GROUPS

SIMON WADSLEY

Contents

Purpose of notes. Please note that these are not notes of the lectures but notes made by the lecturer in preparation for the lectures. This means they may not exactly correspond to what was said and/or written during the lectures.

This version has had all the proofs removed to aid those who wish to revise.

Lecture 1

1. Examples of groups

Groups are fundamentally about symmetry. More precisely they are an algebraic tool designed to abstract the notion of symmetry. Symmetry arises all over mathematics; which is to say that groups arise all over mathematics. Roughly speaking a symmetry is a transformation of an object that preserves certain properties of the object.

As I understand it, the purpose of this course is two-fold. First to introduce groups so that those who follow the course will be familiar with them and be better equipped to study symmetry in any mathematical context that they encounter. Second as an introduction to abstraction in mathematics, and to proving things about abstract mathematical objects.

It is perfectly possible to study groups in a purely abstract manner without geometric motivation. But this seems to both miss the point of why groups are interesting and make getting used to reasoning about abstract objects more difficult. So we will try to keep remembering that groups are about symmetry. So what do we mean by that?

1.1. **A motivating example.**

Question. What are the distance preserving functions from the integers to the integers? That is what are the members of the set

$$\mathrm{Isom}(\mathbb{Z}) := \{f\colon \mathbb{Z} \to \mathbb{Z} \text{ such that } |f(n) - f(m)| = |n - m| \text{ for all } n, m \in \mathbb{Z}\}?$$

These functions might reasonably be called the symmetries of the integers; they describe all the ways of 'rearranging' the integers that preserve the distance between any pair.

Let's begin to answer our question by giving some examples of such functions. Suppose that $a \in \mathbb{Z}$ is an integer. We can define the function 'translation by a' by

$$t_a\colon n \mapsto n + a \text{ for } n \in \mathbb{Z}.$$

For any choice of $m, n \in \mathbb{Z}$

$$|t_a(n) - t_a(m)| = |(n + a) - (m + a)| = |n - m|.$$

Thus t_a is an element of $\mathrm{Isom}(\mathbb{Z})$. We might observe that if a and b are both integers then

$$(t_a \circ t_b)(n) = t_a(b + n) = a + b + n = t_{a+b}(n)$$

for every integer n, that is that $t_{a+b} = t_a \circ t_b$[1]. Moreover t_0 is the identity or 'do nothing' function $\mathrm{id}\colon \mathbb{Z} \to \mathbb{Z}$ that maps every integer n to itself. Thus for every $a \in \mathbb{Z}$, t_{-a} is the inverse of t_a, that is $t_a \circ t_{-a} = \mathrm{id} = t_{-a} \circ t_a$.

[1]This is because two functions $f, g\colon X \to Y$ are the same function, i.e. $f = g$, precisely if they have the same effect on every element of the set they are defined on, i.e. $f(x) = g(x)$ for all $x \in X$.

Suppose now that $f \in \mathrm{Isom}(\mathbb{Z})$ is a symmetry of the integers. Consider the function $g := t_{-f(0)} \circ f$. Then for $n, m \in \mathbb{Z}$,

$$|g(n) - g(m)| = |(f(n) - f(0)) - (f(m) - f(0))| = |f(n) - f(m)| = |n - m|,$$

so $g \in \mathrm{Isom}(\mathbb{Z})$ is also a symmetry of the integers.

Moreover $g(0) = t_{-f(0)}(f(0)) = f(0) - f(0) = 0$, i.e. g fixes the integer 0. What does this tell us about g? For example, what does it tell us about $g(1)$? Since g is a symmetry and $g(0) = 0$ it must be the case that

$$|g(1)| = |g(1) - 0| = |g(1) - g(0)| = |1 - 0| = 1.$$

That is $g(1) = \pm 1$.

If $g(1) = 1$, what else can we say? For any $n \in \mathbb{Z}$,

$$|g(n)| = |g(n) - g(0)| = |n - 0| = |n|$$

i.e. $g(n) = \pm n$. But also,

$$|g(n) - 1| = |g(n) - g(1)| = |n - 1|$$

i.e. $g(n) = 1 \pm (n-1)$. These two conditions together force $g(n) = n$ and so $g = \mathrm{id}$. Now in this case

$$t_{f(0)} = t_{f(0)} \circ \mathrm{id} = t_{f(0)} \circ (t_{-f(0)} \circ f) = (t_{f(0)} \circ t_{-f(0)}) \circ f = \mathrm{id} \circ f = f.$$

Thus f is translation by $f(0)$ in this case.

What about the case when $g(1) = -1$? In this case we still must have $g(n) = \pm n$ for every integer n but now also

$$|g(n) + 1| = |g(n) - g(1)| = |n - 1|$$

i.e. $g(n) = -1 \pm (n - 1)$. These two conditions together force $g(n) = -n$ and so g is the 'reflection about 0'-function

$$s \colon n \mapsto -n \text{ for all } n \in \mathbb{Z}.$$

Now we've seen that $s = g = t_{-f(0)} \circ f$ in this case. It follows that $f = t_{f(0)} \circ s$.

We've now proven that every element of $\mathrm{Isom}(\mathbb{Z})$ is either a translation t_a or of the form $t_a \circ s$ (with $a \in \mathbb{Z}$ in either case). That is all symmtries of $\mathbb{Z}$ are of the form $n \mapsto n + a$ or of the form $n \mapsto a - n$.

It is worth reflecting at this point on some key facts we've used in the argument above which is sometimes known as a 'nailing to the wall argument'.

(1) We've used that the composition of two symmetries of the integers is itself a symmetry of the integers. In fact, we've only used this for some special cases but it is true in general since if $f, g \in \mathrm{Isom}(\mathbb{Z})$ and $n, m \in \mathbb{Z}$ then
$$|f(g(n)) - f(g(m))| = |g(n) - g(m)| = |n - m|.$$
We might note that for $a, n \in \mathbb{Z}$,
$$s(t_a(n)) = s(n + a) = -a - n = t_{-a}(s(n))$$
and so $s \circ t_a = t_{-a} \circ s$. Thus order of composition matters.
(2) We've used that there is a 'do nothing' symmetry of the integers id and that for any other symmetry f, $f \circ \mathrm{id} = f = \mathrm{id} \circ f$.
(3) We've used that symmetries are 'undo-able', that is that given any symmetry f there is a symmetry g such that $g \circ f = \mathrm{id} = f \circ g$ (in fact we've only used this for $f = t_a$ and $f = s$ and only that there is a g such that $g \circ f = \mathrm{id}$ but again it is true as stated. (Why?).

(4) We've used that composition of symmetries is associative, that is that for symmetries f, g and h, $(f \circ g) \circ h = f \circ (g \circ h)$.

We'll see that these properties say precisely that $\mathrm{Isom}(\mathbb{Z})$ is a group.

1.2. **Some initial definitions.** First we need to make some definitions.

Definition. Suppose that S is a set. A *binary operation on* S is a function

$$\circ \colon S \times S \to S; (x, y) \mapsto x \circ y.$$

This defintion means that a binary operation is something that takes an ordered pair of elements of S and uses them to produce an element of S. If $x \circ y = y \circ x$ then we say that x and y *commute* (with respect to $\circ$). We say $\circ$ is commutative if every pair of elements of S commute.

Examples.

(1) Composition of functions is a non-commutative binary operation on $\mathrm{Isom}(\mathbb{Z})$.
(2) Addition, multiplication, and subtraction are all binary operations on $\mathbb{Z}$. Note that addition and multiplication are both commutative operations on $\mathbb{Z}$ but distinct integers never commute with respect to subtraction.
(3) Addition and multiplication are also binary operations on $\mathbb{N} := \{1, 2, 3, \ldots\}$. Subtraction is not a binary operation on $\mathbb{N}$ since $2 - 3 \notin \mathbb{N}$.
(4) Exponentiation: $(a, b) \mapsto b^a$ is a binary operation on $\mathbb{N}$.
(5) If X is any set and $S = \{f : X \to X\}$ is the set of all functions from X to itself then composition of functions is a binary operation on S.

Definition. A binary operation $\circ$ on a set S is *associative* if $(x \circ y) \circ z = x \circ (y \circ z)$ for all $x, y, z \in S$.

This means that when $\circ$ is associative there is a well-defined element $x \circ y \circ z \in S$ i.e. it doesn't matter which of the two $\circ$ we use first. It will be instructive to convince yourself that if $\circ$ is an associative binary operation on S and $w, x, y, z \in S$ then

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

Having done this you should also convince yourself that there is nothing special about four and the obvious generalisation holds for any (finite) number of elements of S whenever $\circ$ is associative. This means that whenever $\circ$ is an associative binary operation we may (and will!) omit brackets, writing for example $w \circ x \circ y \circ z$ without ambiguity. If it is clear what operation we have in mind we will often omit it too, writing $wxyz$, for example.

Examples.

(1) Addition and multiplication are associative when viewed as binary operations on $\mathbb{Z}$ or $\mathbb{N}$. Subtraction is not associative on $\mathbb{Z}$ since $((0-1)-2) = -3$ but $0 - (1 - 2) = 1 \neq -3$.
(2) Exponentiation $(a, b) \mapsto b^a$ is not associative on $\mathbb{N}$ since $2^{3^2} = 2^9$ but $(2^3)^2 = 2^6 \neq 2^9$.
(3) Composition is always an associative operation on the set of functions from X to X since if f, g and h are three such functions and $x \in X$ then

$$((f \circ g) \circ h)(x) = f(g(h(x))) = (f \circ (g \circ h))(x).$$

Definition. A binary operation $\circ$ on a set S *has an identity* if there is some element $e \in S$ such that for all $x \in S$, $e \circ x = x = x \circ e$.

Examples.

(1) 0 is an identity for addition on $\mathbb{Z}$ but addition has no identity on $\mathbb{N}$. 1 is an identity for multiplication on both these sets. Subtraction on $\mathbb{Z}$ does not have an identity since if $e - x = x$ for all $x \in \mathbb{Z}$ then $e = 2x$ for all $x \in \mathbb{Z}$ and this is absurd. Note however that $x - 0 = x$ for all $x \in \mathbb{Z}$. We sometimes say that 0 is a right identity for subtraction to d9escribe this.
(2) $(a, b) \mapsto b^a$ does not have an identity but 1 is a left identity in the obvious sense.
(3) If X is any set then the identity function $\mathrm{id}\colon X \to X; s \mapsto s$ is an identity for composition of functions from X to X.

Lemma. *If a binary operation $\circ$ on a set S has an identity then it is unique.*

□

Lecture 2

Definition. If a binary operation $\circ$ on a set S has an identity e then we say that it *has inverses* if for every $x \in S$ there is some $y \in S$ such that $x \circ y = e = y \circ x$.

Examples.

(1) $+$ on $\mathbb{Z}$ has inverses since for every $n \in \mathbb{Z}$, $n + (-n) = 0 = (-n) + n$. Multiplication does not have inverses on $\mathbb{N}$ or $\mathbb{Z}$ since there is no integer (and therefore no natural number) n such that $2n = 1$.
(2) Multiplication defines an associative binary operation on the rationals $\mathbb{Q}$ with an identity (1) but it still does not have inverses. Although for every non-zero rational q, $1/q$ is also rational and $q \cdot 1/q = 1 = 1/q \cdot q$, 0 is also rational and there is no rational r such that $r \cdot 0 = 1$. However multiplication does have inverses on the set $\mathbb{Q}\backslash\{0\}$.
(3) In general composition on the set of functions $X \to X$ does not have inverses. For example the function $f\colon \mathbb{Z} \to \mathbb{Z}; n \mapsto 0$ has no inverse since if $g\colon \mathbb{Z} \to \mathbb{Z}$ were an inverse then we'd have $f(g(n)) = n$ for all $n \in \mathbb{Z}$ but in fact however g is defined $f(g(1)) = 0$. This idea can be adapted to show that whenever $|X| > 1$ there is a function $f\colon X \to X$ that has no inverse.

Definition. A set G equipped with a binary operation $\circ$ is a *group* if

(i) the operation $\circ$ is associative;
(ii) the operation $\circ$ has an identity;
(iii) the operation $\circ$ has inverses.

Examples.

(1) $\mathrm{Isom}(\mathbb{Z})$ is a group (under composition).
(2) $(\mathbb{Z}, +)$ is a group since $+$ is associative and has an identity and inverses.
(3) $(\mathbb{N}, +)$ is not a group since it does not have an identity.
(4) $(\mathbb{Z}, -)$ is not a group since $-$ is not associative.[2]
(5) $(\mathbb{Z}, \cdot)$ is not a group since it does not have inverses but $(\mathbb{Q}\backslash\{0\}, \cdot)$ is a group.

[2]recall that it also does not have an identity but to see that it is not a group it suffices to see that any one of the three properties fails.

(6) If X is a set with more than one element then the set of functions $X \to X$ is not a group under composition of functions since not all such functions have inverses.

