Groups

Oscar Randal-Williams

https://www.dpmms.cam.ac.uk/∼or257/teaching/notes/groups.pdf

Last updated November 28, 2018. Corrections to or257@cam.ac.uk.

Chapter 1

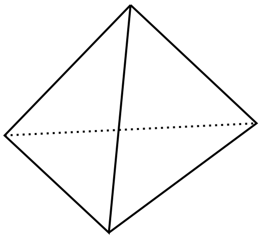
Groups and homomorphisms

1.1 Intrigue

Lecture 1

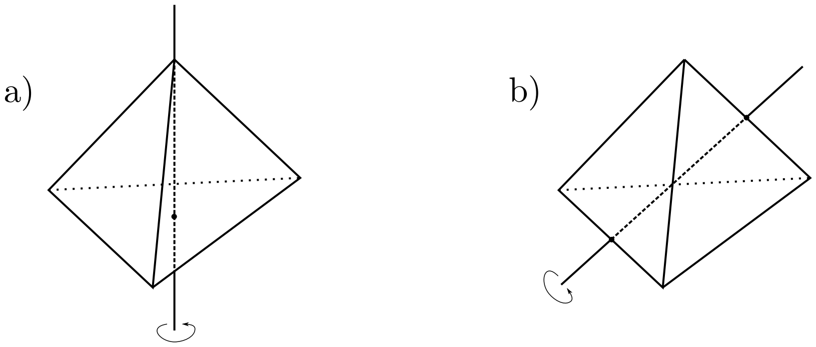
Group theory is the study of symmetry, and is best begun by considering some symmetries. First lets consider those symmetries of the following shape, a regular tetrahedron,

$T =$



which are given by rotations of 3-dimensional space. The most trivial kind of rotational symmetry is to do nothing at all: that is, rotate by 0° about any axis. Apart from this T has two kinds of rotational symmetries.

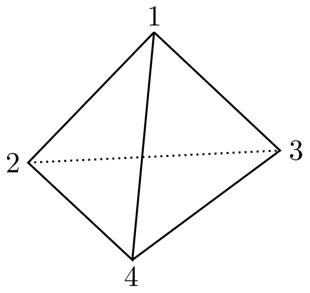
Firstly we can rotate around an axis passing through a vertex and the middle of a face, as in Figure a), and here we can rotate either by 120° or 240°. We can also rotate by 360°, but this leaves every point on the tetrahedron back where it started: it is the same as the "do nothing" rotation.



Secondly we can rotate around an axis passing through the midpoints of two opposite edges, as in Figure b), and here we can rotate by 180°. We can convince ourselves that there are no more rotations; how many have we found? For rotations of type a) there are 4 possible axes, which have 2 rotations (by 120° and 240°) each, so 8 rotations. For rotations of type b) there are 3 possible axes, which have 1 rotation each, so 3 rotations. Adding to these the "do nothing" rotation, and we find that

T has 12 rotational symmetries.

It is not obvious but if we do one rotation and then do another, maybe about a different axis, the result is again a rotation (we will prove this later in the course). Lets see an example of this, for which it is useful to number the vertices of the tetrahedron.



Let us write r for the rotation by 120° about the axis in Figure a), and s for the rotation by 180° about the axis in Figure b). The rotation r moves the vertices as follows

$$\begin{aligned}1 &\mapsto 1\\ 2 &\mapsto 4\\ 3 &\mapsto 2\\ 4 &\mapsto 3\end{aligned}$$

and the rotation s moves the vertices as follows

$$\begin{aligned}1 &\mapsto 3\\ 2 &\mapsto 4\\ 3 &\mapsto 1\\ 4 &\mapsto 2\end{aligned}$$

If we do r first and then do s, the vertices are moved as

$$\begin{aligned}1 &\mapsto 1 \mapsto 3\\ 2 &\mapsto 4 \mapsto 2\\ 3 &\mapsto 2 \mapsto 4\\ 4 &\mapsto 3 \mapsto 1\end{aligned}$$

and some thinking shows that this is a rotation about the axis going through the vertex called "2" and the middle of the opposite face.

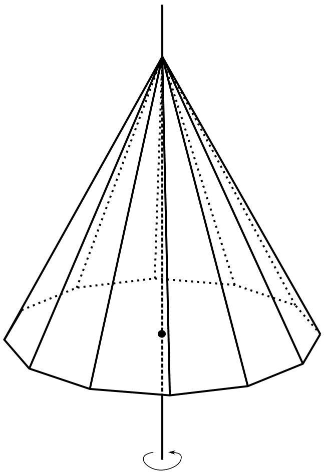
On the other hand if we do s first and then do r, the vertices are moved as

$$\begin{aligned}1 &\mapsto 3 \mapsto 2\\ 2 &\mapsto 4 \mapsto 3\\ 3 &\mapsto 1 \mapsto 1\\ 4 &\mapsto 2 \mapsto 4\end{aligned}$$

and this is a rotation about the axis going through the vertex called “4” and the middle of the opposite face. So it is also a rotation, *but is a different rotation to the one we got by doing r first and then s*!

Now lets consider a new geometrical shape, given by the cone on a dodecagon.

$C =$



The symmetries of C are a bit easier to classify: we may rotate by any multiple of $\frac{360^\circ}{12} = 30^\circ$ around the vertical axis, including the “do nothing” rotation, so this shape also has 12 symmetries, given by the rotations of

$$0^\circ, 30^\circ, 60^\circ, 90^\circ, 120^\circ, 150^\circ, 180^\circ, 210^\circ, 240^\circ, 270^\circ, 300^\circ, 330^\circ$$

about the vertical axis.

Both T and C then have the same number of symmetries, 12, but I am sure that you agree that they do not have the same *kinds* of symmetries. There are several ways of describing the differences; here are two:

(i) All symmetries of T have the property that if we repeat them twice—for those as in Figure b)—or three times—for those as in Figure a)—then we get the “do nothing” symmetry. But if we repeat the “rotate by 30°” symmetry of C two or three times we get rotation by 60° or 90°, neither of which do nothing.

(ii) If we rotate C by $30a^\circ$ and then by $30b^\circ$ then that means rotating it by $30(a+b)^\circ$. This is the same as rotating it by $30(b+a)^\circ$, so is the same as rotating by $30b^\circ$ and then by $30a^\circ$. So the order in which we apply symmetries of C does not matter, whereas we saw that it does matter for T (doing r then s is not the same as doing s then r).

Group theory will allow us to understand these kinds of phenomena. In fact group theory will give us a language, and tools, to describe symmetries of any mathematical object, not just geometrical shapes as we have discussed here.

1.2 Groups

We first make the following definition.[1]

Definition 1.2.1. A *binary operation* $\cdot$ on a set X is a function $\cdot : X \times X \to X$.

The formal definition of a group is then as follows.

Definition 1.2.2. A *group* is a triple $(G, \cdot, e)$ of a set G, a binary operation $\cdot$ on G, and an element $e \in G$ such that

(G1) For all $a, b, c \in G$ we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. (associativity)

(G2) For all $a \in G$ we have $a \cdot e = a$. (identity)

(G3) For each $a \in G$ there exists a $b \in G$ such that $a \cdot b = e$. (inverse)

One can think of G as the collection of symmetries of some object, $e \in G$ as the special “do nothing” symmetry, and $a \cdot b$ as the symmetry given by first doing the symmetry b and then doing the symmetry a.

The axiom (G1) is clear when we consider a, b, and c as being symmetries of some object. The axiom (G2) just says that the “do nothing” symmetry indeed does nothing. The axiom (G3) captures a less obvious property of symmetries: it says that every symmetry can be undone.

Let us discuss some basic properties of this definition. Axiom (G1) says that if we want to “multiply” three elements a, b, and c together in order, then there is a unique way to do so: you should convince yourself (using induction) that it follows from this that there is a unique way to multiply any number of elements together in order, such as

$$(a \cdot (b \cdot c)) \cdot d = ((a \cdot b) \cdot c) \cdot d = (a \cdot b) \cdot (c \cdot d) = a \cdot (b \cdot (c \cdot d)) = a \cdot ((b \cdot c) \cdot d)$$

and so on. Because of this we shall soon be happy to write ab for $a \cdot b$, and abc for $(a \cdot b) \cdot c$ or equally well $a \cdot (b \cdot c)$. Axioms (G2) and (G3) are richer than they first appear: we can already prove some non-obvious results about groups

Theorem 1.2.3. *Let $(G, \cdot, e)$ be a group.*

(i) If $a, b \in G$ are such that $a \cdot b = e$, then $b \cdot a = e$.

(ii) If $a \in G$ then $e \cdot a = a$.

(iii) If $a, b, b' \in G$ are such that $a \cdot b = e$ and $a \cdot b' = e$, then $b = b'$.

(iv) If $e' \in G$ is such that $a \cdot e' = a$ for some $a \in G$, then $e' = e$.

Lecture 2

[1] Recall from IA Numbers and Sets that for sets X and Y a *function* $f : X \to Y$ is a rule that associates to each element $x \in X$ precisely one element $f(x) \in Y$. The *cartesian product* $X \times Y$ is the set whose elements are pairs (x, y) for $x \in X$ and $y \in Y$.

Proof. For (i), we first calculate that

$$\begin{aligned} b &= b \cdot e \text{ by (G2)} \\ &= b \cdot (a \cdot b) \text{ as } a \cdot b = e \text{ by assumption} \\ &= (b \cdot a) \cdot b \text{ by (G1)} \end{aligned}$$

but by (G3) there is a $c \in G$ such that $b \cdot c = e$, and we calculate

$$\begin{aligned} e &= b \cdot c \text{ as } b \cdot c = e \text{ by assumption} \\ &= ((b \cdot a) \cdot b) \cdot c \text{ using the above equation} \\ &= (b \cdot a) \cdot (b \cdot c) \text{ by (G1)} \\ &= (b \cdot a) \cdot e \text{ as } b \cdot c = e \text{ by assumption} \\ &= b \cdot a \text{ by (G2)} \end{aligned}$$

as required.

For (ii), by (G3) and part (i) there is a $b \in G$ such that $a \cdot b = e$ and $b \cdot a = e$ both hold. Then we calculate

$$\begin{aligned} e \cdot a &= (a \cdot b) \cdot a \text{ as } a \cdot b = e \text{ by assumption} \\ &= a \cdot (b \cdot a) \text{ by (G1)} \\ &= a \cdot e \text{ as } b \cdot a = e \text{ by assumption} \\ &= a \text{ by (G2)} \end{aligned}$$

as required.

For (iii), by part (i) we have $b \cdot a = e$ too, and so

$$\begin{aligned} b' &= e \cdot b' \text{ by part (ii)} \\ &= (b \cdot a) \cdot b' \text{ as } b \cdot a = e \\ &= b \cdot (a \cdot b') \text{ by (G1)} \\ &= b \cdot e \text{ as } a \cdot b' = e \text{ by assumption} \\ &= b \text{ by (G2)} \end{aligned}$$

as required.

For (iv), by Axiom (G3) and part (i) there is a $b \in G$ such that $a \cdot b = e$ and $b \cdot a = e$ both hold. But then we calculate

$$\begin{aligned} e &= b \cdot a \text{ by assumption} \\ &= b \cdot (a \cdot e') \text{ as } a \cdot e' = a \text{ by assumption} \\ &= (b \cdot a) \cdot e' \text{ by (G1)} \\ &= e \cdot e' \text{ as } b \cdot a = e \text{ by assumption} \\ &= e' \text{ by part (ii).} \end{aligned}$$

□

Because of part (iii) of this theorem, when b is related to a as in Axiom (G3) then it is unique, and we write $b = a^{-1}$ and call it the *inverse of* a; by part (i) we have

$$a \cdot a^{-1} = e \quad \text{and} \quad a^{-1} \cdot a = e.$$

This implies that $(a^{-1})^{-1} = a$, and that $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

It is convenient to extend this notation as follows. For any element $a \in G$ let $a^0 = e$ and for $n \in \{1, 2, 3, \ldots\}$ inductively define $a^n = a \cdot a^{n-1}$. Similarly, for $n \in \{-1, -2, -3, \ldots\}$ define $a^n = (a^{-1})^{-n}$. This allows us to make sense of a^n for any integer n, and I leave it as an exercise for you to show that the familiar laws of indices

$$a^n \cdot a^m = a^{n+m} \quad \text{and} \quad (a^n)^m = a^{nm}$$

continue to hold for all integers n and m.

Remark 1.2.4. Given a pair $(G, \cdot)$ of a set and a binary operation $\cdot$ on G, and two elements $e, e' \in G$ such that $(G, \cdot, e)$ and $(G, \cdot, e')$ are both groups, then we have

$$\begin{aligned} e' &= e \cdot e' \text{ by Theorem 1.2.3 (ii) in the group } (G, \cdot, e) \\ &= e \text{ using (G2) in the group } (G, \cdot, e') \end{aligned}$$

This means that we could also have defined a group to be a pair $(G, \cdot)$ satisfying (G1) such that there exists an $e \in G$ for which (G2) and (G3) are satisfied.

It is important to realise that although we consider $\cdot$ to be a kind of multiplication, its behaviour will be quite different from the multiplication of numbers that you are used to. One difference is that there is no reason that $a \cdot b$ should be equal to $b \cdot a$. Groups where this does happen are given a special name.

Definition 1.2.5. A group $(G, \cdot, e)$ is *abelian*[2] if for all $a, b \in G$ we have $a \cdot b = b \cdot a$.

Definition 1.2.6. A group $(G, \cdot, e)$ is *finite* if the set G has finitely-many elements. In this case we say that the *order* of this group is the number of elements of G, which we write as $|G|$.

Example 1.2.7.

(i) If $\{e\}$ is the set with a single element, called e, and $\cdot$ is the binary operation given by $e \cdot e = e$, then $(\{e\}, \cdot, e)$ is a group, the *trivial group*.

(ii) $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$, $(\mathbb{C}, +, 0)$ are all abelian groups.

(iii) $(\mathbb{N}, +, 0)$ is not a group, as there is no natural number N such that $1 + N = 0$.

(iv) $(\mathbb{Z}, -, 0)$ is not a group, as the operation of subtraction $-$ is not associative (for example $(1 - 1) - 1 = -1 \neq 1 = 1 - (1 - 1)$).

(v) $(\mathbb{Q}, \times, 1)$ is not a group, as there is no rational number q such that $0 \times q = 1$. But $(\mathbb{Q}\backslash\{0\}, \times, 1)$ is a group, which is abelian. Similarly $(\mathbb{R}\backslash\{0\}, \times, 1)$ and $(\mathbb{C}\backslash\{0\}, \times, 1)$ are abelian groups.

[2] After the Norwegian mathematician Niels Henrik Abel (1802-1829).

(vi) If $X \subset \mathbb{R}^3$ is a solid then

$$(\{\text{rotational symmetries of } X\}, \circ, \text{“do nothing”})$$

is a group, where $\circ$ denotes composition of functions. It might be abelian (like the case $X = C$ in Section 1.1) or it might not (like the case $X = T$ in Section 1.1). It might be finite (like the examples in Section 1.1, which have 12 elements), or it might be infinite, such as when X is the sphere.

(vii) As another example,

$$(\{q \in \mathbb{Q} \text{ such that } q > 0\}, \times, 1)$$

is an abelian group, and similarly with $\mathbb{R}$ instead of $\mathbb{Q}$.

(viii) Of a related flavour,

$$(\{z \in \mathbb{C} \text{ such that } |z| = 1\}, \times, 1)$$

is an abelian group.

(ix) If $n \in \mathbb{N}$, then

$$C_n := (\{z \in \mathbb{C} \text{ such that } z^n = 1\}, \times, 1)$$

is an abelian group (See Example Sheet 1 Q8). It is also finite, and as there are precisely n complex numbers whose nth powers are 1, it has order n.

(x) If $n \in \mathbb{N}$, then the set $\mathbb{Z}_n := \{0, 1, 2, \ldots, n-1\}$ can be given the structure of a group by letting $a +_n b$ be the remainder when $a + b$ is divided by n. Then $(\mathbb{Z}_n, +_n, 0)$ is an abelian group, which is finite of order n.

So far most of these examples have been abelian: examples coming from number systems such as $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ often are. However most groups are not abelian. The symmetries of the tetrahedron as described in in Section 1.1 is one example, and another is as follows.

(xi) Let Isom($\mathbb{R}$) be the set of functions $f : \mathbb{R} \to \mathbb{R}$ which are distance-preserving[3] in the sense that $|f(x) - f(y)| = |x - y|$ for all $x, y \in \mathbb{R}$. With $\cdot = \circ$ given by composition of functions, and $e = \mathrm{Id}$ given by the function $\mathrm{Id}(x) = x$, this is a group. The function $r(x) = -x$ is an element of Isom($\mathbb{R}$), and the function $t(x) = x + 1$ is too. But

$$t(r(x)) = t(-x) = -x + 1$$

is not the same as

$$r(t(x)) = r(x + 1) = -x - 1.$$

Thus $t \circ r \neq r \circ t$, so this group is not abelian.

Lecture 3

(xii) Let $GL_2(\mathbb{R})$ denote the set of all 2×2 matrices with real entries which are invertible. Matrix multiplication defines a binary operation $\cdot$ on $GL_2(\mathbb{R})$, and then the data $(GL_2(\mathbb{R}), \cdot, \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right))$ is a group. Similarly for $GL_2(\mathbb{C})$. △

[3] that is, “isometries”

Definition 1.2.8. We say that a group $(H, \cdot_H, e_H)$ is a *subgroup of* $(G, \cdot_G, e_G)$ if

(i) H is a subset of G (i.e. $H \subset G$),

(ii) $e_H = e_G$, and

(iii) $a \cdot_G b = a \cdot_H b$ for all $a, b \in H$.

We write $(H, \cdot_H, e_H) \leq (G, \cdot_G, e_G)$.

In other words, $(H, \cdot_H, e_H)$ is a group whose elements are given by the subset H of G, and whose identity element and multiplication is the same as that of $(G, \cdot_G, e_G)$. Because the identity element and multiplication are those of G, we can get away with not specifying them: for a group $(G, \cdot_G, e_G)$ it makes sense to ask whether a subset $H \subset G$ "is" a subgroup, meaning whether $e_H := e_G$ lies in H, whether the binary operation $\cdot_G$ determines a binary operation $\cdot_H$ on H, and if so whether $(H, \cdot_H, e_H)$ is a group.

The following lemma gives an efficient way to check this.

Proposition 1.2.9. *Let $(G, \cdot_G, e_G)$ be a group and $H \subset G$ be a non-empty subset. If $a \cdot_G b^{-1} \in H$ for all $a, b \in H$ then there is a unique binary operation $\cdot_H$ and $e_H \in H$ making $(H, \cdot_H, e_H)$ a subgroup of $(G, \cdot_G, e_G)$.*

Proof. As $H \subset G$ is non-empty we may choose a $x \in H$, and then have $e_G = x \cdot_G x^{-1} \in H$. From this it follows that $a^{-1} = e_G \cdot_G a^{-1} \in H$ for all $a \in H$. Now for any $a, b \in H$ we have $a \cdot_G b = a \cdot_G (b^{-1})^{-1} \in H$. So we can define a binary operation

$$\begin{aligned} \cdot_H : H \times H &\longrightarrow H \\ (a, b) &\longmapsto a \cdot_G b \end{aligned}$$

and $e_H := e_G \in H$. We will be finished if $(H, \cdot_H, e_H)$ is a group. Certainly $\cdot_H$ is associative, as $\cdot_G$ is, and we have $a \cdot_H e_H = a \cdot_G e_G = a$ and so on, so the identity axiom holds. For any $a \in H$ we have shown that $a^{-1} \in H$, and $a \cdot_H a^{-1} = a \cdot_G a^{-1} = e_G = e_H$ and so on, so the inverse axiom holds. □

Example 1.2.10.

(i) $(\mathbb{Z}, +, 0) \leq (\mathbb{Q}, +, 0) \leq (\mathbb{R}, +, 0) \leq (\mathbb{C}, +, 0)$,

(ii) any group is a subgroup of itself,

(iii) for any group $(G, \cdot, e)$, $\{e\} \subset G$ is a subgroup, the *trivial subgroup*,

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

(v) if n divides m then the group C_n (from Example 1.2.7 (ix)) is a subgroup of the group C_m,

(vi) the symmetries of the tetrahedron of type b) discussed in Section 1.1, those given by a rotation by 180° about an axis passing through a pair of opposite edges, form a subgroup (having 4 elements) of the group of rotations of the tetrahedron,

(vii) the subset $SL_2(\mathbb{R}) \subset GL_2(\mathbb{R})$ of those 2×2 matrices with determinant equal to 1 is a subgroup. △

Proposition 1.2.11. *The subgroups of* $(\mathbb{Z}, +, 0)$ *are given precisely by the subsets* $n\mathbb{Z} \subset \mathbb{Z}$ *for some* $n \in \mathbb{N}$. *(Here* $n\mathbb{Z} := \{kn \in \mathbb{Z} \,|\, k \in \mathbb{Z}\}$ *denotes the set of multiples of* n.*)*

Proof. We may verify that for each $n \in \mathbb{N}$ the subset $n\mathbb{Z} \subset \mathbb{Z}$ is indeed a subgroup using Proposition 1.2.9. If $a, b \in n\mathbb{Z}$ then $a = na'$ and $b = nb'$, so

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

as required.

Now let $S \subset \mathbb{Z}$ be a subgroup. If $S = \{0\}$ then it is indeed a subgroup (namely the trivial subgroup); if not, let $n \in S$ be the smallest positive element of S. As S is a subgroup it is closed under negation (which is taking the inverse in $(\mathbb{Z}, +, 0)$) and under addition, so $n\mathbb{Z} \subset S$. Suppose for a contradiction that $n\mathbb{Z} \neq S$, so there is a $x \in S \setminus n\mathbb{Z}$, which lies strictly between nk and $n(k + 1)$, but then $x - nk$ lies strictly between 0 and n. It follows that $x - nk$ is a positive element which is smaller than n, which is a contradiction: thus $S = n\mathbb{Z}$. □

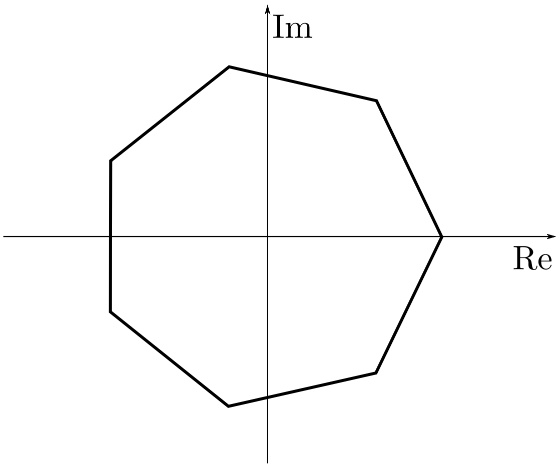
So far we have denoted groups as a triple $(G, \cdot, e)$, and written products as $a \cdot b$. This is quite proper, but is somewhat laborious and can make simple statements look more complicated than they really are.

From now on we shall do as mathematicians do and write G, H, ... for general groups, bearing in mind that when we say "let G be a group" we are implicitly equipping G with a binary operation $\cdot$ and identity $e \in G$. If we want to emphasise in which group e is the identity then we write it as e_G, and we similarly write $\cdot_G$ for $\cdot$.

1.3 Some groups of symmetries

1.3.1 Regular polygons

We will write D_{2n} for the set of symmetries of the regular n-gon, shown below with $n = 7$.



To be concrete we consider the n-gon to lie in the complex plane $\mathbb{C}$, and have vertices at

$$1, e^{2\pi i \frac{1}{n}}, e^{2\pi i \frac{2}{n}}, e^{2\pi i \frac{3}{n}}, \ldots, e^{2\pi i \frac{n-1}{n}}.$$

Then D_{2n} consists of the isometries[4] of the complex plane $\mathbb{C}$ which send the n-gon to itself.

If $f, g : \mathbb{C} \to \mathbb{C}$ are isometries which send the n-gon to itself then so is the composition $f \circ g$: thus $\circ$ defines a binary operation on D_{2n}. We let $\mathrm{Id} \in D_{2n}$ be the isometry $\mathrm{Id}(x) = x$.

Theorem 1.3.1. *The data* $(D_{2n}, \circ, \mathrm{Id})$ *is a group, called the nth* dihedral group. *It has* $2n$ *elements.*[5]

Proof. We must verify the group axioms. Axiom (G1) is clear, as composition of functions is associative. For Axiom (G2) note that if $f \in D_{2n}$ then $(f \circ \mathrm{Id})(x) = f(\mathrm{Id}(x)) = f(x)$ for all x, so $f \circ \mathrm{Id} = f$.

