Groups

Adam Kelly

Updated June 7, 2021

This set of notes is a work-in-progress account of the course 'Groups', originally lectured by Dr. Ana Khukhro in Michaelmas 2020 at Cambridge. These notes are not a transcription of the lectures, but they do roughly follow what was lectured (in content and in structure).

These notes are my own view of what was taught, and should be somewhat of a superset of what was actually taught. I frequently provide different explanations, proofs, examples, and so on in areas where I feel they are helpful. Because of this, this work is likely to contain errors, which you may assume are my own. If you spot any or have any other feedback, I can be contacted at ak2316@cam.ac.uk.

Contents

1 Groups

'Groups' is a course which introduces you to the subject of *Abstract Algebra*. Indeed, while groups are one of the simplest and most basic of all the algebraic structures, they are immensely useful and appear in almost every area of mathematics.

1.1 Definition of a Group

We will begin our study of the subject by defining formally what a group is.

Definition 1.1 (Group)**.** A *group* is a set G with a binary operation[1] $*$ which satisfies the axioms:

- *Identity.* There is an element $e \in G$ such that $g * e = e * g = g$ for every $g \in G$.
- *Inverses.* For every element $g \in G$, there is an element $g^{-1} \in G$ such that $g * g^{-1} = g^{-1} * g = e$.
- *Associativity.* The operation $*$ is associative.

We typically refer to a group as defined above by $(G, *)$, which explicitly states that $*$ is the group operation. When the operation being used is clear, we can refer to the group by just G. We will also be omitting the group's operation symbol quite often, for example writing $gh = g * h$.

In a later section, we will look at some non-trivial examples of groups.

1.1.1 Elementary Properties of Groups

With the notion of a group now defined, we can now consider some basic facts that follow directly from the definition of a group. We will first address whether it is possible for a group to have multiple identity elements, or for an element to have multiple inverses (no).

Proposition 1.2 (Uniqueness of the Identity and Inverse)**.** *Let $(G, *)$ be a group. Then there is a unique identity element, and for every $g \in G$, g^{-1} is unique.*

[1] Some texts include an additional *closure* axiom, but this is implied by $*$ being a binary operation on G.

Proof. To prove that the identity element is unique, let e and e' be identity elements of G. Then $e * e' = e$ and $e * e' = e'$ by definition, giving $e = e'$.

To prove that the inverses are unique, suppose that for some $g, h, k \in G$ we have $g * h = g * k = e$. Then $g^{-1} * g * h = g^{-1} * g * k$, implying $h = k$. The case of $h * g = k * g = e$ follows analogously. □

The next useful fact is the *cancellation law*, whose proof bears a large resemblance to the proof that inverses are unique.

Proposition 1.3 (Cancellation Law)**.** *If $(G, *)$ is a group, and $a, b, c \in G$, then $a * b = a * c$ and $b * a = c * a$ both imply $b = c$.*

Proof. Taking $a * b = a * c$ and left-multiplying by a^{-1} we have $a^{-1} * a * b = a^{-1} * a * c$, that is, $b = c$. The other case follows analogously. □

The last proposition we will prove in this section gives us a useful result about computing inverses.

Proposition 1.4 (Computing Inverses)**.** *Let $(G, *)$ be a group, and let $g, h \in G$. Then the following hold:*

(i) $(g * h)^{-1} = h^{-1} * g^{-1}$.

(ii) $(g^{-1})^{-1} = g$.

Proof.

(i) We have $(g * h) * (h^{-1} * g^{-1}) = g * (h * h^{-1}) * g^{-1} = g * g^{-1} = e$, so $(g * h)^{-1} = h^{-1} * g^{-1}$.

(ii) Similarly, $g^{-1} * g = e$, so $(g^{-1})^{-1} = g$. □

1.1.2 Examples of Groups

It's probably of some use to have concrete examples of groups in your head, so you can get a feel for what they are. In this section we will present some non-trivial examples of groups (and some examples of non-groups).

It should be recognized that commutativity is *not* a group axiom, and the majority of groups are not commutative. We do have a name for groups where the binary operation is commutative though.

Definition 1.5 (Abelian Groups)**.** We say a group $(G, *)$ is *abelian* if $*$ is commutative, that is, if for any $g, h \in G$, $g * h = h * g$.

In this section, we will consider examples of both abelian and non-abelian groups[2]. In the first few cases, the reasons why they are a group are stated. For the others, you should consider how they satisfy the group axioms yourself.

Example 1.6 (The Trivial Group)**.** The *trivial group* is a group whose only element is the identity, $\{e\}$.

Example 1.7 (Additive Group of Integers)**.** $(\mathbb{Z}, +)$ is an group. We have

- The identity element $0 \in Z$, as $a + 0 = 0 + a = a$ for any $a \in \mathbb{Z}$
- The inverse of $a \in \mathbb{Z}$ being $-a$, as $a + (-a) = (-a) + a = 0$.
- The operation $+$ is associative and commutative.

We also have the additive group of rationals $(\mathbb{Q}, +)$, of reals $(\mathbb{R}, +)$, and of complex numbers $(\mathbb{C}, +)$ for the same reasons.

[2] If you are not familiar with some of the concepts used, such as matrices or modular arithmetic, feel free to ignore those examples.

Example 1.8 (Addition Modulo n)**.** Let $n \in \mathbb{N}$, and let $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$ denote the set of residues modulo n. Then $(\mathbb{Z}/n\mathbb{Z}, +)$ is a group (where addition is done modulo n). We have

- The identity element is $0 \pmod{n}$, as $a + 0 \equiv 0 + a \equiv a \pmod{n}$.
- The inverse of $a \in \mathbb{Z}/n\mathbb{Z}$ is $-a$, as $a + (-a) \equiv 0 \pmod{n}$.
- Addition modulo n is associative.

Example 1.9 (Non-Zero Rationals)**.** Let $\mathbb{Q}^\times$ denote the set of non-zero rationals. Then $(\mathbb{Q}^\times, \times)$ is a group.

Similarly, we also have the groups $(\mathbb{R}^\times, \times)$ and $(\mathbb{C}^\times, \times)$.

Example 1.10 (Multiplication Modulo p)**.** Let p be a prime, and let $(\mathbb{Z}/p\mathbb{Z})^\times$ denote the set of non-zero residues modulo p. Then $((\mathbb{Z}/p\mathbb{Z})^\times, \times)$ is a group (where multiplication is done modulo p).

Example 1.11 (General Linear Group)**.** Let $\mathrm{GL}_n(\mathbb{R})$ be the set of $n \times n$ matrices with non-zero determinant. Then $(\mathrm{GL}_n(\mathbb{R}), \times)$ is the *general linear group*[3].