We will sometimes say that G is a group without specifying the operation $\circ$. This is laziness and the operation will always be implicit and either clear what it is (in concrete settings) or unimportant what it is (in abstract settings). We'll nearly always call the identity of a group e (or e_G if we want to be clear which group it is the identity for) if we don't know it by some other name.

Definition. We say that a group G is *abelian* if any pair of elements of G commute.

Definition. We say that a group G is *finite* if it has finitely many elements as a set. We call the number of elements of a finite group G the *order* of G written $|G|$.

Example. For every integer $n \geqslant 1$ we can define a group that is the set $\mathbb{Z}_n := \{0, 1, \dots, n-1\}$ equipped with the operation $+_n$ where $x +_n y$ is the remainder after dividing $x + y$ by n[3]. It is straightforward to see that $\mathbb{Z}_n$ is an abelian group of order n.

Lemma. *Suppose that G is a group.*

(i) inverses are unique i.e. if $g \in G$ there is precisely one element g^{-1} in G such that $g^{-1}g = e = gg^{-1}$;
(ii) for all $g \in G$, $(g^{-1})^{-1} = g$;
(iii) for all $g, h \in G$, $(gh)^{-1} = h^{-1}g^{-1}$ (the shoes and socks lemma).

□

Notation. For each element g in a group G and natural number n we define g^n recursively by $g^1 := g$ and $g^n := gg^{n-1}$ for $n > 1$. We'll also write $g^0 := e$ and $g^n := (g^{-1})^{-n}$ for integers $n < 0$. It follows that $g^a g^b = g^{a+b}$ for all $a, b \in \mathbb{Z}$.

Definition. If G is a group then we say that $g \in G$ has *finite order* if there is a natural number n such that $g^n = e$. If g has finite order, we call the smallest natural number n such that $g^n = e$ the *order* of g and write $o(g) = n$.

1.3. Further geometric examples.

1.3.1. *Symmetry groups of regular polygons.* Suppose we want to consider the set D_{2n} of all symmetries of a regular polygon P with n vertices (for $n \geqslant 3$) living in the complex plane $\mathbb{C}$. By symmetry of P we will mean a distance preserving transformation of the plane that maps P to itself. We might as well assume that the centre of P is at the origin 0 and that one of the vertices is the point $1 = 1 + 0i$[4].

Proposition. *D_{2n} is a group of order $2n$ under composition.*

□

Lecture 3

1.3.2. *Symmetry groups of regular solids.* Suppose that X is a regular solid in $\mathbb{R}^3$. We can consider $\mathrm{Sym}(X)$, the group of distance preserving transformations ρ of $\mathbb{R}^3$ such that $\rho(X) = X$. These form a group. We will consider the cases X a tetrahedron and X a cube later in the course.

[3] $\mathbb{Z}_{12}$ is familiar from everyday life. When is it used?

[4] we'll be able to make precise why this assumption is reasonable later but it should at least seem reasonable already.

1.3.3. *The Symmetric group.* We might hope that given any set X the set of *invertible* functions from X to X forms a group under composition; that is the set of functions $f\colon X \to X$ such that there is some $g\colon X \to X$ such that $f \circ g = \mathrm{id} = g \circ f$. This is true but not immediate: we need to check that composition of functions is a binary operation on this set; that is that the composition of two invertible functions is invertible. Some people would say that we need to check that the binary operation is *closed* but 'closure' is built into our definition of binary operation.

Lemma. *Suppose that $f_1, f_2\colon X \to X$ are invertible. Then $f_1 \circ f_2\colon X \to X$ is invertible.*

□

It follows that for every set X, the set $S(X) = \{f\colon X \to X \mid f \text{ is invertible}\}$ is a group under the composition of functions. It is called the *symmetric group* on X[5]. We call elements of the symmetric group *permutations of* X. If $X = \{1, \dots, n\}$ we write S_n instead on $S(X)$. We will return to the groups S_n later in the course.

1.4. **Subgroups and homomorphisms.** Sometimes when considering the symmetries of an object we want to restrict ourselves to considering symmetries that preserve certain additional properties of the object. In fact we've already seen this, the sets of distance preserving transformations of $\mathbb{C}$ and of $\mathbb{R}^3$ are both groups of symmetries under composition. The groups D_{2n} and Sym(X) for X a regular solid are defined to consist of those symmetries that preserve a certain subset of the whole space. Similary, instead of considering D_{2n}, the group of all symmetries of a regular n-gon we might want to restrict only to those symmetries that preserve orientation, that is the rotations. This idea leads us to the notion of subgroup.

Definition. If $(G, \circ)$ is a group then a subset $H \subset G$ is a *subgroup* if $\circ$ restricts to a binary operation on H[6] and $(H, \circ)$ is a group. We write $H \leqslant G$ to denote that H is a subgroup of G.

Examples.

(1) $\mathrm{Isom}(\mathbb{Z}) \leqslant S(\mathbb{Z})$.
(2) $D_{2n} \leqslant \mathrm{Isom}(\mathbb{C}) \leqslant S(\mathbb{C})$.
(3) $\mathrm{Isom}^+(\mathbb{Z}) := \{f\colon \mathbb{Z} \to \mathbb{Z} \mid f(n) - f(m) = n - m \text{ for all } n, m \in \mathbb{Z}\} \leqslant \mathrm{Isom}(\mathbb{Z})$.
(4) $\mathbb{Z}$ is a subgroup of $(\mathbb{Q}, +)$.
(5) If $H \subset D_{2n}$ consists of all rotations of the n-gon then H is a subgroup.
(6) For any $n \in \mathbb{Z}$, $n\mathbb{Z} := \{an \in \mathbb{Z} \mid a \in \mathbb{Z}\}$ is a subgroup of $(\mathbb{Z}, +)$.
(7) For every group G, $\{e\} \leqslant G$ (the *trivial subgroup*) and $G \leqslant G$ (we call a subgroup H of G with $H \neq G$ a *proper subgroup*).

Lecture 4

Lemma (Subgroup criteria)**.** *A subset H of a group G is a subgroup if and only if the following conditions hold*

(i) for every pair of elements $h_1, h_2 \in H$, $h_1 h_2 \in H$;
(ii) the identity $e \in H$;

[5]The name comes from the fact that it can be viewed as the set of symmetries of the set X. This is quite a subtle idea but you might like to think further about it when you come to revise the course

[6]precisely $h_1 \circ h_2 \in H$ for all $h_1, h_2 \in H$

(iii) for every $h \in H$, $h^{-1} \in H$.

□

Remark. Our subgroup criteria contain no mention of associativity since as noted in the proof it is immediate from the associativity of the operation on G.

There is an even shorter set of criteria for a subset to be a subgroup.

Corollary. *A subset H of G is a subgroup precisely if it is non-empty and $h_1^{-1}h_2 \in H$ for all $h_1, h_2 \in H$.*

□

Example. The set $H = \{f \in \mathrm{Isom}(\mathbb{Z}) | f(0) = 0\}$ is a subgroup of $\mathrm{Isom}(\mathbb{Z})$. We can see this using the corollary. Certainly $\mathrm{id}(0) = 0$ so $H \neq \emptyset$. Moreover if $h_1, h_2 \in H$ then

$$h_1^{-1}h_2(0) = h_1^{-1}(0) = h_1^{-1}h_1(0) = \mathrm{id}(0) = 0.$$

Note that this argument isn't much simpler than verifying conditions (i)-(iii) of the lemma in practice.

We will also be interested in maps between groups. However we won't typically be interested an arbitary functions between two groups but only those that respect the structure of the two groups. More precisely we make the following definition.

Definition. If $(G, \circ)$ and $(H, *)$ are two groups then $\theta\colon H \to G$ is a *group homomorphism* (or just *homomorphism*) precisely if $\theta(h_1 * h_2) = \theta(h_1) \circ \theta(h_2)$ for all $h_1, h_2 \in H$.

Definition. A group homomorphism $\theta\colon H \to G$ is an *isomorphism* if θ is invertible as a function; ie if there is a function $\theta^{-1}\colon G \to H$ such that $\theta \circ \theta^{-1} = \mathrm{id}_G$ and $\theta^{-1} \circ \theta = \mathrm{id}_H$.

Examples.

(1) If $H \leqslant G$ then the inclusion map $\iota\colon H \to G; h \mapsto h$ is a group homomorphism. It is not an isomorphism unless $H = G$.
(2) The function $\theta\colon \mathbb{Z} \to \mathbb{Z}_n$ such that $\theta(a)$ is the remainder after dividing a by n is always a homomorphism from $(\mathbb{Z}, +)$ to $(\mathbb{Z}_n, +_n)$ but never an isomorphism.
(3) If G is any group and $g \in G$ is any element then $\theta\colon \mathbb{Z} \to G$; $n \mapsto g^n$ is a homomorphism from $(\mathbb{Z}, +)$ to G. Indeed every homomorphism from $(\mathbb{Z}, +)$ to G arises in this way.
(4) $\theta\colon \mathbb{Z} \to \mathrm{Isom}^+(\mathbb{Z})$; $n \mapsto t_n$[7] is an isomorphism.
(5) The exponential function defines an isomorphism

$$\exp\colon (\mathbb{R}, +) \to (\{r \in \mathbb{R} \mid r > 0\}, \cdot); a \mapsto e^a.$$

The inverse map is given by $\log = \log_e$.

If you are alert you will be asking why we don't require homomorphisms $\theta\colon H \to G$ to satisfy $\theta(e_H) = e_G$ and $\theta(h^{-1}) = \theta(h)^{-1}$ for all $h \in H$. The following lemma shows that this is because these properties follow from our definition.

Lemma. *Suppose that $\theta\colon H \to G$ is a group homomorphism.*
(i) $\theta(e_H) = e_G$.

[7] recall t_n denotes translation by n

(ii) For all $h \in H$, $\theta(h^{-1}) = \theta(h)^{-1}$.

□

Definition. If $\theta\colon H \to G$ is a group homomorphism then the *kernel of* θ is defined by

$$\ker\theta := \{h \in H \mid \theta(h) = e_G\}$$

and the *image of* θ is defined by

$$\operatorname{Im}\theta := \theta(H).$$

Proposition. *If $\theta\colon H \to G$ is a homomorphism then $\ker\theta$ is a subgroup of H and $\operatorname{Im}\theta$ is a subgroup of G.*

□

Lecture 5

Theorem (Special case of the isomorphism theorem)**.** *A group homomorphism $\theta\colon H \to G$ is an isomorphism if and only if $\ker\theta = \{e_H\}$ and $\operatorname{Im}\theta = G$. In this case, $\theta^{-1}\colon G \to H$ is a group homomorphism (and so also an isomorphism).*

□

Lemma. *The composite of two group homomorphisms is a group homomorphism. In particular the composite of two isomorphisms is an isomorphism.*

□

Definition. We say that a group G is *cyclic* if there is a homomorphism $f\colon \mathbb{Z} \to G$ such that $\operatorname{Im} f = G$. Given such a homomorphism f we call $f(1)$ a *generator* of G.

Note that G is cyclic with generator g if and only if every element of G is of the form g^i with $i \in \mathbb{Z}$. More generally we say that a subset S of G *generates* G if every element of G is a product of elements of S and their inverses — that is if G the unique smallest subgroup of G containing S[8].

Examples.

(1) The identity map $\mathrm{id}\colon \mathbb{Z} \to \mathbb{Z}$; $n \mapsto n$ and the 'reflection about 0' map $s\colon \mathbb{Z} \to \mathbb{Z}$; $n \mapsto -n$ are both homomorphisms with image $\mathbb{Z}$. Thus $\mathbb{Z}$ is cyclic and both 1 and -1 are generators. No other element generates $\mathbb{Z}$.
(2) $\mathbb{Z}_n$ is cyclic. In Numbers and Sets it is proven that an element of $\{0, 1, \ldots, n-1\}$ generates $\mathbb{Z}_n$ if and only if it is coprime to n[9]. The 'if' part is a conseqeunce from Euclid's algorithm; the only if part is elementary.

Lemma. *Suppose that G is a group containing an element g with $g^n = e$. There is a unique group homomorphism $f\colon \mathbb{Z}_n \to G$ such that $f(1) = g$. In particular every group of order n with an element of order n is isomorphic to $\mathbb{Z}_n$.*

□

Notation. We'll write C_n for any group that is cyclic of order n. We've verified that any two such groups are isomorphic.

[8]The curious will be reflecting on why G should have a unique smallest subgroup containing S. Their reflections will do them good

[9]Recall that non-negative integers a, b are coprime if and only if their only common factor is 1.

