2,3\}, \{2,3\} \mapsto^a \{1,3\}, \{3,4\} \mapsto^a \{3,4\}$$
$$\{1,2\} \mapsto^b \{1,3\}, \{1,3\} \mapsto^b \{1,2\}, \{2,3\} \mapsto^b \{2,3\}, \{3,4\} \mapsto^b \{2,4\}$$

$$\{1,2\} \mapsto^c \{1,2\}, \{1,3\} \mapsto^c \{1,4\}, \{2,3\} \mapsto^c \{2,4\}, \{3,4\} \mapsto^c \{3,4\}$$

and

$$\begin{gathered}\{1,2,3\} \mapsto^a \{1,2,3\}, \{1,2,4\} \mapsto^a \{1,2,4\}, \{1,3,4\} \mapsto^a \{2,3,4\}, \\ \{2,3,4\} \mapsto^a \{1,3,4\}, \\ \{1,2,3\} \mapsto^b \{1,2,3\}, \{1,2,4\} \mapsto^b \{1,3,4\}, \{1,3,4\} \mapsto^b \{1,2,4\}, \\ \{2,3,4\} \mapsto^b \{2,3,4\}, \\ \{1,2,3\} \mapsto^c \{1,2,4\}, \{1,2,4\} \mapsto^c \{1,2,3\}, \{1,3,4\} \mapsto^c \{1,3,4\}, \\ \{2,3,4\} \mapsto^c \{2,3,4\}.\end{gathered}$$

Now we can construct a cube on the set of vertices

$$V = \{1, 2, 3, 4, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

for which the set E of edges consists of all pairs $\{i, \bar{j}\}$ with $i \neq j$, and the set F of faces is

$$F = \{1, \bar{2}, 3, \bar{4}\}, \{1, \bar{2}, 4, \bar{3}\}, \{1, \bar{3}, 2, \bar{4}\}, \{\bar{1}, 2, \bar{3}, 4\}, \{\bar{1}, 2, \bar{4}, 3\}, \{\bar{1}, 3, \bar{2}, 4\}$$

We see that the vertices i and $\bar{i}$ are always opposite each other. See diagram:-

From its natural actions on $\{1,2,3,4\}$ and $\{\bar{1},\bar{2},\bar{3},\bar{4}\}$, $\mathcal{S}_4$ inherits actions on the vertices, edges and faces of the cube.

We see that the generator a acts on the vertices as $(1,2)(\bar{1},\bar{2})$, that is, as a reflection in the plane through $3,\bar{4},\bar{3},4$, and b and c act as $(2,3)(\bar{2},\bar{3})$ and $(3,4)(\bar{3},\bar{4})$.

ab acts as

We see that this fixes

and so that ab acts as

abc acts as

This doesn't fix any line or plane, and doesn't correspond to either a rotation of a reflection. Of course it's the composite of the reflection c and the rotation ab.

And in fact if we choose **any** reflection τ that preserves the cube, then there's a rotation ρ for which $abc = \rho\tau$.