Example 1.12 (Special Linear Group)**.** Let $\mathrm{SL}_n(\mathbb{R})$ be the set of $n \times n$ matrices with determinant 1. Then $(\mathrm{SL}_n(\mathbb{R}), \times)$ is the *special linear group*.

Non-Examples of Groups

We will now give some examples of sets with operations that are not groups. It should be useful to think about why each example does not satisfy the group axioms.

Example 1.13 (Non-Examples of Groups)**.** The following are are all *not* groups.

- $(\mathbb{Z}, \times)$
- $(\mathbb{Q}, \times)$
- The set of 2×2 matrices with matrix multiplication.
- $(\mathbb{R}, *)$ where $r * s = r \times r \times s$
- $(\mathbb{N}, *)$ where $n * m = |n - m|$.

1.2 Subgroups

Given any mathematical structure, it can be useful to know about its *substructure*. In the case of a group $(G, *)$, one might ask the question is there some subset $H \subseteq G$ that still acts like a group? This motivates the introduction of *subgroups*.

Definition 1.14 (Subgroups)**.** Let $(G, *)$ be a group. A subset $H \subseteq G$ is a *subgroup* of G if $(H, *)$ is also a group. If H is a subgroup of G, we will write $H \leq G$.

Example 1.15 (Examples of Subgroups)**.** The following are subgroups.

- For any group G, we have the *trivial subgroups* $\{e\} \leq G$ and $G \leq G$.
- $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ with addition.
- $\{0, 2, 4, \ldots\} \leq \mathbb{Z}$ with addition.
- $\mathrm{SL}_n(\mathbb{R}) \leq \mathrm{GL}_n(\mathbb{R})$ with matrix multiplication.

[3] Using matrix multiplication

Checking whether something is a subgroup is easier than checking if something is a group, since we already know about the structure of the group. To check whether H is a subgroup of $(G, *)$, we can just check the following hold:

- *Closure.* $*$ is closed in H.
- *Identity.* $e \in H$.
- *Inverses.* For $h \in H$, we also have $h^{-1} \in H$.

These can all be combined into a single test, that is sometimes known as the 'subgroup checking lemma'.

Lemma 1.16 (Subgroup Criterion)**.** *A subset H of a set G is a subgroup of $(G, *)$ if and only if H is non-empty and $x * y^{-1} \in H$ for all $x, y \in H$.*

Proof Sketch. First check that the conditions of H being non-empty and $x * y^{-1} \in H$ imply that it's a subgroup. Then, show that if H is not a subgroup, then either H is empty or $x * y^{-1} \notin H$ for some $x, y \in H$. □

As an example of using subgroups, let's try to characterize all of the subgroups of $(\mathbb{Z}, +)$.

Theorem 1.17 (Subgroups of $\mathbb{Z}$)**.** *The subgroups of $(\mathbb{Z}, +)$ are precisely the subsets of the form $n\mathbb{Z}$ for $n \in N$, where $n\mathbb{Z} = \{nk \ : \ k \in \mathbb{Z}\}$.*

Proof. First, we prove that $n\mathbb{Z}$ is a subgroup. Fix $n \in \mathbb{N}$.

- *Closure.* Given $nk_1, nk_2 \in n\mathbb{Z}$, then $nk_1 + nk_2 = n\,(k_1 + k_2) \in n\mathbb{Z}$.
- *Identity.* $0 = n \cdot 0 \in n\mathbb{Z}$.
- *Inverses.* The inverse of nk is $-nk = n(-k) \in n\mathbb{Z}$.

Thus each is subgroup. Now we prove that there is no other subgroups.

Let $H \leq Z$. If $H = \{0\}$, then $H \equiv 0\mathbb{Z}$. If not, then take the smallest positive element in H (namely n). since H is a subgroup, it's closed and contains inverses, so $n + n + \cdots + n \in H$ and $-n - n - n - \cdots - n \in H$, so $n\mathbb{Z} \subseteq H$.

Suppose, for a contradiction, there is some $k \in H$ such that $k \neq n\mathbb{Z}$. So, there is some integer n such that $nm < k < n(m + 1)$. But then $0 \leq k - nm < n$, and $k - nm \in H$ which is a contradiction, so $H = n\mathbb{Z}$. □

We can use the definition of a subgroup to prove some elementary facts.

Proposition 1.18 (Elementary Properties of Subgroups)**.** *Let G be a group.*

(i) Let H and K be subgroups of G. Then $H \cap K \leq G$.

(ii) If $K \leq H$ and $H \leq G$ then $K \leq G$ (being a subgroup is transitive).

(iii) If $K \subset H$, $H \leq G$ and $K \leq G$, then $K \leq H$.

Proof. There is multiple ways to prove these, but we will use the subgroup criterion as an example of it being used.

(i) Note that $H \cap K$ is not empty as $e \in H$ and $e \in K$. Then, for any $x, y \in H \cap K$, it suffices to show that $x * y^{-1} \in H$. By the subgroup criterion, we have $x * y^{-1} \in H$ and $x * y^{-1} \in K$, thus $x * y^{-1} \in H \cap K$, and we are done.

(ii) If $K \leq H$, then for any $x, y \in K$, we have $x * y^{-1} \in K$. Then as $K \subset H \subset G$, we must have $x * y^{-1} \in G$, and thus $K \leq H$.

(iii) As $K \leq G$, we know K is non-empty. Thus it suffices to show that $x * y^{-1} \in K$ for any $x, y \in H$. But this is implied by $K \leq G$ and the subgroup criterion, and thus as $K \subset H$, $K \leq H$. □

1.2.1 Generators

We will now consider a certain kind of subgroup, which is specified by some of the elements it contains.

Definition 1.19 (Subgroup Generated By A Subset)**.** For some set $X \subseteq G$, we define the *subgroup generated by* X, $\langle X \rangle$, to be the smallest subgroup of G which contains X.

From this definition, we can see that we must have $e \in \langle X \rangle$ and $X \subseteq \langle X \rangle$. Also, $\langle X \rangle$ must contain all products of elements in X and their inverses. We can put this in a more useful form with the following proposition.

Proposition 1.20. *Let X be a non-empty subset of G. Then $\langle X \rangle$ is the set of elements of G of the form $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_k^{\alpha_k}$ where $x_i \in X$ (not necessarily distinct), $\alpha_i = \pm 1$ and $k \geq 0$ (For $k = 0$, we say the element is e).*

Proof. Let T be the set of such elements. Clearly $T \subseteq \langle X \rangle$, and also clearly T is a subgroup of G. We also have that $X \subseteq T$ so $\langle X \rangle \subseteq T$. Thus $T = \langle X \rangle$. □

Example 1.21. We have $(\mathbb{Z}, +) = \langle 1 \rangle = \langle 2, 3 \rangle$[4], and $\mathbb{Z}/5\mathbb{Z} = \langle 1 \rangle = \langle 3 \rangle$.