Recall that we showed that $D_{2n} = \{r^i, r^i s \mid i = 0, 1, \dots, n-1\}$ where r denotes a rotation by $2\pi/n$ and s denotes a reflection. And that

$$\begin{aligned} r^k \cdot r^l &= r^{k+_n l}, \\ r^k \cdot r^l s &= r^{k+_n l} s, \\ r^k s \cdot r^l &= r^{k+_n (-l)} s \text{ and} \\ r^k s \cdot r^l s &= r^{k+_n (-l)}. \end{aligned}$$

Lemma. *Let $n > 2$ and suppose that G is a group containing elements g, h such that $g^n = e$, $h^2 = e$ and $hgh^{-1} = g^{-1}$. There is a unique group homomorphism $f\colon D_{2n} \to G$ such that $f(r) = g$ and $f(s) = h$. Moreover if $o(g) = n$ and $|G| = 2n$ then f is an isomorphism.*

□

Lecture 6

1.5. **The Möbius Group.** Informally, a Möbius transformation is a function $f\colon \mathbb{C} \to \mathbb{C}$ of the form

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

with $a, b, c, d \in \mathbb{C}$ and $ad - bc \neq 0$. The reason for the condition $ad - bc \neq 0$ is that for such a function if $z, w \in \mathbb{C}$ then

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

so f would be constant if $ad - bc$ were 0.[10]

Unfortunately the function is not well defined if $z = -d/c$ since we may not divide by zero in the complex numbers. This makes composition of Möbius transformations problematic since the image of one Möbius transformation may not coincide with the domain of defintion of another. We will fix this by adjoining an additional point to $\mathbb{C}$ called ∞.[11]

Notation. Let $\mathbb{C}_\infty := \mathbb{C} \cup \{\infty\}$ which we call the *extended complex plane*.

Definition. Given $(a, b, c, d) \in \mathbb{C}^4$ such that $ad - bc \neq 0$ we can define a function $f\colon \mathbb{C}_\infty \to \mathbb{C}_\infty$ as follows:

if $c \neq 0$ then

$$f(z) := \begin{cases} \frac{az+b}{cz+d} & \text{if} \quad z \in \mathbb{C}\backslash\{-d/c\}; \\ \infty & \text{if} \quad z = -d/c; \\ a/c & \text{if} \quad z = \infty; \end{cases}$$

if $c = 0$ then

$$f(z) := \begin{cases} \frac{az+b}{cz+d} & \text{if} \quad z \in \mathbb{C} \\ \infty & \text{if} \quad z = \infty. \end{cases}$$

We call all functions from $\mathbb{C}_\infty$ to $\mathbb{C}_\infty$ that arise in this way *Möbius transformations* and let

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

[10] This is bad because we're really interested in invertible functions

[11] And pronounced 'infinity'.

We'll see another way to interpret this definition later in the course involving projective geometry. But for now we'll work with it as it stands and also take for granted a result that will will prove later.[12]

Theorem. *The set $\mathcal{M}$ defines a subgroup of $S(\mathbb{C}_\infty)$.*

Lemma. *Suppose that $f \in \mathcal{M}$ such that $f(0) = 0$, $f(1) = 1$ and $f(\infty) = \infty$. Then $f = \mathrm{id}$.*

□

Theorem (Strict triple transitivity of Möbius transformations)**.** *If (z_1, z_2, z_3) and (w_1, w_2, w_3) are two sets of three distinct points then there is a unique $f \in \mathcal{M}$ such that $f(z_i) = w_i$ for $i = 1, 2$ and 3.*

□

Definition. Given distinct points $z_1, z_2, z_3, z_4 \in \mathbb{C}_\infty$ the *cross-ratio* of z_1, z_2, z_3, z_4 written $[z_1, z_2, z_3, z_4] := f(z_4)$ where f is the unique Möbius transformation such that $f(z_1) = 0$, $f(z_2) = 1$ and $f(z_3) = \infty$.[13]

Lemma. *If $z_1, z_2, z_3, z_4 \in \mathbb{C}$ then $[z_1, z_2, z_3, z_4] = \frac{(z_4 - z_1)(z_2 - z_3)}{(z_2 - z_1)(z_4 - z_3)}$.*[14]

□

Theorem (Invariance of Cross-Ratio)**.** *For all $z_1, z_2, z_3, z_4 \in \mathbb{C}_\infty$ and $g \in \mathcal{M}$, $[g(z_1), g(z_2), g(z_3), g(z_4)] = [z_1, z_2, z_3, z_4]$.*

□

Proposition. *Every element of $\mathcal{M}$ is a composite of Möbius transformations of the following forms.*

(a) $D_a \colon z \mapsto az = \frac{az+0}{0z+1}$ *with* $a \in \mathbb{C}\backslash\{0\}$ *(rotation/dilations);*
(b) $T_b \colon z \mapsto z + b = \frac{1z+b}{0z+1}$ *with* $b \in \mathbb{C}$ *(translations);*
(c) $S \colon z \mapsto 1/z = \frac{0z+1}{1z+0}$ *(inversion).*

□

Lecture 7

Definition. A *circle* in $\mathbb{C}_\infty$ is a subset that is either of the form $\{z \in \mathbb{C} \mid |z-a| = r\}$ for some $a \in \mathbb{C}$ and $r > 0$[15] or of the form $\{z \in \mathbb{C} \mid a\mathrm{Re}(z) + b\mathrm{Im}(z) = c\} \cup \{\infty\}$ for some $a, b, c \in \mathbb{R}$ with $(a, b) \neq (0, 0)$[16]

It follows that any three distinct points in $\mathbb{C}_\infty$ determine a unique circle in $\mathbb{C}_\infty$.

---

[12] There is a straight-forward if slightly fiddly way to prove it directly that demands care with the point ∞. We will give a slightly more sophisticated but less fiddly proof.

[13] There are 6 essentially different definitions of cross-ratio depending on how we order 0, 1 and ∞ in this definition. It doesn't really matter which we choose as long as we are consistent.

[14] We could've defined the cross-ratio by this formula but we'd need to be more careful when some $z_i = \infty$.

[15] i.e. a usual circle in $\mathbb{C}$

[16] i.e. a line in $\mathbb{C}$ together with ∞

Lemma. *The general equation of a circle in $\mathbb{C}_\infty$ is*

$$Az\bar{z} + B\bar{z} + \bar{B}z + C = 0$$

with $A, C \in \mathbb{R}$, $B \in \mathbb{C}$ and $AC < |B|^2$.[17]

□

Theorem (Preservation of circles)**.** *If $f \in \mathcal{M}$ and C is a circle in $\mathbb{C}_\infty$ then $f(C)$ is a circle in $\mathbb{C}_\infty$.*

□

Corollary. *Four distinct points z_1, z_2, z_3 and z_4 in $\mathbb{C}_\infty$ lie on a circle if and only if $[z_1, z_2, z_3, z_4] \in \mathbb{R}$.*

□

Remark. It is possible to prove the corollary directly and then use a similar argument to deduce that Möbius transformations preserve of circles from it.

Definition. Given two elements x, y of a group G we say y is *conjugate* to x if there is some $g \in G$ such that $y = gxg^{-1}$.

Note that if $y = gxg^{-1}$ then $x = g^{-1}y(g^{-1})^{-1}$ so the notion of being conjugate is symmetric in x and y. Morever if also $z = hyh^{-1}$ then $z = (gh)x(gh)^{-1}$ so if z is conjugate to y and y is conjugate to x then z is conjugate to x.

Proposition. *Every Möbius transformation f except the identity has precisely one or two fixed points. If f has precisely one fixed point it is conjugate to the translation $z \mapsto z + 1$. If f has precisely two fixed points it is conjugate to a map of the form $z \mapsto az$ with $a \in \mathbb{C}\backslash\{0\}$.*

□

Remark. Suppose that $f \in \mathcal{M}$. If $gfg^{-1} \colon z \mapsto z + 1$ then for each $n \geqslant 0$,

$$gf^n g^{-1} = (gfg^{-1})^n \colon z \mapsto z + n$$

so $f^n(z) = g^{-1}(g(z)+n)$ for $z \in \mathbb{C}_\infty$ not fixed by f. Similarly if $gfg^{-1} \colon z \mapsto az$ then for $n \geqslant 0$, $f^n(z) = g^{-1}(a^n g(z))$ for z not fixed by f. Thus we can use conjugation to compute iterates of $f \in \mathcal{M}$ in a simple manner.

Lecture 8

2. Lagrange's Theorem

2.1. Cosets.

Definition. Suppose that $(G, \circ)$ is a group and H is a subgroup. A *left coset* of H in G is a set of the form $g \circ H := \{g \circ h \mid h \in H\}$ for some $g \in G$. Similarly a *right coset* of H in G is a set of the form $H \circ g := \{hg \mid h \in H\}$ for some $g \in G$. We write G/H to denote the set of left cosets of H in G and $H\backslash G$ to denote the set of right cosets of H in G[18].

As usual we will often suppress the $\circ$ and write gH or Hg.

[17] where ∞ is understood to be a solution of this equation precisely if $A = 0$

[18] This latter is a little unfortunate in the $\backslash$ is normally used to denote set-theoretic difference but this should not cause confusion. Why?

Examples.

(1) Suppose $n \in \mathbb{Z}$, so that $n\mathbb{Z} := \{an \mid a \in \mathbb{Z}\}$ is a subgroup of $(\mathbb{Z}, +)$. Then $0 + n\mathbb{Z} = n\mathbb{Z} = n + n\mathbb{Z}$. $1 + n\mathbb{Z} = \{1 + an \mid a \in \mathbb{Z}\} = (1 - n) + n\mathbb{Z}$. More generally, $b + n\mathbb{Z}$ is the set of integers x such that $x - b$ is a multiple of n.[19]

(2) Suppose that $G = D_6 = \{e, r, r^2, s, rs, r^2s\}$ and $H = \{e, s\}$ then

$$\begin{aligned} eH &= \{e, s\} &&= sH \\ rH &= \{r, rs\} &&= rsH \\ r^2H &= \{r^2, r^2s\} &&= r^2sH. \end{aligned}$$

However,

$$\begin{aligned} He &= \{e, s\} &&= Hs \\ Hr &= \{r, r^2s\} &&= Hr^2s \\ Hr^2 &= \{r^2, rs\} &&= Hrs. \end{aligned}$$

Thus left cosets and right cosets need not agree when the group is not abelian. However if $K = \{e, r, r^2\} \leqslant D_6$ then $K = eK = rK = r^2K = Ke = Kr = Kr^2$ and $\{s, rs, r^2s\} = sK = rsK = r^2sK = Ks = Krs = Kr^2s$. So in this case the left and right cosets are the same.

(3) Suppose that $\mathcal{M}$ is the Möbius group and $H = \{f \in \mathcal{M} \mid f(0) = 0\}$. Then, for $g \in \mathcal{M}$,

$$\begin{aligned} gH &= \{f \in \mathcal{M} \mid f(0) = g(0)\} \text{ whereas} \\ Hg &= \{f \in \mathcal{M} \mid f^{-1}(0) = g^{-1}(0)\}. \end{aligned}$$

We'll return to this idea later in the course.

2.2. **Lagrange's Theorem.**

Theorem (Lagrange's Theorem)**.** *Suppose that G is a group and H is a subgroup of G then the left cosets of H in G partition G. In particular if G is finite then $|H|$ divides $|G|$.*

□

Remark. By a very similar argument the right cosets of H in G also partition G.

Corollary. *If G is a finite group, then every element of G has order dividing $|G|$.*

□

Proposition. *Suppose that p is prime. Then every group of order p is isomorphic to C_p.*

□

2.3. **Groups of order at most 8.** In this section we will classify all groups of order at most 8 under the perspective that two groups are the same precisely if they are isomorphic. We've already seen that every group of order $2, 3, 5$ or 7 is isomorphic to the cyclic group of the same order. It is evident that the trivial group is the only group of order 1 up to isomorphism.

Before we begin this we'll need the following construction that enables us to build new groups from old ones.

[19]Note that because the operation on $\mathbb{Z}$ is addition we don't suppress it when we name cosets, i.e. we write $a + n\mathbb{Z}$ rather than $an\mathbb{Z}$ because the latter would create confusion.

Example. Suppose that G and H are groups. We can define a binary operation on $G \times H$ via $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$ for $g_1, g_2 \in G$ and $h_1, h_2 \in H$. We claim that this makes $G \times H$ into a group.

Proof of claim. Since

$$((g_1, h_1)(g_2, h_2))(g_3, h_3) = (g_1 g_2 g_3, h_1 h_2 h_3) = (g_1, h_1)((g_2, h_2)(g_3, h_3))$$

for all $g_1, g_2, g_3 \in G$ and $h_1, h_2, h_3 \in H$, the operation on $G \times H$ is associative.

Since $(e_G, e_H)(g, h) = (g, h) = (g, h)(e_G, e_H)$, (e_G, e_H) is an identity for the operation on $G \times H$.

Finally since $(g^{-1}, h^{-1})(g, h) = (e_G, e_H) = (g, h)(g^{-1}, h^{-1})$ the operation on $G \times H$ has inverses. □

Exercise. Show that if G_1, G_2 and G_3 are groups then $G_1 \times G_2$ is isomorphic to $G_2 \times G_1$ and $(G_1 \times G_2) \times G_3$ is isomorphic to $G_1 \times (G_2 \times G_3)$.