9.4 Actions of C_2 on the cube

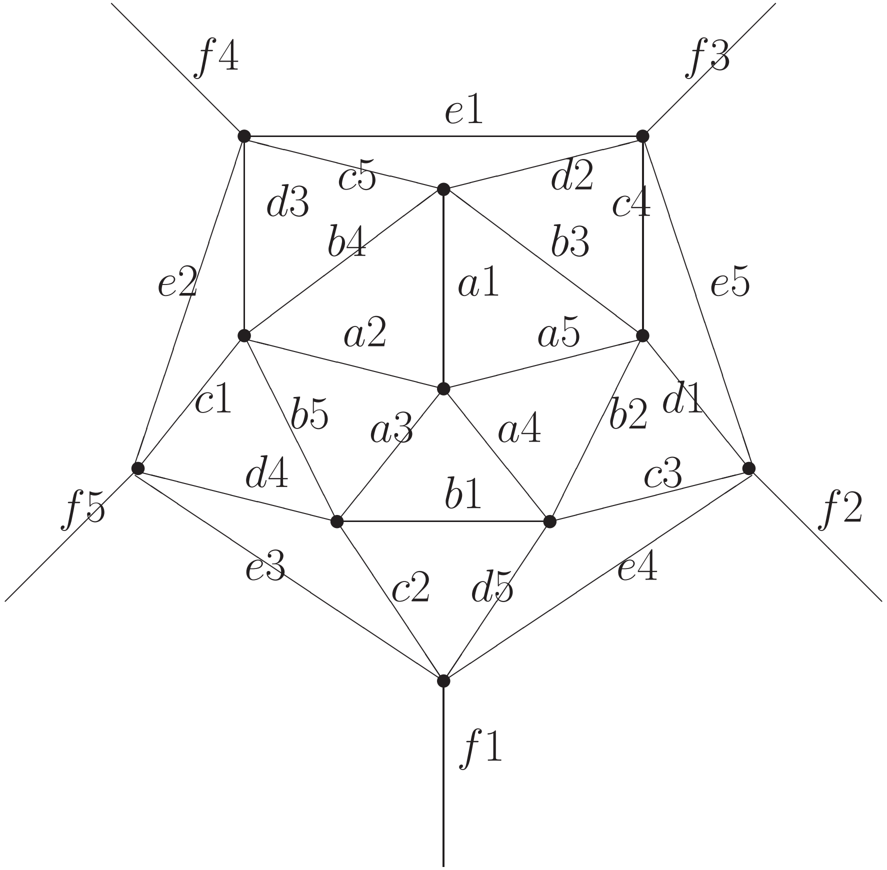
The cyclic group $C_2 = \langle \tau \mid \tau^2 = e \rangle$ acts on the vertices of the cube just described as the **antipodal map**,that is, the permutation

$$(1, \bar{1})(2, \bar{2})(3, \bar{3})(4, \bar{4}).$$

The action preserves the structure of the cube. And indeed the full group of symmetries of the cube is the group $\mathcal{S}_4 \times C_2$, which contains $\mathcal{S}_4$ and C_2 as subgroups, acting on the group as just described.

To see that the rule defines a homomorphism from C_2 to $\mathcal{S}(V)$ we only need to check that τ^2 acts as the identity permutation. (In general, where $G = \langle X \mid R \rangle$, a map from X to $\mathcal{S}(\Omega)$ defines an action of G on Ω provided that each relator in R maps to the identity permutation.)

9.5 $\mathcal{A}_5$ acts on the icosahedron



The diagram shows a framework from which we can build an icosahedron; we just join the free ends of the 5 edges labelled $f1, \ldots, f5$ to a single point behind the figure.

We can examine the effect of various symmetries of that icosahedron on the 30 edges.

The rotation α mapping a_1 to a_2, through $2\pi/5$ about an axis joining the central vertex to the one at the back, acts on the 30 edges as the permutation

$$(a1, a2, a3, a4, a5)(b1, b2, b3, b4, b5)(c1, c2, c3, c4, c5)$$
$$(d1, d2, d3, d4, d5)(e1, e2, e3, e4, e5)(f1, f2, f3, f4, f5).$$

The reflection β in the plane through the edges $a1$ and $f1$ acts on the 30 edges as the permutation

$$(a1)(b1)(e1)(f1)(c1,d1)(a2,a5)(a3,a4)(b2,b5)(b3,b4)$$
$$(c2,d5)(c3,d4)(c4,d3)(c5,d2)(e2,e5)(e3,e4)(f2,f5)(f3,f4).$$

The rotation γ mapping a_1 to $b3$, through $2\pi/3$ about an axis through the centre of the triangle with edges $a1, b3, a5$, acts on the 30 edges as the permutation

$$(a1,b3,a5)(a2,d2,b2)(a3,c5,d1)(a4,b4,c4)(b1,d3,e5)$$
$$(b5,e1,e3)(c1,f3,d5)(c2,e2,f2)(c3,f5,f1)(d4,f4,e4).$$

In fact each of α, β, γ permutes the following 5 sets of 6 edges:-

$\{a1, b1, c1, d1, e1, f1\}, \{a2, b2, c2, d2, e2, f2\}, \{a3, b3, c3, d3, e3, f3\}.$
$\{a4, b4, c4, d4, e4\}, \{a5, b5, c5, d5, e5, f5\}.$

Any 2 edges in each set of six are either parallel or orthogonal. We can call the sets 1,2,3,4,5.