We will verify Axiom (G3) and show D_{2n} has $2n$ elements at the same time, by working out what all elements of D_{2n} are. To do this we need to produce some elements of D_{2n}.

Let $r : \mathbb{C} \to \mathbb{C}$ be the map $z \mapsto z \cdot e^{2\pi i \frac{1}{n}}$, which has the effect of rotating by $\frac{2\pi}{n}$ so preserves our regular n-gon. If $z, w \in \mathbb{C}$ then

$$|r(z) - r(w)| = |z \cdot e^{2\pi i \frac{1}{n}} - w \cdot e^{2\pi i \frac{1}{n}}| = |(z-w) \cdot e^{2\pi i \frac{1}{n}}| = |z-w| \cdot |e^{2\pi i \frac{1}{n}}| = |z-w|$$

so r is an isometry.

Let $s : \mathbb{C} \to \mathbb{C}$ be the map $z \mapsto \bar{z}$, which has the effect of reflecting in the real axis so preserves our regular n-gon. If $z, w \in \mathbb{C}$ then

$$|s(z) - s(w)|^2 = |\bar{z} - \bar{w}|^2 = (\bar{z} - \bar{w}) \cdot \overline{(\bar{z} - \bar{w})} = (\bar{z} - \bar{w}) \cdot (z - w) = |z - w|^2$$

[4] that is, rigid motions, or transformations which preserve distances between points

[5] The subscript on D_{2n} refers to the number of elements of the group, not the number of sides of the polygon, which is n.

so taking the (unique) positive square root shows that s is an isometry.

If we compose r with itself n times then we get Id, so $r \circ (\underbrace{r \circ \cdots \circ r}_{n-1 \text{ times}}) = \mathrm{Id}$. If we compose s with itself we get Id, so $s \circ s = \mathrm{Id}$. Thus r and s have inverses, so if we can show that every element of D_{2n} is a composition of r's and s's then we have verified that $(D_{2n}, \circ, \mathrm{Id})$ is a group. In fact we will show that

$$D_{2n} = \{\mathrm{Id}, r, r^2, r^3, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\},$$

from which it follows both that D_{2n} is a group and that it has $2n$ elements.

Let $f \in D_{2n}$ be some isometry. As 1 is a vertex of the regular n-gon, $f(1)$ must also be a vertex, so must be $e^{2\pi i \frac{k}{n}}$ for some k. But $r^k(1)$ is also $e^{2\pi i \frac{k}{n}}$, so $(r^{-k} \circ f)(1) = r^{-k}(f(1)) = r^{-k}(e^{2\pi i \frac{k}{n}}) = 1$, meaning that $g := r^{-k} \circ f$ is an isometry which fixes 1. Now $e^{2\pi i \frac{1}{n}}$ is a vertex of the n-gon which shares and edge with 1, so $g(e^{2\pi i \frac{1}{n}})$ must be a vertex of the n-gon which shares and edge with $g(1) = 1$. There are only two such vertices, $e^{2\pi i \frac{1}{n}}$ and $e^{2\pi i \frac{n-1}{n}}$.

In the first case g is an isometry which fixes $e^{2\pi i \frac{1}{n}}$ and also 1, and because it just interchanges the vertices among themselves it also fixes their centre of mass, which is

$$\frac{1}{n}\sum_{k=0}^{n-1} e^{2\pi i \frac{k}{n}} = \frac{1}{n}\sum_{k=0}^{n-1} (e^{2\pi i \frac{1}{n}})^k = \frac{1}{n}\frac{1-(e^{2\pi i \frac{1}{n}})^n}{1-e^{2\pi i \frac{1}{n}}} = 0 \text{ because } e^{2\pi i} = 1.$$

Thus g is an isometry of $\mathbb{C}$ fixing three points (0, 1, and $e^{2\pi i \frac{1}{n}}$) and it is an easy exercise that this means $g = \mathrm{Id}$, so $f = r^k$.

In the second case we have $(s \circ g)(e^{2\pi i \frac{1}{n}}) = s(e^{2\pi i \frac{n-1}{n}}) = e^{2\pi i \frac{1-n}{n}} = e^{2\pi i \frac{1}{n}}$ and $(s \circ g)(1) = s(g(1)) = s(1) = \bar{1} = 1$, so $s \circ g$ fixes $e^{2\pi i \frac{1}{n}}$ and also 1, and hence the above argument shows that $s \circ g = \mathrm{Id}$, so $f = r^k \circ s$. □

Lecture 4

In the description

$$D_{2n} = \{\mathrm{Id}, r, r^2, r^3, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\}$$

of the elements of the dihedral group it is obvious how to form certain multiplications: for example the composition of r and s is the element called rs. But what about the composition of s and r? We can work this out using the proof of Theorem 1.3.1, as follows.

First let us consider $(s \circ r)(1) = s(r(1)) = s(e^{2\pi i \frac{1}{n}}) = e^{2\pi i \frac{n-1}{n}}$. This is the same as $r^{n-1}(1) = r^{-1}(1)$, so following the proof we find that $r^{-(n-1)} \circ s \circ r$ fixes 1. Now

$$(r^{-(-1)} \circ s \circ r)(e^{2\pi i \frac{1}{n}}) = e^{2\pi i \frac{1-n}{n}} \cdot \overline{e^{2\pi i \frac{1}{n}} \cdot e^{2\pi i \frac{1}{n}}} = e^{2\pi i \frac{-1-n}{n}} = e^{2\pi i \frac{n-1}{n}}$$

which is the same as $s(e^{2\pi i \frac{1}{n}})$, so following the proof we have $s \circ r^{-(-1)} \circ s \circ r = \mathrm{Id}$. Applying s this gives $r^{-(-1)} \circ s \circ r = s$, and applying r^{-1} it gives

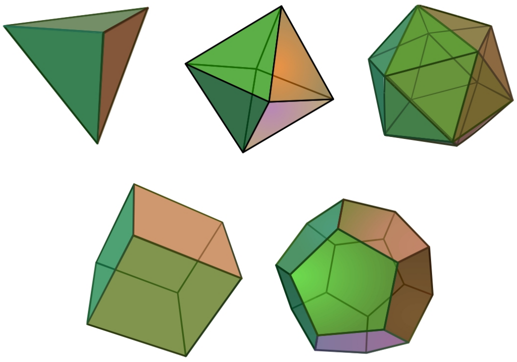
$$s \circ r = r^{-1} \circ s.$$

Thus D_{2n} is not abelian for any $n \geq 3$. This identity tells us how we can always move an s to the right of any r's, so allows us to rewrite any combination of r's and s's in the form $r^a s^b$ for $a, b \in \mathbb{Z}$. For example,

$$\begin{aligned}(r^3 s) \circ (r^2) &= r^3 s r^2 \\ &= r^3 r^{-1} s r \\ &= r^3 r^{-1} r^{-1} s \\ &= rs.\end{aligned}$$

1.3.2 Regular solids

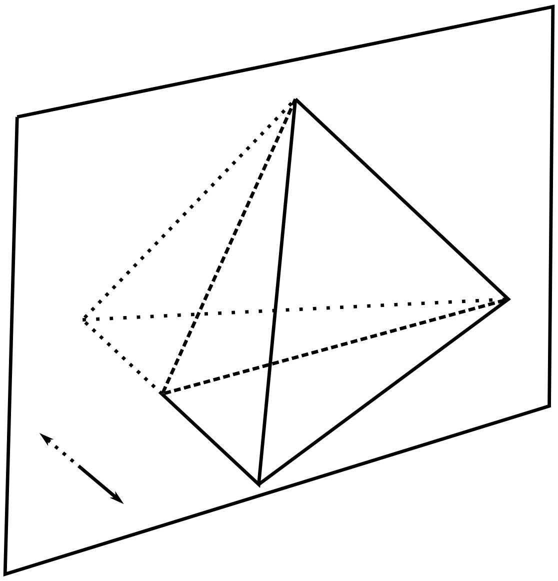
There are just five regular solid convex polyhedra, the Platonic solids[6],



which are the tetrahedron, octahedron, icosahedron, cube, and dodecahedron. For each such solid X there is a group $\mathrm{Isom}(X)$ whose elements are the isometries of $\mathbb{R}^3$ which transform the polyhedron X to itself.

In Section 1.1 we saw that the tetrahedron has 12 rotational symmetries, but it has more isometries, for example the reflection in the plane shown in the following figure

[6] Максим Пе, `https://commons.wikimedia.org/wiki/File:Platonic_solids.jpg`



In total the tetrahedron has 24 isometries, the octahedron and cube both have 48 isometries, and the icosahedron and dodecahedron both have 120 isometries. We will study the isometries of the tetrahedron, cube, and octahedron later, after developing some theory.

1.3.3 Permutations

For a set X, a *permutation* of X is a function $f : X \to X$ which is invertible i.e. such that there exists a function $g : X \to X$ satisfying $(f \circ g)(x) = x$ and $(g \circ f)(x) = x$ for all $x \in X$. In other words, $f \circ g$ and $g \circ f$ are both Id, the identity function of X.

Consider the set $\mathrm{Sym}(X)$ consisting of all permutations of X. If $f, f' \in \mathrm{Sym}(X)$ have inverses g and g' respectively, then $(f \circ f') \circ (g' \circ g) = f \circ (f' \circ g') \circ g = f \circ \mathrm{Id} \circ g = f \circ g = \mathrm{Id}$ and also $(g' \circ g) \circ (f \circ f') = g' \circ (g \circ f) \circ f' = g' \circ \mathrm{Id} \circ f' = g' \circ f' = \mathrm{Id}$, so $f \circ f' \in \mathrm{Sym}(X)$. As we have already used, composition of functions is associative, Id acts as an identity for composition of functions, and by assumption elements of $\mathrm{Sym}(X)$ have inverses. This dicussion proves

Theorem 1.3.2. *For any set X the data* $(\mathrm{Sym}(X), \circ, \mathrm{Id})$ *is a group, called the* symmetric group *of X.*

When $X = \{1, 2, 3, \ldots, n\}$ we will denote this group by S_n, and call it the *nth symmetric group.* Remember than the number of permutations of n objects is $n! := n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1$, so the group S_n has order $n!$. We will study these groups in detail later in the course.

1.4 Homomorphisms

When studying a new mathematical structure—in this case groups—it is essential to study not just the objects themselves but the structure-preserving functions between them.

Definition 1.4.1. If H and G are groups then a function $\phi : H \to G$ is called a *(group) homomorphism* if for all $a, b \in H$ we have $\phi(a \cdot_H b) = \phi(a) \cdot_G \phi(b)$.

If in addition the function ϕ is invertible then it is called a *(group) isomorphism*, and the groups H and G are called *isomorphic*: we write $H \cong G$.

Example 1.4.2.

(i) If H and G are groups then the function $\phi : H \to G$ given by $\phi(h) = e_G$ for all $h \in H$ is a homomorphism.

(ii) If $H \leq G$ then the inclusion function $\mathrm{inc} : H \to G$ given by $\mathrm{inc}(h) = h$ is a homomorphism.

(iii) If C_n denotes the groups from Example 1.2.7 (ix), then if n divides m the function $z \mapsto z^{m/n} : C_m \to C_n$ is a homomorphism.

(iv) The function $x \mapsto e^x : \mathbb{R} \to \{r \in \mathbb{R} \,|\, r > 0\}$ gives a group isomorphism

$$\exp : (\mathbb{R}, +, 0) \longrightarrow (\{r \in \mathbb{R} \,|\, r > 0\}, \times, 1).$$

(v) The determinant gives a homomorphism

$$\det : (GL_2(\mathbb{R}), \cdot, \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)) \longrightarrow (\mathbb{R} \setminus \{0\}, \times, 1). \qquad \triangle$$

At first sight the definition of homomorphism looks too weak: we have not asked that $\phi(e_H) = e_G$ and we not asked that $\phi(a^{-1}) = \phi(a)^{-1}$. But these are actually consequences of the definition.

Lemma 1.4.3. *If $\phi : H \to G$ is a group homomorphism, then*

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

(ii) for all $a \in H$ we have $\phi(a^{-1}) = \phi(a)^{-1}$.

Proof. For (i), apply ϕ to $e_H \cdot_H e_H = e_H$ to get

$$\phi(e_H) \cdot_G \phi(e_H) = \phi(e_H \cdot_H e_H) = \phi(e_H)$$

and now multiply by $\phi(e_H)^{-1}$ to get $\phi(e_H) = e_G$, as required.

For (ii) consider $\phi(a) \cdot_G \phi(a^{-1}) = \phi(a \cdot_H a^{-1}) = \phi(e_H) = e_G$ and $\phi(a^{-1}) \cdot_G \phi(a) = \phi(a^{-1} \cdot_H a) = \phi(e_H) = e_G$. This is the defining property of $\phi(a)^{-1}$, so $\phi(a^{-1}) = \phi(a)^{-1}$. □

It is a trivial but important observation that the composition of two group homomorphisms is again a group homomorphism: if $\phi : H \to G$ and $\psi : G \to K$ are homomorphisms, then

$$(\psi \circ \phi)(a \cdot_H b) = \psi(\phi(a \cdot_H b)) = \psi(\phi(a) \cdot_G \phi(b)) = \psi(\phi(a)) \cdot_K \psi(\phi(b)) = (\psi \circ \phi)(a) \cdot_K (\psi \circ \phi)(b).$$

Definition 1.4.4. If $\phi : H \to G$ is a group homomorphism then

(i) the *image* of ϕ is

$$\mathrm{Im}(\phi) := \{g \in G \,|\, g = \phi(h) \text{ for some } h \in H.\}$$

(ii) the *kernel* of ϕ is

$$\mathrm{Ker}(\phi) := \{h \in H \,|\, \phi(h) = e_G.\}$$

Proposition 1.4.5. *If $\phi : H \to G$ is a group homomorphism then* $\mathrm{Im}(\phi)$ *is a subgroup of G and* $\mathrm{Ker}(\phi)$ *is a subgroup of H.*

Proof. We will use Proposition 1.2.9. For $\mathrm{Im}(\phi)$ we have $\phi(e_H) = e_G$ so $e_G \in \mathrm{Im}(\phi)$ so this set is not empty. If $a, b \in \mathrm{Im}(\phi)$ then $a = \phi(x)$ and $b = \phi(y)$, so

$$a \cdot_G b^{-1} = \phi(x) \cdot_G \phi(y)^{-1} = \phi(x) \cdot_G \phi(y^{-1}) = \phi(x \cdot_H y^{-1})$$

lies in $\mathrm{Im}(\phi)$, as required.

For $\mathrm{Ker}(\phi)$ we have $\phi(e_H) = e_G$ so $e_H \in \mathrm{Ker}(\phi)$ so this set is not empty. If $a, b \in \mathrm{Ker}(\phi)$ then we have

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

so $a \cdot_H b^{-1} \in \mathrm{Ker}(\phi)$, as required. □

The following lemma will be useful for checking whether a homomorphism is an isomorphism. We will later see that this is a special case of a much more general result.

Lemma 1.4.6. *If $\phi : H \to G$ is a homomorphism, then it is an isomorphism if and only if* $\mathrm{Im}(\phi) = G$ *and* $\mathrm{Ker}(\phi) = \{e_H\}$. *In this case $\phi^{-1} : G \to H$ is also an isomorphism.*

Proof. Suppose first that the function ϕ is invertible. Firstly, every $g \in G$ is equal to $\phi(\phi^{-1}(g))$, so $\mathrm{Im}(\phi) = G$. Secondly, if $\phi(h) = e_G$ then as $\phi(e_H) = e_G$ too, applying ϕ^{-1} shows that $h = e_H$, so e_H is the only element of $\mathrm{Ker}(\phi)$.

Now suppose that $\mathrm{Im}(\phi) = G$ and $\mathrm{Ker}(\phi) = \{e_H\}$. By the first condition every element of G is of the form $\phi(h_g)$ for some $h_g \in H$, so we can define a function $\psi : G \to H$ by $\psi(g) := h_g$. By construction this satisfies $\phi(\psi(g)) = g$. Now

$$\phi(h^{-1} \cdot_H \psi(\phi(h))) = \phi(h)^{-1} \cdot_G \phi(\psi(\phi(h))) = \phi(h)^{-1} \cdot_G \phi(h) = e_G$$

and so $h^{-1} \cdot_H \psi(\phi(h)) \in \mathrm{Ker}(\phi)$, so this must be e_H, and so $\psi(\phi(h)) = h$. Thus ψ is the inverse to ϕ, showing that ϕ is invertible.

For the last part, let $a, b \in G$. We can write $a = \phi(\phi^{-1}(a))$ and $b = \phi(\phi^{-1}(b))$, and hence calculate

$$\phi^{-1}(a \cdot_G b) = \phi^{-1}(\phi(\phi^{-1}(a)) \cdot_G \phi(\phi^{-1}(b))) = \phi^{-1}(\phi(\phi^{-1}(a) \cdot_H \phi^{-1}(b))) = \phi^{-1}(a) \cdot_H \phi^{-1}(b)$$

as required. □

Recall from IA Numbers and Sets that a function $f : X \to Y$ is called *surjective* (or *a surjection*) if for each $y \in Y$ there exists some $x \in X$ such that $f(x) = y$. It is called *injective* (or *an injection*) if whenever $f(x) = f(x')$ for some $x, x' \in X$, then $x = x'$. It is called *bijective* (or *a bijection*) if it is both surjective and injective; in this case there is a (unique) function $f^{-1} : Y \to X$ such that $f^{-1}(f(x)) = x$ and $f(f^{-1}(y)) = y$ for all $x \in X$ and all $y \in Y$, called the *inverse* of f. What we have so far been calling an *invertible function* is the same as a bijection. It is very useful to be able to refer to the properties of injectivity and surjectivity individually, even if we are mainly interested in bijections.

1.5 Cyclic groups

Lecture 5

In Example 1.2.7 (ix) we have defined for $n \in \mathbb{N}$ the group

$$C_n = (\{z \in \mathbb{C} \text{ such that } z^n = 1\}, \times, 1).$$

The elements of this group are the n complex numbers

$$1, e^{2\pi i \frac{1}{n}}, e^{2\pi i \frac{2}{n}}, e^{2\pi i \frac{3}{n}}, \ldots, e^{2\pi i \frac{n-2}{n}}, e^{2\pi i \frac{n-1}{n}},$$

and, writing $\xi := e^{2\pi i \frac{1}{n}}$, these are

$$1 = \xi^0, \xi = \xi^1, \xi^2, \xi^3, \ldots, \xi^{n-2}, \xi^{n-1}.$$

This group therefore has the property that every element is equal to ξ^k for some $k \in \mathbb{Z}$. It is convenient to formalise this property as follows.

Definition 1.5.1. A group G is *cyclic* if there is a $a \in G$ such that every element of G is equal to a^k for some $k \in \mathbb{Z}$. We call such an a a *generator* of G.

Example 1.5.2.

(i) The groups C_n are cyclic, as described above.

(ii) The group $(\mathbb{Z}, +, 0)$ is cyclic. To see this take $a := 1$. Then a^k, in this group, is the integer $k \in \mathbb{Z}$, so every element of this group is of the form a^k. △

Example 1.5.3. As another example, the groups $\mathbb{Z}_n$ described in Example 1.2.7 (x) are cyclic. To see this take $a := 1$ then for $0 \leq k \leq n-1$ the element a^k in this group is $k \in \mathbb{Z}_n$, so every element of this group is of the form a^k.

But this example is not really new, as the function $\phi : \mathbb{Z}_n \to C_n$ given by $\phi(k) = \xi^k$ is a group homomorphism and a bijection, so is a group isomorphism. △

The following theorem shows that, considered up to isomorphism, Example 1.5.2 gives all examples of cyclic groups. They are obviously all non-isomorphic to each other, as they have different numbers of elements.

Theorem 1.5.4. *A cyclic group is isomorphic to some C_n or to $(\mathbb{Z}, +, 0)$.*

Proof. Let G be a cyclic group and $a \in G$ be a generator, and consider the set

$$S := \{k \in \mathbb{N}_{>0} \,|\, a^k = e\}.$$

If S is not empty, let n be the smallest number it contains and consider the function

$$\begin{aligned} \phi : C_n = \{\xi^0, \xi^1, \dots, \xi^{n-1}\} &\longrightarrow G \\ \xi^k &\longmapsto a^k. \end{aligned}$$

Note that if $0 \leq k, l < n$ and $k + l \geq n$ then we can write $k + l = n + r$ with $0 \leq r < n$, and as $\xi^n = 1$ we have $\xi^{k+l} = \xi^r$. If $k + l < n$ then we set $r = k + l$, and also have $\xi^{k+l} = \xi^r$. As $a^n = e$ we also have $a^{k+l} = a^r$ in both cases. Now we calculate

$$\phi(\xi^k \cdot \xi^l) = \phi(\xi^{k+l}) = \phi(\xi^r) = a^r = a^{k+l} = a^k \cdot a^l = \phi(\xi^k) \cdot \phi(\xi^l)$$

so ϕ is a homomorphism. As G is cyclic generated by a, and every power of a is equal to a^k for some $0 \leq k < n$ as $a^n = 1$, ϕ is surjective. If ϕ is not injective then there is a $0 < k < n$ with $\phi(\xi^k) = e$, so $a^k = e$. But then $k \in S$ is smaller than n, a contradiction: thus ϕ is also injective, so is a bijection and hence a group isomorphism.

If S is empty then consider the function

$$\begin{aligned} \phi : \mathbb{Z} &\longrightarrow G \\ k &\longmapsto a^k. \end{aligned}$$

This satisfies $\phi(k+l) = a^{k+l} = a^k \cdot a^l = \phi(k) \cdot \phi(l)$ so is a homomorphism, and is surjective as a is a generator of G. If it is not injective then the kernel is a subgroup of $\mathbb{Z}$, so is $k\mathbb{Z}$ for some $k \in \mathbb{N}_{>0}$. But then $e = \phi(k) = a^k$ so $k \in S$, a contradiction. □

Because of this theorem it is convenient to write C_∞ for the group $(\mathbb{Z}, +, 0)$, and then to allow ourselves to write C_n for any cyclic group of size n.

Definition 1.5.5. If G is a group and $g \in G$, the *order* of g is the smallest $k \in \mathbb{N}$ such that $g^k = e$, and is written $\mathrm{ord}(g) = k$. If there is no such k then we say that g has *infinite order*, and write $\mathrm{ord}(g) = \infty$.

For $g \in G$ we may consider the subset $\langle g \rangle \subset G$ consisting of all those elements of G of the form g^k for some $k \in \mathbb{Z}$. If $g^k, g^l \in \langle g \rangle$ then

$$g^k \cdot (g^l)^{-1} = g^k \cdot g^{-l} = g^{k-l} \in \langle g \rangle$$

and so $\langle g \rangle$ is a subgroup of G (by Proposition 1.2.9). By definition the group $\langle g \rangle$ is cyclic, and g is a generator for it, so by Theorem 1.5.4 we have $\langle g \rangle \cong C_n$ for a unique $n = 1, 2, 3, \dots, \infty$. Unravelling definitions, we see that this n is precisely the order of g.

1.6 The Möbius group

1.6.1 Möbius transformations

We would like to study transformations $f : \mathbb{C} \to \mathbb{C}$ of the form $f(z) = \frac{az+b}{cz+d}$ for $a, b, c, d \in \mathbb{C}$, but to make such transformations into a group we must be a little careful.

Firstly, the expression $\frac{az+b}{cz+d}$ does not yet have a meaning at $z = -\frac{d}{c}$, as then we are dividing by 0 and there is no sensible complex number we can choose it to be. To circumvent this we will work not with the complex numbers but with the *extended complex numbers*

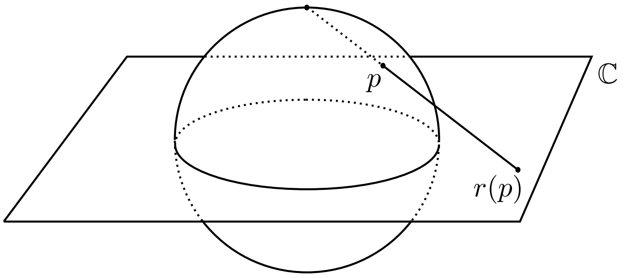
$$\hat{\mathbb{C}} := \mathbb{C} \cup \{\infty\},$$

where we add a single new element to the complex numbers, called ∞.