Lecture 9

Theorem (Direct Product Theorem)**.** *Suppose that $H_1, H_2 \leqslant G$ such that*

(i) $H_1 \cap H_2 = \{e\}$;
(ii) if $h_1 \in H_1$ and $h_2 \in H_2$ then h_1 and h_2 commute;
(iii) for all $g \in G$ there are $h_1 \in H_1$ and $h_2 \in H_2$ such that $g = h_1 h_2$.

Then there is an isomorphism $H_1 \times H_2 \to G$.

□

We also need the following result that also appeared on the first example sheet.

Lemma. *If G is a group such that every non-identity element has order two*[20] *then G is abelian.*

□

We also recall that every a group of order n with an element of order n is isomorphism to C_n and that every group of order $2n$ that has an element g of order n and an element h of order 2 such that $hg = g^{-1}h$ is isomorphic to D_{2n}.

Proposition. *Every group of order 4 is isomorphic to precisely one of C_4 and $C_2 \times C_2$.*

□

Proposition. *Every group of order 6 is isomorphic to precisely one of C_6 or D_6.*

□

Example. The following set of matrices form an non-abelian group Q_8 of order 8

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

It is common to write

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ and } \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Then $Q_8 = \{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$. Then we can compute that $\mathbf{1}$ is an identity, $-\mathbf{1}$ has order 2 commutes with everything and multiplies as you'd expect given the notation.

[20] Of course in any group the identity has order 1

Morever $\mathbf{i}, \mathbf{j}$ and $\mathbf{k}$ all have order 4 (all of them square to $-\mathbf{1}$), $\mathbf{ij} = \mathbf{k} = -\mathbf{ji}$, $\mathbf{ki} = \mathbf{j} = \mathbf{ik}$ and $\mathbf{jk} = \mathbf{i} = -\mathbf{kj}$.

Exercise. Verify that Q_8 is a group.

Lecture 10

Proposition. *Every group of order* 8 *is isomorphic to precisely one of* C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_8 *or* Q_8.

□

2.4. The Quaternions.

Definition. The *quaternions* are the set of matrices

$$\mathbb{H} := \{a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{R}\} \subset \mathrm{Mat}_2(\mathbf{C})$$

where as before

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ and } \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

The sum or product of two elements of $\mathbb{H}$ lives in $\mathbb{H}$ and $+$ and $\cdot$ obey the same associativity and distributivity laws as $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ with identities 0 and $\mathbf{1}$ respectively. Although the multiplication in $\mathbb{H}$ is not commutative (since $\mathbf{ij} = -\mathbf{ji}$), $(\mathbf{H}, +)$ is an abelian group and $(\mathbf{H}\backslash\{0\}, \cdot)$ is a (non-abelian) group.[21] To see the latter we can define 'quaternionic conjugation' by

$$(a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})^* = a\mathbf{1} - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$$

and then verifying that if $x = a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ then

$$xx^* = x^*x = (a^2 + b^2 + c^2 + d^2)\mathbf{1}$$

so $x^{-1} = \frac{1}{a^2+b^2+c^2+d^2}x^*$ for $x \neq 0$.

2.5. Fermat–Euler theorem.

We can define a multiplication operation on the set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ by setting $a \cdot_n b$ to be the remainder after dividing ab by n.

Definition. Let $U_n := \{a \in \mathbb{Z}_n \mid \exists b \in \mathbb{Z}_n \text{ s.t. } a \cdot_n b = 1\}$ be the set of invertible elements of $\mathbb{Z}_n$ with respect to $\cdot_n$.

It is a result from Numbers and Sets that follows from Euclid's algorithm that $|U_n| = \varphi(n)$ where $\varphi(n)$ denotes the number of elements of $\mathbb{Z}_n$ coprime to n. Indeed $U_n = \{a \in \mathbb{Z}_n \mid (a, n) = 1\}$.

Lemma. $(U_n, \cdot_n)$ *is an abelian group.*

□

Theorem (Fermat–Euler Theorem)**.** *If* $(a, n) = 1$ *then* $a^{\varphi(n)} \equiv 1 \mod n$.

□

[21] We say that $\mathbb{H}$ is a division algebra. $\mathbb{R}, \mathbb{C}$ and $\mathbb{H}$ are the only division algebras that are finite dimensional as vector spaces over $\mathbb{R}$.

Lecture 11

3. Group Actions

We started the course by saying that groups are fundamentally about symmetry but the connection has been opaque for the last three lectures. In this chapter we will discuss how to recover the notion of symmetry from the group axioms.

3.1. **Definitions and examples.**

Definition. An *action* of a group G on a set X is a function

$$\cdot\colon G \times X \to X; (g, x) \mapsto g \cdot x$$

such that for all $x \in X$

(i) $e \cdot x = x$;
(ii) $g \cdot (h \cdot x) = (gh) \cdot x$ for all $g, h \in G$.

Examples.

(1) $\mathrm{Isom}(\mathbb{Z})$ acts on $\mathbb{Z}$ via $f \cdot n = f(n)$.
(2) The Möbius group $\mathcal{M}$ acts on the extended complex plane $\mathbb{C}_\infty$ via $f \cdot z = f(z)$.
(3) Generalising both the examples above, if $H \leqslant S(X)$ then H acts on X via $h \cdot x = h(x)$. We call this the *natural action* of H on X.
(4) $\mathcal{M}$ also acts on the set of circles in $\mathbb{C}_\infty$. We proved in §1.5 that if $f \in \mathcal{M}$ and $C \subset \mathbb{C}_\infty$ is a circle then $f(C) \subset \mathbb{C}_\infty$ is also a circle so $(f, C) \mapsto f(C)$ is a function. Moreover for all circles C the conditions $\mathrm{id}(C) = C$ and $f(g(C)) = (fg)(C)$ for $f, g \in \mathcal{M}$ are both clear.
(5) D_{2n} acts on the set of points a regular n-gon. D_{2n} also acts on the set of vertices of a regular n-gon and on the set of edges of a regular n-gon.
(6) If X is a regular solid then $\mathrm{Sym}(X)$ acts on the set of points (and on the sets of vertices/edges/faces) of X.
(7) If $H \leqslant G$ then G acts on G/H, the set of left cosets of G in H via $g \cdot kH = gkH$ for $g, k \in G$. To see this we need to check that if $kH = k'H$ then $gkH = gk'H$. But if $kH = k'H$ then $k' = kh$ for some $h \in H$ so $gk' = gkh \in gk'H \cap gkH$ and $gkH = gk'H$ by Lagrange. Given this we see that for all $k \in G$, $ekH = kH$ and $g_1(g_2kH) = (g_1g_2)kH$ for all $g_1, g_2 \in G$.
(8) For any group G and set X we can define the *trivial action* via $g \cdot x = x$ for all $g \in G$ and $x \in X$.

Theorem. *For every group G and set X there is a $1-1$ correspondence*

$$\{\textit{actions of } G \textit{ on } X\} \longleftrightarrow \{\theta\colon G \to S(X) \mid \theta \textit{ is a homomorphism}\}$$

such that an action $\cdot\colon G \times X \to X$ corresponds to the homomorphism $\theta\colon G \to S(X)$ given by $\theta(g)(x) = g \cdot x$.

□

Definition. We say that an action of G on X is *faithful* if the kernel of the corresponding homomorphism $G \to S(X)$ is the trivial group.

3.2. **Orbits and Stabilisers.**

Definition. Suppose a group G acts on a set X and that $x \in X$. The *orbit* of x under the action is given by

$$\mathrm{Orb}_G(x) := \{g \cdot x \mid g \in G\} \subset X.$$

The *stabiliser* of x under the action is given by

$$\mathrm{Stab}_G(x) := \{g \in G \mid g \cdot x = x\} \subset G.$$

Thus an action is faithful precisely if $\bigcap_{x \in X} \mathrm{Stab}_G(x) = \{e\}$.

Examples.

(1) Under the natural action of $\mathrm{Isom}(\mathbb{Z})$ on $\mathbb{Z}$, for all $n \in \mathbb{Z}$

$$\mathrm{Orb}_{\mathrm{Isom}(\mathbb{Z})}(n) = \mathbb{Z}$$

and

$$\mathrm{Stab}_{\mathrm{Isom}(\mathbb{Z})} = \{\mathrm{id}, m \mapsto 2n - m\}$$

(2) Under the natural action of $\mathcal{M}$ on $\mathbb{C}_\infty$, for all $z \in \mathbb{C}_\infty$

$$\mathrm{Orb}_{\mathcal{M}}(z) = \mathbb{C}_\infty$$

and

$$\mathrm{Stab}_{\mathcal{M}}(\infty) = \left\{ z \mapsto \frac{az + b}{0c + d} \mid ad \neq 0 \right\}.$$

(3) Under the action of D_{2n} on the set of points of a regular n-gon the orbit of a vertex of the n-gon is the set of all vertices of the n-gon and the stabliser of a vertex consists of the identity and reflection in the line through the centre of the n-gon and the vertex.[22]

(4) For the left coset action of G on G/H defined earlier

$$\mathrm{Orb}_G(eH) = G/H$$

and

$$\mathrm{Stab}_G(eH) = \{g \in G \mid gH = eH\} = H.$$

More generally

$$\mathrm{Stab}_G(kH) = \{g \in G \mid gkH = kH\} = \{g \in G \mid k^{-1}gkH = H\} = kHk^{-1}.$$

(5) For the trivial action of G on X and any $x \in X$,

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

Lemma. *Suppose that G is a group acting on a set X.*

(i) Each stabiliser $\mathrm{Stab}_G(x)$ is a subgroup of G.

(ii) The orbits $\mathrm{Orb}_G(x)$ partition X. In particular if X is finite and the distinct orbits are $\mathcal{O}_1, \ldots, \mathcal{O}_m$ then

$$|X| = \sum_{i=1}^{m} |\mathcal{O}_i|$$

□

[22] It would be instructive to think about what the orbits and stabilisers of other points of n-gon are under the action of D_{2n}.

Lecture 12

Definition. We say that an action of G on X is *transitive* if there is only one orbit i.e. if $X = \mathrm{Orb}_G(x)$ for any $x \in X$.

Theorem (Orbit-Stabiliser Theorem)**.** *Suppose a group G acts on a set X and $x \in X$. There is a (natural) invertible function*

$$G/\operatorname{Stab}_G(x) \to \mathrm{Orb}_G(x).$$

In particular if G is finite

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

□

Examples.

(1) For the natural action of $\mathrm{Isom}(\mathbb{Z})$ on $\mathbb{Z}$ the set of left cosets of $\mathrm{Stab}_{\mathrm{Isom}(\mathbb{Z})}(0) = \{e, n \mapsto -n\}$ in $\mathrm{Isom}(\mathbb{Z})$ is in bijection with $\mathbb{Z}$. We secretly used this fact when we computed $\mathrm{Isom}(\mathbb{Z})$ in the first lecture.

(2) For the usual action of D_{2n} on the vertices of the n-gon and v such a vertex we see that $|D_{2n}| = |\operatorname{Stab}_{D_{2n}}(v)||\operatorname{Orb}_{D_{2n}}(v)| = 2n$. Again we secretly used this when we computed $|D_{2n}| = 2n$.

(3) The symmetric group S_n acts on $X = \{1, 2, \dots, n\}$ via the natural action $f \cdot x = f(x)$. Then $\mathrm{Orb}_{S_n}(n) = X$ since for each $i \in X$ the function $f_i \colon X \to X$; $f_i(i) = n$, $f_i(n) = i$, $f_i(x) = x$ for $x \notin \{i, n\}$ is an element of S_n. Thus $|S_n| = n \operatorname{Stab}_{S_n}(n)$. But $\mathrm{Stab}_{S_n}(n)$ is isomorphic to S_{n-1} by restricting $f \in S_n$ that fixes n to a permutation of $\{1, \dots, n-1\}$. Thus $|S_n| = n|S_{n-1}|$. Since $|S_1| = 1$[23] we deduce that $|S_n| = n!$.

Lecture 13

Fact. If $f \colon \mathbb{R}^3 \to \mathbb{R}^3$ is an isometry that fixes 4 non-coplanar points then f is the identity.

(4) Let X be a regular tetrahedron. Then $\mathrm{Sym}(X)$ acts transitively on the set of 4 vertices of X and the stabiliser of a vertex $v \in X$ consists of three rotations and three reflections. Thus $|\operatorname{Sym}(X)| = 6 \cdot 4 = 24$.

This calculation enables us to prove that $\mathrm{Sym}(X) \simeq S_4$: if we label the vertices by the numbers $1, 2, 3, 4$ then the action of $\mathrm{Sym}(X)$ on the vertices defines a homomorphism $\theta \colon \mathrm{Sym}(X) \to S_4$. Since any isometry of $\mathbb{R}^3$ fixing all four vertices is the identity we can conclude that $\ker\theta = \{\mathrm{id}\}$. By counting we can deduce $\operatorname{Im}\theta = S_4$.