Then we see that α permutes the 5 sets as $(1, 2, 3, 4, 5)$, β as $(2, 5)(3, 4)$, and γ as $(1, 3, 5)$. Each of those permutations is even, so in $\mathcal{A}_5$. In fact we can see that every even permutation of $\{1, 2, 3, 4, 5\}$ corresponds to some symmetry of the icosahedron (in fact to two different symmetries, as we shall see soon).

9.6 C_2 acts on the icosahedron

$C_2 = \langle \tau \mid \tau^2 = 1 \rangle$ acts on the vertices, edges and faces of the icosahedron.

The antipodal symmetry maps each vertex, edge or face to the vertex, edge or face opposite it on the icosahedron. Clearly that symmetry has order 2. In that action C_2 preserves the sets $1, 2, 3, 4, 5$ of six edges, that is, acts as the identity permutation on the set $\{1, 2, 3, 4, 5\}$. Indeed, for any symmetry ρ of the icosahedron, ρ and $\rho\tau$ correspond to the same permutation in $\mathcal{A}_5$.

NB for any choice of 3 mutually perpendicular planes Π_1, Π_2, Π_3, each bisecting the icosahedron, the antipodal map can be decomposed as the composite of successive reflections in the three planes.

9.7 The group of the dodecahedron

Each of the 30 edges of the dodecahedron that is dual to the icosahedron is perpendicular to a corresponding edge of the icosahedron. So it's clear that the 30 edges of the dodecahedron also fall into 5 sets of 6 edges that are mutually parallel and orthogonal. Hence we see the same action of $\mathcal{A}_5$ for the dodecahedron, and similarly the antipodal map provides an action of C_2.

This explains why the symmetry groups of both icosahedron and dodecahedron are isomorphic to $\mathcal{A}_5 \times C_2$.

9.8 A useful action of C_m

Let A be any set. We define an action of $C_m = \langle t | t^m = e \rangle$ on the set A^m of all m-tuples of elements from A as follows.

$$(a_1, a_2, \ldots, a_m) \mapsto^t (a_2, a_3, \ldots, a_m, a_1)$$

We deduce from the product rule that

$$(a_1, a_2, \ldots, a_m) \mapsto^{t^i} (a_{i+1}, a_{i+2}, \ldots, a_m, a_1, \ldots, a_i)$$

It is straightforward to verify that the rules define permutations of the set. And we see that t^m acts as the identity permutation, as required.

We'll meet this action when we prove Cauchy's theorem, Theorem 10.1.

9.9 Action of $\mathbb{Z}^2$ on $\mathbb{R}^2$

The free abelian group $\langle a, b \mid ab = ba \rangle$ acts on the Euclidean plane $\mathbb{R}^2$ via

$$(x, y) \mapsto^a (x+1, y), \quad (x, y) \mapsto^b (x, y+1).$$

We check easily that these two maps are bijections from $\mathbb{R}^2$ to $\mathbb{R}^2$.

Then since $$\begin{aligned} a[b[(x,y)]] &= a[(x, y+1)] = (x+1, y+1) \\ &= b[(x+1, y)] = b[a[(x,y)]], \end{aligned}$$

we see that the two maps commute.

This verifies that we have defined an action of $\mathbb{Z}^2$ on $\mathbb{R}^2$.

This group is the fundamental group of the torus.

9.10 The coset action

Proposition 9.2 *For groups G, H with $H \subseteq G$, the set of rules $xH \mapsto^g gxH$ defines an action of G on the set G/H of left cosets of H in G.*

Proof: First we verify that the maps are permutations of G/H. The map $xH \mapsto gxH$ is clearly surjective since for any coset yH, $yH = g[(g^{-1}y)H]$, and injective since

$$\begin{aligned} g[x_1H] &= g[x_2H] \Rightarrow gx_1H = gx_2H \\ &\Rightarrow g^{-1}gx_1H = g^{-1}gx_2H \Rightarrow x_1H = x_2H \end{aligned}$$

So the rules define elements of $\mathcal{S}(G/H)$.