In the above examples, we found that there was some subset of the elements in each of the group where if we considered the subgroup generated by those elements, we get the entire group. There is a special name for such subsets.

Definition 1.22 (Generators)**.** If X is a subset of G such that $\langle X \rangle = G$, then we call X a *generating set* of G.

Notably, these generators are not necessarily unique, as can be seen in the example above.

1.3 Homomorphisms

Imagine you had two groups, G and H and you wanted to think of a function from H to G that preserved some of the structure of the group. Let's say the function was $\phi : H \to G$. We could take any two elements $h_1, h_2 \in H$, and we could find $h_1 h_2$, and then apply ϕ to get $\phi(h_1 h_2)$. Alternatively, we could try and find $\phi(h_1)$ and $\phi(h_2)$, and then get $\phi(h_1)\phi(h_2)$. If these were the same, then the function ϕ would indeed preserve some of the structure of the group. This motivates the introduction of *homomorphisms*.

Definition 1.23 (Homomorphism)**.** Let $(G, *_G)$ and $(H, *_H)$ be groups. A function $\phi : H \to G$ is a *group homomorphism* if for all $a, b \in H$,

$$\phi(a *_H b) = \phi(a) *_G \phi(b).$$

Example 1.24 (Inclusion Function)**.** If $H \leq G$, then the function $\iota : H \to G$ that has $\iota(h) = h$ for $h \in H$ is a homomorphism. It is also injective.

Example 1.25. The function $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ with $\phi(k) = k \pmod n$ is a homomorphism, since for $k, l \in \mathbb{Z}$,

$$\phi(k + l) = (k + l) \bmod n = (k \bmod n) + (l \bmod n) = \phi(k) + \phi(l).$$

ϕ is also surjective, since $\{0, 1, \cdots, n-1\}$ are all the possible residues modulo n.

Example 1.26. The function $\phi : (\mathbb{R}, +) \to (\mathbb{R}^*, \cdot)$ where $x \to e^x$ is a homomorphism. We have

$$\phi(x + y) = e^{x+y} = e^x \cdot e^y = \phi(x) \cdot \phi(y).$$

It is injective, as $e^x = e^y$ implies $x = y$ using logarithms, and surjective, as given $a \in \mathbb{R}^*$, $\phi(\log a) = e^{\log a} = a$.

[4]Note that we write $\langle 2, 3 \rangle$ instead of $\langle \{2, 3\} \rangle$.

We can see some natural consequences of this definition of a homomorphism, which shows how well it preserves the group's structure.

Proposition 1.27 (Properties of Homomorphisms)**.** *Let $\phi : H \to G$ be a homomorphism.*

(i) $\phi(e_h) = e_g$.

(ii) $\phi(h^{-1}) = \phi(h)^{-1}$ *for all* $h \in H$.

(iii) If $\psi : G \to K$ is another homomorphism, then $\psi \circ \phi : H \to K$ is also a homomorphism.

Proof.

(i) We have $e_H *_H e_H = e_H$, so $\phi(e_H * e_H) = \phi(e_H) *_G \phi(e_H) = \phi(e_H)$, so by the cancellation law, $\phi(e_H) = e_G$.

(ii) Consider $\phi(h) *_G \phi(h^{-1}) = \phi(h *_H h^{-1}) = \phi(e_H) = e_G$, by (i). So $\phi(h)*_G = \phi(h^{-1}) = e_G$ which is the defining property of an inverse, so $\phi(h^{-1}) = \phi(h)^{-1}$.

(iii) We have

$$\begin{aligned}(\psi \circ \phi)(a*_H) &= \psi(\phi(a *_H b)) \\ &= \psi(\phi(a) *_G \phi(b)) \\ &= \psi(\phi(a)) *_K \psi(\phi(b)) \\ &= (\psi \circ \phi)(a) *_K (\psi \circ \phi)(b),\end{aligned}$$

so $\psi \circ \phi$ is a homomorphism from $H \to K$. □

There is a special case of homomorphism, which we can use to define when two groups 'are the same'.

Definition 1.28 (Isomorphism)**.** If a function $\phi : H \to G$ is bijection, and ϕ is also a homomorphism from $H \to G$, then we say it is an *isomorphism*. We say two groups H, G are *isomorphic*, written $H \cong G$ if there is an isomorphism from $H \to G$.

Having an isomorphism between two groups can be thought of in a few ways. Because we have a bijection function between the two groups, the groups must have the same order. But also, because a homomorphism preserves the structure of the group, we must also have the same group-structure within each group. Thus, when we have two isomorphic groups, we can think of them as two different descriptions of the same group.

For example, we might claim that 'there is exactly one group of order 2', and what we mean is that for any group of order 2, we can find an isomorphism to any other group of order 2.

Example 1.29. Consider the group $G = \{1, i, -1, -i\}$ with complex multiplication. Then $G \cong \mathbb{Z}/4\mathbb{Z}$. This is isomorphic with the isomorphism $\phi : G \to \mathbb{Z}/4\mathbb{Z}$, where

$$\begin{aligned}\phi(1) &= 0, \\ \phi(i) &= 1, \\ \phi(-1) &= 2, \\ \phi(-i) &= 3\end{aligned}$$

The general case is true too, where the group $H = \{e^{2\pi ik/n} : 0 \le k \le n-1\}$ with complex multiplication is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Example 1.30 ($\mathbb{Z}$'s subgroups are isomorphic)**.** $\mathbb{Z} \cong n\mathbb{Z}$ for $n \in \mathbb{Z}$, as defined in Theorem 1.17.

It's worth noting that because isomorphisms are bijective, we have the following result.

Proposition 1.31 (Inverses of isomorphisms are isomorphisms)**.** *Let $\phi : H \to G$ be an isomorphism. Then $\phi^{-1} : G \to H$ is also an isomorphism.*

Proof Sketch. Check that ϕ^{-1} is a homomorphism. □

1.3.1 Kernels

When dealing with homomorphisms, say $\phi : H \to G$, it is useful to be able to think about what elements in H our homomorphism 'reaches'. Another useful idea is thinking about what elements in H get mapped to the identity of G. To think about these questions, we use concepts of a homomorphism's *image* and *kernel*.