Remark 1.6.1. One can think of $\hat{\mathbb{C}}$ as the sphere, using the following construction known as *stereographic projection.* Let

$$S^2 := \{(x, y, z) \in \mathbb{R} \mid x^2 + y^2 + z^2 = 1\}$$

be the unit sphere, and define a function $r : S^2 \to \hat{\mathbb{C}}$ by sending a point $p = (x, y, z) \in S^2$ to the intersection point $r(p)$ of the line going from the north pole $N = (0, 0, 1)$ through the point (x, y, z) with the xy-plane (which we consider to be the complex plane).



Such a line is uniquely defined for $(x, y, z) \neq (0, 0, 1)$, and we define $r(0, 0, 1) = \infty$. You can then check that r is a bijection.

For $a, b, c, d \in \mathbb{C}$ we then define a function $f : \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ by

$$f(z) = \begin{cases} \frac{az+b}{cz+d} & \text{if } z \neq \infty, -\frac{d}{c} \\ \infty & \text{if } z = -\frac{d}{c} \\ \frac{a}{c} & \text{if } z = \infty \end{cases} \in \hat{\mathbb{C}}.$$

It will be convenient to always write this as $\frac{az+b}{cz+d}$, where the special cases are interpreted using $\frac{1}{0} = \infty$ and $\frac{a\infty}{c\infty} = \frac{a}{c}$. (These interpretations are particular to $\hat{\mathbb{C}}$, and you should not try to use them elsewhere.)

Secondly, we have

$$\frac{az+b}{cz+d} = \frac{a(cz+d)}{c(cz+d)} - \frac{ad-bc}{c(cz+d)}$$

so if $ad-bc=0$ then this function is $\frac{a}{c}$ for many values of z, so does not have an inverse. As we wish such maps to form a group, we must exclude this: we say that such a function is a *Möbius transformation* if $ad-bc \neq 0$, and we define

Lecture 6

$$\mathcal{M} := \{f : \hat{\mathbb{C}} \to \hat{\mathbb{C}} \,|\, f \text{ is a Möbius transformation}\}.$$

Taking $a=d=1$ and $b=c=0$ gives $f(z)=z$, so the identity map of $\hat{\mathbb{C}}$ is a Möbius transformation. If f' is the Möbius transformation given by a',b',c',d' then for most values of z the following calculation is valid:

$$\begin{aligned} f'(f(z)) &= \frac{a'(\frac{az+b}{cz+d})+b'}{c'(\frac{az+b}{cz+d})+d'} \\ &= \frac{a'(az+b)+b'(cz+d)}{c'(az+b)+d'(cz+d)} \\ &= \frac{(a'a+b'c)z+(a'b+b'd)}{(c'a+d'c)z+(c'b+d'd)} \\ &=: \frac{a''z+b''}{c''z+d''} \end{aligned}$$

where

$$\begin{bmatrix} a'' & b'' \\ c'' & d'' \end{bmatrix} = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

so

$$a''d''-b''c'' = \det \begin{bmatrix} a'' & b'' \\ c'' & d'' \end{bmatrix} = \det \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = (a'd'-c'b')(ad-bc) \neq 0,$$

which says that $f' \circ f$ agrees at most points z with the Möbius transformation given by a'',b'',c'',d''. One can laboriously check that they also agree at the remaining exceptional values of z, so the composition of Möbius transformations is again a Möbius transformation.

Theorem 1.6.2. *The data* $(\mathcal{M}, \circ, \mathrm{Id})$ *is a group.*

Proof. Axiom (G1) is satisfied as composition of functions is associative, and Axiom (G2) also holds as $f \circ \mathrm{Id} = f$ for *any* function f. To verify (G3) consider the Möbius transformation $g(z) = \frac{dz-b}{-cz+a}$: it is easy to see that $f \circ g = \mathrm{Id}$ using the formula for composition of Möbius transformations above. □

For $a \in \mathbb{C}$ consider the Möbius transformation $\frac{1}{z-a}$. This sends the point $a \in \mathbb{C} \subset \hat{\mathbb{C}}$ to the point $\infty \in \hat{\mathbb{C}}$, so its inverse $\frac{az+1}{z}$ sends ∞ to a. This means that the point $\infty \in \hat{\mathbb{C}}$ *is not special in any way*, as there are elements of $\mathcal{M}$ which interchange it with any other point of $\hat{\mathbb{C}}$. You should spend some time thinking about this from the point of view of Remark 1.6.1.

Proposition 1.6.3. *Every Möbius transformation is a composition of Möbius transformations of the following forms:*

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

(ii) $f(z) = z + b$, *(translation)*

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

Proof. Let $\frac{az+b}{cz+d}$ be a Möbius transformation. If $c \neq 0$ then $\frac{az+b}{cz+d} = \frac{a}{c} + \frac{bc-ad}{c(cz+d)}$ which is the composition

$$z \overset{(i)}{\mapsto} cz \overset{(ii)}{\mapsto} cz + d \overset{(i)}{\mapsto} c(cz+d) \overset{(iii)}{\mapsto} \frac{1}{c(cz+d)} \overset{(i)}{\mapsto} \frac{bc-ad}{c(cz+d)} \overset{(ii)}{\mapsto} \frac{a}{c} + \frac{bc-ad}{c(cz+d)}.$$

If $c = 0$ then $\frac{az+b}{cz+d} = \frac{az+b}{d} = \frac{a}{d}z + \frac{b}{d}$ is the composition

$$a \overset{(i)}{\mapsto} \frac{a}{d}z \overset{(ii)}{\mapsto} \frac{a}{d}z + \frac{b}{d}.$$ □

1.6.2 Fixed points, transitivity, and conjugation

Definition 1.6.4. A *fixed point* of a Möbius transformation $f : \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ is a $z_0 \in \hat{\mathbb{C}}$ such that $f(z_0) = z_0$.

Theorem 1.6.5. *A Möbius transformation with at least 3 fixed points is the identity.*

Proof. Let $f(z) = \frac{az+b}{cz+d}$. If ∞ is a fixed point then $\infty = f(\infty)$ and so $c = 0$. If z_0 is another fixed point, which now is not ∞, then it satisfies $z_0 = \frac{az_0+b}{d}$ which we can rearrange to

$$(d-a)z_0 - b = 0.$$

This is a linear equation so has at most 1 solution (namely $z_0 = \frac{b}{d-a}$) unless $b = 0$ and $a = d$, but then $f = \mathrm{Id}$. The latter must occur if f has 3 fixed points.

On the other hand if ∞ is not a fixed point then there are three complex numbers satisfying $z_0 = \frac{az_0+b}{cz_0+d}$, so satisfying

$$cz_0^2 + (d-a)z_0 - b = 0.$$

But this is a quadratic equation, so has at most 2 solutions unless $b = c = 0$ and $a = d$, but then $f = \mathrm{Id}$. The latter must occur if f has 3 fixed points. □

Theorem 1.6.6. *If* $z_1, z_2, z_3 \in \hat{\mathbb{C}}$ *and* $w_1, w_2, w_3 \in \hat{\mathbb{C}}$ *are two triples of distinct points, then there is a unique* $f \in \mathcal{M}$ *such that* $f(z_1) = w_1$, $f(z_2) = w_2$, *and* $f(z_3) = w_3$.

Proof. Suppose first that $w_1 = 0$, $w_2 = 1$, and $w_3 = \infty$. If $z_i \neq \infty$ for all i then we can take

$$f(z) = \frac{(z_2 - z_3)(z - z_1)}{(z_2 - z_1)(z - z_3)}.$$

If $z_1 = \infty$ then use $\frac{z_2-z_3}{z-z_3}$. If $z_2 = \infty$ then use $\frac{z-z_1}{z-z_3}$. If $z_3 = \infty$ then use $\frac{z-z_1}{z_2-z_1}$.

Now for any w_i as above we can first find a h sending $(z_1, z_2, z_3) \mapsto (0, 1, \infty)$, and we may also find a g sending $(w_1, w_2, w_3) \mapsto (0, 1, \infty)$, so $f := g^{-1} \circ h$ is a Möbius transformation satisfying the required property.

We now need to show that this is unique. If $k \in \mathcal{M}$ is another Möbius transformation satisfying this property, then $k^{-1} \circ f$ fixes the points z_1, z_2, and z_3, so is the identity by Theorem 1.6.5. □

The slogans of Theorems 1.6.6 and 1.6.5 are

"there are Möbius transformations sending any 3 points to any other 3 points"

and

"if two Möbius transformations agree at 3 points, then they are equal".

We introduce the following notion now, but will return to it in more detail later in these notes.

Lecture 7

Definition 1.6.7. If G is a group then elements $a, b \in G$ are called *conjugate* if there is a $g \in G$ such that $b = gag^{-1}$. (Note that $a = g^{-1}bg$, too, and if b and c are also conjugate, via $c = hbh^{-1}$, then we have $c = (hg)a(hg)^{-1}$ so a and c are conjugate.)

Applying this concept to the Möbius group, we will make use of the following simple observation: a Möbius transformation f fixes a point x if and only if gfg^{-1} fixes $g(x)$. In particular, if f fixes exactly n points then gfg^{-1} also fixes exactly n points. The following theorem shows that a partial converse to this also holds.

Theorem 1.6.8. *Every Möbius transformation f except the identity has 1 or 2 fixed points. If f has precisely 1 fixed point then it is conjugate to $z \mapsto z+1$. If f has precisely 2 fixed points then it is conjugate to $z \mapsto az$ for some $a \in \mathbb{C} \setminus \{0\}$.*

Proof. We already saw in Theorem 1.6.5 that if $f \neq \mathrm{Id}$ then it has at most 2 fixed points. By considering the quadratic equation $cz^2 + (d-a)z - b = 0$ for $z \in \mathbb{C}$, which must have some solution, we see that f must have at least 1 fixed point.

If f has precisely 1 fixed point, say z_0, choose a $z_1 \in \mathbb{C}$ which is not fixed by f, and consider $(z_1, f(z_1), z_0)$. These are distinct points (if $f(z_1) = z_0$ then $z_1 = f^{-1}(z_0) = z_0$, as z_0 is fixed by f) so there is a Möbius transformation g sending $(z_1, f(z_1), z_0) \mapsto (0, 1, \infty)$. Now gfg^{-1} fixes ∞ and sends 0 to 1, so must be equal to $z \mapsto az + 1$ for some $a \in \mathbb{C}$. If $a \neq 1$ then this has $z_0 = \frac{1}{1-a}$ as a fixed point, contradicting that ∞ is the only fixed point of gfg^{-1}. Thus $a = 1$ and $gfg^{-1}(z) = z + 1$.

I forgot to say this last part in lectures.

If f has precisely 2 fixed points z_0 and z_1, let g be any Möbius transformation sending $(z_0, z_1) \mapsto (0, \infty)$, so gfg^{-1} fixes 0 and ∞. If $(gfg^{-1})(1) = a$ then we must have gfg^{-1} must be equal to $z \mapsto az$. □

We may use this theorem to efficiently calculate iterates f^n, $n \in \mathbb{N}$, of a Möbius transformation f. We can find a $g \in \mathcal{M}$ such that gfg^{-1} is either $z \mapsto z + 1$ or $z \mapsto az$. Now

$$(gfg^{-1})^n = (gfg^{-1})(gfg^{-1}) \cdots (gfg^{-1}) = gf\cancel{(g^{-1}g)}f \cdots fg^{-1} = gf^ng^{-1}$$

so in the first case we have $f^n = g^{-1}(z \mapsto z + n)g$ and in the second case we have $f^n = g^{-1}(z \mapsto a^n z)g$.

1.6.3 Circles

Definition 1.6.9. A *circle* in $\hat{\mathbb{C}}$ is the set of $z \in \hat{\mathbb{C}}$ which satisfy the equation

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

where $A, C \in \mathbb{R}$ and $|B|^2 > AC$. We consider $\infty \in \hat{\mathbb{C}}$ to be a solution to this equation if and only if $A = 0$.

This may not sound like circles you are used to! However, for $b \in \mathbb{C}$ and $r \in \mathbb{R}$ greater than 0, the set

$$\{z \in \mathbb{C} \text{ such that } |z - b| = r\}$$

is the circle of radius r centred at b, and this can be written as the set of solutions to

$$(z - b)\overline{(z - b)} - r = 0$$

or in other words $z\bar{z} - b\bar{z} - \bar{b}z + b\bar{b} - r = 0$, which is a special case of the above with $A = 1$, $B = -b$, and $C = b\bar{b} - r$. So ordinary circles in $\mathbb{C}$ are an example of "circles" as in Definition 1.6.9.

On the other hand, for $a, b, c \in \mathbb{R}$ the set

$$\{z \in \mathbb{C} \text{ such that } a\mathrm{Re}(z) + b\mathrm{Im}(z) = c\} \cup \{\infty\}$$

is a straight line in $\mathbb{C}$ (and ∞), and this can be written as the set of solutions to

$$\overline{\frac{a + ib}{2}}z + \frac{a + ib}{2}\bar{z} - c = 0,$$

which is a special case of the above with $A = 0$, $B = \frac{a+ib}{2}$, and $C = -c$. So straight lines in $\mathbb{C}$ (and ∞) are also an example of "circles" as in Definition 1.6.9.

I leave it as an exercise to show that the set of solutions to the equation in Definition 1.6.9 are always of one of these two forms: a circle in $\mathbb{C}$ or a line in $\mathbb{C}$ along with ∞. The reason for calling all of these "circles" is that under stereographic projection (as in Remark 1.6.1) they all become circles on the sphere.

Theorem 1.6.10. *Möbius transformations send circles in $\hat{\mathbb{C}}$ to circles in $\hat{\mathbb{C}}$.*

Proof. By Proposition 1.6.3 it is enough to check this for the Möbius transformations $z \mapsto az$, $z \mapsto z + b$, and $z \mapsto \frac{1}{z}$. If we write $S_{A,B,C}$ for the circle given by the solutions to

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

I messed up these formulæ in lectures.

then under $z \mapsto az$ it is sent to the circle $S_{A/a\bar{a},B/\bar{a},C}$, and under $z \mapsto z + b$ it is sent to the circle $S_{A,B-Ab,C+Ab\bar{b}-\bar{B}b-B\bar{b}}$. Under $z \mapsto w = \frac{1}{z}$ solutions to the above equation become solutions to

$$A + \bar{B}\bar{w} + Bw + Cw\bar{w} = 0$$

so $S_{A,B,C}$ is sent to $S_{C,\bar{B},A}$. □

As a circle is determined by 3 points on it, and Möbius transformations are determined by where they send 3 points, in practice it is very easy to find Möbius transformations sending a given circle to another given circle. For example, to send the unit circle in $\mathbb{C}$ to the circle $\mathbb{R} \cup \{\infty\}$, we just observe that $(-1, i, 1)$ lie on the unit circle, and $(-1, 0, 1)$ lie on the real axis, so we need any Möbius transformation fixing ± 1 and sending i to 0. For example, $\frac{z-i}{1-iz}$ will do.

1.6.4 The cross-ratio

We will study the relationship between the Möbius transformations and the so-called cross-ratio. The following is a temporary definition: we will make a better one later, after developing a little theory.

Definition 1.6.11 (Temporary)**.** Given four distinct points $z_1, z_2, z_3, z_4 \in \hat{\mathbb{C}}$, their *cross-ratio* is[7]

$$[z_1, z_2, z_3, z_4] := \frac{(z_4 - z_1)(z_2 - z_3)}{(z_2 - z_1)(z_4 - z_3)} \in \hat{\mathbb{C}},$$

to be interpreted carefully if any z_i is equal to ∞, for example as

$$[\infty, z_2, z_3, z_4] = \frac{\cancel{(z_4 - \infty)}(z_2 - z_3)}{\cancel{(z_2 - \infty)}(z_4 - z_3)} = \frac{z_2 - z_3}{z_4 - z_3}$$

and so on.

This definition is not very satisfying, as (i) we have no idea what the *meaning* of the cross-ratio is, and (ii) there is an *ad hoc* rule for evaluating it when some z_i is ∞. We reinterpret the cross-ratio as follows.

Corollary 1.6.12 (Re-definition)**.** *If $z_1, z_2, z_3, z_4 \in \hat{\mathbb{C}}$ are distinct then their cross-ratio is*

$$[z_1, z_2, z_3, z_4] = f(z_4),$$

where $f \in \mathcal{M}$ is the unique Möbius transformation satisfying $f(z_1) = 0$, $f(z_2) = 1$, and $f(z_3) = \infty$.

Proof. As in the proof of Theorem 1.6.6, if $z_i \neq \infty$ for all i, then

$$f(z) = \frac{(z_2 - z_3)(z - z_1)}{(z_2 - z_1)(z - z_3)}$$

ia *a* Möbius transformation satisfying $f(z_1) = 0$, $f(z_2) = 1$, and $f(z_3) = \infty$, and is the unique such. It satisfies $f(z_4) = [z_1, z_2, z_3, z_4]$ by definition of the cross-ratio.

If $z_1 = \infty$ then use $\frac{z_2 - z_3}{z - z_3}$. If $z_2 = \infty$ then use $\frac{z - z_1}{z - z_3}$. If $z_3 = \infty$ then use $\frac{z - z_1}{z_2 - z_1}$. □

Using this new—better—definition, we can show that the cross-ratio is unchanged under Möbius transformations.

[7] There are $4! = 24$ possible conventions for this, given by permuting the z_i, and many conventions are in use. Always say what you mean by the cross-ratio!

Theorem 1.6.13. *If $z_1, z_2, z_3, z_4 \in \hat{\mathbb{C}}$ and $g \in \mathcal{M}$, then*

$$[g(z_1), g(z_2), g(z_3), g(z_4)] = [z_1, z_2, z_3, z_4].$$

Proof. Let $f \in \mathcal{M}$ be the unique Möbius transformation satisfying $f(z_1) = 0$, $f(z_2) = 1$, and $f(z_3) = \infty$, so that $f(z_4) = [z_1, z_2, z_3, z_4]$. Now $f \circ g^{-1}(g(z_1)) = 0$, $f \circ g^{-1}(g(z_2)) = 1$, and $f \circ g^{-1}(g(z_3)) = \infty$, and $f \circ g^{-1}$ is the unique such Möbius transformation, so

$$[g(z_1), g(z_2), g(z_3), g(z_4)] = (f \circ g^{-1})(g(z_4)) = f(z_4) = [z_1, z_2, z_3, z_4]$$

as required. □

Corollary 1.6.14. *Points $z_1, z_2, z_3, z_4 \in \hat{\mathbb{C}}$ lie on a circle if and only if $[z_1, z_2, z_3, z_4] \in \mathbb{R}$.*

Proof. Let g be the unique Möbius transformation sending (z_1, z_2, z_3) to $(0, 1, \infty)$, so that $[z_1, z_2, z_3, z_4] = g(z_4)$. If S denotes the circle passing through (z_1, z_2, z_3), it is sent by g to the circle passing through $(0, 1, \infty)$, which is $\mathbb{R} \cup \{\infty\}$. Thus z_4 lies on C if and only if $g(z_4)$ lies on $\mathbb{R} \cup \{\infty\}$, so $[z_1, z_2, z_3, z_4] \in \mathbb{R}$, as required. □

Chapter 2

Group actions

2.1 Actions of groups

Lecture 8

We motivated our definition of a group G as the symmetries of an object X, but in the actual definition of a group we abstracted the properties that symmetries of an object have and there was no longer an X. Here we will redress this, and explain how we can think of G as giving symmetries of some X.

Definition 2.1.1. An *action* of a group $(G, \cdot, e)$ on a set X is a function $* : G \times X \to X$ satisfying

(A1) For all $x \in X$ we have $e * x = x$. (identity)

(A2) For all $a, b \in G$ and $x \in X$ we have $(a \cdot b) * x = a * (b * x)$. (associativity)

Most of the examples of groups be have seen have sets which they naturally act on.

Example 2.1.2.

(i) Any group G acts on any set X by the *trivial action* $g * x = x$.

(ii) Any group G acts on the set $X = G$ by the so-called *left regular action* $g * g' = g \cdot g'$.

(iii) The symmetric group $\mathrm{Sym}(X)$ acts on X by $f * x = f(x)$.

(iv) The group of symmetries of a solid X acts on the set of points of X (or the set of vertices of X, or edges of X).

(v) The dihedral group D_{2n} acts on the set of vertices of the regular n-gon.

(vi) The Möbius group $\mathcal{M}$ acts on $\hat{\mathbb{C}}$ by Möbius transformations. △

There is a different but equivalent way of thinking about group actions, as follows, and it is very useful to be able to pass between the two descriptions.

Theorem 2.1.3. *An action $*$ of a group G on a set X is the same as a homomorphism $\rho : G \to \mathrm{Sym}(X)$.*

Proof. Given an action $*$ and a $g \in G$, consider the function

$$\begin{aligned} t_g : X &\longrightarrow X \\ x &\longmapsto g * x. \end{aligned}$$

There is a similar function $t_{g^{-1}}$, and these satisfy

$$\begin{aligned} t_{g^{-1}}(t_g(x)) &= g^{-1} * (g * x) \\ &= (g^{-1} \cdot g) * x \text{ by (A2)} \\ &= e * x \text{ by (G3)} \\ &= x \text{ by (A1)} \end{aligned}$$

so $t_{g^{-1}} \circ t_g = \mathrm{Id}$, and similarly $t_g \circ t_{g^{-1}} = \mathrm{Id}$. Thus t_g is an invertible function, so is an element of $\mathrm{Sym}(X)$. This discussion defines a function

$$\begin{aligned} \rho : G &\longrightarrow \mathrm{Sym}(X) \\ g &\longmapsto t_g. \end{aligned}$$

Now $t_{g \cdot g'}(x) = (g \cdot g') * x$ is the same as $g * (g' * x)$ by (A2), which is $t_g(t_{g'}(x))$. This holds for all $x \in X$, so $t_{g \cdot g'} = t_g \circ t_{g'}$, or in other words $\rho(g \cdot g') = \rho(g) \circ \rho(g')$, so ρ is a homomorphism, as required.

Conversely, suppose that a homomorphism $\rho : G \to \mathrm{Sym}(X)$ is given, and define a function

$$\begin{aligned} * : G \times X &\longrightarrow X \\ (g, x) &\longmapsto \rho(g)(x). \end{aligned}$$

Now $e * x = \rho(e)(x) = \mathrm{Id}(x) = x$, so (A1) is satisfied. Also

$$(a \cdot b) * x = \rho(a \cdot b)(x) = (\rho(a) \circ \rho(b))(x) = \rho(a)(\rho(b)(x)) = a * (b * x)$$

so (A2) is satisfied. □

Using this construction we may prove the following theorem of Cayley.

Theorem 2.1.4 (Cayley)**.** *Any group is isomorphic to a subgroup of some symmetric group.*

Proof. Consider the left regular action of G on the set $X = G$ as in Example 2.1.1 (ii). By the construction in Theorem 2.1.3 this corresponds to a homomorphism $\rho : G \to \mathrm{Sym}(G)$. The image $\mathrm{Im}(\rho)$ of ρ is a subgroup of $\mathrm{Sym}(G)$, and we may consider ρ as a homomorphism $\rho : G \to \mathrm{Im}(\rho)$. If $g \in \mathrm{Ker}(\rho)$ then $g * h = h$ for all $h \in G$, but as $g * h = g \cdot h$ it then follows that $g = e$, so $\mathrm{Ker}(\rho) = \{e\}$. It then follows from Lemma 1.4.6 that $\rho : G \to \mathrm{Im}(\rho)$ is an isomorphism, so G is isomorphic to $\mathrm{Im}(\rho)$, which is a subgroup of $\mathrm{Sym}(G)$. □

You might think this means that a typical group cannot be so complicated, as it is just some group of permutations of a set: in fact it really means that symmetric groups are very complicated indeed.

Definition 2.1.5. Let G act on X.

(i) The *orbit* of $x \in X$ is

$$Gx := \{y \in X \mid y = g * x \text{ for some } g \in G\}.$$

The action is called *transitive* if $Gx = X$ for all $x \in X$.

(ii) The *stabiliser* of $x \in X$ is

$$G_x := \{g \in G \mid g * x = x\}.$$

In other words it is the set of those elements of G which fix x.

(iii) The *kernel* of the action is the kernel of the associated homomorphism $\rho : G \to \mathrm{Sym}(X)$. In other words it is the set of those elements of G which fix all $x \in X$; we can also describe it as $\cap_{x \in X} G_x$. The action is called *faithful* if its kernel is $\{e\}$.