To verify the product rule (and hence see that we have a homomorphism from G to $\mathcal{S}(G/H)$), we note that for $g_1, g_2 \in G$, $xH \in G/H$,

$$(g_1g_2)[xH] = (g_1g_2)xH = g_1(g_2x)H = g_1[g_2xH] = g_1[g_2[xH]].$$

□

The coset action is important in the proof of Sylow's theorems, Theorems 10.3,10.5.

9.11 The left regular action and Cayley's theorem

The coset action of G on the cosets of the identity subgroup is commonly known as the **left regular action**. We think of this as an action of G on itself (although technically the set of cosets of $\{e\}$ isn't actually G but a set of singleton sets in correspondence with G). It's defined by the rules

$$x \mapsto^g gx.$$

The proof of Cayley's theorem, one of the big early theorems in group theory, is based on the left regular action of G

Theorem 9.3 (Cayley's theorem) *Let G be a group. Then G is isomorphic to a subgroup of $\mathcal{S}(G)$.*

Proof: The left regular action of G (proved to be an action by proposition 9.2) provides a homomorphism from G to $\mathcal{S}(G)$.

The kernel of that homomorphism is $\{g : gx = x, \forall x \in G\}$. But $gx = x \iff g = e$. Hence the homomorphism has trivial kernel, and so defines an isomorphism from G to a subgroup of $\mathcal{S}(G)$. □

The proof may seem very short, but of course it depends on proposition 9.2.

9.12 Conjugation action

Proposition 9.4 *The set of rules $x \mapsto^g gxg^{-1}$, (that is $x \mapsto^g x^g$) for $x, g \in G$ defines an action of G on itself.*

(The proof is left as an exercise for the lecture.)

Proposition 9.5 *For any subgroup H of G, the set of rules*

$$xHx^{-1} \mapsto^{g} gxHx^{-1}g^{-1}$$

(that is, $H^{x} \mapsto^{g} H^{gx}$) for $x, g \in G$, defines an action of G on the set of conjugates of H.

Proof as exercise.

Note that, for $x \in G$, and a subgroup H, the set $\{x^{g} : g \in G\}$ is called the **conjugacy class** of x, and the set $\{H^{g} : g \in G\}$ the conjugacy class of H.

The conjugation action is important in the proof of Sylow's third theorem, Theorem 10.6.

9.13 Stabilisers

Definition 9.6 *Where G is a group acting on a set Ω and $\alpha \in \Omega$, the* **stabiliser** *of α,* $\mathsf{stab}(\alpha)$, *(or* $\mathsf{stab}_G(\alpha)$*) is defined to be*

$$\{g \in G : g[\alpha] = \alpha\}$$

Sometimes the notation G_α is used instead of $\mathsf{stab}(\alpha)$

Note that the kernel of the action is the intersection of all the stabilisers,

$$\bigcap_{\alpha\in\Omega} \mathsf{stab}(\alpha)$$

Examples 9.7

E.g.1 For the natural action of $\mathcal{S}_4$ on $\{1, 2, \ldots 4\}$,

$$\begin{aligned} \text{stab}(1) &= \{(),\ (2,3,4),\ (2,4,3),\ (2,3),\ (2,4),\ (3,4)\} \\ \text{stab}(2) &= \\ \text{stab}(3) &= \\ \text{stab}(4) &= \end{aligned}$$

We see that each stabiliser is a subgroup isomorphic to $\mathcal{S}_3$. In general, for $\mathcal{S}_n$ in its natural action, the stabiliser of any element of $\{1, 2, \ldots, n\}$ is a subgroup isomorphic to S_{n-1}.

E.g.2 for the natural action of D_8, specified as the permutation group

$$\begin{aligned} D_8 = \{&(),\ (1,2,3,4),\ (1,4,3,2),\ (1,3)(2,4),\ (1,2)(3,4),\ (1,4)(2,3), \\ &(1,3),\ (2,4)\}, \end{aligned}$$

stab(1) $=$

stab(2) $=$

stab(3) $=$

stab(4) $=$

E.g.3 For the action of $\mathcal{S}_4$ on the set of unordered pairs from $\{1,2,3,4\}$, the stabiliser of $\{1,2\}$ is the subgroup $\langle(1,2),\ (3,4)\rangle$, and the stabiliser of $\{1,3\}$ is the subgroup $\langle(1,3),\ (2,4)\rangle$. Both have order 4.