Definition 1.32 (Image)**.** Let $\phi : H \to G$ be a homomorphism. We define the *image* of ϕ to be the set

$$\text{img}(\phi) = \{g \in G \ : \ g = \phi(h) \text{ for some } h \in H\}.$$

Definition 1.33 (Kernel)**.** Let $\phi : H \to G$ be a homomorphism. We define the *kernel* of ϕ to be the set

$$\ker(\phi) = \{h \in H \ : \ \phi(h) = e_G\}.$$

Indeed, while both of these are subsets of G and G respectively, they are also subgroups.

Proposition 1.34 (The Image and Kernel are Subgroups)**.** *Let H and G be groups and let $\phi : H \to G$ be a homomorphism. Then* $\text{img}(\phi)$ *is a subgroup of G, and* $\ker(\phi)$ *is a subgroup of H.*

Proof. We consider the two sets separately.

1. We will show $\text{img}(\phi) \leq G$. For any $x, y \in \text{img}(\phi)$, let $x = \phi(x')$ and $y = \phi(y')$ for $x', y' \in H$. Then
$$\phi(x'y'^{-1}) = \phi(x')\phi(y')^{-1} = xy^{-1} \in \text{img}(\phi),$$
thus by the subgroup criterion $\text{img}(\phi) \leq G$.

2. Now we show $\ker(\phi) \leq H$. For $x, y \in \ker(\phi)$, we have $xy^{-1} \in \ker(\phi)$, as
$$\phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(x)\phi(y)^{-1} = e_G,$$
so again using the subgroup criterion, $\ker(\phi) \leq H$.

□

Example 1.35. $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, where $\phi(k) = k \pmod n$ has $\text{img}(\phi) = \mathbb{Z}/n\mathbb{Z}$ and $\ker(\phi) = n\mathbb{Z}$.

One of the beauties of introducing the kernel and image is that it allows us to easily see whether a homomorphism is surjective or injective.

Proposition 1.36 (Surjectivity and Injectivity Criterion)**.** *Let $\phi : H \to G$ be a homomorphism.*

(i) ϕ is surjective iff $\text{img}(\phi) = G$.

(ii) ϕ is injective iff $\ker(\phi) = \{e\}$.

Proof. The first is true by definition, so we prove (ii). Suppose ϕ is injective, then as we have $\phi(e_H) = e_G$, so e_H must be the only element sent to e_G (by the definition of injectivity), which implies that $\ker(\phi) = \{e_H\}$. Now suppose that $\ker(\phi) = \{e_h\}$. Then if $\phi(a) = \phi(b)$ for some $a, b \in H$, we have $\phi(ab^{-1}) = \phi(a)\phi(b)^{-1} = \phi(b)\phi(b)^{-1} = e_G$. However, this implies $ab^{-1} = e_H$, so $a = b$, and ϕ is injective. □

1.3.2 Direct Products

How can we easily find a group that will have two given groups G, H as subgroups? With the aim of getting the simplest construction possible, we can 'stick them together': by defining a group operation on the product $G \times H = \{(g, h) \ : \ g \in G, h \in H\}$ (a set of ordered pairs).

Definition 1.37 (Direct Product)**.** The *direct product* of two groups G, H is the set $G \times H$ with the operation of component-wise composition,

$$(g_1, h_1) * (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2).$$

Proposition 1.38. *The direct product of two groups G and H is a group.*

Proof Sketch. Check everything component-wise. □

This group contains subgroups isomorphic to G and H, taking $G \times \{e_H\}$ and $\{e_G\} \times H$.

A useful idea might be to try and recognize when a group is a direct product of two groups. This can be done with the following theorem.

Theorem 1.39 (Direct Product Theorem)**.** *Let $H, K \leq G$ such that*

(i) $H \cap K = \{e\}$

(ii) $\forall h \in H$ *and* $k \in K$*, we have* $hk = kh$

(iii) $\forall g \in G$*, there exists* $h \in H$*,* $k \in K$ *such that* $g = hk$

then $G \cong H \times K$*.*

Proof. Consider the function $\phi : H \times K \to G$, where $\phi(h, k) = hk$. ϕ is a homomorphism, as

$$\phi((h_1, k_1) \cdot (h_2, k_2)) = \phi(h_1 h_2, k_1 k_2) = h_1 h_2 k_1 k_2 = h_1 k_1 h_2 k_2 = \phi(h_1, k_1)\phi(h_2, k_2).$$

ϕ is surjective by (ii), and now we will show ϕ is injective. Suppose that $(h, k) \in \ker \phi$. Then $h = k^{-1}$, which implies that $h, k \in H \cap K$ by (i), and thus $(h, k) = (e_H, e_K)$. Thus $\ker \phi = \{(e_H, e_K)\}$, so ϕ is injective by the injectivty criterion. □

We now have two ways to think about the direct product.

- If we have two groups H, K, we can form their direct product $H \times K$, and view H and K as subgroups, namely $H \times \{e_k\}$ and $\{e_H\} \times K$.
- Given a group with subgroups H and K, which satisfy the conditions of the direct product theorem, then we know that we are really dealing with $H \times K$.

Indeed these are just two descriptions of the same thing. The convention is often to refer to $H \times \{e_k\}$ and $\{e_H\} \times K$ as just H and K respectively.

2 Important Groups

Now that we have seen some properties of groups, we will now consider some important examples of groups.

2.1 Cyclic Groups

Recall the notion of a generator from Definition 1.22.

Definition 2.1 (Cyclic)**.** If G is a group and there is some $a \in G$ such that $\langle a \rangle = G$, then we say G is *cyclic*.

Notably, if this is the case, for all $b \in G$, there exists $k \in \mathbb{Z}$ such that $b = a^k$.

Example 2.2 (Examples of Cyclic Groups)**.** The following groups are all cyclic.

- $(\mathbb{Z}, +)$, which is generated by $\langle 1 \rangle$ or $\langle -1 \rangle$.
- $(\mathbb{Z}/n\mathbb{Z}, +)$, generated by $\langle 1 \rangle$. Indeed, any k coprime to n will satisfy $\langle k \rangle = \mathbb{Z}/n\mathbb{Z}$.
- Let $G = \{e^{2\pi ik/n} : 0 \leq k \leq n-1\}$. Then $(G, \cdot)$ is generated by $\langle e^{2\pi ik/n} \rangle$ where k is coprime to n.

These groups all have the same 'feel' to them, and indeed they are all isomorphic to the following group.

Definition 2.3 (Cyclic Group C_n)**.** Let C_n be the group of elements $\{e = a^0, a, a^2, \ldots, a^{n-1}\}$, where $a^k * a^j = a^{k+j \pmod n}$. Then $(C_n, *)$ is the *cyclic group of order* n.