(5) Let X be a cube. Then $\mathrm{Sym}(X)$ acts transitively on the set of 6 faces of X and the stabiliser $H := \mathrm{Stab}_{\mathrm{Sym}(X)}(F)$ of a face F acts transitively on the set of 4 vertices contained in it[24]. If v is one of these vertices and w is the diagonally opposite vertex in F then

$$\mathrm{Stab}_H(v) = \{e, \text{reflection in plane containing } v, w \text{ and the centre of } X\}^{25}.$$

[23] Or if you prefer $|S_0| = 1$

[24] This can be seen by considering rotations about an axis through the centre of F and the centre of its opposite face.

[25] Since if an isometry of $\mathbb{R}^3$ fixes all vertices of F and the centre of X then it is the identity.

Thus

$$\mathrm{Sym}(X) = 6|H| = 6 \cdot |\operatorname{Orb}_H(v)||\operatorname{Stab}_H(v)| = 6 \cdot 4 \cdot 2 = 48.$$

3.3. **Conjugacy classes.**

Definition. If G is a group then the *conjugation action* of G on itself is given by $\cdot\colon G \times G \to G$; $g \cdot x = gxg^{-1}$.

Note that the conjugation action is indeed an action since for $g, h, x \in G$,

$$e \cdot x = exe^{-1} = x$$

and

$$g \cdot (h \cdot x) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = (gh) \cdot x.$$

Definition. The orbits of G on itself under the conjugation action are called the *conjugacy classes* of G: the orbit of $x \in G$ will be denoted $\mathrm{ccl}(x)$; i.e.

$$\mathrm{ccl}(x) = \{gxg^{-1} \mid g \in G\}.^{26}$$

The stabliser of $x \in G$ under this action is called the *centraliser* of x and will be denoted $C_G(x)$.

Examples.

(1) Suppose $G = \mathrm{Isom}(\mathbb{Z}) = \{t_a\colon n \mapsto a + n, s_a\colon n \mapsto a - n \mid a \in \mathbb{Z}\}$. Let $H := \{t_a \mid a \in \mathbb{Z}\}$ denote the subgroup of translations We know that for any $a, b \in \mathbb{Z}$,

$$t_b t_a t_b^{-1} = t_a$$

and for $n \in \mathbb{Z}$,

$$s_b t_a s_b^{-1}(n) = s_b t_a(b - n) = s_b(a + b - n) = n - a$$

ie

$$s_b t_a s_b^{-1} = t_{-a}$$

so for $a \neq 0$

$$C_G(t_a) = H \text{ and } \mathrm{ccl}(t_a) = \{t_a, t_{-a}\}^{27}.$$

Similarly for $n \in \mathbb{Z}$

$$t_b s_a t_b^{-1}(n) = t_b s_a(n - b) = t_b(a - (n - b)) = (2b + a - n) = s_{2b+a}(n)$$

and

$$s_b s_a s_b^{-1}(n) = s_b s_a(b - n) = s_b(a - (b - n)) = b - (a + n - b) = 2b - a - n = s_{2b-a}(n)$$

so as $a \equiv -a \mod 2$

$$C_G(s_a) = \{t_0, s_a\} \text{ and } \mathrm{ccl}(s_a) = \{s_{a+2b} \mid b \in \mathbb{Z}\}.$$

That is there are two conjugacy classes of reflections $\mathrm{ccl}(s_0)$ and $\mathrm{ccl}(s_1)$.[28]

---

[26] Since conjugacy classes are orbits of an action they partition G; that is every element of G lies in precisely one conjugacy class.

[27] Of course $C_G(t_0) = G$ and $\mathrm{ccl}(t_0) = \{t_0\}$.

[28] What is the geometric meaning of this?

(2) We saw in section 1.5 that in the Möbius group $\mathcal{M}$ the conjugacy class of $z \mapsto z+1$ consists of all Möbius transformations with precisely one fixed point i.e.

$$\mathrm{ccl}(z \mapsto z+1) = \{f \in \mathcal{M} \mid f \text{ has precisely one fixed point}\}$$

and that every Möbius transformation with precisely two fixed points is in the same conjugacy class as a Möbius transformation of the form $z \mapsto az$. We will return later to the question of when $\mathrm{ccl}(z \mapsto az) = \mathrm{ccl}(z \mapsto bz)$ and what the centralisers of these elements are.[29] Of course $\mathrm{ccl}(\mathrm{id}) = \{\mathrm{id}\}$ and $C_{\mathcal{M}}(\mathrm{id}) = \mathcal{M}$.

Definition. The kernel of the homomorphism $G \to S(G)$ given by the conjugation action of G on itself is called the *centre* of G and written $Z(G)$.

Lemma. *Suppose that G is a group.*

(a) For $x \in G$, $C_G(x) = \{g \in G \mid xg = gx\}$.
(b) $Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\} = \bigcap_{x \in G} C_G(x)$.
(c) $Z(G) = \{g \in G \mid |\mathrm{ccl}(g)| = 1\}$.

□

3.4. **Cayley's Theorem.** Cayley's Theorem will tell us that every group is isomorphic to a subgroup of a symmetric group.

Definition. If G is a group then the *left regular action* of G on itself is given by the function $\cdot\colon G \times G \to G$; $g \cdot x = gx$.

Example. The left regular action of $\mathbb{Z}$ on itself is by translations. i.e. the corresponding homomorphism $\mathbb{Z} \to S(\mathbb{Z})$ is given by $n \mapsto t_n$.[30]

Lemma. *The left regular action of G on G is an action that is both tra nsitive and faithful.*

□

Lecture 14

Theorem (Cayley's Theorem)**.** *If G is a group then G is isomorphic to a subgroup of $S(G)$.*

□

It perhaps should be said that this theorem is simultaneously deep and almost useless. Deep because it tells us that anything satisfying our abstract definition of a group can be viewed as symmetries of something. Almost useless because knowing this doesn't really help prove things about groups.

3.5. **Cauchy's Theorem.**

Theorem (Cauchy's Theorem)**.** *Supppose that p is a prime and G is a finite group whose order is a multiple of p. Then G contains an element of order p.*

□

[29] Spoiler: $\mathrm{ccl}(z \mapsto az) = \mathrm{ccl}(z \mapsto bz)$ if and only if $b \in \{a, 1/a\}$, $C_G(z \mapsto z+1) = \{\text{translations in } \mathcal{M}\}$ and, for $a \neq 1$, $C_G(z \mapsto az) = \{\text{dilations/rotations in } \mathcal{M}\}$. Can you prove these facts now? Hint: if $g(z \mapsto az)g^{-1} = z \mapsto bz$ for $g \in \mathcal{M}$ what can you say about $g(0)$ and $g(\infty)$?

[30] recall t_n denotes translation by n

4. Quotient Groups

4.1. **Normal subgroups.** Suppose that G is a group. Let $\mathscr{P}(G)$ denote the set of subsets of G, i.e. the power set of G. There is a natural binary operation on $\mathscr{P}(G)$ given by

$$AB := \{ab \mid a \in A, b \in B\}.$$

Examples.

(1) If $A \in \mathscr{P}(G)$ then $A\emptyset = \emptyset = \emptyset A$. If A is non-empty then $AG = G = GA$.
(2) If $H \leqslant G$ then the binary operation on $\mathscr{P}(G)$ restricts to a binary operation on $\mathscr{P}(H)$.
(3) If $H \leqslant G$ then the sets $\{g\}H$ are precisely the left cosets gH of H in G.

Lemma. *This operation on $\mathscr{P}(G)$ is associative and has an identity but does not have inverses.*

□

We'll be particularly interested in the product of two cosets under this operation — in particular if $H \leqslant G$ we'd like to use it to put a group structure on the set of left cosets G/H of H in G. If G is abelian then this is straightforward:

$$g_1Hg_2H = \{g_1h_1g_2h_2 \mid h_1, h_2 \in H\} = \{g_1g_2h_1h_2 \mid h_1, h_2 \in H\} = g_1g_2H$$

and one can easily[31] show that this does define a group structure on G/H. However in general things are not so straightforward.

Example. Consider $G = D_6 = \{e, r, r^2, s, rs, r^2s\}$ where r denotes a non-trivial rotation in the group and s a reflection.

If H is the subgroup of rotations $\{e, r, r^2\}$ then the cosets of H in G are H and sH. We can compute

$$\begin{aligned} HH &= H \\ HsH &= sH \\ sHH &= sH \text{ and} \\ sHsH &= H. \end{aligned}$$

So G/H with this operation is isomorphic to C_2.

However if K is the subgroup $\{e, s\}$ of G then

$$rKr^2K = \{r, rs\}\{r^2, r^2s\} = \{e, r^2s, s, r^2\}$$

which is not a left coset of K in G.

Proposition. *Suppose $H \leqslant G$. The product of two left cosets of H in G is always a left coset of H in G if and only if $gHg^{-1} = H$[32] for all $g \in G$. In this case $g_1Hg_2H = g_1g_2H$ for all $g_1, g_2 \in G$.*

□

[31] and we will later

[32] Here gHg^{-1} means $\{g\}H\{g^{-1}\}$

Lecture 15

Remark. Notice that along the way we proved that whenever $gHg^{-1} \subset H$ for all $g \in G$, in fact $gHg^{-1} = H$ for all $g \in G$.

Definition. We say that a subgroup H of a group G is *normal* if $gHg^{-1} = H$ for all $g \in G$.

> **Warning.** To show that a subset of G is a normal subgroup we must show that it is a subgroup as well as that it satisfies the above conditon.

Examples.

(1) If G is abelian then every subgroup is normal.
(2) The group $\mathrm{Isom}^+(\mathbb{Z})$ is normal in $\mathrm{Isom}(\mathbb{Z})$ but the subgroup $\{\mathrm{id}_{\mathbb{Z}}, s\colon n \mapsto -n\}$ is not normal is $\mathrm{Isom}(\mathbb{Z})$.
(3) The subgroup of rotations in D_{2n} is normal in D_{2n} but no subgroup generated by a reflection is normal in D_{2n}.
(4) $\mathrm{Stab}_{\mathcal{M}}(\infty)$ is not a normal subgroup of $\mathcal{M}$.

Lemma. *A subgroup H of a group G is normal if and only if every left coset is a right coset.*[33]

□

Proposition. *If H is a normal subgroup of G then the restriction of the binary operation on $\mathscr{P}(G)$ makes G/H into a group such that $g_1Hg_2H = g_1g_2H$.*

Definition. We call G/H the *quotient group* of G by H.

□

4.2. The isomorphism theorem.

Theorem (The (first) isomorphism theorem)**.** *Suppose that $f\colon G \to H$ is a group homomorphism. Then $\ker f$ is a normal subgroup of G, $\mathrm{Im}\, f$ is a subgroup of H and f induces an isomorphism*

$$\overline{f}\colon G/\ker f \xrightarrow{\simeq} \mathrm{Im}\, f$$

given by $\overline{f}(g \ker f) = f(g)$.

□

Remark. Often a good way to prove that a subset of a group G is a normal subgroup is to show that it is the kernel of some homomorphism from G to another group.

[33] We'll often just say coset in this case.

Lecture 16

Example. The homomorphism $\mathbb{Z} \to \mathbb{Z}_n$ that sends a to the remainder after dividing a by n has kernel $n\mathbb{Z}$ and image $\mathbb{Z}_n$. Thus it induces an isomorphism $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\simeq} \mathbb{Z}_n$.[34]

Example. Let $\theta\colon (\mathbb{R}, +) \to (\mathbb{C}\backslash\{0\}, \cdot)$ be given by $\theta(r) = e^{2\pi i r}$. Then $\theta(r+s) = e^{2\pi i(r+s)} = \theta(r)\theta(s)$ so θ is a homomorphism. Moreover

$$\operatorname{Im}\theta = S^1 := \{z \in \mathbb{C} \mid |z| = 1\},$$

the unit circle in $\mathbb{C}$ and

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

thus we can deduce that $\mathbb{R}/\mathbb{Z} \simeq S^1$.

Example. Let $\theta\colon D_{2n} \to \{\pm 1\}$ such that

$$\theta(g) := \begin{cases} +1 & \text{if} \quad g \text{ is a rotation} \\ -1 & \text{if} \quad g \text{ is a reflection.} \end{cases}$$

Then we can verify that θ is a homomorphism since the product of two reflections or two rotations is a rotation and the product of a rotation and a reflection in either order is a reflection. Moreover $\operatorname{Im}\theta = \{\pm 1\}$ and $\ker\theta$ is the subgroup of all rotations of the regular n-gon. Thus $D_{2n}/\{\text{rotations in } D_{2n}\} \simeq C_2$.