When D_8 acts on the same set, stab$(\{1,2\}))$ is the cyclic subgroup $\langle(1,2)(3,4)\rangle$ of D_8, which has order 2, while stab$(\{1,3\})$ is the subgroup $\langle(1,3),\ (2,4)\rangle$, of order 4.

E.g.4 For the coset action of a group G on the set G/H,

$$\begin{aligned} \text{stab}(H) &= \{g : gH = H\} = H \\ \text{stab}(xH) &= \{g : gxH = xH\} = \{g : x^{-1}gxH = H\} \\ &= \{g : x^{-1}gx \in H\} = \{g : g \in xHx^{-1}\} \\ &= xHx^{-1} =: H^x. \end{aligned}$$

When H is the identity subgroup, i.e. in the case of the left regular action, the stabiliser of any element x is { g: gx=x}, that is, the identity subgroup. An action in which every stabiliser is the identity subgroup is called a **regular action** (and the left regular action is an example of such).

E.g.5 Let a group G act on itself by conjugation. Then, for $x \in G$,

$$\text{stab}(x) = \{g : gxg^{-1} = x\} = \{g : gx = xg\}$$

This subgroup is called the **centraliser** of x in G.

E.g.6 Let G be any group, H a subgroup, and let Ω be the conjugacy class of H in G, with G acting according to the rule

$$g[H^x] = H^{gx}, \forall g, x, \in G$$

Then the stabiliser of H is

$$\{g \in G : H^g = H\}$$

This subgroup is known as the **normaliser** of H in G, written $N_G(H)$.

Proposition 9.8 *Where G is a group acting on a set Ω and $\alpha \in \Omega$,*

(a) stab(α) *is a subgroup of G.*

(b) *if $\beta \in G$ and $\beta = x[\alpha]$ for $x \in G$,* stab$(\beta) =$ stab$(\alpha)^x$.

Proof:

(a) We need to verify from the definition of the stabiliser that

(1) $e \in$ stab(α),
(2) if $g_1, g_2 \in$ stab(α), then $g_1 g_2 \in$ stab(α),
(3) if $g \in$ stab(α), then $g^{-1} \in$ stab(α),
In order to prove (1), we need to recall that every homomorphism maps the identity to the identity.

(b) We verify from the definition that if $g \in \mathsf{stab}(\alpha)$ then $xgx^{-1} \in \mathsf{stab}(\beta)$, while if $h \in \mathsf{stab}(\beta)$ then $x^{-1}hx \in \mathsf{stab}(\alpha)$.

□

Examples 9.9

Recall that for the natural action of $\mathcal{S}_4$ on $\{1, 2, 3, 4\}$ the stabilisers of 1 and 4 are the subgroups

$$\begin{aligned} \text{stab}(1) &= \{(),\ (2,3),\ (2,4),\ (3,4),\ (2,3,4),\ (2,4,3)\} \\ \text{stab}(4) &= \{(),\ (1,2),\ (1,3),\ (2,3),\ (1,2,3),\ (1,3,2)\} \end{aligned}$$

Both subgroups are isomorphic to $\mathcal{S}_3$, and

$$\text{stab}(4) = \text{stab}(1)^{(1,4)} = \text{stab}(1)^{(1,4)(2,3)} = \text{stab}(4)^{(1,4,3,2)} \ldots$$

Each of the three conjugating elements map 1 to 4.

We can examine similarly the other examples in Examples 9.7.

9.14 Orbits and transitivity

Definition 9.10 *Where G is a group acting on a set Ω and $\alpha \in \Omega$, the set $\{g[\alpha] : g \in G\}$ is called the* **orbit** *of α under the action of G, written* $\mathrm{orb}(\alpha)$ *or* $\mathrm{orb}_G(\alpha)$*, or sometimes $G\alpha$. We call the size of* $\mathrm{orb}(\alpha)$ *its* **length**.

If $\mathrm{orb}(\alpha)$ *is the whole of Ω then we say that G acts* **transitively** *on Ω. In this case, for any pair of elements $\beta, \gamma \in \Omega$, there is an element $g \in G$ with $g(\beta) = \gamma$ Otherwise we say that G acts* **intransitively**.

NB: Notice that even when G acts intransitively on a set Ω it acts transitively on each of the orbits of elements α of Ω. Basically the orbits are the subsets of Ω on which G acts transitively.