Theorem 2.4 (Cyclic Groups are Isomorphic)**.** *A cyclic group G is isomorphic to $\mathbb{Z}$ or to C_n for some $n \in \mathbb{N}$.*

Proof. As G is cyclic, we have $\langle b \rangle = G$, for some $b \in G$. Now let's suppose that there's some n such that $b^n = e$. Then define $\phi : C_n \to G$ by $\phi(a^k) = b^k$ for $0 \leq k \leq n-1$. Then for any a^j and $a^k \in C_n$, we trivially have that $\phi(a^j a^j) = \phi(a^{j+k}) = b^{j+k} = b^j b^k = \phi(a^j)\phi(a^k)$. Thus ϕ is a homomorphism. ϕ is also surjective as all elements in G can be written as b^k, $0 \leq k < n$. It is also injective, since $\phi(a^k) = e \implies b^k = e$ and so $k = 0$ (otherwise it contradicts the minimality of n). So ϕ is an isomorphism, and $G \cong C_n$.

If there is no such n, then we define $\phi : \mathbb{Z} \to G$ by $\phi(k) = b^k$. Then $\phi(k+m) = b^{k+m} = b^k b^m = \phi(k)\phi(m)$, so ϕ is a homomorphism. It is also clearly surjective. Now suppose $m \in \ker(\phi)$. Then $\phi(m) = b^m = e$, and $\phi(-m) = b^{-m} = e$, so if $m \neq 0$, we would get a contradiction to the fact that there is no $n > 0$ with $b^n = e$. So $m = 0$, $\ker(\phi) = \{0\}$ and ϕ must be an isomorphism. Thus $G \cong \mathbb{Z}$. □

Because of this theorem, we will often just write C_n or $\mathbb{Z}$ for a cyclic group, regardless of its description.

Proposition 2.5. *Cyclic groups are abelian.*

Proof Sketch. Check definitions. □

The idea of there being some k such that $g^k = e$ for some g is a frequently occurring concept.

Definition 2.6 (Order of an Element)**.** The *order of an element* $g \in G$ is the smallest $n \in \mathbb{N}$ such that $g^n = e$. This is sometimes written $\text{ord}_G(g) = n$. If there is no such n, we say g has *infinite order*.

Theorem 2.7 (Fundamental Theorem of Orders)**.** *Let G be a group, and let $g \in G$ have finite order n. Then if $g^k = 1$, we have $n \mid k$.*

Proof. By the division algorithm, we can write $k = qn + r$ uniquely with $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Then we have

$$g^k = g^{qn+r} = g^{qn} g^r = (g^n)^q g^r = g^r = e.$$

But we defined n to be the smallest positive power for which $g^n = e$, and as $r < n$, we must have $r = 0$, otherwise we contradict the minimality of n. Thus $k = qn$, that is, $n \mid k$. □

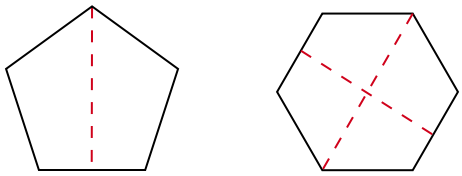
2.2 Dihedral Group

Group theory is frequently thought of as the 'algebraic study of symmetry'. With this rather vague claim in mind, we will now look at some groups related to geometry – the symmetries of a regular n-gon. Let's define what we mean by a 'symmetry' of a regular polygon.

Definition 2.8. A *symmetry* of a regular n-gon is a transformation of the n-gon, so that when the transformed n-gon is placed on the original n-gon, it exactly covers it.

Definition 2.9. The *dihedral group* D_{2n} is the group of symmetries of a regular n-gon, where the group operation is the composition of symmetries.

Clearly in this group, we will have n rotations (clockwise) of the angle $\frac{2\pi k}{n}$, $0 \leq k < n$ ($k = 0$ gives the identity or 'do nothing' symmetry). There is also n reflections.



Odd Even

When n is odd, the n reflections are in axis through the center and each of the vertices. For even n, we have $n/2$ reflections in axis through pairs of opposite vertices, and $n/2$ reflections in axes through pairs of opposite midpoints of edges.

From this you should count $2n$ elements, and we will now see that there is no other elements.

Proposition 2.10. *A regular n-gon has $2n$ symmetries.*

Proof. Let $g \in D_{2n}$. Since g is a symmetry of our n-gon, it must send vertices to vertices and edges to edges. So if v_1 is a vertex who's adjacent vertices are v_2 and v_n and we have $g(v_1) = v_i$, then we must know $g(v_1)$ and $g(v_n)$, so we must know exactly what g. Since there is n possibilities for where v_1 is sent, and 2 possibilities for where v_2 is sent, there must be $2n$ elements in total. □

Proposition 2.11. *D_{2n} is a group.*

Proof. We have closure by 'composition of symmetries are also symmetries', identity with the 'do nothing' symmetry and also inverses, as a rotation by $\frac{2\pi k}{n}$ has an inverse of a $\frac{2\pi(n-k)}{n}$ rotation, and reflections are self inverse. We also have associativity, as the composition of functions is associative. Thus D_{2n} is a group. □

It's possible to generate every element in the group with just a single rotation and a reflection. Let r be the rotation by $\frac{2\pi}{n}$, and let s be the reflection about the axis through v_1 and the center. Then r^k gives the rotation by $\frac{2\pi k}{n}$ and we can perform any reflection by first rotating the n-gon, then applying the reflection, and then rotating back.

D_{2n} is also not abelian, and indeed we have $rs = sr^{-1}$.

Aside: Group Presentations

One way to write groups is with a *presentation*. This is an expression of the form

$$\langle \text{generators} \mid \text{relations between generators} \rangle.$$

As an example, we can express the cyclic and dihedral groups using generators as follows

$$C_n = \langle a \mid a^n = e \rangle$$
$$D_{2n} = \langle r, s \mid r^n = e,\ s^2 = e,\ rs = sr^{-1} \rangle$$

You should be able to deduce all things that are true in the group from the relations in the presentation. However, you should be aware that there are some 'caveats', for example if we wrote down

$$\langle r, s \mid r^n = e,\ s^2 = e \rangle \neq D_{2n}.$$

It is, in general, quite hard to write down a presentation for a given group, or even to determine the group from a given presentation. In this course, we will not look at the 'mathematical tools' which allow us to discuss presentations in a rigorous way.