Example (Group-theoretic understanding of qth powers mod p). Let p and q be distinct primes and $G = (\mathbb{Z}_p\backslash\{0\}, \cdot_p)$. Define

$$\theta\colon G \to G; x \mapsto x^q.$$

Then for $x, y \in G$, $\theta(xy) = (xy)^q = x^q y^q = \theta(x)\theta(y)$ i.e. θ is a homomorphism. Then

$$\ker\theta = \{x \in G \mid x^q = 1\} = \{x \in G \mid o(x) = 1 \text{ or } q\}.$$

We now divide into two cases.

First suppose that q is not a factor of $p-1$. Since $|G| = p-1$, G has no elements of order q by Lagrange. Thus $\ker\theta = \{1\}$. It follows that θ induces an isomorphism $G \simeq \operatorname{Im}\theta$. By counting we can conclude that $\operatorname{Im}\theta = G$. In particular we see that every element of $\mathbb{Z}_p$ is a qth power when p is not 1 mod q.

Next suppose that q is a factor of $p-1$. In this case G does have an element of order q by Cauchy's Theorem. Thus $|\ker\theta| \geqslant q$.[35] Since $G/\ker\theta \simeq \operatorname{Im}\theta$ and $|G/\ker\theta| = |G|/|\ker\theta| \leqslant \frac{p-1}{q}$ we see that $\mathbb{Z}_p$ has at most $\frac{p-1}{q} + 1$ qth-powers when p is 1 mod q.[36]

Example. If G acts on a set X and $K = \{g \in G \mid g(x) = x \text{ for all } x \in X\} = \bigcap_{x\in X} \operatorname{Stab}_G(x)$ then the homomorphism $G \to S(X)$ given by the action induces an isomorphism from G/K to a subgroup of $S(X)$. Thus the action of G on X induces a faithful action of G/K on X.[37]

---

[34] The notation $\mathbb{Z}_n$ as we have defined it is rarely used and instead $\mathbb{Z}/n\mathbb{Z}$ is used to describe essentially the same thing.

[35] Since an element of order q generates a subgroup of order q contained in the kernel. In fact it is not too hard to prove that $\ker\theta$ has precisely q elements.

[36] In fact precisely this many.

[37] This means that to understand all actions of a group G it is equivalent to understand all faithful actions of all quotients of G.

Example. Suppose that X is a regular tetrahedron in $\mathbb{R}^3$. X has six edges and each edge has four neighbours.[38] Thus we can partition the set of edges into three pairs with each pair consisting of non-adjacent edges. Let P denote the set of such pairs. Then the action of $\mathrm{Sym}(X)$ on X induces an action on P since if $f \in \mathrm{Sym}(X)$ and v and w are non-adjacent edges of X then $f(v)$ and $f(w)$ are also non-adjacent edges of X. Thus by the last example there is a homomorphism $\theta\colon \mathrm{Sym}(X) \to S(P)$. It is easy to verify by hand that $\mathrm{Im}\,\theta = S(P)$. Then the isomorphism theorem we can deduce that $\mathrm{Sym}(X)/\ker\theta \simeq S(P)$. We showed earlier than $\mathrm{Sym}(X) \simeq S_4$ and it is straightforward to see that $S(P) \simeq S_3$.[39] Thus we can deduce that S_4 has a normal subgroup K such that $S_4/K \simeq S_3$.[40]

Lecture 17

5. Matrix groups

Suppose that throughout this section $\mathbb{F}$ denotes either $\mathbb{R}$ or $\mathbb{C}$.

5.1. **The general and special linear groups.** Let $M_n(\mathbb{F})$ denote the set of $n \times n$ matrices with entries in $\mathbb{F}$.

Here are some facts proven in Vectors and Matrices.

Facts.

(1) Every element A of $M_n(\mathbb{F})$ defines a linear map $\underline{A}\colon \mathbb{F}^n \to \mathbb{F}^n$ via $\underline{A}\colon v \mapsto Av$.[41] Moreover every linear map $\mathbb{F}^n \to \mathbb{F}^n$ arises in this way and A can be recovered from $\underline{A}$ since the ith column of A is $\underline{A}(e_i)$ where e_i denotes the element of $\mathbb{F}^n$ with ith entry 1 and all other entries 0.
(2) $\underline{AB}$ corresponds to the composite $\underline{A} \circ \underline{B}$. Thus associativity of multiplication of (square) matrices follows from associativity of composition of functions $\mathbb{F}^n \to \mathbb{F}^n$.
(3) The matrix I_n with 1s down the main diagonal and 0s elsewhere is an identity for matrix multiplication on $M_n(\mathbb{F})$. Moreover $\underline{I_n} = \mathrm{id}_{\mathbb{F}^n}$.
(4) There is a function $\det\colon M_n(\mathbb{F}) \to \mathbb{F}$ such that A has an inverse in $M_n(\mathbb{F})$ if and only if $\det A \neq 0$. Moreover $\det(AB) = \det(A)\det(B)$ for any $A, B \in M_n(\mathbb{F})$ and $\det I_n = 1$.

Definition. The *general linear group* $GL_n(\mathbb{F}) := \{A \in M_n(\mathbb{F}) \mid \det A \neq 0\}$ is the group of invertible $n \times n$ matrices with entries in $\mathbb{F}$.

Proposition. *$GL_n(\mathbb{F})$ is a group under matrix multiplication.*

□

Remark. There is a natural action of $GL_n(\mathbb{F})$ on $\mathbb{F}^n$ via $(A, v) \mapsto Av$. One can show that the homomorphism $GL_n(\mathbb{F}) \to S(\mathbb{F}^n)$ coming from this action induces an isomorphism $GL_n(\mathbb{F})$ with the subgroup of $S(\mathbb{F}^n)$ consisting of all invertible linear maps $\mathbb{F}^n \to \mathbb{F}^n$.

[38] There are two edges sharing each vertex of a given edge.

[39] Or $S(P) \simeq D_6$ if you prefer

[40] Can you say which elements of S_4 live in K? There must be four of them by Lagrange. If you find this too hard at this stage then try again when you revise the course having studied the groups S_n in more detail.

[41] Recall that $\underline{A}$ is linear means that $\underline{A}(\lambda v + \mu w) = \lambda\underline{A}(v) + \mu\underline{A}(w)$ for all $\lambda, \mu \in \mathbb{F}$ and $v, w \in \mathbb{F}^n$.

Lemma. *The function* $\det\colon GL_n(\mathbb{F}) \to (\mathbb{F}\backslash\{0\}, \cdot)$ *is a group homomorphism with image* $\mathbb{F}\backslash\{0\}$.

□

Definition. The *special linear group* $SL_n(\mathbb{F})$ is the kernel of $\det\colon GL_n(\mathbb{F}) \to \mathbb{F}\backslash\{0\}$ i.e.

$$SL_n(\mathbb{F}) := \{A \in M_n(\mathbb{F}) \mid \det A = 1\}.$$

Remarks.

(1) The action of $GL_n(\mathbb{F})$ on $\mathbb{F}^n$ induces an action of $SL_n(\mathbb{F})$ on $\mathbb{F}^n$ by restriction and the resulting homomorphism $SL_n(\mathbb{F}) \to S(\mathbb{F}^n)$ induces an isomorphism of $SL_n(\mathbb{F})$ with the subgroup of $S(\mathbb{F}^n)$ consisting of volume preserving linear maps $\mathbb{F}^n \to \mathbb{F}^n$.
(2) $SL_n(\mathbb{F})$ a normal subgroup of $GL_n(\mathbb{F}$ and $GL_n(\mathbb{F})/SL_n(\mathbb{F}) \simeq \mathbb{F}\backslash\{0\}$.

Examples.

$$\begin{aligned} GL_2(\mathbb{F}) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc \neq 0 \right\} \text{ and} \\ SL_2(\mathbb{F}) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - dc = 1 \right\} \end{aligned}$$

5.2. **Möbius maps as projective linear transformations.**

Notation. Given $v \in \mathbb{C}^2\backslash\{0\}$ let $[v]$ denote the (unique) line $\{\lambda v \mid \lambda \in \mathbb{C}\}$ through 0 and v in $\mathbb{C}^2$. The set of all such lines is called the *complex projective line* typically written $\mathbb{P}^1(\mathbb{C})$.

The following lemma gives a parameterisation of the elements of $\mathbb{P}^1(\mathbb{C})$.

Lemma. *Every element of* $\mathbb{P}^1(\mathbb{C})$ *is either of the form* $\left[\begin{pmatrix} z \\ 1 \end{pmatrix}\right]$ *with* $z \in \mathbb{C}$ *or* $\left[\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right]$. *Moreover these lines are all distinct.*

□

It follows that we may identify $\mathbb{C}_\infty$ and $\mathbb{P}^1(\mathbb{C})$ via $z \mapsto \left[\begin{pmatrix} z \\ 1 \end{pmatrix}\right]$ for $z \in \mathbb{C}$ and $\infty \mapsto \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right]$.

Proposition. $GL_2(\mathbb{C})$ *acts on* $\mathbb{P}^1(\mathbb{C})$ *via* $(A, [v]) \mapsto [Av]$ *for* $v \in \mathbb{C}^2\backslash\{0\}$.

□

We note that under this action of $GL_2(\mathbb{C})$ on $\mathbb{P}^1(\mathbb{C})$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \left[\begin{pmatrix} z \\ 1 \end{pmatrix}\right] = \left[\begin{pmatrix} az + b \\ cz + d \end{pmatrix}\right] = \left[\begin{pmatrix} \frac{az+b}{cz+d} \\ 1 \end{pmatrix}\right] \text{ when } z \neq -d/c,$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \left[\begin{pmatrix} -d/c \\ 1 \end{pmatrix}\right] = \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right],$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right] = \left[\begin{pmatrix} a \\ c \end{pmatrix}\right] = \left[\begin{pmatrix} \frac{a}{c} \\ 1 \end{pmatrix}\right] \text{ when } c \neq 0, \text{ and}$$

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \cdot \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} \right] = \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} \right].$$

Thus, under the identification of $\mathbb{C}_\infty$ with $\mathbb{P}^1(\mathbb{C})$, the homomorphism

$$\theta \colon GL_2(\mathbb{C}) \to S(\mathbb{C}_\infty)$$

corresponding to this action sends the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to the Möbius map represented by $z \mapsto \frac{az+b}{cz+d}$, and so $\operatorname{Im}\theta = \mathcal{M}$. Thus $\mathcal{M}$ is a subgroup of $S(\mathbb{C}_\infty)$.

Moreover $\ker\theta$ consists of invertible matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ fixing every line through the origin in $\mathbb{C}^2$.

Now

$$\operatorname{Stab}_{GL_2(\mathbb{C})}\left(\left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} \right] \right) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{C}) \mid c = 0 \right\},$$

$$\operatorname{Stab}_{GL_2(\mathbb{C})}\left(\left[\begin{pmatrix} 0 \\ 1 \end{pmatrix} \right] \right) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{C} \mid b = 0 \right\} \text{ and}$$

$$\operatorname{Stab}_{GL_2(\mathbb{C})}\left(\left[\begin{pmatrix} 1 \\ 1 \end{pmatrix} \right] \right) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{C}) \mid a + b = c + d \right\}.$$

Since a Möbius transformation that fixes three distinct points is the identity, $\ker\theta$ is the intersection of these three sets i.e.

$$\ker(GL_2(\mathbb{C}) \to \mathcal{M}) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \neq 0 \right\}$$

is the group of non-zero scalar matrices.[42]

Thus $PGL_2(\mathbb{C}) := GL_2(\mathbb{C})/\{\lambda I \mid \lambda \in \mathbb{C} \neq 0\} \simeq \mathcal{M}$. It is not hard to see that a similar argument shows that $PSL_2(\mathbb{C}) := SL_2(\mathbb{C})/\{\pm I\} \simeq \mathcal{M}$.

We can summarize this discussion with the following theorem.

Theorem. *The action of $GL_2(\mathbb{C})$ on $\mathbb{P}^1(\mathbb{C})$ induces an isomorphism from $PGL_2(\mathbb{C})$ to $\mathcal{M}$. In particular $\mathcal{M}$ is a subgroup of $S(\mathbb{C}_\infty)$.*

Lecture 18

5.3. **Change of basis.** Recall that if $\underline{A}$ is a linear map $\mathbb{F}^n \to \mathbb{F}^n$ corresponding to the matrix A and $e_1, \dots, e_n$ is the standard basis for $\mathbb{F}^n$ then $\underline{A}(e_i) = \sum_{j=1}^n A_{ji} e_j$.