Theorem 2.1.6. *Let G act on X.*

(i) For each $x \in X$, G_x is a subgroup of G.

(ii) The orbits $\{Gx\}$ partition X.

Proof. For part (i), let $a, b \in G_x$. First note that

$$x = e * x = (b^{-1} \cdot b) * x = b^{-1} * (b * x) = b^{-1} * x,$$

as $b * x = x$, so $b^{-1} \in G_x$. Now

$$(a \cdot b^{-1}) * x = a * (b^{-1} * x) = a * x = x$$

so $a \cdot b^{-1} \in G_x$, and so G_x is a subgroup of G by Proposition 1.2.9.

For part (ii), first note that every element of X certainly lies in some orbit. Now suppose that $(Gx) \cap (Gy) \neq \varnothing$, so that we may choose a $z \in (Gx) \cap (Gy)$. As $z \in Gx$ there is a $g \in G$ such that $z = g * x$, and as $z \in Gy$ there is a $g' \in G$ such that $z = g' * y$. Now any element of Gy may be written as $g'' * y$ for some $g'' \in G$, but then

$$g'' * y = g'' * ((g')^{-1} * z) = g'' * ((g')^{-1} * (g * x)) = (g'' \cdot (g')^{-1} \cdot g) * x$$

which lies in Gx. This shows that $Gy \subset Gx$, and the analogous argument shows the reverse inclusion too. □

Strictly speaking what we have described in Definition 2.1.1 is a *left* action of a group G on a set X. A *right action* of G on X is a function

$$\bullet : X \times G \longrightarrow X$$

such that $x \bullet e = x$ and $x \bullet (a \cdot b) = (x \bullet a) \bullet b$ for all $x \in X$ and all $a, b \in G$. We will write xG for the orbit of x for a right action of G, but use the same notation G_x for the stabiliser. The analogue of Theorem 2.1.6 holds for right actions, with the same proof.

Left and right actions are actually equivalent, as follows: if $*$ is a left action then $x \bullet g := g^{-1} * x$ defines a right action, and if $\bullet$ is a right action then $g * x := x \bullet g^{-1}$ defines a left action. We will always mean left actions, unless we specify otherwise. Lecture 9

Definition 2.1.7. If G has a left action on X then we write $G\backslash X$ for the *set of orbits*. That is

$$G\backslash X := \{\mathcal{O} \subset X \mid \mathcal{O} = Gx \text{ for some } x \in X\}.$$

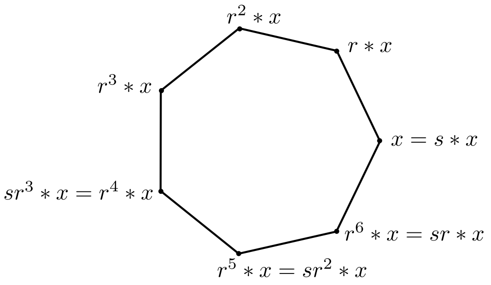
If G has a right action on X then we write X/G for the set of orbits, which is

$$X/G := \{\mathcal{O} \subset X \mid \mathcal{O} = xG \text{ for some } x \in X\}.$$

Theorem 2.1.6 contains several ideas which one must struggle to get used to. An orbit is a subset $\mathcal{O} \subset X$ which happens to be equal to Gx for some $x \in X$, and in this case it will also equal to Gx' for any $x' \in \mathcal{O}$. While it is often useful to choose an element $x \in \mathcal{O}$ to be able to say $\mathcal{O} = Gx$, we must then make sure that whatever we do with this orbit does not depend on this choice.

So far in mathematics you have probably thought of sets (such as $\mathbb{C}$) as being collections of objects (such as complex numbers) which you want to study, and constructions with sets (such as $\mathbb{C} \setminus \{0\}$) as making more precise which objects to consider. This is a valid use of sets, but in advanced mathematics certain sets *are* the objects we want to study. There is a psychological leap you will need to make—which takes time and practice—between thinking of sets as collections of interesting objects and thinking of sets as interesting objects in their own right.

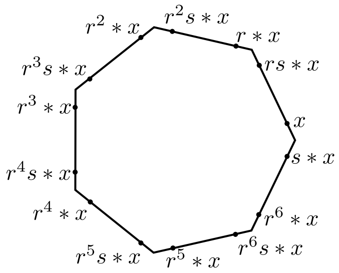
Example 2.1.8. By definition the group $G = D_{2n}$ acts on the regular n-gon, which here we shall call X. As indicated in the following figure, if $x \in X$ is a vertex then its orbit Gx has size n, and is given by the set of vertices.



It is easy to convince yourself that in this case the stabiliser G_x of x is just the identity map and the reflection in the line passing through 0 and x (in the figure it is the subgroup $\{\mathrm{Id}, s\}$ of D_{14}), so is a group of order 2. So we have

$$|Gx| \cdot |G_x| = n \cdot 2 = 2n = |G|.$$

On the other hand, suppose that $x \in X$ lies on an edge, and not in the middle of an edge. As indicated in the following figure its orbit Gx has size $2n$.

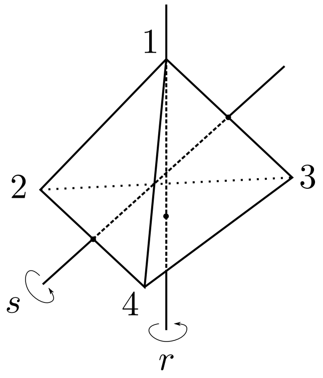


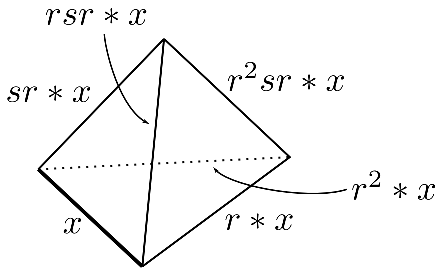
It is easy to convince yourself that in this case the stabiliser G_x of x is just the identity map, so is the trivial subgroup of D_{2n}. So we have

$$|Gx| \cdot |G_x| = 2n \cdot 1 = 2n = |G|. \qquad \triangle$$

Example 2.1.9. Let G be the group of rotational symmetries the regular tetrahedron, as in Section 1.1. It acts on the tetrahedron itself, but also acts on various sets associated with the tetrahedron.

As a first example, G acts on the set V of vertices of the tetrahedron. This is a set of size 4, and we can name the vertices $1, 2, 3, 4$ as in the first figure below.





It is then easy to see that the action of G on V is transitive, i.e. there is a single orbit, or in other words we can get from any element to any other by acting with elements of G. For example to get from 1 to 4 we can go

$$1 \overset{s}{\mapsto} 3 \overset{r}{\mapsto} 2 \overset{r}{\mapsto} 4,$$

which also show us how to get from 1 to 2 or 1 to 3. It is easy to convince yourself that the stabiliser of the vertex 1 is $\{\mathrm{Id}, r, r^2\}$, a cyclic group of order 3. Thus

$$|G1| \cdot |G_1| = 4 \cdot 3 = 12 = |G|.$$

As a second example, acts on the set E of edges of the tetrahedron. This is a set of size 6, and as in the second figure above we see that the G-action on E is transitive: we can get from the edge labelled x to any other. We have $s * x = x$ (the element $s \in G$ "turns the edge x around", but this is the same edge), and it is easy to convince yourself that the stabiliser of the edge x is $\{\mathrm{Id}, s\}$. Thus

$$|Gx| \cdot |G_x| = 6 \cdot 2 = 12 = |G|. \qquad \triangle$$

We have now seen many examples where the identity $|Gx| \cdot |G_x| = |G|$ holds, and we will soon show that this is true for any action of any finite group on any set: this is the so-called *Orbit-Stabiliser Theorem.* In the examples above we saw that given an $x \in X$ it is relatively easy to work out its orbit, and is typically not hard to come up with *some* elements in its stabiliser G_x, but it is not usually completely obvious whether we have found *all* elements in the stabiliser (in the examples I said "it is easy to convince yourself..."). The Orbit-Stabiliser Theorem is very useful for this, as rearranging it tells us that there are precisely $|G_x| = \frac{|G|}{|Gx|}$ to find.

Our goal is now to prove the Orbit-Stabiliser Theorem, for which we will have to make some preparations which are very important in their own right.

2.2 The regular action

In Example 2.1.2 (ii) we already saw the *left regular action* of the group G on the set $X = G$, given by $g * g' = g \cdot g'$. Similarly, there is a right action of G on the set $X = G$ given by $g' \bullet g = g' \cdot g$. If $H \leq G$ is a subgroup then we similarly obtain a left action of the group H on the set G via

$$\begin{aligned} * : H \times G &\longrightarrow G \\ (h, g) &\longmapsto h \cdot g, \end{aligned}$$

which we again call the *left regular action of H on G*, and a right action of H on the set G via

$$\begin{aligned} \bullet : G \times H &\longrightarrow G \\ (g, h) &\longmapsto g \cdot h, \end{aligned}$$

called the *right regular action of H on G.* These actions are so fundamental that their orbits have special names.

Definition 2.2.1. A *left coset* of H in G is an orbit of the right regular action of H on G. We write G/H for the set of orbits of this action, and call it the *set of left cosets.*

Similarly, a *right coset* of H in G is an orbit of the left regular action of H on G, and we write $H \backslash G$ for the set of orbits of this action, the *set of right cosets.*

Let us work out what this means. If $g \in G$ then its left coset is

$$gH := \{g' \in G \,|\, g' = g \cdot h \text{ for some } h \in H\}$$

and its right coset is

$$Hg := \{g' \in G \,|\, g' = h \cdot g \text{ for some } h \in H\}.$$

That is, they are the sets of all elements of G we can get by multiplying g by elements of H on the right or left respectively. As above, we write

$$G/H := \{\mathcal{O} \subset G \,|\, \mathcal{O} = gH \text{ for some } g \in G\}$$

for the set of left cosets of H, and

$$H\backslash G := \{\mathcal{O} \subset G \,|\, \mathcal{O} = Hg \text{ for some } g \in G\}$$

for the set of right cosets of H.

Because orbits are disjoint or equal, we have

$$gH = g'H \iff g' \in gH \iff g' = g \cdot h \text{ for some } h \in H \iff g^{-1}g' \in H$$

and

$$Hg = Hg' \iff g' \in Hg \iff g' = h \cdot g \text{ for some } h \in H \iff g'g^{-1} \in H$$

which gives us a useful criterion for checking whether left or right cosets are equal. We often write H for the cosets eH or He, as these are equal sets.

Example 2.2.2.

(i) For the subgroup $2\mathbb{Z} \subset \mathbb{Z}$ of $(\mathbb{Z}, +, 0)$ given by the even integers, we have n and n' lie in the same left coset precisely if $n' - n$ is even. So there are two left cosets: the even integers, and the odd integers. Using additive notation[1], it is natural to call these cosets $2\mathbb{Z}$ and $1 + 2\mathbb{Z}$.

(ii) More generally, the subgroup $n\mathbb{Z} \subset \mathbb{Z}$ has n left cosets, corresponding to the possible remainders when dividing by n.

(iii) The symmetries of the equilateral triangle (the regular 3-gon) is D_6, and we have seen that its 6 elements can be written as

$$\{\mathrm{Id}, r, r^2, s, rs, r^2s\},$$

which we can compose with each other using the identities $r^3 = \mathrm{Id}$, $s^2 = \mathrm{Id}$, and $sr = r^{-1}s = r^2s$. In particular both

$$R := \{\mathrm{Id}, r, r^2\} \text{ and } S := \{\mathrm{Id}, s\}$$

are subgroups. The left cosets of R are

$$\begin{aligned} R = \mathrm{Id}R &= \{\mathrm{Id}, r, r^2\}, \\ sR &= \{s, sr, sr^2\} = \{s, r^2s, r^4s\} = \{s, r^2s, rs\}, \end{aligned}$$

and the right cosets of R are

$$\begin{aligned} R = R\mathrm{Id} &= \{\mathrm{Id}, r, r^2\}, \\ Rs &= \{s, rs, r^2s\}. \end{aligned}$$

[1] It would be confusing to write $02\mathbb{Z}$ and $12\mathbb{Z}$.

The left cosets of S are

$$\begin{aligned} S = \mathrm{Id}S &= \{\mathrm{Id}, s\}, \\ rS &= \{r, rs\}, \\ r^2S &= \{r^2, r^2s\} \end{aligned}$$

but on the other hand $Sr = \{r, sr\} = \{r, r^2s\}$ is a right coset of S. Notice that it is not equal to any left coset of S, but all right cosets of R were equal to left cosets of R. We will investigate this phenomenon later in these notes.

(iv) Let $\mathcal{M}_0 \leq \mathcal{M}$ be the subgroup of the Möbius group given by the stabiliser of $0 \in \hat{\mathbb{C}}$ for the usual left action by Möbius transformations, so

$$\mathcal{M}_0 = \{g \in \mathcal{M} \mid g(0) = 0\}.$$

Now $f\mathcal{M}_0 = f'\mathcal{M}_0$ if and only if $f^{-1}f' \in \mathcal{M}_0$, i.e. if and only if $f^{-1}f'(0) = 0$, or in other words if and only if $f'(0) = f(0)$. So two Möbius transformations represent the same left coset precisely when they act the same way on 0. △

Lecture 10

2.2.1 Lagrange's theorem

To our discussion so far we add the following simple observation: if G is a group and $H \leq G$ then for any $g \in G$ the functions

$$h \mapsto gh : H \longrightarrow gH$$

and

$$x \mapsto g^{-1}x : gH \longrightarrow H$$

are inverse to each other, so gH is in bijection with H. (Similarly, Hg is in bijection with H.)

Recall that we write $|X|$ for the number of elements in a set X, when it is finite.

Theorem 2.2.3 (Lagrange)**.** *If G is a finite group and $H \leq G$ is a subgroup, then $|G| = |H| \cdot |G/H|$. In particular $|H|$ divides $|G|$.*

Proof. Consider the right regular action of H on the set G. By Theorem 2.1.6 (ii) the left cosets $\{gH\}$ partition the set G. As observed above each gH is in bijection with H, so has $|H|$ elements. Thus G is partitioned into $|G/H|$-many sets each of which has $|H|$ elements, so $|G| = |H| \cdot |G/H|$ as required. □

One can repeat the argument with right cosets, giving $|G| = |H| \cdot |H\backslash G|$. This implies that $|G/H| = |H\backslash G|$; it is interesting to try to prove this by finding a bijection between G/H and $H\backslash G$.

Definition 2.2.4. If G is a group and $H \leq G$ is a subgroup, then the *index* of H in G is $|G/H|$, as long as the set G/H is finite (and ∞ otherwise).

Lagrange's theorem then says that if G is finite and $H \leq G$ then the index of H in G may be calculated as $\frac{|G|}{|H|}$. Lagrange's theorem has several easy consequences for the structure of finite groups.

Corollary 2.2.5. *If G is a finite group and $g \in G$, then* $\mathrm{ord}(g)$ *divides* $|G|$*.*

Proof. We have seen that $\mathrm{ord}(g)$ is the same as the order of the subgroup $\langle g \rangle$ of G. But $|\langle g \rangle|$ divides $|G|$ by Lagrange's theorem, giving the conclusion. □

Corollary 2.2.6. *If G is a finite group and $g \in G$, then $g^{|G|} = e$.*

Proof. By the previous corollary we can write $|G| = \mathrm{ord}(g) \cdot N$ for some $N \in \mathbb{Z}$. Then $g^{|G|} = (g^{\mathrm{ord}(g)})^N$ but $g^{\mathrm{ord}(g)} = e$ by definition, and $e^N = e$, giving the conclusion. □

Corollary 2.2.7. *If G is a finite group with order $|G|$ equal to a prime number, then G is cyclic and is generated by any non-identity element.*

Proof. As $|G|$ is a prime number it is greater than 1, so G contains some non-identity element: let g be any such element. Its order is then not 1, but divides $|G|$ which is a prime number: thus $\mathrm{ord}(g) = |G|$. Thus the cyclic group $\langle g \rangle$ has $|G|$ elements, and is a subgroup of G: it must then be equal to G. □

Here is a perhaps surprising application of Lagrange's theorem to a problem in number theory. You will see a different proof of this in IA Numbers and Sets.

To set the stage we must introduce another binary operation on the set $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, different from the "addition modulo n" operation $+_n$ we considered before: we let $a \cdot_n b$ be the remainder left when $a \cdot b$ is divided by n. This binary operation is associative but it *does not* make $\mathbb{Z}_n$ into a group. Although $1 \in \mathbb{Z}_n$ does act as an identity element, we have $0 \cdot_n x = 0$ for all x, so $0 \in \mathbb{Z}_n$ can have no inverse with respect to this binary operation. Which elements do have inverses? If a is coprime to n then we can write $a \cdot b + m \cdot n = 1$ for some integers b and m, but then $a \cdot_n b = 1$ so a indeed has an inverse. Conversely, if $a \cdot_n b = 1$ then $a \cdot b = 1 + m \cdot n$ for some $m \in \mathbb{Z}$, so any common factor of a and n would divide 1. Thus the elements with inverses are precisely those which are coprime to n, and we can set

$$U_n := \{a \in \mathbb{Z}_n \,|\, \text{there is a } b \in \mathbb{Z}_n \text{ such that } a \cdot_n b = 1\} = \{a \in \mathbb{Z}_n \,|\, a \text{ is coprime to } n\}.$$

Using the first description $(U_n, \cdot_n, 1)$ is easily seen to be a group. The set U_n is a subset of $\{0, 1, 2, \ldots, n-1\}$ so is finite, and we write

$$\varphi(n) := |U_n|$$

for the size of this group: the function φ is called *Euler's totient function*, and by definition $\varphi(n)$ counts the numbers less than n which are coprime to n. For example, if p is a prime number then $\varphi(p) = p - 1$ and $\varphi(p^2) = p(p-1)$.

Theorem 2.2.8 (Euler–Fermat)**.** *If a is coprime to n then $a^{\varphi(n)} \equiv 1 \mod n$.*

Proof. By Euclid's algorithm we can write $a = x + m \cdot n$ for some $x \in \{0, 1, \ldots, n-1\}$, and as a is coprime to n, x is too. Thus $x \in U_n$, so by Corollary 2.2.6 we have $x^{\varphi(n)} = x^{|U_n|} = 1$. But

$$a^i = (x + m \cdot n)^i = x^i + \binom{i}{1} x^{i-1} \cdot m \cdot n + \binom{i}{2} x^{i-2} \cdot (m \cdot n)^2 + \cdots \equiv x^i \mod n$$

and so $a^{\varphi(n)} \equiv 1 \mod n$ as required. □

2.2.2 The Orbit-Stabiliser Theorem

Theorem 2.2.9 (Orbit-Stabiliser Theorem)**.** *If a group G acts on a set X and $x \in X$, then the functions*

$$\begin{aligned} \phi : G/G_x &\longrightarrow Gx \\ gG_x &\longmapsto g * x \end{aligned}$$

and

$$\begin{aligned} \psi : Gx &\longrightarrow G/G_x \\ g * x &\longmapsto gG_x \end{aligned}$$

are well-defined and inverse to each other.

Proof. Let us first show that ϕ is well-defined, so suppose that $gG_x = g'G_x$. Then $g' = g \cdot h$ for $h \in G_x$, but this means that we may calculate

$$g' * x = (g \cdot h) * x = g * (h * x) = g * x$$

because $h * x = x$ as $h \in G_x$. Thus $\phi(gG_x) = \phi(g'G_x)$, as required.

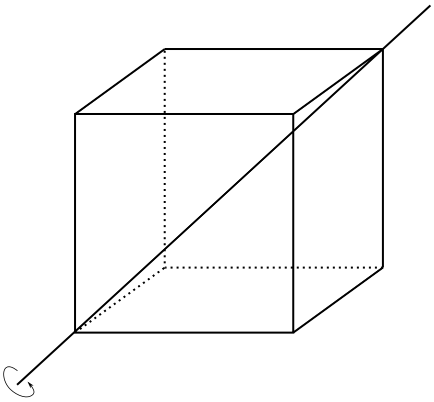
Let us now show that ψ is well-defined, so suppose that $g*x = g'*x$. Then $g^{-1}g' \in G_x$, and so $g'G_x = gG_x$. Thus $\psi(g * x) = \psi(g' * x)$ as required.

Finally, given that the functions are well-defined it is obvious they are inverse to each other. □

Corollary 2.2.10 (Counting version of the Orbit-Stabiliser Theorem)**.** *If a finite group G acts on a set X then we have $|G| = |G_x| \cdot |Gx|$.*

Proof. Combine the Orbit-Stabiliser Theorem with Lagrange's Theorem. □

Example 2.2.11. Let us use the Orbit-Stabiliser theorem to work out the size of the group G of rotational symmetries of the cube. To do so we let it act on the set X of vertices of the cube. We have $|X| = 8$, and there is one orbit for the action of G on X, as a vertex can be taken to any adjacent vertex by an evident rotation.



The stabiliser of a vertex $v \in X$ is the subgroup of rotations about the axis passing through v and the vertex opposite it, and there are 3 such rotations. Thus $|G| = |G_v| \cdot |Gv| = 3 \cdot 8 = 24$. △

Lecture 11

We saw as a consequence of Lagrange's theorem that if G is a finite group and $g \in G$, then the order of g divides $|G|$. The following theorem of Cauchy is a partial converse to this.

Theorem 2.2.12 (Cauchy)**.** *Let G be a finite group and p be a prime number which divides $|G|$. Then G has an element of order p.*

Proof. Let $Y := G^p = \underbrace{G \times G \times \cdots \times G}_{p \text{ times}}$, and let

$$X := \{(g_1, g_2, \ldots, g_p) \in Y \mid g_1 \cdot g_2 \cdots g_p = e\}.$$

In other words, X is the set consisting of lists of p elements of G whose product is e. We have $|Y| = |G|^p$. On the other hand, in the definition of X the elements $(g_1, g_2, \ldots, g_{p-1})$ uniquely determine g_p, as $g_p = (g_1 \cdot g_2 \cdots g_{p-1})^{-1}$, so we have $|X| = |G|^{p-1}$.

Let H denote the cyclic group of order p, which the discussion in Section 1.5 shows that the elements of this group are $\{1 = \xi^0, \xi, \xi^2, \ldots, \xi^{p-1}\}$ where $\xi = e^{2\pi i \frac{1}{n}}$. This group acts on the set X by *rotation*, using the formula

$$\xi^i * (g_1, g_2, \ldots, g_p) = (g_{i+1}, g_{i+2}, \ldots, g_p, g_1, g_2, \ldots, g_i).$$

Note that

$$\begin{aligned} g_{i+1} \cdot g_{i+2} \cdots g_p \cdot g_1 \cdot g_2 \cdots g_i &= (g_{i+1} \cdot g_{i+2} \cdots g_p) \cdot (g_1 \cdot g_2 \cdots g_p) \cdot (g_{i+1} \cdot g_{i+2} \cdots g_p)^{-1} \\ &= (g_{i+1} \cdot g_{i+2} \cdots g_p) \cdot e \cdot (g_{i+1} \cdot g_{i+2} \cdots g_p)^{-1} \\ &= e \end{aligned}$$

so this does indeed lie in the set X. It is easy to verify the axioms (A1) and (A2).

By the corollary to the Orbit-Stabiliser Theorem applied to this action, for each $x \in X$ we have $p = |H| = |H_x| \cdot |Hx|$, and as p is a prime number it follows that each orbit of this action has size 1 or p. Furthermore, if $(g_1, g_2, \ldots, g_p)$ is an element lying in an orbit of size 1 then

$$(g_1, g_2, \ldots, g_p) = \xi * (g_1, g_2, \ldots, g_p) = (g_2, \ldots, g_p, g_1)$$

and so $g_1 = g_2 = g_3 = \cdots = g_p$, but also $g_1 \cdot g_2 \cdots g_p = e$. Thus the orbits of size 1 are precisely given by the lists $(g, g, \ldots, g)$ such that $g^p = e$, i.e. g has order 1 or p. There is precisely one element of order 1, namely e, so this says that

$$(\#\text{ of orbits of size } 1) = 1 + (\#\text{ of elements of } G \text{ of order } p). \tag{$*$}$$

As X is a disjoint union of orbits, it follows that

$$|X| = 1 \cdot (\#\text{ of orbits of size } 1) + p \cdot (\#\text{ of orbits of size } p)$$

but on the other hand $|X| = |G|^{p-1}$ and p divides $|G|$, so p divides $|X|$. Putting these facts together we find that p divides (# of orbits of size 1). Combining this with $(*)$, it follows that there are at least $p - 1$ elements of order p, as required. □

2.3 The conjugation action

There is another way that a group can act on itself, different to the regular action discussed in the last section: via conjugation.