Example 2.12. The group

$$\left\langle a, b, c \mid aba^{-1}b^{-1} = b,\ bcb^{-1}c^{-1} = c,\ cac^{-1}a^{-1} = a \right\rangle = \{e\},$$

but the group

$$\left\langle a, b, c, d \mid aba^{-1}b^{-1} = b,\ b < b^{-1}c^{-1} = c,\ cdc^{-1}d^1 = d,\ dad^{-1}a^1 = a \right\rangle$$

is the *Higman group*, and it is infinite. It should be clear from this example that it is quite hard to determine a group from just its presentation.

2.3 Permutation Groups

We are now going to discuss groups made up of *permutations*.

Definition 2.13 (Permutations)**.** Given a set X, a *permutation* of X is a bijective function $\sigma : X \to X$. The set of all permutations of X is denoted $\operatorname{Sym} X$.

Theorem 2.14. *For any set X, $\operatorname{Sym} X$ is a group with respect to composition.*

Proof. We check the group axioms individually.

- *Closure.* The composition of two bijective functions from $X \to X$ is a bijective function from $X \to X$.
- *Associativity.* Composition of functions is associative.
- *Identity.* The identity function $\mathrm{id}(x) = x$ is bijective.
- *Inverses.* Every bijective function has a bijective inverse.

Thus $\operatorname{Sym} X$ is a group. □

Definition 2.15 (Symmetric Group)**.** If $|X| = n$, we write S_n for (the isomorphism class of) $\operatorname{Sym} X$. S_n is the *symmetric group* on n elements.

It should be reasonably clear that $|S_n| = n(n-1)\cdots 1 = n!$. We will also normally use $X = \{1, 2, 3, \ldots, n\}$ when we study S_n. When dealing with permutation groups, it's helpful to have some notation to express permutations. For a general $\sigma \in S_n$, we write

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}.$$

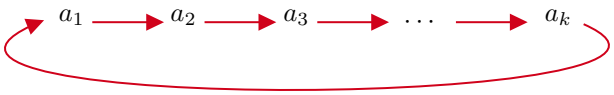
Example 2.16. If we had some $\sigma \in S_3$ such that $\sigma(1) = 2$, $\sigma(2) = 3$, and $\sigma(3) = 1$, we would write

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

A slightly better notation for when we have a permutation that 'cycles' some elements $a_1, \cdots a_k \in \{1, 2, \ldots, n\}$ and leaves the other elements unchanged, we can write

$$\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_k \end{pmatrix}$$

which denotes the permutation mapping the elements as follows



The cyclic nature of this notation also implies that the two permutations $(a_1\ a_2\ \cdots\ a_k) = (a_2\ a_3\ \cdots\ a_k\ a_1)$. To define this notation slightly more formally, we have

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_k \end{pmatrix}(x) = \begin{cases} a_{i+1} & \text{if } x = a_i,\ (i < k) \\ a_1 & \text{if } x = a_k \\ x & \text{if } x \notin \{a_1, a_2, \ldots, a_k\}. \end{cases}$$

We distinguish between permutations that can be written directly in this form in the following way.

Definition 2.17 (Cycles and Transpositions)**.** A permutation of the form $\sigma = (a_1\ a_2\ \cdots\ a_k)$ is a *k-cycle*. If $k = 2$ then we call it a *transposition*.

As cycles are permutations, we can compose them.

Example 2.18 (Composing Cycles)**.** If we consider the composition of two cycles (1 2 3 4)(3 2 4), this should be a permutation in S_4. Indeed we have

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

So we actually have that the composition of these cycles is also a cycle[5], namely (1 2 3 4)(3 2 4) = (1 2).

In the example above, the two cycles involved elements that were in both cycles. We have a specific term for when this is not the case.

Definition 2.19 (Disjoint Cycles)**.** We say that two cycles are *disjoint* if no number appears in both cycles.

Lemma 2.20. *Disjoint cycles commute.*

Proof. Let $\sigma, \tau \in S_n$ be two disjoint cycles. We want to show that $\sigma\tau = \tau\sigma$, that is, for any $x \in \{1, 2, \ldots, n\}$, we have $\sigma(\tau(x)) = \tau(\sigma(x))$. We have two cases.

If x is in neither σ or τ, then $\sigma(x) = \tau(x) = x$, and thus $\sigma(\tau(x)) = \tau(\sigma(x)) = x$.

Otherwise x is in exactly one of σ or τ. WLOG let it be in σ. Then $\sigma(x)$ is also in σ (and hence not τ), so $\tau(x) = x$ and $\tau(\sigma(x)) = \sigma(x)$. Thus $\sigma(\tau(x)) = \sigma(x)$, so they commute. □

Slightly more surprising is the following theorem

Theorem 2.21 (Writing Permutations with Cycles)**.** *Any $\sigma \in S_n$ can be written uniquely[6] as the composition of disjoint cycles.*

[5] This is, in general, not the case

[6] Up to the order of the cycles in the composition

Proof. First we show that any permutation can be written as the composition of cycles. Take $\sigma \in S_n$, and consider $1, \sigma(1), \sigma^2(1), \ldots$. Since $\{1, 2, \ldots, n\}$ is finite, there must exist $a > b$ such that $\sigma^a(1) = \sigma^b(1)$. So $\sigma^{a-b}(1) = 1$. Now let $k > 0$ be the smallest integer such that $\sigma^k(1) = 1$, which must exist by the previous argument. Then for $0 \leq l < m < k$, if $\sigma^m(1) = \sigma^l(1)$, then $\sigma^{m-l}(1) = 1$, which contradicts the minimality of k. So all of $1, \sigma(1), \sigma^2(1), \ldots, \sigma^k(1)$ are distinct. This gives us our first cycle $(1\ \sigma(1)\ \sigma^2(1)\ \sigma^{k-1}(1))$. We can repeat this process for the next number in $\{1, 2, \ldots, n\}$ that has not already appeared, until eventually every element has appeared. As σ is a bijection, no element can reappear.

We now show that this composition of cycles is unique up to the order of composition. Suppose we have two such decompositions

$$\begin{aligned}\sigma &= (a_1\ \cdots\ a_{k_1})(a_{k_{1+i}}\ \cdots\ a_{k_2})\cdots(a_{k_{m-1}}\ \cdots\ a_{k_m}) \\ &= (b_1\ \cdots\ b_{k_1})(b_{k_{1+i}}\ \cdots\ b_{k_2})\cdots(b_{k_{m-1}}\ \cdots\ b_{k_m})\end{aligned}$$

and each $j \in \{1, 2, \ldots, n\}$ appears exactly once in both. Then we have $a_1 = b_t$ for some t, and the other numbers in the cycle are uniquely determined by $\sigma(a_1), \sigma^2(a_1), \ldots$. So we have

$$(a_1\ \cdots\ a_{k_1})(\cdots) = (b_t\ \cdots)(\cdots),$$

since disjoint cycles commute and we can 'cycle' the elements in cycles. If we continue this, we will find that all other cycles match too. □

Now let's consider an element $\sigma \in S_n$, and specifically we will look at the order of σ.