Examples 9.11

E.g.1 The natural action of $\mathcal{S}_n$ on $\{1, 2, 3, \ldots, n\}$ is transitive. For given $i, j \in \Omega$,

E.g.2 The left regular action of G on itself is transitive. For given $x, y \in G$,

E.g.3 $\mathcal{S}_4$ acts transitively on the set

$$\Omega = \{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\}.$$

When i, j, k, l are all distinct, the element $g = (i,k)(j,l)$ maps $\{i,j\}$ to $\{k,l\}$, while where i, j, k are all distinct the element $g = (j,k)$ maps $\{i,j\}$ to $\{i,k\}$. But D_8 has two orbits on Ω, namely:

That's not surprising, since D_8 is the group of symmetries of a square with vertices 1,2,3,4, edges $\{1,2\}$,$\{2,3\}$,$\{3,4\}$,$\{4,1\}$.

E.g.3 $\mathcal{S}_4$ has two orbits in its action on the vertices of the cube described in Subsection 9.3, the sets $\{1, 2, 3, 4\}$, and $\{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$. These form the vertices of two tetrahedra within the cube. (These are the white and black tetrahedra we described in the introduction.)

E.g.4 Given groups G, H with $H \subset G$, the left coset action of G on G/H is transitive, but the same action of the subgroup H on G/H is not, e.g. $\{H\}$ is an orbit of length 1.

9.15 Equivalent actions

Definition 9.12 *Let G be a group that acts on two sets Ω_1 and Ω_2. We say that the two actions are equivalent if there is a bijection $f : \Omega_1 \to \Omega_2$ with the property that*

$$\forall \alpha \in \Omega_1, \forall g \in G, \ f(g[\alpha]) = g[f(\alpha)]$$

The function f is called an **equivalence** *between the two actions.*

Example 9.13

The natural action of $\mathcal{S}_4$ on $\Omega_1 = \{1, 2, 3, 4\}$ is equivalent to its action on $\Omega_2 = \{a, b, c, d\}$ defined by the rules

$$a \mapsto^{(1,2)} b, \ b \mapsto^{(1,2)} a, \ c \mapsto^{(1,2)} c, \ d \mapsto^{(1,2)} d$$

$$a \mapsto^{(1,3)} c,\ c \mapsto^{(1,3)} a,\ b \mapsto^{(1,3)} b,\ d \mapsto (1,3)d$$
$$a \mapsto^{(1,4)} d,\ d \mapsto^{(1,4)} a,\ b \mapsto (1,4)b,\ c \mapsto^{(1,4)} c$$

(Since the elements $(1,2)$, $(1,3)$, $(1,4)$ generate the group the action of the whole group on Ω_2 is defined by the action of these elements).

Define $f : \Omega_1 \to \Omega_2$ by $f(1) = a$, $f(2) = b$, $f(3) = c$, $f(4) = d$. Then for all $i \in \{1,2,3,4\}$, for all $g \in \mathcal{S}_4$, $g[f(i)] = f(g[i])$.

Theorem 9.14 *Let G be a group, acting transitively on a set Ω. Let α be an element of Ω, and let $H = \text{stab}(\alpha)$. Then the action of G on Ω is equivalent to the action of G on the left cosets of* $\text{stab}(\alpha)$ *by left multiplication.*

Proof:. Define $f : G/H \to \Omega$ by $f(xH) = x[\alpha]$. f will be our equivalence.

First we check that f is well defined as a function.

Next we verify that f is surjective.

Also f is injective.

Finally, we see that the two actions are equivalent, since for any $g \in G$, $f(g[xH]) =$.

□

Corollary 9.15 *Where a finite group G acts on a set Ω and $\alpha \in \Omega$, the length of* $\mathrm{orb}(\alpha)$ *is equal to* $|G : \mathrm{stab}(\alpha)|$ *and must divide* $|G|$.