If $f_1, \dots, f_n$ is another basis for $\mathbb{F}^n$ then there is an invertible linear map $\underline{P}$ such that $\underline{P}(e_i) = f_i$ for $i = 1, \dots, n$. i.e. $\underline{P}$ corresponds to the matrix P whose columns $f_1, \dots, f_n$ and $f_i = \sum_{j=1}^n P_{ji} e_j$ for $i = 1, \dots, n$. It follows that for $j = 1, \dots, n$,

$$\sum_{k=1}^n P^{-1}_{kj} f_k = \sum_{k=1}^n P^{-1}_{kj} \sum_{l=1}^n P_{lk} e_l = \sum_{l=1}^n (PP^{-1})_{lj} e_l = e_j.$$

[42] We can see this another way: the kernel of θ is certainly contains in the intersection of these three stabilisers so it would suffice to check that any scalar matrix is in the kernel ie $[\lambda I_2 v] = [v]$ for all non-zero λ in $\mathbb{C}$. Indeed this is how we showed that a Möbius map that fixes 0, 1 and ∞ is the identity in §1.5.

Then

$$\begin{aligned}\underline{A}(f_i) &= \underline{AP}(e_i)\\ &= \sum_{j=1}^{n}(AP)_{ji}e_j\\ &= \sum_{j=1}^{n}(AP)_{ji}(\sum_{k=1}^{n}P^{-1}_{kj}f_k)\\ &= \sum_{k=1}^{n}(P^{-1}AP)_{ki}f_k\end{aligned}$$

Thus $P^{-1}AP$ represents $\underline{A}$ with respect to the basis $f_1, \ldots, f_n$.

Proposition. *$GL_n(\mathbb{F})$ acts on $M_n(\mathbb{F})$ by conjugation.*

□

It is now straightforward to see that two distinct matrices in $M_n(\mathbb{F})$ represent the same linear map with respect to different bases if and only if they are in the same $GL_n(\mathbb{F})$-orbit under this conjugation action.

Example (See Vectors and Matrices). If $\underline{A}\colon \mathbb{C}^2 \to \mathbb{C}^2$ is a linear map then precisely one of the following three things is true:

(i) there is a basis for $\mathbb{C}^2$ such that $\underline{A}$ is represented by a matrix of the form
$$\begin{pmatrix}\lambda & 0\\ 0 & \mu\end{pmatrix}$$
with $\lambda, \mu \in \mathbb{C}$ distinct — in this case $\{\lambda, \mu\}$ is determined by $\underline{A}$[43] but they may appear in either order in the matrix;

(ii) there is a basis for $\mathbb{C}^2$ such that $\underline{A}$ is represented by a matrix of the form
$$\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix}$$
with $\lambda \in \mathbb{C}$ — in this case λ is determined by $\underline{A}$ indeed $\underline{A} = \lambda\,\mathrm{id}_{\mathbb{C}^2}$ and $\underline{A}$ is represented by this matrix with respect to every basis;

(iii) there is a basis for $\mathbb{C}^2$ such that $\underline{A}$ is represented by a matrix of the form
$$\begin{pmatrix}\lambda & 1\\ 0 & \lambda\end{pmatrix}$$
again λ is determined by $\underline{A}$.[44]

We may interpret this group-theoretically: every $GL_2(\mathbb{C})$-orbit in $M_2(\mathbb{C})$ with respect to the conjugation action is one of the following:

$$\mathcal{O}_{\lambda,\mu} := \mathrm{Orb}_{GL_2(\mathbb{C})}\left(\begin{pmatrix}\lambda & 0\\ 0 & \mu\end{pmatrix}\right) \text{ with } \lambda, \mu \in \mathbb{C} \text{ distinct},$$

$$\mathcal{O}^{(1)}_{\lambda} := \mathrm{Orb}_{GL_2(\mathbb{C})}\left(\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix}\right) \text{ with } \lambda \in \mathbb{C} \text{ and}$$

[43] λ and μ are its eigenvalues and the basis vectors are the corresponding eigenvectors

[44] it is the unique eigenvalue of $\underline{A}$ and $\underline{A} \neq \lambda\,\mathrm{id}_{\mathbb{C}}$.

$$\mathcal{O}^{(2)}_\lambda := \mathrm{Orb}_{GL_2(\mathbb{C})}(\left(\begin{pmatrix}\lambda & 1\\ 0 & \lambda\end{pmatrix}\right) \text{ with } \lambda \in \mathbb{C}.$$

These are all disjoint except that $\mathcal{O}_{\lambda,\mu} = \mathcal{O}_{\mu,\lambda}$. More explicitly,

$$\mathcal{O}_{\lambda,\mu} = \{A \in M_2(\mathbb{C}) \mid \det(tI_2 - A) = (t-\lambda)(t-\mu) \text{ for all } t \in \mathbb{C}\},$$

$$\mathcal{O}^{(1)}_\lambda = \{\lambda I_2\} \text{ and}$$

$$\mathcal{O}^{(2)}_\lambda = \{A \in M_2(\mathbb{C}) \mid \det(tI - A) = (t-\lambda)^2 \text{ for all } t \in \mathbb{C}, A \neq \lambda I_2\}.$$

We can also compute

$$\begin{pmatrix}\lambda & 0\\ 0 & \mu\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix} = \begin{pmatrix}a\lambda & b\lambda\\ c\mu & d\mu\end{pmatrix}$$

and

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}\lambda & 0\\ 0 & \mu\end{pmatrix} = \begin{pmatrix}a\lambda & b\mu\\ c\lambda & d\mu\end{pmatrix}$$

so that for $\lambda \neq \mu$,

$$\mathrm{Stab}_{GL_2(\mathbb{C})}\left(\begin{pmatrix}\lambda & 0\\ 0 & \mu\end{pmatrix}\right) = \left\{\begin{pmatrix}a & 0\\ 0 & d\end{pmatrix} \mid ad \neq 0\right\}$$

and $\mathrm{Stab}_{GL_2(\mathbb{C})}(\lambda I_2) = GL_2(\mathbb{C})$.

Similarly

$$\begin{pmatrix}\lambda & 1\\ 0 & \lambda\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix} = \begin{pmatrix}a\lambda + c & b\lambda + d\\ c\lambda & d\lambda\end{pmatrix}$$

and

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}\lambda & 1\\ 0 & \lambda\end{pmatrix} = \begin{pmatrix}a\lambda & a + b\lambda\\ c\lambda & c + d\lambda\end{pmatrix}$$

so

$$\mathrm{Stab}_{GL_2(\mathbb{C})}\left(\begin{pmatrix}\lambda & 1\\ 0 & \lambda\end{pmatrix}\right) = \left\{\begin{pmatrix}a & b\\ 0 & a\end{pmatrix} \mid a \neq 0\right\}.$$

All other stabilisers are conjugate to these ones. We can easily read off the conjugacy classes and centralisers in $GL_2(\mathbb{C})$ by restricting to the case $\lambda, \mu \neq 0$.

Exercise. Deduce that in $\mathcal{M} \simeq PGL_2(\mathbb{C})$, $\mathrm{ccl}(z \mapsto az) = \mathrm{ccl}(z \mapsto z \mapsto bz)$ if and only if $b \in \{a, 1/a\}$ thus provide a description of all the conjugacy classes in $\mathcal{M}$ and compute centralisers of suitable representatives of each class.

Lecture 19

5.4. **The orthogonal and special orthogonal groups.** Recall that any (square) matrix A has a transpose A^T with $A^T_{ij} = A_{ji}$ and $\det A^T = \det A$. Moreover if A, B are square matrices of the same size then $(AB)^T = B^T A^T$.

Definition. The *orthogonal group* $O(n) := \{A \in M_n(\mathbb{R}) \mid A^T A = I_n = AA^T\} \subset GL_n(\mathbb{R})$ is the group of orthogonal $n \times n$ matrices.

Lemma. *$O(n)$ is a subgroup of $GL_n(\mathbb{R})$.*

□

Recall that $\mathbb{R}^n$ comes with an inner product $v \cdot w = \sum_{i=1}^n v_i w_i$ which defines a length function on $\mathbb{R}^n$ via $|v| = (v \cdot v)^{1/2}$. We also recall the definition of Kronecker's delta

$$\delta_{ij} := \begin{cases} 1 & \text{if} \quad i = j; \\ 0 & \text{if} \quad i \neq j. \end{cases}$$

A basis $f_1, \ldots, f_n$ of $\mathbb{R}^n$ is said to be *orthonormal* if $f_i \cdot f_j = \delta_{ij}$.[45]

Lemma.

(a) If $\{f_1, \ldots, f_n\} \subset \mathbb{R}^n$ such that $f_i \cdot f_j = \delta_{ij}$ for all $1 \leqslant i, j \leqslant n$, then $\{f_1, \ldots, f_n\}$ is an orthonormal basis for $\mathbb{R}^n$.
(b) If $v, w \in \mathbb{R}^n$ then $v \cdot w = \frac{1}{4}(|v + w|^2 - |v - w|^2)$.

□

Proposition. *Suppose that $A \in M_n(\mathbb{R})$. The following are equivalent:*

(i) $A \in O(n)$;
(ii) $Av \cdot Aw = v \cdot w$ for all $v, w \in \mathbb{R}^n$;
(iii) the columns of A form an orthonormal basis;
(iv) $|Av| = |v|$ for all $v \in \mathbb{R}^n$.

□

Thus $O(n)$ is isomorphic to the subgroup of $S(\mathbb{F}^n)$ consisting of linear maps that preserve the scalar product or equivalently to the subgroup of $S(\mathbb{F}^n)$ consisting of linear maps that preserve length.

The conjugation action $GL_n(\mathbb{R})$ on $M_n(\mathbb{R})$ restricts to an action of $O(n)$ on $M_n(\mathbb{R})$. The equivalence of (i) and (iii) in the propostion shows that two distinct matrices in $M_n(\mathbb{R})$ are in the same $O(n)$-orbit if and only if they represent the same linear map with respect to two different orthonormal bases (see the last lecture).

Proposition. $\det\colon O(n) \to (\mathbb{R}\backslash\{0\}, \cdot)$ *has image* $\{\pm 1\}$.

□

Definition. The *special orthogonal group*

$$SO(n) := O(n) \cap SL_n(\mathbb{R}) = \ker(\det\colon O(n) \to \{\pm 1\}).$$

$SO(n)$ is isomorphic to the subgroup of $S(\mathbb{R}^n)$ consisting of linear maps that preserve the scalar product and orientation.[46] It is a normal subgroup of $O(n)$ and $O(n)/SO(n) \simeq C_2$.

There are complex versions of the orthogonal group and the special orthogonal group called the unitary group and the special unitary group. We won't have time to discuss them but they do appear on Example Sheet 4.

---

[45] There is a little apparent notational ambiguity here since we use subscripts to index the basis vectors as well as to index the coordinates of a vector. Each f_i is in $\mathbb{R}^n$ so can be written as $\sum_{k=1}^n (f_i)_k e_k$ and $f_i \cdot f_j = \sum_{k=1}^n (f_i)_k (f_j)_k$.

[46] I have not defined an orientation of $\mathbb{R}^n$. One way would be as an $SO(n)$-orbit of orthonormal bases for $\mathbb{R}^n$ which would make this completely tautological. There are more sophisticated ways that make it less so. With this definition the next sentence gives that there are exactly two orientations of $\mathbb{R}^n$.

Lecture 20

5.5. **Reflections.**

Definition. Suppose that $n \in \mathbb{R}^m$ has length 1 then the *reflection in the plane normal to* n is the function $R_n \colon \mathbb{R}^m \to \mathbb{R}^m$ given by

$$R_n(x) = x - 2(x \cdot n)n.$$

Note that if $y \cdot n = 0$ then $R_n(y) = y$, and $R_n(n) = n - 2n = -n$.

Lemma. *Suppose $n \in \mathbb{R}^m$ has length 1 then*

(a) $R_n \in O(m)$;
(b) $\mathbb{R}^m$ *has a basis with respect to which* R_n *is represented by a diagonal matrix* D *such that* $D_{11} = -1$, $D_{ii} = 1$ *for* $2 \leqslant i \leqslant m$;
(c) $(R_n)^2 = \mathrm{id}_{\mathbb{R}^m}$ *and;*
(d) $\det R_n = -1$.

□

Proposition. *If $x, y \in \mathbb{R}^m$ with $x \neq y$ but $x \cdot x = y \cdot y$ then there is $n \in \mathbb{R}^m$ of unit length such that $R_n(x) = y$. Moreover n may be chosen to be parallel to $x - y$.*

□

Theorem. *Every element of $O(3)$ is a product of at most three reflections of the form R_n with $n \in \mathbb{R}^3$ of length 1.* [47]

□

Proposition. *If $A \in O(2)$ then either*

(i) $A = SO(2)$ *and there is some $0 \leqslant \theta < 2\pi$ such that*

$$A = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$$ [48] *or*

(ii) $A \notin SO(2)$ *and $A = R_n$ for some $n \in \mathbb{R}^2$ of unit length.*

□

Theorem. *If $A \in SO(3)$ then there is some non-zero $v \in \mathbb{R}^3$ such that $Av = v$.* [49]

□

Lecture 21

Corollary. *Every A in $SO(3)$ is conjugate in $SO(3)$ to a matrix of the form*

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & \sin\theta \\ 0 & -\sin\theta & \cos\theta \end{pmatrix}.$$

□

[47] There is nothing special about three here. In general every element of $O(m)$ is a product of at most m reflections of the form R_n. The proof is exactly similar to this one.