Definition 2.22. The set of cycle lengths of the disjoint cycle decomposition of a permutation σ is its *cycle type*.

Example 2.23. $(1\ 2\ 3)(5\ 6)$ has a cycle type of $3, 2$ (or $2, 3$).

Theorem 2.24. *The order of $\sigma \in S_n$ is the least common multiple of the cycle lengths in its cycle type.*

Proof. First note that the order of a k-cycle is k. Suppose that $\sigma = \tau_1\tau_2\cdots\tau_r$, where τ_i is a cycle disjoint to the others. Then we have $\sigma^m = \tau_1^m\tau_2^m\cdots\tau_r^m$, since disjoint cycles commute. Let each τ_i be a k_i-cycle, then if $\sigma^m = e$, we have $\tau_1^m\tau_2^m\cdots\tau_r^m = e$, and thus $\tau_i^m = e$ for all im as they are disjoint. By the fundamental theorem of orders, we must have $k_i \mid m$, and thus $m = \operatorname{lcm}(k_1, k_2, \ldots, k_r)$ by minimality. □

This theorem gives us an easy way to find the order of the elements in S_n: write them in cycle notation.

Disjoint cycle notation is a useful way to express elements of S_n. Another useful notation is writing elements as the product of transpositions.

Theorem 2.25 (Writing Permutations with Transpositions)**.** *Let $\sigma \in S_n$. Then σ is a product of transpositions.*

Proof. It suffices to show that we can write any cycle as a product of transpositions. We observe that

$$\begin{pmatrix}a_1 & a_2 & \cdots & a_k\end{pmatrix} = \begin{pmatrix}a_1 & a_2\end{pmatrix}\begin{pmatrix}a_2 & a_3\end{pmatrix}\cdots\begin{pmatrix}a_{k-1} & a_k\end{pmatrix}.$$

□

Unlike the disjoint cycle decomposition, this isn't unique. For example, $(1\ 2\ 3\ 4) = (1\ 2)(2\ 3)(3\ 4) = (1\ 2)(2\ 3)(1\ 2)(3\ 4)(1\ 2)$. However, the pairity of the number of transpositions *is* invariant among decompositions.

Theorem 2.26 (Parity of Transpositions)**.** *Writing $\sigma \in S_n$ as a product of transpositions in different ways, the number of transpositions used is always either even or odd, that is, the pairity is invariant with respect to σ.*

Proof. Let's write $\chi(\sigma)$ for the number of cycles in σ in its disjoint cycle decomposition, including any 1-cycles. We will consider what happens to $\chi(\sigma)$ when we multiply σ by a transposition $\tau = (c\ d)$.

- If a cycle does not contain c or d, it will not be affected.
- If c and d are in the same cycle, say $(c\ a_2\ a_3\ \cdots\ a_{k-1}\ d\ a_{k+1}\ \cdots\ a_l)$, then composing with $(c\ d)$ gives $(c\ a_{k+1}\ \cdots\ a_l)(d\ a_2\ \cdots\ a_{k-1})$. So $\chi(\sigma\tau) = \chi(\sigma) + 1$.
- If c and d are in different cycles, we have

$$(c\ a_2\ \cdots\ a_k)(d\ b_2\ \cdots\ b_l)(c\ d) = (c\ b_2\ \cdots\ b_e\ d\ a_2\ \cdots\ a_k).$$

  So $\chi(\sigma\tau) = \chi(\sigma) - 1$.

Thus for any σ and any transposition τ, $\chi(\sigma) \equiv \chi(\sigma\tau) + 1 \pmod 2$. We know that $\chi(\sigma)$ is uniquely determined by σ, and if we write

$$\sigma = e\tau_1 \cdots \tau_k = e\tau_1' \cdots \tau_l',$$

we can use our result to get

$$\chi(\sigma) \equiv \chi(e) + k \equiv n + k \pmod 2$$
$$\chi(\sigma) \equiv \chi(e) + l \equiv n + l \pmod 2,$$

and thus $k \equiv l \pmod 2$. □

Because of this invariance, we can distinguish between odd and even permutations.

Definition 2.27 (Sign of a Permutation)**.** Writing $\sigma \in S_n$ as a product of transpositions $\sigma = \tau_1\tau_2\cdots\tau_k$, the *sign* of σ is defined as $\operatorname{sign}(\sigma) = (-1)^k$. If k is even, we say that σ is *even*, and if k is odd, we say that σ is *odd*.

Proposition 2.28. *For $n \geq 2$, $\operatorname{sign} : S_n \to \{\pm 1\}$ is a surjective homomorphism.*

Proof. We already know that sign is well defined, and if $\chi(\sigma) = k$ and $\chi(\sigma') = l$ for $\sigma, \sigma' \in S_n$, then $\sigma\sigma'$ can be written with $k + l$ transpositions, so $\operatorname{sign}(\sigma\sigma') = (-1)^{k+l} = (-1)^k(-1)^l = \operatorname{sign}(\sigma)\operatorname{sign}(\sigma')$, so sign is a homomorphism. It is also surjective since $\operatorname{sign}(e) = 1$ and $\operatorname{sign}(1\ 2) = -1$. □

There is an important group that comes from sign being a homomorphism.

Definition 2.29 (Alternating Group)**.** The *alternating group* A_n is the kernel of the homomorphism $\operatorname{sign} : S_n \to \{\pm 1\}$, that is, it's the group of even permutations.

2.4 Möbius Groups

In the previous section we discussed many of the properties of permutations of a finite set. In this section, we will look at some permutations of an infinite set. We will be looking at functions $\mathbb{C} \to \mathbb{C}$ - but since $\mathbb{C}$ has some intrinsic geometric properties (lines, circles, etc) unlike $\{1, 2, \ldots, n\}$, we will restrict ourselves to functions that interact well with its geometry.