Proof: The action of G on orb(α) is equivalent to its action on the left cosets of stab(α). Hence in particular the two sets have the same size. And

$$|G : \text{stab}(\alpha)| = |G|/|\text{stab}(\alpha)|,$$

by Lagrange's theorem, so the orbit length divides $|G|$. □

Corollary 9.16 *Let G be a group, and $x \in G$. Then the length (.i.e. size) of the conjugacy class of x is equal to the index of the centraliser of x in G, which must divide $|G|$.*

10 Sylow theorems

The results which follow explain to what extent the converse of Lagrange's theorem is true; their proofs use group actions.

10.1 Cauchy's theorem

Theorem **10.1 (Cauchy)** *Suppose that G is a finite group and that p is a prime dividing $|G|$. Then G contains an element of order p.*

Proof: Let Ω be the set of all p-tuples $(x_1, x_2, \ldots, x_p)$ of elements of G for which $x_1 x_2 \cdots x_p = e$. Then $|\Omega| = |G|^{p-1}$ (in such a p-tuple

$x_1, \ldots x_{p-1}$ can be chosen arbitrarily, but then x_p is fixed).

Now the cyclic group $C = \langle \tau \mid \tau^p = e \rangle$ acts on Ω via the rule

$$\tau[(x_1, \ldots, x_p)] = (x_2, x_3, \ldots, x_p, x_1)$$

The length of every orbit of C on Ω must divide $|C| = p$, and hence is either 1 or p. Also the sum of all the orbit lengths is $|\Omega|$, which is divisible by p. Hence the number of orbits of length 1 is divisible by p, or rather the number of elements of Ω fixed by τ is divisible by p. So either there are no such elements or there are at least p.

Since $(e, e, e, \cdots, e)$ is certainly fixed by τ, there must be another element. That must have the form $(x, x, x, \cdots, x)$ where $x \neq e$ and (by definition of Ω) $x^p = e$. Then x has order p. □

Using Cauchy's theorem 10.1 and Cayley's theorem 9.3 it is straightforward to prove the following.

Proposition 10.2 *Let G be a group of order $2n$, where n is an odd integer. Then G has a normal subgroup of order n.*

Proof: By Cauchy's theorem G has an element x of order 2. Now consider the image of x as a permutation in the symmetric group $\mathcal{S}(G)$ (under the left regular action of Cayley's theorem). For each $g \in G$, $x[g] = xg$, $x[xg] = x^2g = eg = g$. So as a permutation in $\mathcal{S}(G)$, x decomposes as a product of n disjoint 2-cycles. Since n is odd, x is an odd permutation.

Now let H be the set of elements of G which correspond to even permutations of $\mathcal{S}(G)$. Then H is a proper subgroup by the above. So, by earlier results, H is normal of index 2. $\square$

NB This result need not hold when n is even. Recall that $\mathcal{A}_4$, which has order 12, has no subgroup of order 6.

10.2 Sylow theorems

Theorem **10.3 (Sylow's first theorem)** *Let G be a finite group of order $p^a b$ for $a \geq 1$ some integer b not divisible by p. Then G contains subgroups of order p^r for each $r \leq a$.*

NB The subgroups of order p^a are called the **Sylow p-subgroups** of G.

Proof: (due to Wielandt) We consider the action of G defined by the rule $X \mapsto^g gX = \{gx : x \in X\}$, on the set Ω of all subsets of G with p^r elements.

$$|\Omega| = \binom{p^a b}{p^r}$$

Expanding that binomial coefficient as a quotient of products as usual, and observing that for $0 < i < p^r$ the same power of p divides $p^a b - i$ as $p^r - i$, we see that $|\Omega|$ is divisible by p^{a-r} but not by p^{a-r+1}.

The sum of the orbit lengths is $|\Omega|$, so there must be an orbit $\mathcal{O}$ whose length k is not divisible by p^{a-r+1}.

Choose $X \in \mathcal{O}$, and let $H = \text{stab}(X)$. Then $|G : H| = k$, so $|H| = |G|/k = p^a b/k$. Since p^{a-r+1} does not divide k, certainly p^r divides $|H|$, and hence $p^r \leq |H|$.

Since $H = \text{stab}(X)$, for all $x \in X$ $Hx \subseteq X$. So $|Hx| \leq |X|$, and hence $|H| \leq |X| = p^r$.

So H is a subgroup of G of order p^r. □

Examples 10.4

E.g.1 $\mathcal{S}_3$ has order $6 = 2 \times 3$. There are 3 Sylow 2-subgroups, each cyclic of order 2, a single, normal Sylow 3-subgroup of order 3.