Definition 2.3.1. The *conjugation action* of the group G on the set G is given by

$$g * h := g \cdot h \cdot g^{-1}.$$

This is indeed an action as $e * h = e \cdot h \cdot e^{-1} = h$ and

$$\begin{aligned} k * (g * h) &= k * (g \cdot h \cdot g^{-1}) \\ &= k \cdot (g \cdot h \cdot g^{-1}) \cdot k^{-1} \\ &= (k \cdot g) \cdot h \cdot (k \cdot g)^{-1} \\ &= (k \cdot g) * h. \end{aligned}$$

Definition 2.3.2. The *conjugacy classes* of G are the orbits of the conjugation action. The conjugacy class of $h \in G$ is written $\mathrm{ccl}(h)$ and is

$$\mathrm{ccl}(h) := \{k \in G \ s.t.\ k = g \cdot h \cdot g^{-1} \text{ for some } g \in G\}.$$

The *centraliser* of h is the stabiliser of $h \in G$ for the conjugation action, is written as $C_G(h)$ and is

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

The *centre* of G is the kernel of the conjugation action, is written $Z(G)$ and is

$$Z(G) := \{g \in G \ s.t.\ g \cdot h \cdot g^{-1} = h \text{ for all } h \in G\}.$$

Example 2.3.3.

(i) Let $G = D_{2n}$ be the nth dihedral group, whose elements are

$$D_{2n} = \{\mathrm{Id}, r, r^2, r^3, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\},$$

and in which we have $r^n = \mathrm{Id}$, $s^2 = \mathrm{Id}$, and $sr = r^{n-1}s$. We have

$$\begin{aligned} s * r^i &= sr^is^{-1} = sr^is \\ &= r^{(n-1)i}s^2 = r^{n-i}, \end{aligned}$$

and $r * r^i = r^i$: using the properties of an action this determines $g * r^i$ for any $g \in D_{2n}$.

We have

$$\begin{aligned} s * (r^is) &= s(r^is)s^{-1} = sr^i \\ &= r^{(n-1)i}s = r^{n-i}s, \end{aligned}$$

and

$$\begin{aligned} r * (r^is) &= r(r^is)r^{-1} \\ &= r^{i+2}s : \end{aligned}$$

using the properties of an action this determines $g * (r^is)$ for any $g \in D_{2n}$.

(ii) In the Möbius group $\mathcal{M}$, we have seen that a Möbius transformation with precisely 1 fixed point is conjugate to $z \mapsto z+1$, and a Möbius transformation with precisely 2 fixed points is conjugate to $z \mapsto az$ for some $a \in \mathbb{C}$. We have *not* shown that $z \mapsto az$ and $z \mapsto a'z$ are not conjugate if $a \neq a'$, because this is not true. △

Definition 2.3.4. If H is a subgroup of G and $g \in G$, then the *conjugate* of H by g is

$$gHg^{-1} := \{k \in G \ s.t. \ k = g \cdot h \cdot g^{-1} \text{ for some } h \in H\}.$$

Lemma 2.3.5. *If H is a subgroup of G and $g \in G$, then the conjugate gHg^{-1} is a subgroup of G.*

Proof. We apply Proposition 1.2.9. As $geg^{-1} = e$, we have $e \in gHg^{-1}$, so it is not empty. If $a, b \in gHg^{-1}$, then $a = ghg^{-1}$ and $b = gkg^{-1}$ for $h, k \in H$, and so

$$\begin{aligned} a \cdot b^{-1} &= (ghg^{-1}) \cdot (gkg^{-1})^{-1} \\ &= ghg^{-1}gk^{-1}g^{-1} \\ &= ghk^{-1}g^{-1} \end{aligned}$$

which lies in gHg^{-1} as $hk^{-1} \in H$. □

Chapter 3

Finite groups

Lecture 12

3.1 The quaternions

Consider the complex matrices

$$\mathbf{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \mathbf{i} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$$
$$\mathbf{j} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \qquad \mathbf{k} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

The data $(\{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}, \cdot, \mathbf{1})$ is then a group, called Q_8, having 8 elements. It is easy to verify axiom (G1) (as matrix multiplication is associative) and axiom (G2) (as $\mathbf{1}$ is the identity matrix), and axiom (G3) follows from observing that $x^4 = \mathbf{1}$ for any element of Q_8, so x^3 is an inverse to x.

It is interesting to play around with the multiplication in this group to get a feeling for it. One finds amusing formulas such as

$$(-\mathbf{1})^2 = \mathbf{1}$$
$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1}$$
$$\mathbf{ij} = \mathbf{k}, \quad \mathbf{jk} = \mathbf{i}, \quad \mathbf{ki} = \mathbf{j}$$
$$\mathbf{ji} = -\mathbf{k}, \quad \mathbf{kj} = -\mathbf{i}, \quad \mathbf{ik} = -\mathbf{j}.$$

3.2 Direct products

As a tool for describing groups of small order, we first introduce another way of constructing new groups out of old groups.

Definition 3.2.1. If $(G, \cdot_G, e_G)$ and $(H, \cdot_H, e_H)$ are groups then we define a binary operation $\cdot_{G\times H}$ on the set $G \times H$ via

$$(g_1, h_1) \cdot_{G\times H} (g_2, h_2) := (g_1 \cdot_G g_2, h_1 \cdot_H h_2).$$

It is then easy to prove the following lemma: we skip the proof.

Lemma 3.2.2. *If $(G, \cdot_G, e_G)$ and $(H, \cdot_H, e_H)$ are groups then $(G \times H, \cdot_{G\times H}, (e_G, e_H))$ is a group, called the* direct product *of G and H.* □

We will write $G\times H$ for the group $(G\times H, \cdot_{G\times H}, (e_G, e_H))$, leaving the binary operation and identity element implicit. You should convince yourself that $G \times H$ is isomorphic to $H \times G$, and that for groups G, H, and K, the groups $(G \times H) \times K$ and $G \times (H \times K)$ are isomorphic.

Theorem 3.2.3 (Chinese Remainder Theorem)**.** *If $n, m \in \mathbb{N}$ have no common factors then the homomorphism*

$$\begin{aligned} \phi : \mathbb{Z}_{nm} &\longrightarrow \mathbb{Z}_n \times \mathbb{Z}_m \\ a &\longmapsto (a \mod n, a \mod m) \end{aligned}$$

is an isomorphism.

Proof. Firstly, this is indeed a homomorphism. Both groups have $n \cdot m$ elements, so to see that it is an isomorphism it is enough to show that $\mathrm{Ker}(\phi)$ is trivial. If $a \in \mathrm{Ker}(\phi)$ then $(a \mod n, a \mod m) = (0, 0)$ so $n \mid a$ and $m \mid a$. As n and m have no common factors, it follows that $nm \mid a$, so $a = 0$. □

The following theorem gives us a criterion to recognise when a group G is isomorphic to a direct product $H_1 \times H_2$.

Theorem 3.2.4 (Direct Product Theorem)**.** *Let H_1 and H_2 be subgroups of G. If*

(i) $H_1 \cap H_2 = \{e\}$,

(ii) if $h_1 \in H_1$ and $h_2 \in H_2$ then $h_1h_2 = h_2h_1$, and

(iii) for each $g \in G$ there are $h_1 \in H_1$ and $h_2 \in H_2$ such that $g = h_1h_2$,

then G is isomorphic to $H_1 \times H_2$.

Proof. Consider the function

$$\begin{aligned} \phi : H_1 \times h_2 &\longrightarrow G \\ (h_1, h_2) &\longmapsto h_1 \cdot h_2. \end{aligned}$$

We have

$$\begin{aligned} \phi((h_1, h_2) \cdot (h_1', h_2')) &= \phi((h_1h_1', h_2h_2')) \\ &= h_1h_1'h_2h_2' \\ &= h_1h_2h_1'h_2' \text{ as } h_i'h_2 = h_2h_1' \text{ by (ii)} \\ &= \phi(h_1, h_2) \cdot \phi(h_1', h_2') \end{aligned}$$

so ϕ is a homomorphism. It is surjective, by (iii). If $\phi(h_1, h_2) = e$ then $h_1h_2 = e$ and so $h_1 = h_2^{-1}$ lies in both H_1 and H_2, so must be e by (i). Thus $(h_1, h_2) = (e, e)$, so ϕ is an isomorphism. □

3.3 Groups of small order

In this section we will classify all finite groups having at most 8 elements. We start with the following preparatory result.

Proposition 3.3.1. *If a finite group G has all non-identity elements of order 2, then G is isomorphic to $C_2 \times C_2 \times \cdots \times C_2$.*

Proof. We first show that G must be abelian: if $a, b \in G$ then we must have $(ab)^2 = e$, so $abab = e$, and so $ab = b^{-1}a^{-1}$. But as $a^2 = b^2 = e$ too, $a^{-1} = a$ and $b^{-1} = b$, so we get $ab = ba$.

Let $a_1 \in G$ be a non-identity element, and consider the subgroup $G_1 = H_1 = \langle a_1 \rangle \cong C_2$ of G. If $|G| = 2$ then $G = G_1 \cong C_2$ so we are done. If $|G| > 2$ then we can find an $a_2 \in G$ which is not in G_1. Let $H_2 \cong C_2$ be the subgroup of G generated by a_2, and G_2 be the subgroup generated by a_1 and a_2. Then G_1 and H_2 are subgroups of G_2, $G_1 \cap H_2 = \{e\}$, G_2 is abelian, and every element of G_2 is the product of an element of G_1 with one of H_2, so by the direct product theorem we have $G_2 \cong G_1 \times H_2$. If $|G| = 4$ then $G = G_2 \cong G_1 \times H_2 \cong C_2 \times C_2$ and we are done.

Continuing in this way, if we have found $G_{n-1} \leq G$ with

$$G_{n-1} \cong \underbrace{C_2 \times C_2 \times \cdots \times C_2}_{n-1 \text{ times}}$$

and $|G| > 2^{n-1}$ then we can find a $a_n \in G$ which is not in G_{n-1}, set $H_n = \langle a_n \rangle$, and let G_n be the subgroup generated by $a_1, a_2, \ldots, a_n$. Then $G_{n-1} \cap H_n = \{e\}$, G_n is abelian, and every element of G_n is the product of an element of G_{n-1} with one of H_n, so by the direct product theorem we have $G_n \cong G_{n-1} \times H_n$, isomorphic to a product of n copies of C_2.

As $|G|$ is finite this process must terminate, giving $G = G_n$ for some n. □

We now begin our classification.

1. Prime order. If G is a finite group with $|G| = p$ a prime number, then any non-identity element $g \in G$ has order p, by Lagrange's theorem, so $G = \langle g \rangle$ is a cyclic group. Thus $G \cong C_p$. (This is Corollary 2.2.7.)

Lecture 13

2. Order 4. We will show that a group G of order 4 is isomorphic to either C_4 or $C_2 \times C_2$, and that these are not isomorphic. They are not isomorphic as C_4 has an element of order 4 and $C_2 \times C_2$ does not.

If $g \in G$ then $\mathrm{ord}(g)$ divides 4, by Lagrange's theorem, so is 1, 2 or 4 (and is 1 if and only if $g = e$). If there is a $g \in G$ of order 4 then $G = \langle g \rangle$ is cyclic, so $G \cong C_4$. Otherwise, all non-identity elements of G have order 2, and so Proposition 3.3.1 applies, showing that $G \cong C_2 \times C_2$.

2. Order 6. We will show that a group G of order 6 is isomorphic to either C_6 or S_3, and that these are not isomorphic. They are not isomorphic as C_6 has an element of order 6 and S_3 does not.

If $g \in G$ then $\mathrm{ord}(g)$ divides 6, by Lagrange's theorem, so is 1, 2, 3 or 6 (and is 1 if and only if $g = e$). If there is a $g \in G$ of order 6 then $G = \langle g \rangle$ is cyclic, so $G \cong C_6$. Otherwise, all non-identity elements of G have order 2 or 3.

In this case, by Cauchy's theorem we may find an element $s \in G$ of order 2. The set $G/\langle s \rangle$ of left $\langle s \rangle$-cosets then has 3 elements, and this has a left G-action via

$$g * (g'\langle s \rangle) = gg'\langle s \rangle.$$

This determines a homomorphism

$$\rho : G \longrightarrow \mathrm{Sym}(G/\langle s \rangle) \cong S_3.$$

If $\rho(g) = e$ then we have $e\langle s\rangle = g * (e\langle s\rangle) = g\langle s\rangle$, so $g \in \langle s\rangle$ and hence $g = e$ or $g = s$. In the latter case we have $sk\langle s\rangle = k\langle s\rangle$ for all $k \in G$, so $k^{-1}sk \in \langle s\rangle$, and so $k^{-1}sk = s$ for all $k \in G$. (We could not have $k^{-1}sk = e$, as then rearranging gives $s = e$ a contradiction.) Now by Cauchy's theorem again we may find an element $r \in G$ of order 3. Then $sr \neq e$,

$$(sr)^2 = srsr = s^2r^2 = r^2 \neq e$$

and

$$(sr)^3 = srsrsr = s^3r^3 = s \neq e$$

so sr must have order 6, a contradiction. Thus $\mathrm{Ker}(\rho) = \{e\}$, so ρ is an injective homomorphism between groups of the same size, and hence an isomorphism.

This proof was not given in lectures; it is closer to the proofs in the case of order 8.

Here is an alternative proof for the last case. By Cauchy's theorem, as 2 and 3 are prime numbers dividing 6 we can find elements $s \in G$ of order 2 and $r \in G$ of order 3. The subgroup $\langle r\rangle \leq G$ has index 2 and does not contain s (as $\langle r\rangle = \{e, r, r^2\}$ consists of elements of order 1 or 3), so the cosets of $\langle r\rangle$ are $e\langle r\rangle$ and $s\langle r\rangle$. The element rs does not lie in $\langle r\rangle$, as then we would have $s \in \langle r\rangle$, so $rs \in s\langle r\rangle$, and hence $rs \in \{s, sr, sr^2\}$ and so $s^{-1}rs \in \{e, r, r^2\}$. We can't have $s^{-1}rs = e$, as then we would have $r = ss^{-1} = e$, so $s^{-1}rs \in \{r, r^2\}$.
If $s^{-1}rs = r$, so $rs = sr$, then we have

$$(sr)^2 = s^2r^2 = r^2 \neq e \text{ and } (sr)^3 = s^3r^3 = s \neq e$$

so rs must have order 6, a contradiction. Thus we must have $s^{-1}rs = r^2 = r^{-1}$, but then we recognise the group G as being the dihedral group D_6.

3. Order 8. We will show that a group G of order 8 is isomorphic to either C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_8 or Q_8, and that these are not isomorphic. They are not isomorphic as: C_8, $C_4 \times C_2$, and $C_2 \times C_2 \times C_2$ are abelian and D_8 or Q_8 are not; the first three are then distinguished by the maximal order of their elements; Q_8 has a single element of order 2, namely $-\mathbf{1}$, whereas D_8 has r^2, s, and r^2s of order 2, so D_8 or Q_8 are not isomorphic.

If $g \in G$ then $\mathrm{ord}(g)$ divides 8, by Lagrange's theorem, so is 1, 2, 4 or 8 (and is 1 if and only if $g = e$). If G has an element of order 8 then $G \cong C_8$ as above. If all non-identity elements of G have order 2, then Proposition 3.3.1 applies, showing that $G \cong C_2 \times C_2 \times C_2$.

The remaining cases are there is an element $f \in G$ of order 4, but no element of order 8. In this case $\langle f\rangle \leq G$ is a subgroup of order 4, so has two left cosets $\langle f\rangle$ and $g\langle f\rangle$ and hence

$$G = \{e, f, f^2, f^3, g, gf, gf^2, gf^3\}.$$

If $g^2 \in g\langle f\rangle$ then we would have $g \in \langle f\rangle$, a contradiction, so $g^2 \in \langle f\rangle$. This we must have g^2 equal to e, f, f^2, or f^3. If $g^2 = f$ or f^3 then $g^4 = f^2 \neq e$ and so g has order 8, a contradiction: thus we must have $g^2 = e$ or $g^2 = f^2$.

Lecture 14

Suppose first that $g^2 = e$. The element fg must lie in the coset $\langle f\rangle$ or $g\langle f\rangle$, but it cannot be $\langle f\rangle$ as then we would have $g \in \langle f\rangle$, so $fg \in g\langle f\rangle$. Thus $fg \in \{g, gf, gf^2, gf^3\}$, and so $g^{-1}fg \in \{e, f, f^2, f^3\}$. The element f has order 4 so its conjugate $g^{-1}fg$ does too, and hence $g^{-1}fg \in \{f, f^3\}$.

- If $g^{-1}fg = f$, so $fg = gf$, then we see that G is abelian. We can then apply the Direct Product Theorem with $H_1 = \langle f\rangle$ and $H_2 = \langle g\rangle$ to give $G \cong \langle f\rangle \times \langle g\rangle \cong C_4 \times C_2$.
- If $g^{-1}fg = f^3 = f^{-1}$ then we recognise G as the group D_8, with $r = f$ and $s = g$.

Suppose next that $g^2 = f^2$. Again we must have $fg \in g\langle f\rangle$ so $g^{-1}fg \in \{e, f, f^2, f^3\}$, but this must have order 4 so $g^{-1}fg \in \{f, f^3\}$.

- If $g^{-1}fg = f$ then G is abelian again. Then gf^{-1} has order 2 (as $(gf^{-1})^2 = gf^{-1}gf^{-1} = g^2f^{-2} = e$) and we can apply the Direct Product Theorem with $H_1 = \langle f\rangle$ and $H_2 = \langle gf^{-1}\rangle$ to give $G \cong \langle f\rangle \times \langle gf^{-1}\rangle \cong C_4 \times C_2$.
- If $g^{-1}fg = f^3 = f^{-1}$ then one checks that the bijection

$$\begin{aligned}\phi : G &\longrightarrow Q_8\\ e &\longmapsto \mathbf{1}\\ f &\longmapsto \mathbf{i}\\ f^2 &\longmapsto -\mathbf{1}\\ f^3 &\longmapsto -\mathbf{i}\\ g &\longmapsto \mathbf{j}\\ gf &\longmapsto -\mathbf{k}\\ gf^2 &\longmapsto -\mathbf{j}\\ gf^3 &\longmapsto \mathbf{k}\end{aligned}$$

is a homomorphism, so is a group isomorphism.

Chapter 4

Quotient groups and the isomorphism theorem

4.1 Normal subgroups

Definition 4.1.1. A subgroup $H \leq G$ is called *normal* if for every $h \in H$ and $g \in G$ we have $ghg^{-1} \in H$. In this case we write $H \lhd G$.

This condition is equivalent to asking that $gHg^{-1} = H$ for all $g \in G$. In other words, a normal subgroup is precisely a fixed point for the action of G by conjugation on the set of subgroups of G.

Example 4.1.2.

1. In any group G, the subgroups $\{e\}$ and G are normal.

2. The subgroup $\langle r \rangle \leq D_{2n}$ is normal, but the subgroup $\langle s \rangle \leq D_{2n}$ is *not* normal (for $n \geq 3$, which is when we have defined these groups).

3. If G is abelian then every subgroup is normal (as $ghg^{-1} = h$). △

Lemma 4.1.3. *A subgroup $H \leq G$ is normal if and only if $Hg = gH$ for all $g \in G$.*

Proof. Suppose that H is normal, and let $h \in H$. Then $ghg^{-1} \in H$, so $gh \in Hg$: this holds for all h, so $gH \subset Hg$, and the reverse inclusion holds by the same argument.

Suppose now that $Hg = gH$ for all $g \in G$. If $h \in H$ then $gh \in gH = Hg$ so $gh = h'g$ for some $h' \in H$, so $ghg^{-1} = h' \in H$. This holds for all $h \in H$, so H is normal. □

Corollary 4.1.4. *If $H \leq G$ has index 2 (i.e. $|G/H| = 2$) then H is normal in G.*

Proof. As H has index 2, it has 2 left cosets in G, so we can write $G = H \cup gH$ for some $g \in G$. It also has 2 right cosets in G, so we can write $G = H \cup Hg'$ for some $g' \in G$. Now $g \notin H$ so $g \in Hg'$, so $Hg = Hg'$. But then Hg and gH are both equal to the complement of H in G, so are equal to each other. □

Proposition 4.1.5. *If $\phi : G \to K$ is a group homomorphism, then* $\mathrm{Ker}(\phi)$ *is a normal subgroup of G.*

Proof. Let $k \in \mathrm{Ker}(\phi)$, so $\phi(k) = e$. Then if $g \in G$ we have

$$\begin{aligned} \phi(gkg^{-1}) &= \phi(g) \cdot \phi(k) \cdot \phi(g^{-1}) \\ &= \phi(g) \cdot e \cdot \phi(g^{-1}) \\ &= \phi(g) \cdot \phi(g^{-1}) \\ &= \phi(g \cdot g^{-1}) \\ &= \phi(e) \\ &= e \end{aligned}$$

so $gkg^{-1} \in \mathrm{Ker}(\phi)$. Thus $\mathrm{Ker}(\phi)$ is normal in G. □

4.2 Quotient groups

Recall that if $H \leq G$ then G/H denotes the set of left cosets of H. We could *try* to define a group operation on the set G/H by the formula

$$(g_1H) \cdot (g_2H) := g_1g_2H,$$

but we must worry about whether this is well-defined: the same coset may be represented by many elements of G, and we must show that the answer obtained does not depend on which representative of each coset we choose.

If $g_1H = g_1'H$ and $g_2H = g_2'H$, then $g_1' = g_1h_1$ and $g_2' = g_2h_2$. Thus

$$g_1'g_2'H = g_1h_1g_2h_2H = g_1h_1g_2H = g_1g_2(g_2^{-1}h_1g_2)H$$

which is equal to g_1g_2H if and only if $g_2^{-1}h_1g_2 \in H$. To be well-defined this must hold for all $g_2 \in G$ and for all $h_1 \in H$, i.e. H *must be normal in* G.

Theorem 4.2.1. *If H is a normal subgroup of G, then*

$$(g_1H) \cdot (g_2H) := g_1g_2H$$

is a well-defined binary operation on the set G/H of left cosets, and the data $(G/H, \cdot, eH)$ is a group.

Proof. The discussion above shows that this binary operation on G/H is well-defined. We have

$$\begin{aligned} (g_1H \cdot g_2H) \cdot g_3H &= (g_1g_2H) \cdot g_3H \\ &= ((g_1g_2)g_3)H \\ &= (g_1(g_2g_3))H \text{ by axiom (G1) for } G \\ &= g_1H \cdot (g_2H \cdot g_3H) \end{aligned}$$

so axiom (G1) is satisfied. We have $gH \cdot eH = (g \cdot e)H = gH$, so axiom (G2) is satisfied. Finally, we have $gH \cdot g^{-1}H = (g \cdot g^{-1})H = eH$ so axiom (G3) is satisfied. □

Definition 4.2.2. If H is a normal subgroup of G, then the *quotient group* is the set G/H of left cosets with the group structure described in Theorem 4.2.1.

Example 4.2.3.

1. Any subgroup of an abelian group is normal, as $ghg^{-1} = gg^{-1}h = h$. For the subgroup $n\mathbb{Z} \leq \mathbb{Z}$ consider the function

   $$\begin{aligned} \phi : \mathbb{Z}_n &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ k &\longmapsto k + n\mathbb{Z} \end{aligned}$$

   sending $k \in \{0, 1, \ldots, n-1\}$ to the coset of $n\mathbb{Z}$ in $\mathbb{Z}$ represented by k. This is a bijection. If $k, k' \in \mathbb{Z}_n$ satisfy $k + k' = r + m \cdot n$ for $r \in \mathbb{Z}_n$ then $k +_n k' = r$, by definition. Thus Lecture 15

   $$\begin{aligned} \phi(k +_n k') &= \phi(r) \\ &= r + n\mathbb{Z} \\ &= (k + k') + n\mathbb{Z} \text{ as } (k + k') - r \in n\mathbb{Z} \\ &= (k + n\mathbb{Z}) + (k' + n\mathbb{Z}) \text{ by definition of the group operation on } \mathbb{Z}/n\mathbb{Z} \\ &= \phi(k) + \phi(k') \end{aligned}$$

   so ϕ is a homomorphism. Thus $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

2. Let $R = \{Id, r, r^2, \ldots, r^{n-1}\} \leq D_{2n}$. This is a subgroup, and is normal, as $(r^i s)r^j(r^i s)^{-1} = r^i s r^j s^{-1} r^{-i} = r^i r^{-j} r^{-i} = r^{-j} \in R$. Thus we have a quotient group D_{2n}/R. This group has order $|D_{2n}/R| = |D_{2n}|/|R| = 2n/n = 2$, so must be isomorphic to C_2.