[48] i.e. A is a rotation

[49] That is every rotation in $\mathbb{R}^3$ has an axis.

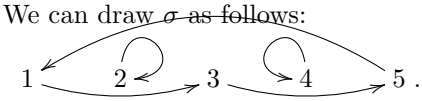
6. Permutations

Recall that a *permutation* of a set X is an element of the group $S(X)$; that is an invertible function $X \to X$. In this chapter we will study permutations of finite sets. More particularly we will study permutations of $[n] := \{1, 2, \ldots, n\}$. Since there is a 1-1 correspondence (i.e. invertible function) between any finite set and $[n]$ for some value of n this amounts to the same thing.

6.1. **Permutations as products of disjoint cycles.**

Definition. We say that a permutation $\sigma\colon [n] \to [n]$ is a *cycle* if the natural action of the cyclic subgroup of S_n generated by σ has precisely one orbit of size greater than one.

Example. If $\sigma\colon [5] \to [5]$ such that $\sigma(1) = 3$, $\sigma(2) = 2$, $\sigma(3) = 5$, $\sigma(4) = 4$ and $\sigma(5) = 1$ then $\sigma \in S_5$. We can draw σ as follows:



We can compute $\sigma^k(2) = 2$ and $\sigma^k(4) = 4$ for all $k \in \mathbb{Z}$. We can also compute $\sigma^2(1) = \sigma(3) = 5$, $\sigma^2(3) = \sigma(5) = 1$ and $\sigma^2(5) = \sigma(1) = 3$. Finally $\sigma^3(1) = \sigma(5) = 1$, $\sigma^3(3) = \sigma(1) = 3$ and $\sigma^3(5) = \sigma(3) = 5$. So $\sigma^3 = \mathrm{id}$, the group generated by σ is $\{\mathrm{id}, \sigma, \sigma^2\}$ and the orbits are $\{1, 3, 5\}$, $\{2\}$ and $\{4\}$. Thus σ is a cycle.

Suppose that σ is a cycle of order k. Then σ generates the subgroup

$$\langle\sigma\rangle := \{\mathrm{id}, \sigma, \ldots, \sigma^{k-1}\}.$$

For any $b \in [n]$ in an orbit of size 1

$$\sigma^i(b) = b \text{ for all } i \in \mathbb{Z}$$

and if $a \in [n]$ is in the orbit of size greater than one then for $c = \sigma^j(a) \in \mathrm{Orb}_{\langle\sigma\rangle}(a)$,

$$\sigma^i(c) = \sigma^{i+j}(a) = \sigma^j(\sigma^i(a)).$$

Thus $\sigma^i(c) = c$ whenever $\sigma^i(a) = a$. i.e. $\sigma^i \in \mathrm{Stab}_{\langle\sigma\rangle}(a)$ only if $\sigma^i = \mathrm{id}$. Thus $\mathrm{Stab}_{\langle\sigma\rangle}(a) = \{e\}$ and $|\mathrm{Orb}_{\langle\sigma\rangle}(a)| = k$.

Notation. If σ is a cycle of order k such that the orbit of size greater than one contains the element $a \in [n]$ then we write

$$\sigma = (a\sigma(a)\sigma^2(a)\cdots\sigma^{k-1}(a)).$$

The discussion above shows that the elements $a, \sigma(a), \ldots, \sigma^{k-1}(a)$ are all distinct and exhaust the orbit of a under $\langle\sigma\rangle$. Thus $(a\sigma(a)\cdots\sigma^{k-1}(a))$ uniquely determines σ since $\sigma(b) = b$ for $b \notin \{a, \sigma(a), \ldots, \sigma^{k-1}(a)\}$ and $\sigma(\sigma^i(a)) = \sigma^{i+_k 1}(a)$.

Example. If $\sigma\colon [5] \to [5]$ is as in the example above then $\sigma = (135) = (351) = (513)$.

Definition. We say that $(a_1, \ldots, a_k)$ and $(b_1, \ldots, b_l)$ are *disjoint cycles* if

$$\{a_1, \ldots, a_k\} \cap \{b_1, \ldots, b_l\} = \emptyset.$$

Lemma.

(a) *For $a_1, \ldots, a_m \in [n]$ distinct*

$$(a_1a_2\cdots a_m) = (a_2a_3\cdots a_ma_1) = (a_3a_4\cdots a_ma_1a_2) = \cdots$$

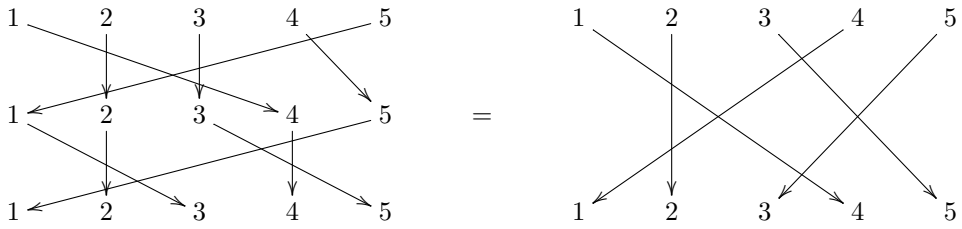
i.e. cycles can be cycled.

(b) *If σ and τ are disjoint cycles then $\sigma\tau = \tau\sigma$ i.e. disjoint cycles commute.*

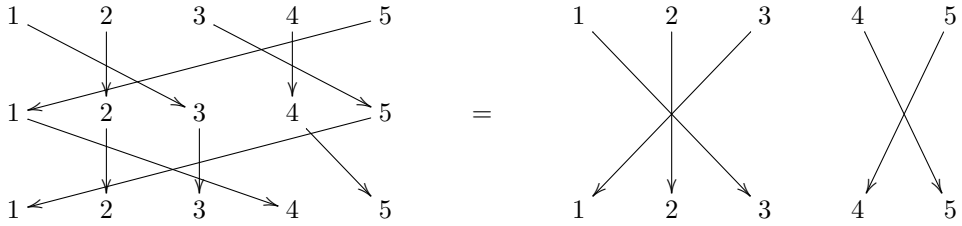
□

Theorem (Disjoint cycle decomposition)**.** *Every $\pi \in S_n$ may be written as a (possibly empty) product of disjoint cycles. Moreover the representation of π as a product of disjoint cycles is unique up to reordering.*

Example. Consider (135) and (145) in S_5. How is (135)(145) expressed as a product of disjoint cycles? We can chase elements one at a time. (145) sends 1 to 4 and (135) fixes 4. (145) sends 4 to 5 and (135) sends 5 to 1. Thus (14) is one of the cycles in the disjont cycle decompositon of (135)(145). 2 is fixed by both (145) and (135) so we can ignore it. (145) fixes 3 and (135) sends 3 to 5. (145) sends 5 to 1 and (135) sends 1 to 3. So (35) is another cycle in the decomposition. It follows that (135)(145) = (14)(35). Pictorally



whereas



i.e. (145)(135) = (13)(45).

□

Lecture 22

Lemma. *If π is a product of disjoint cycles of order $n_1, n_2, \ldots, n_k$ then*

$$o(\pi) = \mathrm{lcm}(n_1, \ldots, n_k).$$

□

6.2. **Permuations as products of transpositions.**

Definition. We call a cycle of order 2 a *transposition.*

Lemma. *Every $\pi \in S_n$ is a product of transpositions.*

□

Remark. The representation of π as a product of transpositions is not unique. For example

$$(12)(23)(34) = (1234) = (14)(13)(12).$$

Despite the remark it is true that $\pi \in S_n$ cannot be written both as a product of an even number of transpositions and as a product of an odd number of transpositions.

Theorem. *Given $\pi \in S_n$ let $l(\pi)$ be the number of orbits of $\langle \pi \rangle$ in $[n]$. For any $\pi \in S_n$ and any transposition $(ab) \in S_n$,*

$$l(\pi(ab)) = l(\pi) \pm 1.$$

□

Corollary. *There is a well-defined group homomorphism*

$$\epsilon \colon S_n \to (\{\pm 1\}, \cdot)$$

such that $\epsilon(\pi) = 1$ if π is a product of an even number of transpositions and $\epsilon(\pi) = -1$ if π is a product of an odd number of transpositions. Moreover, for $n \geqslant 2$, $\operatorname{Im} \epsilon = \{\pm 1\}$.

□

Definition. Given $\pi \in S_n$ we say that π is *even* if $\epsilon(\pi) = 1$ and that π is *odd* if $\epsilon(\pi) = -1$.

Remark. Notice that a cycle of odd order is even and a cycle of even order is odd.[50]

Definition. The *alternating group* on $[n]$, $A_n := \ker(\epsilon \colon S_n \to \{\pm 1\})$ is the normal subgroup of S_n consisting of all even permutations.

Since $|S_n| = n!$ it follows easily from the isomorphism theorem that, for $n \geqslant 2$, $|A_n| = \frac{n!}{2}$.

Lecture 23

6.3. **Conjugacy in S_n and in A_n.** We now try to understand the conjugacy classes in S_n and in A_n. In S_n they have a remarkably simple description.

Lemma. *If $\sigma \in S_n$ and $(a_1 \cdots a_m)$ is a cycle then*

$$\sigma(a_1 \cdots a_m)\sigma^{-1} = (\sigma(a_1) \cdots \sigma(a_m)).$$

□

Theorem (Conjugacy classes in S_n)**.** *Two elements of S_n are conjugate if and only if they are the product of the same number of disjoint cycles of each length.*[51]

□

Example. Conjugacy classes in S_4

representative element	e	(12)	(12)(34)	(123)	(1234)
cycle type	1^4	2.1^2	2^2	3.1	4
number of elements in class	1	6	3	8	6
size of centraliser	24	4	8	3	4
sign	1	-1	1	1	-1

[50] This is just another of those frustrating facts of life.

[51] We sometimes say that they have the same *cycle type*.

Corollary (Conjugacy classes in A_n)**.** *If $\pi \in A_n$ then its conjugacy class in A_n is equal to its conjugacy class in S_n if and only if $C_{S_n}(\pi)$ contains an odd element. Moreover if $C_{S_n}(\pi) \subset A_n$ then the conjugacy class of π in S_n is a union of two conjugacy classes in A_n of equal size.*

□

Example (Conjugacy classes in A_4).

The even cycle types in S_4 are 1^4, 2^2 and 3.1. Now $(12) \in C_{S_4}(e)$ and $(12) \in C_{S_4}((12)(34))$ so the centralisers of elements of conjugacy classes of cycle type 1^4 and 2^2 contain elements of odd order. Thus these classes are the same in A_4 and S_4.

Since $C_{S_4}((123))$ has order 3 it must be generated by (123) and so it is equal to $C_{A_4}((123))$. Thus the conjugacy class with cycle type 3.1 splits into two parts of equal size.

representative element	e	(12)(34)	(123)	(132)
cycle type	1^4	2^2	3.1	3.1
number of elements in class	1	3	4	4
size of centraliser	12	4	3	3

Corollary. *A_4 has no subgroup of index 2.*

□

Lecture 24

6.4. **Simple groups.**

Definition. We say a non-trivial group G is *simple* if G has no normal subgroups except itself and its trivial subgroup.

Since if N is a normal subgroup of G one can view G as 'built out of' N and G/N, one way to try to understand all groups is to first understand all simple groups and then how they can fit together.

Example. If p is prime then C_p is simple since C_p has no non-trivial proper subgroups. These are the only abelian simple groups.

Theorem. *A_5 is simple.*

□

The remainder of the course is non-examinable.

In fact we can prove a stronger result.

Theorem. *A_n is simple for all $n \geqslant 5$.*

Remark. A_4 is not simple since it has a normal subgroup of order 4 namely $V := \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$. $A_3 \simeq C_3$ is simple, A_2 is trivial so not simple.

□

A triumph of late 20th century mathematics was the classification of all finite simple groups. Roughly speaking this says that every finite simple group is either

- cyclic of prime order;
- an alternating group;
- a matrix group over a field of finite order (for example $PSL_n(\mathbb{Z}/p\mathbb{Z})$);

- one of 26 so-called sporadic simple groups the largest of which is known as 'the monster' and has approximately 8×10^{53} elements.

One first important step in the proof was a result by Feit and Thompson that there is no non-abelian simple group of odd order that first appeared as a circa 250 page paper in 1963. The first proof of the whole classification theorem was annouced in the early 1980s. It ran to over ten of thousand pages spread across a large number of journal articles by over 100 authors. It turned out not to be quite complete. In 2004 it appeared to experts to be complete.

In this course we have seen a little of how symmetry can be understood using the language of groups. But even when considering only finite groups there is much more to learn.