E.g.2 S_4 has order $24 = 2^3 \times 3$.

There are 4 Sylow 3 subgroups, each cyclic of order 3.

The Sylow 3-subgroups:

There are 2 kinds of subgroups or order 2, 3 kinds of subgroups of order 4, e.g.:

There are 3 Sylow 2-subgroups, each isomorphic to D_8, each the group of symmetries of one of the 3 squares with vertices labelled $1, 2, 3, 4$, namely:

Theorem 10.5 (Sylow's second theorem) *Let G be a group of order $p^a b$ for p prime, some $a \geq 1$, and b not divisible by p. Then the Sylow p-subgroups of G are all conjugate.*

Proof: Let P, Q be two Sylow p-subgroups of G.

Consider the action of Q on G/P by left multiplication. The length of each orbit divides $|Q| = p^a$, so is either 1 or a power of p.

But the orbit lengths sum to $|G/P| = b$, which is not divisible by p. So there must be an orbit xP of length 1. Then

$$g \in Q \Rightarrow g[xp] = gxP = xP \Rightarrow x^{-1}gx \in P \Rightarrow g \in xPx^{-1}.$$

So $Q \subseteq P^x$, and hence, since both Q and P^x have order p^a, $Q = P^x$. That is, P and Q are conjugate. □

Theorem 10.6 (Sylow's third theorem) *Let G be a group of order $p^a b$ for p prime, some $a \geq 1$, and b not divisible by p. Let k be the number of Sylow p-subgroups of G. Then k divides b and is congruent to 1 mod p.*

Proof: Let Ω be the set of all Sylow p-subgroups, and choose $P \in \Omega$. Let P be a Sylow p-subgroup of G.

Since Ω is a single conjugacy class, $k = |\Omega| = |G : N_G(P)|$. Since $P \subseteq N_G(P) \subseteq G$, p^a divides $|N_G(P)|$, and so k divides b.

Now consider the action of P on Ω by conjugation. Every orbit has length 1 or a power of p, and P itself is in an orbit of length 1.

If Q is also in an orbit of length 1, then $P \subseteq N_G(Q)$. Then also $Q \subseteq N_G(Q)$, so P and Q are both Sylow p-subgroups of $N_G(Q)$. Then, for some $x \in N_G(Q)$, $P = Q^x$. But $x \in N_G(Q) \Rightarrow Q^x = Q \Rightarrow P = Q$. So $\{P\}$ is the only orbit of length 1; all other orbits have length divisible by p. Then the total length of the union of all the orbits is congruent to 1 mod p. $\square$

10.3 Applying the theorems

The following result is also useful.

Proposition 10.7 *Suppose that G has precisely one Sylow p-group H. Then $H \trianglelefteq G$.*

Proof: If $g \in G$ then H^g is a subgroup of G of the same order as H, and hence is also a Sylow p-subgroup. So $H^g = H$ for all $g \in G$. Hence $H \trianglelefteq G$. □

Exercise 10.8 *Let G be a group of order 12. Prove that G has a normal subgroup of order either 3 or 4.*

Solution: The Sylow 3-subgroups of G have order 3. By Sylow's third theorem, there are m of these, where m divides 4 and is congruent to 1 mod 3. So $m = 1$ or 4.

When $m = 1$, then H is a normal subgroup of G of order 3.

Otherwise, G has 4 subgroups of order 3, and hence 8 elements of order 3, and at most 4 other elements. So at most 4 elements of G lie in Sylow 2-subgroups. Since each Sylow 2-subgroup has order 4, there can be only be one such subgroup. Hence it is a normal subgroup, of order 4. $\square$

Exercise 10.9 *Let G be a group of order pq, where p and q are primes, and $p \neq q$, then G has a normal subgroup of order p or q.*

Solution: Let H be a Sylow p-subgroup (of order p) and K a Sylow q-subgroup (of order q). The number m of conjugates of H divides q and is congruent to 1 mod p, while the number n of conjugates of K divides p and is congruent to 1 mod q. So if $q \leq p$, $m = 1$, while if $p \leq q$, $n = 1$. In the first case $H \lhd G$, in the second case $K \lhd G$. □