3. Let $K = \{Id, r^2\} \leq D_8$. This is again a normal subgroup, as in the last example, so we have a quotient group D_8/K, which has order $|D_8|/|K| = 8/2 = 4$. We may write its elements as

   $$eK, rK, sK, rsK,$$

   and note that: $(rK) \cdot (rK) = r^2K = eK$ as $r^2 \in K$; $(sK) \cdot (sK) = s^2K = eK$ as $s^2 = e$; $(rsK) \cdot (rsK) = rsrsK = rr^{-1}ssK = eK$. Thus every non-identity element has order 2, so by our classification $D_8/K \cong C_2 \times C_2$.

4. Let $K = \{\mathbf{1}, -\mathbf{1}\} \leq Q_8$. This is a normal subgroup, so we have a quotient group Q_8/K of order 4. We may write its elements as

   $$\mathbf{1}K, \mathbf{i}K, \mathbf{j}K, \mathbf{k}K$$

   and note that all the nontrivial such elements have order 2. Thus by our classification $Q_8/K \cong C_2 \times C_2$.

5. In the last two examples we see that D_8 and Q_8 both have normal subgroups isomorphic to C_2 with associated quotient groups isomorphic to $C_2 \times C_2$, and yet these groups are *not* isomorphic. △

4.3 The Isomorphism Theorem

Theorem 4.3.1. *Let $\phi : G \to H$ be a homomorphism. Then the function*

$$\begin{aligned} \bar{\phi} : G/\mathrm{Ker}(\phi) &\longrightarrow \mathrm{Im}(\phi) \\ g\mathrm{Ker}(\phi) &\longmapsto \phi(g), \end{aligned}$$

is well-defined and is a group isomorphism.

Proof. We know from Proposition 4.1.5 that $\mathrm{Ker}(\phi) \lhd G$, so we indeed have a quotient group $G/\mathrm{Ker}(\phi)$.

If $g\mathrm{Ker}(\phi) = g'\mathrm{Ker}(\phi)$ then $g' = g \cdot h$ for some $h \in \mathrm{Ker}(\phi)$. Thus

$$\begin{aligned} \phi(g') &= \phi(g \cdot h) \\ &= \phi(g) \cdot \phi(h) \\ &= \phi(g) \cdot e \text{ as } h \in \mathrm{Ker}(\phi) \\ &= \phi(g) \end{aligned}$$

and hence $\bar{\phi}(g\mathrm{Ker}(\phi)) = \bar{\phi}(g'\mathrm{Ker}(\phi))$, which shows that $\bar{\phi}$ is well-defined.

We have

$$\begin{aligned} \bar{\phi}(a\mathrm{Ker}(\phi) \cdot b\mathrm{Ker}(\phi)) &= \bar{\phi}(ab\mathrm{Ker}(\phi)) \\ &= \phi(ab) \\ &= \phi(a) \cdot \phi(b) \\ &= \bar{\phi}(a\mathrm{Ker}(\phi)) \cdot \bar{\phi}(b\mathrm{Ker}(\phi)) \end{aligned}$$

so $\bar{\phi}$ is a homomorphism.

The function $\bar{\phi}$ is surjective, as the set $\mathrm{Im}(\phi)$ consists by definition of the elements of the form $\phi(g)$. If $\bar{\phi}(a\mathrm{Ker}(\phi)) = e$ then $\phi(a) = e$, so $a \in \mathrm{Ker}(\phi)$, but then $a\mathrm{Ker}(\phi) = e\mathrm{Ker}(\phi)$. Thus the kernel of $\bar{\phi}$ is $\{a\mathrm{Ker}(\phi)\}$, so $\bar{\phi}$ is injective. □

Example 4.3.2.

1. The function $\phi : (\mathbb{Z}, +, 0) \to (\mathbb{Z}_n, +_n, 0)$ given by

$$\phi(k) = \text{ remainder left when } k \text{ is divided by } n$$

is a homomorphism (by definition of $+_n$), has $\mathrm{Im}(\phi) = \mathbb{Z}_n$, and has $\mathrm{Ker}(\phi) = n\mathbb{Z}$. This gives another proof that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

2. The function $\phi : (\mathbb{R}, +, 0) \to (\mathbb{C} \setminus \{0\}, \times, 1)$ given by $\phi(t) = e^{2\pi i t}$ is a homomorphism. It has

$$\mathrm{Im}(\phi) = \{z \in \mathbb{C}\, s.t.\, |z| = 1\} =: S^1,$$

the unit complex numbers, and $\mathrm{Ker}(\phi) = \mathbb{Z}$, giving $\mathbb{R}/\mathbb{Z} \cong S^1$.

3. If G and H are groups, then $\{e\} \times H$ is a subgroup of $G \times H$, and moreover is a normal subgroup, as

$$(g,h)\cdot(e,h')\cdot(g,h)^{-1} = (g\cdot e\cdot g^{-1}, h\cdot h'\cdot h^{-1}) = (e, h\cdot h'\cdot h^{-1}) \in \{e\} \times H.$$

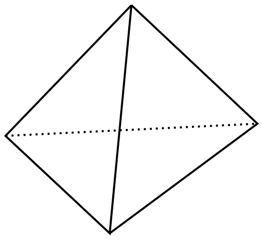
We can calculate the quotient $G \times H/\{e\} \times H$ as follows: the function

$$\begin{aligned} \pi : G \times H &\longrightarrow G \\ (g,h) &\longmapsto g \end{aligned}$$

is a surjective homomorphism with kernel $\{e\}\times H$, so by the Isomorphism Theorem $G \times H/\{e\} \times H \cong G$.

Lecture 16

4. Let G be the group of *all* isometries of the regular tetrahedron

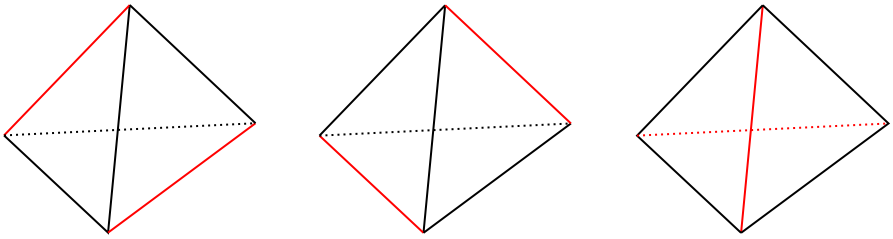
$T =$ 

(not just the rotations). This group acts on the set V of vertices of T, of which there are 4, giving a homomorphism

$$\rho : G \longrightarrow \mathrm{Sym}(V) \cong S_4.$$

This homomorphism is injective: if an isometry fixes all 4 vertices then it must be the identity. The group S_4 has $4! = 4\cdot 3\cdot 2\cdot 1 = 24$ elements, and $G \cong G/\mathrm{Ker}(\rho) \cong \mathrm{Im}(\rho) \leq \mathrm{Sym}(V) \cong S_4$ so $|G|$ divides 24. The group G contains 12 rotations, but also contains e.g. a reflection in the plane going through two vertices and the middle of the opposite edge. Thus $|G| > 12$, and as $|G|$ divides 24 we must have $|G| = 24$. Thus ρ is an isomorphism, and $G \cong S_4$.

The group G also acts on the set X of opposite pairs of edges of T, of which there are 3 as shown below.



This gives a homomorphism

$$\phi : G \longrightarrow \mathrm{Sym}(X) \cong S_3.$$

We see that rotating in the vertical axis cycles through the 3 pairs of opposite edges shown above, so $\mathrm{Im}(\phi)$ contains an element of order 3. We see that a reflection in the plane going through two vertices and the middle of the opposite edge fixes one pair of opposite edges and swaps the other two, so $\mathrm{Im}(\phi)$ contains an element of order 2. By Lagrange's theorem we then have that 2 and 3 both divide $|\mathrm{Im}(\phi)|$, so 6 divides $|\mathrm{Im}(\phi)|$. On the other hand $\mathrm{Im}(\phi) \leq \mathrm{Sym}(X) \cong S_3$ so $|\mathrm{Im}(\phi)|$ divides $|S_3| = 3 \cdot 2 \cdot 1 = 6$, and hence ϕ is surjective. We therefore have $\frac{G}{\mathrm{Ker}(\phi)} \cong S_3$, and so, using the isomorphism ρ, there is a normal subgroup $K \lhd S_4$ such that

$$\frac{S_4}{K} \cong S_3. \qquad \triangle$$

4.4 Simple groups

When $H \lhd G$ then we may decompose the problem of understanding G into the problems of understanding H, of understanding G/H, and understanding how these fit together to make up G. This is a powerful technique, but some groups are impervious to it, as they contain no non-trivial normal subgroups.

Definition 4.4.1. A non-trivial group G is *simple* if its only normal subgroups are $\{e\}$ and G.

For example, if p is a prime number then C_p is simple. We will discover some more simple groups shortly.

Chapter 5

Permutations

5.1 Permutations, cycles, and transpositions

Recall that for a set X we denote by $\mathrm{Sym}(X)$ the group whose elements are invertible functions $\sigma : X \to X$. Such a function is also called a *permutation*. When $X = \{1, 2, 3, \ldots, n\}$ then we call this group S_n. As we have already used a few times, $|S_n| = n! = n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1$.

Definition 5.1.1. Given a list $a_1, a_2, \ldots, a_k \in \{1, 2, \ldots, n\}$ of distinct elements, the *k-cycle*

$$(a_1 a_2 \cdots a_k) \in S_n$$

is the permutation given by

$$(a_1 a_2 \cdots a_k)(i) = \begin{cases} a_{j+1} & \text{if } i = a_j \text{ for } j < k \\ a_1 & \text{if } i = a_k \\ i & \text{if } i \neq a_j \text{ for any } j. \end{cases}$$

This is indeed an invertible function from the set $\{1, 2, \ldots, n\}$ to itself, as the k-cycle $(a_k a_{k-1} \cdots a_2 a_1)$ is an inverse for it. Note that a cycle $(a_1 a_2 \cdots a_k)$ moves every element in the subset $\{a_1, a_2, \ldots, a_k\} \subset \{1, 2, \ldots, n\}$, and fixes every element outside of this subset.

A 2-cycle is often called a *transposition*, as (ab) is the permutation which transposes a and b, and leaves all other elements fixed.

Cycles $(a_1 a_2 \cdots a_k)$ and $(b_1 b_2 \cdots b_l)$ are called *disjoint* if $a_i \neq b_j$ for any i and j.

Example 5.1.2. As cycles are permutations, they can be composed. Let us calculate what permutation in S_4 the composition $(1234)(324)$ gives. Recall that permutations are—first of all—functions, so $\sigma\tau$ means "apply the function τ first, then apply the function σ". Thus we have

$$\begin{aligned} ((1234)(324))(1) &= (1234)((324)(1)) \\ &= (1234)(1) \text{ as } (324) \text{ fixes } 1 \\ &= 2 \text{ as } (1234) \text{ sends } 1 \text{ to } 2 \end{aligned}$$

and

$$\begin{aligned} ((1234)(324))(2) &= (1234)((324)(2)) \\ &= (1234)(4) \text{ as } (324) \text{ sends } 2 \text{ to } 4 \\ &= 1 \text{ as } (1234) \text{ sends } 4 \text{ to } 1 \end{aligned}$$

and

$$\begin{aligned}((1234)(324))(3) &= (1234)((324)(3))\\ &= (1234)(2) \text{ as } (324) \text{ sends 3 to 2}\\ &= 3 \text{ as } (1234) \text{ sends 2 to 3}\end{aligned}$$

and

$$\begin{aligned}((1234)(324))(4) &= (1234)((324)(4))\\ &= (1234)(3) \text{ as } (324) \text{ sends 4 to 2}\\ &= 4 \text{ as } (1234) \text{ sends 3 to 4}\end{aligned}$$

so the permutation (1234)(324) swaps 1 and 2 and fixes 3 and 4: it is equal to the transposition (12).

As another example, let us consider (324)(1234). The analogous calculation shows that this permutation is $1 \mapsto 4$, $2 \mapsto 2$, $3 \mapsto 3$, $4 \mapsto 1$, so this permutation is (14). This still happens to be a transposition (however this is a coincidence), but is a different transposition: the group S_n is not abelian (unless $n \leq 2$). △

Lemma 5.1.3.

(i) Cycles can be cycled: we have $(a_1 a_2 \cdots a_k) = (a_k a_1 a_2 \cdots a_{k-1})$.

(ii) Disjoint cycles commute: if $\sigma, \tau \in S_n$ are disjoint cycles then $\sigma\tau = \tau\sigma$.

Proof. For (i), we have

$$(a_k a_1 a_2 \cdots a_{k-1})(i) = \begin{cases} a_1 & \text{if } i = a_k \\ a_{j+1} & \text{if } i = a_j \text{ for } 1 \leq j < k \\ a_k & \text{if } i = a_{k-1} \\ i & \text{if } i \neq a_j \text{ for any } j, \end{cases}$$

but this is precisely the same as $(a_1 a_2 \cdots a_k)(i)$.

For (ii), let $\sigma = (a_1 a_2 \cdots a_k)$ and $\tau = (b_1 b_2 \cdots b_l)$ be disjoint cycles. For $i \in \{a_1, a_2, \ldots, a_k\}$, we have

$$\sigma\tau(i) = \sigma(i) \text{ as } i \in \{a_1, a_2, \ldots, a_k\} \text{ is fixed by } \tau$$

but

$$\tau\sigma(i) = \sigma(i) \text{ as } \sigma(i) \in \{a_1, a_2, \ldots, a_k\} \text{ is fixed by } \tau$$

so $\sigma\tau(i) = \tau\sigma(i)$. If $i \notin \{a_1, a_2, \ldots, a_k\}$ then $\tau(i) \notin \{a_1, a_2, \ldots, a_k\}$ too, as τ fixes each a_j, so

$$\sigma\tau(i) = \tau(i) \text{ as } \tau(i) \notin \{a_1, a_2, \ldots, a_k\} \text{ is fixed by } \sigma$$

and

$$\tau\sigma(i) = \tau(i) \text{ as } i \notin \{a_1, a_2, \ldots, a_k\} \text{ is fixed by } \sigma$$

and so $\sigma\tau = \tau\sigma$. □

Theorem 5.1.4 (Disjoint Cycle Decomposition). *Every permutation in S_n is a composition of disjoint cycles. The expression of an element $\sigma \in S_n$ as a composition of disjoint cycles*

$$\sigma = (a^1_1 a^1_2 \cdots a^1_{k_1})(a^2_1 a^2_2 \cdots a^2_{k_2}) \cdots (a^r_1 a^r_2 \cdots a^r_{k_r}),$$

in which every element of $\{1, 2, \ldots, n\}$ appears, is unique up to

(i) cycling the terms in a cycle, and

(ii) reordering the cycles.

Lecture 17

Note that the ambiguity allowed in (i) and (ii) is necessary by Lemma 5.1.3. By insisting that every element of $\{1, 2, \ldots, n\}$ appear, we are saying that we should remember that there can be cycles of length 1. So, for example, the transposition $(12) \in S_4$ should be written as $(12)(3)(4)$, and the transposition $(12) \in S_5$ should be written as $(12)(3)(4)(5)$.

Proof. We proceed by induction on n: if $n = 1$ there is nothing to show, as the group S_1 is trivial. Let $\sigma \in S_n$, and consider the sequence $1, \sigma(1), \sigma^2(1), \ldots$.

Claim: there is a $k \in \mathbb{N}$ such that $\sigma^k(1) = 1$ and $1, \sigma(1), \sigma^2(1), \ldots, \sigma^{k-1}(1)$ are all distinct.

Proof of claim. As the set $\{1, 2, \ldots, n\}$ is finite, we must eventually find that $\sigma^a(1) = \sigma^b(1)$ for some $a \geq b$, but then $\sigma^{a-b}(1) = 1$.

Let k be minimal such that $\sigma^k(1) = 1$ (such a k exists, by the first part). If $0 \leq i < j < k$ are such that $\sigma^i(1) = \sigma^j(1)$, then $\sigma^{j-i}(1) = 1$, which contradicts k being minimal. □

Now the permutation

$$\tau = \sigma \circ (1\sigma(1)\sigma^2(1) \cdots \sigma^{k-1}(1))^{-1}$$

fixes the set $\{1, \sigma(1), \sigma^2(1), \ldots, \sigma^{k-1}(1)\}$, so is a permutation of the set $X := \{1, 2, \ldots, n\} \setminus \{1, \sigma(1), \sigma^2(1), \ldots, \sigma^{k-1}(1)\}$. This has strictly fewer than n elements, so by induction τ may be written as a composition of disjoint cycles in the set X. But then

$$\sigma = \tau \circ (1\sigma(1)\sigma^2(1) \cdots \sigma^{k-1}(1))$$

is a composition of disjoint cycles, as the sets X and $\{1, \sigma(1), \sigma^2(1), \ldots, \sigma^{k-1}(1)\}$ are disjoint.

For the uniqueness part, suppose that

$$(a^1_1 a^1_2 \cdots a^1_{k_1})(a^2_1 a^2_2 \cdots a^2_{k_2}) \cdots (a^r_1 a^r_2 \cdots a^r_{k_r}) = (b^1_1 b^1_2 \cdots b^1_{l_1})(b^2_1 b^2_2 \cdots b^2_{l_2}) \cdots (b^s_1 b^s_2 \cdots b^s_{l_r})$$

are two disjoint cycle decompositions in which every element of $\{1, 2, \ldots, n\}$ appears. We must have $a^1_1 = b^j_i$ for some i and j. Applying σ then shows that $a^1_2 = b^j_{i+1}$ and so on, cycling the indices round if necessary. As we require precisely k_1 iterations of σ to bring a^1_1 back to itself, the same is true of b^j_i, and so $k_1 = l_j$. But then the sequence

$(a^1_1, a^1_2, \ldots, a^1_{k_1})$ and the sequence $(b^j_1, b^j_2, \ldots, b^j_{l_j})$ are related by cycling ($j-1$ times). We may then cancel the cycle $(a^1_1 a^1_2 \cdots a^1_{k_1}) = (b^j_1 b^j_2 \cdots b^j_{l_j})$ from both sides, obtaining a simpler problem. After finitely-many such steps, we have shown that the two collections of cycles are the same up to reordering and cycling. □

Lemma 5.1.5. *If*

$$\sigma = (a^1_1 a^1_2 \cdots a^1_{k_1})(a^2_1 a^2_2 \cdots a^2_{k_2}) \cdots (a^r_1 a^r_2 \cdots a^r_{k_r})$$

is a disjoint cycle decomposition, the order of σ is the lowest common multiple of the k_i's.

Proof. We have

$$\sigma^j = (a^1_1 a^1_2 \cdots a^1_{k_1})^j (a^2_1 a^2_2 \cdots a^2_{k_2})^j \cdots (a^r_1 a^r_2 \cdots a^r_{k_r})^j$$

as disjoint cycles commute with each other. The order of a cycle $(b_1 b_2 \cdots b_r)$ is r, so when $l := \operatorname{lcm}\{k_i\}$ we have

$$(a^i_1 a^i_2 \cdots a^i_{k_i})^l = ((a^i_1 a^i_2 \cdots a^i_{k_i})^{k_i})^{l/k_i} = e^{l/k_i} = e$$

and so the order of σ divides l.

On the other hand if σ has order m then, rearranging, we have

$$(a^1_1 a^1_2 \cdots a^1_{k_1})^m = ((a^2_1 a^2_2 \cdots a^2_{k_2})^m \cdots (a^r_1 a^r_2 \cdots a^r_{k_r})^m)^{-1}$$

but the left-hand side fixes all a^j_i with $j \neq 1$ and the right-hand side fixes all a^j_i with $j = 1$, so both sides must be the identity permutation. Thus k_1 divides m; the same goes for all k_i, so the the lowest common multiple of the k_i divides m. It follows that $m = l$. □

5.2 The sign of a permutation

We wish to explain how to associate to each permutation $\sigma \in S_n$ a sign ± 1, which measures how many transpositions are necessary to form σ. We first need to know that it can be formed using transpositions.

Proposition 5.2.1. *Every permutation in S_n is a composition of transpositions.*

This *does not say* disjoint transpositions, which would be false: we have $(123) = (12)(23)$, but the only compositions of disjoint transpositions in S_3 are (12), (23), and (13). It also *does not say* that an expression as a composition of transpositions is unique: we have

$$(1234) = (12)(23)(34) = (41)(12)(23)$$

for example.

Proof. We proceed by induction on n. The group S_1 is trivial, and every permutation of $\{1\}$ is the composition of no transpositions.

For $\sigma \in S_n$, we have a transposition $(n\sigma(n))$. Now the permutation $(n\sigma(n)) \circ \sigma$ fixes n, so we may consider it as a permutation of $\{1, 2, \ldots, n-1\}$, or in other words as an element of S_{n-1}. By induction $\tau = (n\sigma(n)) \circ \sigma$ is a composition of transpositions, so $\sigma = (\sigma(n)n) \circ \tau$ is too. □

We wish to define the *sign* of a permutation σ as

$$\operatorname{sign}(\sigma) := (-1)^{\#\text{of transpositions needed to write } \sigma \text{ as a composition of transpositions}}$$

but because elements $\sigma \in S_n$ cannot be written uniquely as a composition of transpositions, we must worry about whether this is well-defined. Lecture 18

Theorem 5.2.2. *The function* sign : $S_n \to \{1, -1\}$ *described above is well-defined.*

Proof. We will use the fact that elements of S_n can be written as a composition of disjoint cycles in which every element of $\{1, 2, \ldots, n\}$ appears, unique up to reordering the cycles and cycling the terms in a cycle. Let $\ell(\sigma)$ denote the number of cycles when σ is written in this way. So

$$\begin{aligned} \ell(e) &= \ell((1)(2)(3)\cdots(n)) = n, \text{ and} \\ \ell((12)) &= \ell((12)(3)(4)\cdots(n)) = n-1. \end{aligned}$$

For a transposition (cd), where we can suppose $c < d$ without loss of generality, consider the composition $\sigma(cd)$.

(i) If c and d lie in the same cycle of σ, say in $(ca_2a_3\cdots a_{i-1}da_{i+1}\cdots a_{i+j})$, then as

$$(ca_2a_3\cdots a_{i-1}da_{i+1}\cdots a_{i+j})(cd) = (ca_{i+1}\cdots a_{i+j})(da_2a_3\cdots a_{i-1})$$

we have $\ell(\sigma(cd)) = \ell(\sigma) + 1$.

(ii) If c and d lie in different cycles of σ, say in $(ca_{i+1}\cdots a_{i+j})(da_2a_3\cdots a_{i-1})$, then as

$$(ca_{i+1}\cdots a_{i+j})(da_2a_3\cdots a_{i-1})(cd) = (ca_2a_3\cdots a_{i-1}da_{i+1}\cdots a_{i+j})$$

we have $\ell(\sigma(cd)) = \ell(\sigma) - 1$.

In either case we have $\ell(\sigma(cd)) \equiv \ell(\sigma) + 1 \mod 2$.

If σ can be written as the composition of k transpositions, then we can obtain it from e by composing with k transpositions and so

$$\begin{aligned} \ell(\sigma) &\equiv \ell(e) + k \mod 2 \\ &\equiv n + k \mod 2, \end{aligned}$$

hence

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

But the right-hand side clearly only depends on the permutation σ, and not on how we choose to write it as a composition of transpositions. □

Corollary 5.2.3. *The function* $\mathrm{sign}: S_n \to \{1, -1\} = C_2$ *is a group homomorphism.*

Proof. If σ can be written as a composition of a transpositions and τ can be written as a composition of b transpositions, then $\sigma\tau$ can be written as the composition of $a+b$ transpositions. Thus

$$\mathrm{sign}(\sigma\tau) = (-1)^{a+b} = (-1)^a \cdot (-1)^b = \mathrm{sign}(\sigma) \cdot \mathrm{sign}(\tau). \qquad \square$$

If $\mathrm{sign}(\sigma) = 1$ then σ is called an *even permutation*, and if $\mathrm{sign}(\sigma) = -1$ then σ is called an *odd permutation*.

Definition 5.2.4. The *alternating group* A_n is the subgroup of S_n consisting of even permutations.

In other words A_n is the kernel of the homomorphism $\mathrm{sign}: S_n \to C_2$, so is a normal subgroup of S_n. As $\mathrm{sign}((12)) = -1$, this homomorphism is surjective as long as $n \geq 2$, so A_n has index 2 in S_n as long as $n \geq 2$.

It is quite convenient to be able to calculate the sign of a permutation from a description in terms of (possibly disjoint) cycles. This may be done as follows.

Lemma 5.2.5. *The sign of a cycle* $(a_1 a_2 \cdots a_r)$ *is* $(-1)^{r-1}$.

Proof. We have $(a_1 a_2 \cdots a_r) = (a_1 a_r)(a_1 a_{r-1}) \cdots (a_1 a_3)(a_1 a_2)$, a composition of $r-1$ transpositions. □

This means that a cycle of even length is odd, and a cycle of odd length is even,[1] so if σ is written as a composition of cycles, then $\mathrm{sign}(\sigma) = (-1)^{\#\text{cycles of even length}}$.

5.3 Conjugation in S_n and A_n

When two elements of S_n are conjugate is remarkably easy to check. We start with the case of a single cycle.

Proposition 5.3.1. *If* $\sigma \in S_n$ *then* $\sigma(a_1 a_2 \cdots a_k)\sigma^{-1} = (\sigma(a_1)\sigma(a_2)\cdots\sigma(a_k))$.

Proof. We simply check that both sides evaluate to the same thing on each $i \in \{1, 2, \ldots, n\}$.

If $\sigma^{-1}(i) \notin \{a_1, a_2, \ldots, a_k\}$ then

$$(a_1 a_2 \cdots a_k)(\sigma^{-1}(i)) = \sigma^{-1}(i)$$

and so applying σ to this gives i. For the right-hand side, as $i \notin \{\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k)\}$ the permutation $(\sigma(a_1)\sigma(a_2)\cdots\sigma(a_k))$ also fixes i.

If $\sigma^{-1}(i) = a_j$, then

$$\begin{aligned}(\sigma(a_1 a_2 \cdots a_k)\sigma^{-1})(i) &= (\sigma(a_1 a_2 \cdots a_k))(\sigma^{-1}(i)) \\ &= (\sigma(a_1 a_2 \cdots a_k))(a_j) \\ &= \sigma(a_{j+1}) \text{ interpreting } a_{k+1} = a_1 \text{ if necessary}\end{aligned}$$

but this is also the result of applying $(\sigma(a_1)\sigma(a_2)\cdots\sigma(a_k))$ to $i = \sigma(a_j)$. □

[1] Weird.

Corollary 5.3.2. *Elements $\tau, \tau' \in S_n$ are conjugate if and only if when they are written as a composition of disjoint cycles (in which every element of $\{1, 2, \ldots, n\}$ appears) they have the same number of cycles of each length.*

Lecture 19

Proof. If

$$\tau = (a_1^1 a_2^1 \cdots a_{k_1}^1)(a_1^2 a_2^2 \cdots a_{k_2}^2) \cdots (a_1^r a_2^r \cdots a_{k_r}^r)$$

is a disjoint cycle decomposition and $\sigma \in S_n$, then by the proposition we have

$$\sigma\tau\sigma^{-1} = (\sigma(a_1^1)\sigma(a_2^1) \cdots \sigma(a_{k_1}^1))(\sigma(a_1^2)\sigma(a_2^2) \cdots \sigma(a_{k_2}^2)) \cdots (\sigma(a_1^r)\sigma(a_2^r) \cdots \sigma(a_{k_r}^r))$$

which is again a disjoint cycle decomposition, so τ and $\sigma\tau\sigma^{-1}$ have the same number of cycles of each length.

Conversely, if τ and τ' the same number of cycles of each length, then after reordering their cycles we may find disjoint cycle decompositions

$$\begin{aligned}\tau &= (a_1^1 a_2^1 \cdots a_{k_1}^1)(a_1^2 a_2^2 \cdots a_{k_2}^2) \cdots (a_1^r a_2^r \cdots a_{k_r}^r)\\ \tau' &= (b_1^1 b_2^1 \cdots b_{k_1}^1)(b_1^2 b_2^2 \cdots b_{k_2}^2) \cdots (b_1^r b_2^r \cdots b_{k_r}^r)\end{aligned}$$

in which every element of $\{1, 2, \ldots, n\}$ appears. We may then define a function $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ by

$$\sigma(a_j^i) = b_j^i,$$

and this is indeed a permutation, as it is surjective (because each element of $\{1, 2, \ldots, n\}$ is some b_j^i). By construction $\tau' = \sigma\tau\sigma^{-1}$, so τ and τ' are conjugate. □

For a permutation $\sigma \in S_n$, we may record it conjugacy class as $1^{a_1}2^{a_2}3^{a_3} \cdots n^{a_n}$, where a_i denotes the number of i-cycles when σ is written as a composition of disjoint cycles in which every element of $\{1, 2 \ldots, n\}$ appears. We call such a string the *cycle type* of σ.

Recall that the conjugacy class of $g \in G$ is its orbit for the conjugation action of G on itself, and the centraliser

$$C_G(g) := \{h \in G \, s.t. \, hgh^{-1} = g\}.$$

of g is its stabiliser under this action.

Lemma 5.3.3. *If $\tau \in S_n$ has cycle type $1^{a_1}2^{a_2}3^{a_3} \cdots n^{a_n}$ then the order of its centraliser is*

$$|C_{S_n}(\tau)| = 1^{a_1}(a_1!)2^{a_2}(a_2!)3^{a_3}(a_3!) \cdots n^{a_n}(a_n!).$$

Proof. The centraliser of τ consists of those $\sigma \in S_n$ such that $\sigma\tau\sigma^{-1} = \tau$. If

$$\tau = (a_1^1 a_2^1 \cdots a_{k_1}^1)(a_1^2 a_2^2 \cdots a_{k_2}^2) \cdots (a_1^r a_2^r \cdots a_{k_r}^r)$$

is a disjoint cycle decomposition, then we have

$$\sigma\tau\sigma^{-1} = (\sigma(a_1^1)\sigma(a_2^1) \cdots \sigma(a_{k_1}^1))(\sigma(a_1^2)\sigma(a_2^2) \cdots \sigma(a_{k_2}^2)) \cdots (\sigma(a_1^r)\sigma(a_2^r) \cdots \sigma(a_{k_r}^r))$$

which is again a disjoint cycle decomposition, so must differ from the expression for τ by cycling cycles and permuting cycles, by the uniqueness part of Theorem 5.1.4. There are $a_i!$ ways of reordering the cycles of length i, and i^{a_i} ways of cycling the a_i-many i-cycles. This gives the claimed formula. □

By the Orbit-Stabiliser theorem, if $\tau \in S_n$ has cycle type $1^{a_1}2^{a_2}3^{a_3}\cdots n^{a_n}$ we therefore have

$$|\mathrm{ccl}(\tau)| = \frac{n!}{1^{a_1}(a_1!)2^{a_2}(a_2!)3^{a_3}(a_3!)\cdots n^{a_n}(a_n!)}.$$

Example 5.3.4. Let us use this to describe the conjugacy classes in S_4. They are given by strings $1^{a_1}2^{a_2}3^{a_3}4^{a_4}$ with $\sum_{i=1}^{4} i \cdot a_i = 4$, so

$$1^4, 1^2 2^1, 2^2, 1^1 3^1, 4^1.$$

The conjugacy class 1^4 has a single element, $e = (1)(2)(3)(4)$. The centraliser of e is the whole group S_n.

The conjugacy class $1^2 2^1$ consists of transpositions, and a typical element is $(12)(3)(4)$. This conjugacy class has size

$$\frac{4!}{1^2 \cdot 2! \cdot 2^1 \cdot 1!} = 6,$$

and has $|C_{S_4}((12)(3)(4))| = 1^2 \cdot 2! \cdot 2^1 \cdot 1! = 4$. Once we know the order of $C_{S_4}((12)(3)(4))$ is 4, it is easy to guess the elements which centralise $(12)(3)(4)$: they are

$$e, (12), (34), (12)(34).$$

The conjugacy class 2^2 consists of "double transpositions", and a typical element is $(12)(34)$. This conjugacy class has size

$$\frac{4!}{2^2 \cdot 2!} = 3,$$

and consists of $(12)(34)$, $(13)(24)$, and $(14)(23)$. We have $|C_{S_4}((12)(34))| = 2^2 \cdot 2! = 8$. It is an exercise to work out what the group $C_{S_4}((12)(34))$ is.

The conjugacy class $1^1 3^1$ consists of 3-cycles, and a typical element is $(123)(4)$. This conjugacy class has size

$$\frac{4!}{1^1 \cdot 1! \cdot 3^1 \cdot 1!} = 8,$$

and has $|C_{S_4}((123)(4))| = 1^1 \cdot 1! \cdot 3^1 \cdot 1! = 3$. In this case it is easy to check that $C_{S_4}((123)(4))$ is the cyclic group generated by (123).

The conjugacy class 4^1 consists of 4-cycles, and a typical element is (1234). This conjugacy class has size

$$\frac{4!}{4^1 \cdot 1!} = 6,$$

and has $|C_{S_4}((1234))| = 4^1 \cdot 1! = 4$. In this case it is easy to check that $C_{S_4}((1234))$ is the cyclic group generated by (1234). △

If $H \lhd G$ and $h \in H$, then every conjugate ghg^{-1} is also in H: thus, H is a union of conjugacy classes. This can be useful for finding normal subgroups, or showing they cannot exist.

Example 5.3.5. Let us search for normal subgroups $H \lhd S_4$. Certainly any such H contains the identity element, so contains the conjugacy class 1^4.

If H contains the conjugacy class $1^2 2^1$ of transpositions then $H = S_4$, as symmetric groups are generated by transpositions.

If H contains the conjugacy class 2^2 of 3 double transpositions, then we can notice that

$$K := \{e, (12)(34), (13)(24), (14)(23)\}$$

is indeed a subgroup, and so is a normal subgroup. If H is any larger than K then it is covered by one of the other cases.

If H contains the conjugacy class $1^1 3^1$ of 8 3-cycles, then it contains ≥ 9 elements, so must have 12 or 24 elements by Lagrange's theorem. Suppose it has 12 elements. As 3-cycles are even, they lie in A_4, so $H \cap A_4$ is a subgroup of H which also has ≥ 9 elements, so must be equal to H by Lagrange's theorem again. Thus H must be equal to the normal subgroup $A_4 \lhd S_4$.

If H contains the conjugacy class 4^1 of 6 4-cycles, then it contains the product

$$(1234)(1324) = (142)$$

so also contains the conjugacy class $1^1 3^1$ too, so is A_4 or S_4 by the previous case.

Thus we find that the normal subgroups of S_4 are

$$\{e\}, \quad K, \quad A_4, \quad S_4$$

with quotient groups

Lecture 20

$$S_4/\{e\} \cong S_4, \quad S_4/K \cong S_3, \quad S_4/A_4 \cong C_2, \quad S_4/S_4 = \{e\}.$$

The second example should be compared with Example 4.3.2 part 4. △

Now that we have seen that conjugacy classes in S_n are easy to describe, lets ask about conjugacy classes in A_n.

Remark 5.3.6. Recall that we write $\mathrm{ccl}(h)$ for the conjugacy class of an element h: let us write $\mathrm{ccl}_G(h)$ to emphasise that we mean the conjugacy class of h in the group G.

As $A_n \leq S_n$, elements of A_n which are conjugate in A_n are also conjugate in S_n, so

$$\mathrm{ccl}_{A_n}(\sigma) \subseteq \mathrm{ccl}_{S_n}(\sigma),$$

but we need not have equality. For example, the permutations (123) and (132) lie in A_3, and are conjugate in S_3 as they have the same number of cycles of each length. But they are not conjugate in A_3, as $A_3 \cong C_3$ is abelian, so conjugate elements are equal. On the other hand if we consider these permutations as lying in A_5 then they are conjugate, as

$$((23)(45))(123)((23)(45))^{-1} = (132)$$

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

For $\sigma \in A_n \subset S_n$, using the orbit-stabiliser theorem for the conjugation action shows that

$$\begin{aligned}|S_n| &= |\mathrm{ccl}_{S_n}(\sigma)| \cdot |C_{S_n}(\sigma)|\\ |A_n| &= |\mathrm{ccl}_{A_n}(\sigma)| \cdot |C_{A_n}(\sigma)|\end{aligned}$$

and as $|S_n| = 2|A_n|$ there are two possibilities:

(i) $|\mathrm{ccl}_{A_n}(\sigma)| = |\mathrm{ccl}_{S_n}(\sigma)|$ and $|C_{A_n}(\sigma)| = \frac{1}{2}|C_{S_n}(\sigma)|$, or

(ii) $|\mathrm{ccl}_{A_n}(\sigma)| = \frac{1}{2}|\mathrm{ccl}_{S_n}(\sigma)|$ and $|C_{A_n}(\sigma)| = |C_{S_n}(\sigma)|$.

Now $C_{A_n}(\sigma) = C_{S_n}(\sigma) \cap A_n$, so for each $\sigma \in A_n$ there are two possibilities:

(i) $C_{S_n}(\sigma)$ contains an odd element, and $\mathrm{ccl}_{A_n}(\sigma) = \mathrm{ccl}_{S_n}(\sigma)$, or

(ii) $C_{S_n}(\sigma)$ consists of even elements, and $\mathrm{ccl}_{S_n}(\sigma)$ is the union of two conjugacy classes in A_n, $\mathrm{ccl}_{A_n}(\sigma)$ and another.

Example 5.3.7. Let us use this to describe conjugacy classes in A_4. Each conjugacy class of even elements in S_4 yields 1 or 2 conjugacy classes in A_4, depending on whether their elements are centralised by an odd element or not.

The conjugacy class 1^4 in S_4 consisted of the identity element, which is of course its own conjugacy class in A_4 too.

The conjugacy class $1^2 2^1$ in S_4 consisted of the transpositions, but these are odd so do not lie in A_4.

The conjugacy class 2^2 in S_4 consisted of the double transpositions, which are even and do lie in A_4. The double transposition $(12)(34)$ is centralised by the odd element (12), so this remains a single conjugacy class in A_4.

The conjugacy class $1^1 3^1$ in S_4 consisted of the 3-cycles, which are even and do lie in A_4. The centraliser of such an element is a cyclic group of order 3 so does not contain an odd element. Thus this conjugacy class of size 8 in S_4 splits into 2 conjugacy classes of size 4 in A_4. A direct check shows that these two conjugacy classes are

$$\begin{aligned}&\{(123), (142), (134), (243)\}\\ &\{(132), (143), (124), (234)\}.\end{aligned}$$

The conjugacy class 4^1 in S_4 consisted of the 4-cycles, but these are odd so do not lie in A_4. △

Example 5.3.8. Let us search for normal subgroups $H \lhd A_4$, which of course contain the identity element.

If H contains the conjugacy class 2^2 of S_4, of double transpositions, which is also a conjugacy class in A_4, then we could have

$$H = K = \{e, (12)(34), (13)(24), (14)(23)\}$$

which is normal in A_4.

The other conjugacy classes in A_4 are the two whose union is the conjugacy class $1^1 3^1$ of 3-cycles in S_4. If $(123) \in H$, say, then $(123)(123) = (132) \in H$ too, so H must contain both conjugacy classes or none. But if it includes both then it has ≥ 9 elements, so must be A_4 itself.

Thus $\{e\}, K, A_4$ are the only normal subgroups of A_4, so

$$A_4/\{e\} \cong A_4, \quad A_4/K \cong C_3, \quad A_4/A_4 = \{e\}$$

are the only quotient groups of A_4. △

We will use these ideas to prove that the group A_5 is simple.

Theorem 5.3.9. *The group A_5 is simple.*

Proof. The group S_5 has $5! = 120$ elements, and its conjugacy classes may be summarised as

Conjugacy class	1^5	$2^1 1^3$	$2^2 1^1$	$3^1 1^2$	$3^1 2^1$	$4^1 1^1$	5^1
Typical element	e	(12)	(12)(34)	(123)	(123)(45)	(1234)	(12345)
Size	1	10	15	20	20	30	24
Sign	+	-	+	+	-	-	+

In A_5 we only see the conjugacy classes of even elements. The odd element (12) centralises (12)(34), so its conjugacy class stays intact; the odd element (45) centralises (123), so its conjugacy class stays intact.

The centraliser of (12345) in S_5 has order $5^1 \cdot 1! = 5$, so must just be the cyclic group generated by (12345) itself. This consist of even elements, so the conjugacy class of (12345) splits into two conjugacy classes in A_4 of size 12 each. The conjugacy classes of A_5 may be summarised as

Conjugacy class	1^5	$2^2 1^1$	$3^1 1^2$	5^1	5^1
Typical element	e	(12)(34)	(123)	(12345)	(21345)
Size	1	15	20	12	12

Now if $H \lhd A_5$, then $|H|$ divides $|A_5| = 60$ by Lagrange's theorem, and H is a union of conjugacy classes. But the only sum of sizes of these conjugacy classes, including that of e, which divides 60 is 1 or $1 + 15 + 20 + 12 + 12 = 60$, so the only normal subgroups of A_5 are $\{e\}$ and A_5. □

In fact, the groups A_n are simple for all $n \geq 5$, as you will see in IB Groups, Rings, and Modules. On the other hand, we have seen that A_4 is not simple.

Chapter 6

Groups of matrices

6.1 The general and special linear groups

Lecture 21

In this chapter we will write

$$\mathbb{F} \text{ for either } \mathbb{R} \text{ or } \mathbb{C},$$

when we make statements which apply to both.

Let us write

$$M_{n\times m}(\mathbb{F}) := \{n \times m \text{ matrices with entries in } \mathbb{F}\}.$$

Matrix multiplication is a function

$$\cdot : M_{n\times m}(\mathbb{F}) \times M_{m\times l}(\mathbb{F}) \longrightarrow M_{n\times l}(\mathbb{F}),$$

and in particular gives a binary operation

$$\cdot : M_{n\times n}(\mathbb{F}) \times M_{n\times n}(\mathbb{F}) \longrightarrow M_{n\times n}(\mathbb{F})$$

on the set of $n \times n$ matrices. This is associative, and furthermore the identity matrix

$$I_n := \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

is an identity element for this binary operation. However, not all matrices are invertible: you have seen in IA Vectors & Matrices a criterion in terms of the determinant for matrices to be invertible, namely

$$\text{a matrix } X \text{ is invertible if and only if } \det(X) \neq 0.$$

Definition 6.1.1. The nth *general linear group* over $\mathbb{F}$ is

$$GL_n(\mathbb{F}) := \{X \in M_{n\times m}(\mathbb{F}) \; s.t. \; \det(X) \neq 0\}.$$

The above discussion proves the following.

Lemma 6.1.2. *The data $(GL_n(\mathbb{F}), \cdot, I_n)$ is a group.* □

The determinant satisfies $\det(A \cdot B) = \det(A) \times \det(B)$, and so

$$\det : (GL_n(\mathbb{F}), \cdot, I_n) \longrightarrow (\mathbb{F} \setminus \{0\}, \times, 1)$$

is a group homomorphism.

Definition 6.1.3. The nth *special linear group* over $\mathbb{F}$ is the kernel of $\det : GL_n(\mathbb{F}) \to \mathbb{F} \setminus \{0\}$, so is

$$SL_n(\mathbb{F}) := \{X \in M_{n\times m}(\mathbb{F}) \, s.t. \, \det(X) = 1\}.$$

It is a normal subgroup of $GL_n(\mathbb{F})$.

In fact $\det : GL_n(\mathbb{F}) \to \mathbb{F} \setminus \{0\}$ is surjective, as for any $\lambda \in \mathbb{F} \setminus \{0\}$ we have

$$\det \begin{bmatrix} \lambda & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix} = \lambda,$$

and so by the isomorphism theorem we have

$$\frac{GL_n(\mathbb{F})}{SL_n(\mathbb{F})} \cong \mathbb{F} \setminus \{0\}.$$

The group $GL_n(\mathbb{F})$ acts on $\mathbb{F}^n$, where we think of $\mathbb{F}^n$ as column vectors, via

$$\begin{aligned} GL_n(\mathbb{F}) \times \mathbb{F}^n &\longrightarrow \mathbb{F}^n \\ (A, v) &\longmapsto Av. \end{aligned}$$

This corresponds to a homomorphism

$$\rho : GL_n(\mathbb{F}) \longrightarrow \mathrm{Sym}(\mathbb{F}^n)$$

which is injective, and whose image consists of those bijections $\mathbb{F}^n \to \mathbb{F}^n$ which are linear maps. This gives an isomorphism from $GL_n(\mathbb{F})$ to the group of invertible linear maps from $\mathbb{F}^n$ to itself.

6.2 Change of basis

You have seen in IA Vectors & Matrices that if a matrix $A \in M_{n\times n}(\mathbb{F})$ represents a linear map α in the standard basis $\{e_1, e_2, \dots, e_n\}$ of $\mathbb{F}^n$, and if $\{f_1, f_2, \dots, f_n\}$ is another basis, then the matrix for α in the second basis is given by $P^{-1}AP$, where P is the (invertible) matrix with entries determined by

$$f_j = \sum_{j=1}^{n} P_{ij} e_i.$$

Proposition 6.2.1. *The group $GL_n(\mathbb{F})$ acts on the right on $M_{n\times n}(\mathbb{F})$ by*

$$\begin{aligned} \bullet : M_{n\times n}(\mathbb{F}) \times GL_n(\mathbb{F}) &\longrightarrow M_{n\times n}(\mathbb{F}) \\ (A, P) &\longmapsto P^{-1}AP, \end{aligned}$$

and the orbit of A is given by all matrices representing the same linear map as A in different bases.

Proof. We have

$$(A \bullet P) \bullet Q = (P^{-1}AP) \bullet Q = Q^{-1}P^{-1}APQ = (PQ)^{-1}A(PQ) = A \bullet PQ$$

and $A \bullet I_n = I_n^{-1}AI_n = A$, so the two axioms for a right group action are satisfied.

By the discussion above, $P^{-1}AP$ is a matrix representing the same linear map as A in a new basis $\{f_1, f_2, \ldots, f_n\}$, related to the standard basis by $f_j = \sum_{j=1}^{n} P_{ij}e_i$. □

Example 6.2.2. In the discussion of Jordan normal form in IA Vectors & Matrices you have seen that any $A \in M_{2\times2}(\mathbb{C})$ is conjugate to one of

$$\begin{bmatrix}\lambda_1 & 0\\ 0 & \lambda_2\end{bmatrix} \text{ with } \lambda_1 \neq \lambda_2, \begin{bmatrix}\lambda & 0\\ 0 & \lambda\end{bmatrix}, \text{ or } \begin{bmatrix}\lambda & 1\\ 0 & \lambda\end{bmatrix}. \tag{6.2.1}$$

In the first case the numbers $\lambda_1, \lambda_2 \in \mathbb{C}$ are uniquely associated to the matrix A: they are its eigenvalues. But their order is not unique, as

$$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}^{-1} \begin{bmatrix}\lambda_1 & 0\\ 0 & \lambda_2\end{bmatrix} \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} = \begin{bmatrix}\lambda_2 & 0\\ 0 & \lambda_1\end{bmatrix}.$$

Apart from this, no two matrices in the list (6.2.1) are conjugate: the matrices $\begin{bmatrix}\lambda & 0\\ 0 & \lambda\end{bmatrix}$ are scalar multiples of the identity matrix, so are only conjugate to themselves; the matrices $\begin{bmatrix}\lambda & 1\\ 0 & \lambda\end{bmatrix}$ are characterised by having a repeated eigenvalue λ but only a 1-dimensional eigenspace; the matrices $\begin{bmatrix}\lambda_1 & 0\\ 0 & \lambda_2\end{bmatrix}$ are characterised by having distinct eigenvalues. There therefore have a complete description of the orbits of $GL_2(\mathbb{C})$ acting on $M_{2\times2}(\mathbb{C})$ by conjugation.

Let us work out the stabilisers of this action. A matrix $P \in GL_2(\mathbb{C})$ stabilises $A \in M_{2\times2}(\mathbb{C})$ if $P^{-1}AP = A$, or equivalently if $AP = PA$.

For the first type of orbit we have

$$\begin{bmatrix}\lambda_1 & 0\\ 0 & \lambda_2\end{bmatrix} \begin{bmatrix}a & b\\ c & d\end{bmatrix} = \begin{bmatrix}\lambda_1 a & \lambda_1 b\\ \lambda_2 c & \lambda_2 d\end{bmatrix}$$

and

$$\begin{bmatrix}a & b\\ c & d\end{bmatrix} \begin{bmatrix}\lambda_1 & 0\\ 0 & \lambda_2\end{bmatrix} = \begin{bmatrix}\lambda_1 a & \lambda_2 b\\ \lambda_1 c & \lambda_2 d\end{bmatrix}$$

which are equal if and only if $\lambda_2 c = \lambda_1 c$ and $\lambda_1 b = \lambda_2 b$. But $\lambda_1 \neq \lambda_2$, so we must have $b = c = 0$. Thus the stabiliser of $\begin{bmatrix}\lambda_1 & 0\\ 0 & \lambda_2\end{bmatrix}$ is

$$\left\{ \begin{bmatrix}a & 0\\ 0 & d\end{bmatrix} \in GL_2(\mathbb{C}) \right\}.$$

For the second type of orbit, as we already pointed out these are scalar multiples of the identity matrix so are stabilised by the whole of $GL_2(\mathbb{C})$.

For the third type of orbit we have

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

and

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

which are equal if and only if $c = 0$ and $a = d$. Thus the stabiliser of $\begin{bmatrix}\lambda & 1\\ 0 & \lambda\end{bmatrix}$ is

$$\left\{\begin{bmatrix}a & b\\ 0 & a\end{bmatrix} \in GL_2(\mathbb{C})\right\}.$$

△

6.3 Möbius transformations revisited

Recall that Möbius transformations $f \in \mathcal{M}$ may be written as $f(z) = \frac{az+b}{cz+d}$ with $a, b, c, d \in \mathbb{C}$ and $ad - bc \neq 0$. Furthermore, we have seen that if $f'(z) = \frac{a'z+b'}{c'z+d'}$ is another Möbius transformation then $f'(f(z)) = \frac{a''z+b''}{c''z+d''}$ where

$$\begin{bmatrix}a'' & b''\\ c'' & d''\end{bmatrix} = \begin{bmatrix}a' & b'\\ c' & d'\end{bmatrix}\begin{bmatrix}a & b\\ c & d\end{bmatrix}.$$

This implies that the function

$$\begin{aligned}\phi : SL_2(\mathbb{C}) &\longrightarrow \mathcal{M}\\ \begin{bmatrix}a & b\\ c & d\end{bmatrix} &\longmapsto \frac{az+b}{cz+d}\end{aligned}$$

is a group homomorphism. Lecture 22

Proposition 6.3.1. *The homomorphism ϕ is surjective, and its kernel is $\{I_2, -I_2\}$.*

Proof. If $f(z) = \frac{az+b}{cz+d}$ is a Möbius transformation then we may form the matrix $\begin{bmatrix}a & b\\ c & d\end{bmatrix}$, which lies in $GL_2(\mathbb{C})$ as $\det\begin{bmatrix}a & b\\ c & d\end{bmatrix} = ad - bc \neq 0$. However its determinant need not be equal to 1, so it need not lie in $SL_2(\mathbb{C})$. However, if we write its determinant as $ad - bc = \Delta^2$ then

$$\det\begin{bmatrix}a/\Delta & b/\Delta\\ c/\Delta & d/\Delta\end{bmatrix} = \frac{ad-bc}{\Delta^2} = 1$$

so $\begin{bmatrix}a/\Delta & b/\Delta\\ c/\Delta & d/\Delta\end{bmatrix} \in SL_2(\mathbb{C})$. But

$$\phi\left(\begin{bmatrix}a/\Delta & b/\Delta\\ c/\Delta & d/\Delta\end{bmatrix}\right) = \frac{\frac{a}{\Delta}z + \frac{b}{\Delta}}{\frac{c}{\Delta}z + \frac{d}{\Delta}} = \frac{az+b}{cz+d},$$

which shows that ϕ is surjective.

If $\phi(\begin{bmatrix} a & b \\ c & d \end{bmatrix})$ is the identity map, then $\frac{az+b}{cz+d} = z$ for all z. This can only happen if $c = b = 0$ and $a = d$, so that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}.$$

But as this matrix is in $SL_2(\mathbb{C})$ its determinant, which is a^2, must be 1, so $a = \pm 1$. □

By the isomorphism theorem we therefore have

$$\mathcal{M} \cong \frac{SL_2(\mathbb{C})}{\{I_2, -I_2\}}.$$

The quotient group $\frac{SL_2(\mathbb{C})}{\{I_2,-I_2\}}$ is known as the *projective special linear group*, and is denoted $PSL_2(\mathbb{C})$.

6.4 The orthogonal and special orthogonal groups

Recall that the *transpose* of a matrix $A \in M_{n\times m}(\mathbb{F})$ is the matrix $A^T \in M_{m\times n}(\mathbb{F})$ with $(A^T)_{ij} = A_{ji}$. It satisfies $(AB)^T = B^T A^T$.

Definition 6.4.1. The nth *orthogonal group* is

$$O(n) := \{P \in GL_n(\mathbb{R})\, s.t.\, P^T P = I_n\}.$$

Lemma 6.4.2. *$O(n)$ is a subgroup of $GL_n(\mathbb{R})$.*

Proof. Let $P, Q \in O(n)$, and consider PQ^{-1}. We have

$$\begin{aligned}(PQ^{-1})^T(PQ^{-1}) &= (Q^{-1})^T P^T P Q^{-1} \\ &= (Q^{-1})^T Q^{-1} \text{ as } P^T P = I_n.\end{aligned}$$

Now as $Q \in O(n)$ we have $Q^T Q = I_n$, so that $Q^T = Q^{-1}$. Thus

$$(Q^{-1})^T Q^{-1} = (Q^{-1})^T Q^T = (QQ^{-1})^T = I_n^T = I_n,$$

so $PQ^{-1} \in O(n)$. Thus $O(n)$ is indeed a subgroup of $GL_n(\mathbb{R})$. □

Note that if $P \in O(n)$ then $P^{-1} = P^T$, as $P^T P = I_n$.

Recall that $\mathbb{R}^n$ has the standard inner product given by

$$x \cdot y = \sum_{i=1}^{n} x_i y_i.$$

If we think of elements of $\mathbb{R}^n$ as being column vectors, then

$$x \cdot y = x^T y.$$

Thus if we consider $P \in GL_n(\mathbb{R})$ as having columns given by vectors $f_1, f_2, \ldots, f_n$, so that P is the change-of-basis matrix from the standard basis to $\{f_1, f_2, \ldots, f_n\}$, then

$$(P^TP)_{ij} = f_i^T f_j = f_i \cdot f_j$$

and so

$$P \in O(n) \iff f_i \cdot f_j = \delta_{ij} := \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases} \tag{6.4.1}$$

That is, $P \in O(n)$ if and only if the columns of P form an orthonormal basis.

Example 6.4.3. The group $O(n)$ acts on $M_{n\times n}(\mathbb{R})$ by conjugation, via $GL_n(\mathbb{R})$. With respect to this action matrices A and B lie in the same orbit if they represent the same linear map with respect to two orthonormal bases. △

Proposition 6.4.4. *A matrix $P \in GL_n(\mathbb{R})$ lies in $O(n)$ if and only if $Px \cdot Py = x \cdot y$ for all $x, y \in \mathbb{R}^n$.*

Proof. If $P \in O(n)$ then we have $Px \cdot Py = (Px)^T Py = x^T P^T P y = x^T y = x \cdot y$, as $P^TP = I_n$. Conversely, if $Px \cdot Py = x \cdot y$ for all $x, y \in \mathbb{R}^n$ then taking $x = e_i$ and $y = e_j$ to be basis vectors we have

$$Pe_i \cdot Pe_j = e_i \cdot e_j = \delta_{ij}$$

so the vectors $Pe_1, Pe_2, \ldots, Pe_n$ are orthonormal. These are the columns of the matrix P, so $P \in O(n)$ by the criterion (6.4.1). □

Recall that the length of a vector is $|v| = \sqrt{v \cdot v}$, and the angle $v\angle w$ between vectors v and w is related to the inner product by the formula $v \cdot w = |v||w| \cos(v\angle w)$.

Corollary 6.4.5. *If $P \in O(n)$ and $v \in \mathbb{R}^n$ then $|Pv| = |v|$. If $w \in \mathbb{R}^n$ is another vector then $Pv\angle Pw = v\angle w$.*

Proof. For the first part, we have $|Pv| = \sqrt{Pv \cdot Pv} = \sqrt{v \cdot v} = |v|$, using the last proposition.

For the second part we have

$$\begin{aligned} \cos(Pv\angle Pw) &= \frac{Pv \cdot Pw}{|Pv||Pw|} \\ &= \frac{v \cdot w}{|v||w|} \text{ by the last proposition and the first part of this corollary} \\ &= \cos(v\angle w), \end{aligned}$$

and so $Pv\angle Pw = v\angle w$, as the function $\cos : [0, \pi] \to [-1, 1]$ is injective. □

A standard property of the determinant is that $\det(X^T) = \det(X)$. Thus if $P \in O(n)$, so $P^TP = I_n$, then we have

$$1 = \det(I_n) = \det(P^TP) = \det(P^T)\det(P) = \det(P)\det(P),$$

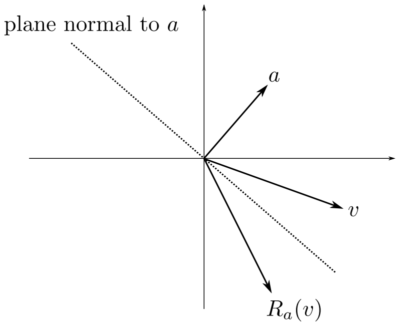
so $\det(P) = \pm 1$.

Definition 6.4.6. The nth *special orthogonal group* is

$$SO(n) := \operatorname{Ker}(\det : O(n) \to C_2) = \{P \in GL_n(\mathbb{R}) \, s.t. \, P^TP = I_n \text{ and } \det(P) = 1\}.$$

6.5 Reflections

Lecture 23



Definition 6.5.1. If $a \in \mathbb{R}^n$ is a vector of length 1, then the *reflection* in the plane normal to a is the linear map $R_a : \mathbb{R}^n \to \mathbb{R}^n$ given by

$$R_a(v) := v - 2(v \cdot a)a.$$

Lemma 6.5.2. *R_a lies in $O(n)$.*

Proof. Let $v, w \in \mathbb{R}^n$, Then

$$\begin{aligned} R_a(v) \cdot R_a(w) &= (v - 2(v \cdot a)a) \cdot (w - 2(w \cdot a)a) \\ &= (v \cdot w) - 2(w \cdot a)(v \cdot a) - 2(v \cdot a)(w \cdot a) + 4(v \cdot a)(w \cdot a)(a \cdot a) \\ &= v \cdot w \text{ as } a \cdot a = 1, \end{aligned}$$

so $R_a \in O(n)$ by the criterion in Proposition 6.4.4. □

Lemma 6.5.3. *If $P \in O(n)$ then $PR_aP^{-1} = R_{Pa}$.*

Proof. We have

$$\begin{aligned} PR_aP^{-1}(v) &= P(P^{-1}v - 2(P^{-1}v \cdot a)a) \\ &= v - 2(P^{-1}v \cdot a)Pa \end{aligned}$$

but $P^{-1}v \cdot a = (P^{-1}v)^T a = v^T(P^{-1})^T a = v \cdot Pa$ as $P^{-1} = P^T$, so

$$\begin{aligned} &= v - 2(v \cdot Pa)Pa \\ &= R_{P_a}(v). \end{aligned}$$ □

We can easily establish further basic properties of R_a. First, for any vector v we have

$$\begin{aligned} R_a(R_a(v)) &= R_a(v) - 2(R_a(v) \cdot a)a \\ &= (v - 2(v \cdot a)a) - 2((v - 2(v \cdot a)a) \cdot a)a \\ &= v - 2(v \cdot a)a - 2(v \cdot a)a + 4(v \cdot a)(a \cdot a)a \\ &= v \text{ as } a \cdot a = 1 \end{aligned}$$

so $R_a \circ R_a = \mathrm{Id}$. Thus the only possible eigenvalues of R_a are ± 1. Both eigenvalues arise, as if $v = a$ then

$$\begin{aligned} R_a(a) &= a - 2(a \cdot a)a \\ &= a - 2(a \cdot a)a \\ &= a - 2a \text{ as } a \cdot a = 1 \\ &= -a \end{aligned}$$

so a is an eigenvector with eigenvalue -1, and if v lies in the plane normal to a then

$$R_a(v) = v - 2(v \cdot a)a = v \qquad \text{as } v \cdot a = 0$$

so v is an eigenvector with eigenvalue $+1$. If we choose a basis $f_2, f_3, \ldots, f_n$ for the plane normal to a, and set $f_1 := a$, then $\{f_1, f_2, \ldots, f_n\}$ is a basis for $\mathbb{R}^n$, and in this basis the linear map R_a is represented by the matrix

$$\begin{bmatrix} -1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{bmatrix}.$$

In particular, we see that $\det(R_a) = -1$, so that R_a *does not* lies in $SO(n)$.

6.6 Reflections and rotations in $\mathbb{R}^2$

Theorem 6.6.1. *Every element of $SO(2)$ is of the form*

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

for some $0 \leq \theta < 2\pi$. This is an anticlockwise rotation of $\mathbb{R}^2$ about the origin by an angle of θ.

Proof. Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SO(2)$, so $A^T A = I_2$ and $\det(A) = 1$. This gives that $A^T = A^{-1}$, so

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix} = \frac{1}{1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

and $ad - bc = 1$, so $a = d$ and $b = -c$, and hence $a^2 + c^2 = 1$. Thus we may write $a = \cos\theta$ and $c = \sin\theta$ for a unique $0 \leq \theta < 2\pi$, as claimed. This is indeed a rotation by θ. □

Theorem 6.6.2. *Every element of $O(2) \setminus SO(2)$ is a reflection.*

Proof. Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in O(2) \setminus SO(2)$, so $A^T A = I_2$ and $\det(A) = -1$. This gives that $A^T = A^{-1}$, so

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix} = \frac{1}{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

and $ad - bc = -1$, so $a = -d$ and $b = c$, and hence $a^2 + c^2 = 1$. Thus we may write $a = \cos\theta$ and $c = \sin\theta$ for a unique $0 \leq \theta < 2\pi$, so that

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

One can check with the double angle formulas that

$$\begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} \begin{bmatrix} \sin\theta/2 \\ -\cos\theta/2 \end{bmatrix} = - \begin{bmatrix} \sin\theta/2 \\ -\cos\theta/2 \end{bmatrix}$$

and

$$\begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} \begin{bmatrix} \cos\theta/2 \\ \sin\theta/2 \end{bmatrix} = \begin{bmatrix} \cos\theta/2 \\ \sin\theta/2 \end{bmatrix}$$

so $\begin{bmatrix} \sin\theta/2 \\ -\cos\theta/2 \end{bmatrix}$ and $\begin{bmatrix} \cos\theta/2 \\ \sin\theta/2 \end{bmatrix}$ are orthogonal eigenvectors of A with eigenvalues -1 and $+1$ respectively. Thus we recognise that A is a matrix for the reflection in the plane orthogonal to the unit vector $\begin{bmatrix} \sin\theta/2 \\ -\cos\theta/2 \end{bmatrix}$. □

Corollary 6.6.3. *Every element of $O(2)$ is a composition of (at most two) reflections.*

Proof. We have seen that every element of $O(2)\setminus SO(2)$ is a reflection. If $A \in SO(2)$ then $A = \left(A \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \right) \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ and $A \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ has determinant -1 so lies in $O(2) \setminus SO(2)$ and is hence a reflection, so A is the composition of two reflections. □

6.7 Reflections and rotations in $\mathbb{R}^3$

Lecture 24

Theorem 6.7.1. *If $A \in SO(3)$ then there is a unit vector $v \in \mathbb{R}^3$ such that $Av = v$.*

Proof. Such a v is an eigenvector of A with eigenvalue 1, so we need to show that 1 is indeed an eigenvalue of A. This is the same as showing that $\det(A - I) = 0$. To do this, we calculate

$$\begin{aligned}
\det(A-I) &= \det(A - A^T A) \text{ as } A \in O(3) \\
&= \det((I - A^T)A) \\
&= \det(I - A^T)\det(A) \\
&= \det(I - A^T) \text{ as } A \in SO(3) \\
&= \det(I - A) \text{ as } \det(B^T) = \det(B) \\
&= \det((-I)(A - I)) \\
&= \det(-I)\det(A - I) \\
&= -\det(A - I) \text{ as } \det(-I) = (-1)^3 = -1 \text{ for } 3 \times 3 \text{ matrices}
\end{aligned}$$

and so $\det(A - I) = 0$ as required. □

Corollary 6.7.2. *Every $A \in SO(3)$ is conjugate (in $SO(3)$) to a matrix of the form*

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

Proof. By the theorem we can find a unit vector f_1 such that $Af_1 = f_1$, and we may extend this to an orthonormal basis $\{f_1, f_2, f_3\}$. Then for $i \in \{2, 3\}$ we have

$$Af_i \cdot f_1 = Af_i \cdot Af_1 = f_i \cdot f_1 = 0$$

so that Af_i lies in the span of f_2 and f_3. In other words, A restricts to an orthogonal transformation of $\langle f_2, f_3 \rangle$, which again has determinant 1, so gives an element of $SO(2)$. Thus, by Theorem 6.6.1, in the basis $\{f_1, f_2, f_3\}$ the matrix A has the form claimed.

Finally, as the f_i form an orthonormal basis, the change of basis matrix P is an orthogonal matrix. If P lies in $SO(3)$ we are done, and if not replacing f_1 by $-f_1$ gives a new change of basis matrix P' which does lie in $SO(3)$ and also conjugates A into the claimed form. □

Corollary 6.7.3. *Every element of $O(3)$ may be written as the composition of (at most three) reflections.*

Proof. Suppose first that $A \in SO(3)$. By the previous corollary A is conjugate to

$$B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{bmatrix},$$

and the matrix $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ is a composition of at most two reflections by Corollary 6.6.3. Thus B is also a composition of at most two reflections, so A is too (as the conjugate of a reflection is a reflection.)

If $A \in O(3) \setminus SO(3)$ then $\det(A) = -1$ and we have

$$A = \left(A \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right) \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

where $A \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ has determinant $+1$ so lies in $SO(3)$, and hence is a composition of at most two reflections. Thus A is a composition of at most three reflections. □

6.8 Vista

Not on the schedules

Whenever we have a number system in which we may both add and multiply elements, we may consider matrices with entries in that number system. For example, we have considered the integers modulo n, which we write as $\mathbb{Z}_n$, and we can both add and multiply these.

Consider for example

$$GL_2(\mathbb{Z}_5) := \{2 \times 2 \text{ matrices with entries in } \mathbb{Z}_5, \text{ which are invertible}\}.$$

It is not hard to see that a 2×2 matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ has an inverse, which will be given by the usual formula, if and only if $ad - bc$ has a multiplicative inverse in $\mathbb{Z}_5$. In other words, it must lie in the subset $U_5 \subset \mathbb{Z}_5$ which we discussed in Section 2.2.1. As 5 is a prime number, $U_5 = \{1, 2, 3, 4\}$ is simply the non-zero numbers modulo 5. This is a group of order 4.

There are $5^4 = 625$ possible 2×2 matrices with entries in $\mathbb{Z}_5$. To work out the order of $GL_2(\mathbb{Z}_5)$ it is easier to count the non-invertible matrices: those $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $ad - bc = 0$.

If $a = 0$ then b and c must satisfy $bc = 0$, so either $b = 0$ (and c and d) can be anything, or else $c = 0$ (and b and d) can be anything. This gives $5^2 + 5^2 = 50$, but we have double counted those where both $c = 0$ and $b = 0$ (and d is anything): there are 5 of these, so in fact there are 45 such matrices.

If $a \neq 0$ then we can uniquely solve $ad - bc = 0$ for d given any b and c, and any $a \neq 0$. There are $5 \times 5 \times 4 = 100$ such matrices.

In total we get 145 non-invertible matrices, so the number of invertible matrices is

$$|GL_2(\mathbb{Z}_5)| = 625 - 145 = 480.$$

We can define the subgroup $SL_2(\mathbb{Z}_5)$ as those matrices of determinant 1. As usual this is the kernel of $\det : GL_2(\mathbb{Z}_5) \to U_5$, which is surjective, so

$$|SL_2(\mathbb{Z}_5)| = \frac{480}{4} = 120.$$

Finally, the matrices $\{I_2, 4I_2\} \subset SL_2(\mathbb{Z}_5)$ form a normal subgroup (in fact, central: recall that 4 plays the role of -1 in $\mathbb{Z}_5$, so this is like $\{I_2, -I_2\}$), so we can form the quotient group $PSL_2(\mathbb{Z}_5) = SL_2(\mathbb{Z}_5)/\{I_2, 4I_2\}$ with

$$|PSL_2(\mathbb{Z}_5)| = \frac{120}{2} = 60 = 2^2 \cdot 3 \cdot 5.$$

This has a reasonable size, and in fact has the same size as A_5.

One can analyse the conjugacy classes in the group $PSL_2(\mathbb{Z}_5)$ in an elementary but laborious way, by choosing a matrix, working out the size of its centraliser, and hence working out the size of its conjugacy class. When the size of all the conjugacy classes found add up to 60, we are done. The result is as follows.

Conjugacy class	$\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$	$\begin{bmatrix}2 & 0\\0 & 3\end{bmatrix}$	$\begin{bmatrix}0 & 4\\1 & 1\end{bmatrix}$	$\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}$	$\begin{bmatrix}1 & 4\\0 & 1\end{bmatrix}$
Order	1	2	3	5	5
Centraliser size	60	4	3	5	5
Conjugacy class size	1	15	20	12	12

Note that the features of this table are identical to that for A_5, so the argument in Theorem 5.3.9 applies to $PSL_2(\mathbb{Z}_5)$ and shows that this group is also simple. In fact, we have the following.

I messed this up in lectures.

Theorem 6.8.1. *$PSL_2(\mathbb{Z}_5) \cong A_5$.*

Proof. Write $G := PSL_2(\mathbb{Z}_5)$. Note that

$$H := \left\{ \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}2 & 0\\0 & 3\end{bmatrix}, \begin{bmatrix}0 & 2\\2 & 0\end{bmatrix}, \begin{bmatrix}0 & 1\\4 & 0\end{bmatrix} \right\}$$

forms a subgroup of G of order 4. Every element $g \in G$ of order 2 is conjugate to $h := \begin{bmatrix}2 & 0\\0 & 3\end{bmatrix}$, as there is a single conjugacy class of elements of order 2, so $g = khk^{-1}$ and so $g \in kHk^{-1}$. Thus the conjugates of the subgroup H contain every element of order 2. There are 15 elements of order 2, and H contains 3 elements of order 2, so there must be at least 5 conjugates of H in G.

Considering the action of G on the set X of subgroups of G by conjugation, with $G_H \leq G$ denoting the subgroup of those elements which conjugate H to itself, we certainly have $H \leq G_H$ and so 2^2 divides $|G_H|$. The orbit-stabiliser theorem gives

$$2^2 \cdot 3 \cdot 5 = |G| = |G_H| \cdot |\text{ conjugates of } H\ |,$$

so there are either 5 or 15 conjugates of H. If there were 15 conjugates of H, each having 3 elements of order 2, then (as there are only 15 elements of order 2) some pair of conjugates have to share ≥ 2 elements of order 2, but such groups must then be equal, a contradiction. Thus there are precisely 5 conjugates of H.

The action of G by conjugation on the set of 5 conjugates of H gives a homomorphism

$$\phi : G \longrightarrow S_5.$$

The kernel of this is a normal subgroup of G, so is trivial or is G (because we have shown that G is simple). It is not the whole of G, as G acts transitively on the set of conjugates of H, so must be trivial, i.e. ϕ is injective. Then $\phi(G)$ is a subgroup of S_5 of index $\frac{5!}{60} = 2$, so is normal by Corollary 4.1.4. But then $A_5 \cap \phi(G)$ is a normal subgroup of A_5, and it cannot be trivial (as it has index at most 2 in A_5) so must be the whole of A_5. In other words $\phi(G) = A_5$, so ϕ gives an isomorphism from $G = PSL_2(\mathbb{Z}_5)$ to A_5. □