More precisely, we will be looking at functions of the form $f : \mathbb{C} \to \mathbb{C}$, where

$$f(z) = \frac{az + b}{cz + d},$$

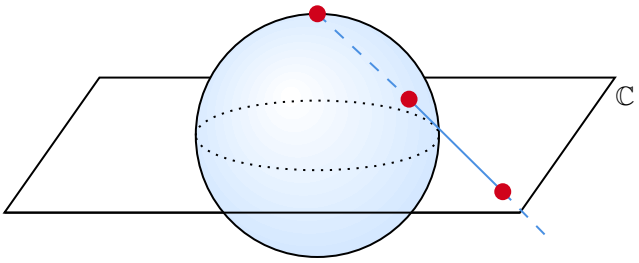
with $a, b, c, d \in \mathbb{C}$ and $ad - bc \neq 0$. We have this condition because

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

so if $ad - bc = 0$, we would have $f(z) = f(w)$ and f would be constant. We want to avoid this case as we wish to somehow form a group from these functions.

We also have another point which could cause some trouble, namely when $z = -d/c$, and the denominator of f is 0. To fix this, we are going to introduce a new point '∞' to $\mathbb{C}$ to form the *extended complex plane* , $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$. This can be visualized through 'stereographic projection'.

Consider a sphere with the complex plane cutting it at the equator.



We get a correspondence between points on the sphere and points in $\mathbb{C}$ by drawing a line from the north pole to a point on the sphere, and seeing where it intersects the plane as shown. The north pole corresponds to ∞ in $\hat{\mathbb{C}}$.

Definition 2.30 (Möbius Maps)**.** A *Möbius map* is a function $f : \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ of the form

$$f(z) = \frac{az + b}{cz + d},$$

with $a, b, c, d \in \mathbb{C}$ and $ad - bc \neq 0$, and with $f(-d/c) = \infty$ and

$$f(\infty) = \begin{cases} \frac{a}{c} & \text{if } c \neq 0 \\ \infty & \text{if } c = 0 \end{cases}.$$

Let's look at some properties of Möbius maps.

Proposition 2.31. *Möbius maps are bijections* $\hat{\mathbb{C}} \to \hat{\mathbb{C}}$.

Proof Sketch. Define $f^{-1}(z) = \frac{dz-b}{-cz+a}$, and check that $f^{-1}(f(z)) = z$. □

We now have the main result of this section.

Theorem 2.32 (Möbius Group)**.** *The set of Möbius maps forms a group* $\mathcal{M}$ *under composition.*

Proof.

- *Closure.* Let $f_1(z) = \frac{a_1 z+b_1}{c_1 z+d_1}$ and $f_2(z) = \frac{a_2 z+b_2}{c_2 z+d_2}$. Then

$$f_2(f_1(z)) = \frac{(a_1a_2 + b_2c_1)z + (a_2b_1 + b_2d_1)}{(c_2a_1 + d_2c_1)z + (c_2b_1 + d_1d_2)} = \frac{a'z + b'}{c'z + d'},$$

  and $a'd' - b'c' \neq 0$.

- *Identity.* Letting $a = 1, b = 0, c = 0$ and $d = 1$ gives $f(z) = z$.

- *Inverses.* For $f(z) = \frac{az+b}{cz+d}$, we have $f^{-1}(z) = \frac{dz-b}{-cz+a}$.

Thus the set of Möbius maps form a group. □

Remark. When working with Möbius maps in $\hat{\mathbb{C}}$, we will (somewhat improperly) use the notation '$\frac{1}{\infty} = 0$', '$\frac{1}{0} = \infty$' and '$\frac{a\infty}{c\infty} = \frac{a}{c}$' – but take care not to use this notation accidentally in other circumstances.

This group has an interesting set of generators, which provide some insight as to what Möbius maps do to the extended complex plane.

Theorem 2.33 (Generators of $\mathcal{M}$)**.** *Every Möbius map can be written as a composition of maps of the following forms:*

1. $f(z) = az$, $a \neq 0$ – *dilation/rotation;*
2. $f(z) = z + b$ – *translation;*
3. $f(z) = \frac{1}{z}$ – *inversion;*

Proof. Let $f(z) = \frac{az+b}{cz+d}$. Then if $c \neq 0$, $f(z)$ is the composition

$$z \longmapsto z + \frac{d}{c} \longmapsto \frac{1}{z + \frac{d}{c}} \longmapsto \frac{(-ad+bc)c^{-2}}{z + \frac{d}{c}}$$
$$\longmapsto \frac{a}{c} + \frac{(-ad+bc)c^{-2}}{z + \frac{d}{c}} = \frac{az+b}{cz+d}.$$

If $c = 0$, then $z \mapsto \frac{a}{d}z \mapsto \frac{a}{d}z + \frac{b}{d}$. □

3 Lagrange's Theorem

We will now begin to add to our algebraic toolkit by developing some results that will shed some light on the internal structure of a group with respect to a subgroup. We will begin by defining the notion of a *coset*, which will be used frequently throughout the rest of the course.

Definition 3.1 (Coset)**.** Let G be a group and H a subgroup of G. For any element $g \in G$, the symbol

$$gH = \{gh \ : \ h \in H\}$$

is the set of elements gh, where h ranges over elements of H. gH is a *left coset* of H in G. We can also define $Hg = \{hg \ : \ h \in H\}$ which is the *right coset* of H in G.

The cosets of H in G are subsets of G, but they aren't (typically) subgroups. You should think of a coset as being a 'translated copy' of H that has the same number of elements as H, but may or may not be a subgroup.

Example 3.2 (Cosets of $2\mathbb{Z}$)**.** Let $H = 2\mathbb{Z} \leq Z$. Then (using additive notation) the coset $0 + 2\mathbb{Z} = \{0 + k : k \in 2\mathbb{Z}\}$. The coset $1 + 2\mathbb{Z} = \{1 + k : k \in 2\mathbb{Z}\}$ is the set of all odd integers.

These are the only cosets we can obtain with this subgroup, as if we fix some $n \in \mathbb{Z}$, then $n + 2\mathbb{Z}$ will be in $2\mathbb{Z}$ if n is even, and in $1 + 2\mathbb{Z}$ if n is odd.

Example 3.3. Let $H = \{e, (1\ 2)\} \leq S_3 = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$.

Considering the cosets of H, we have

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

and so all together we have 3 distinct cosets.

From the last example, there are some notable details:

- Whenever we choose the identity element, we get the subgroup back: $eH = H$.
- Also, whenever we choose an element of H, we get H back: $hH = H$ for $h \in H$.
- The cosets of a subgroup are always the same size as that subgroup.
- Every element in G appears in at least one coset, that is, $\bigcup_{g \in G} gH = G$.

This leads up to *Lagrange's Theorem.*

Theorem 3.4 (Lagrange's Theorem)**.** *Let $H \leq G$ be a subset of a finite group G. Then*

(i) $|H| = |gH|$ *for all* $g \in G$*;*

(ii) For $g_1, g_2 \in G$*, either* $g_1H = g_2H$ *or* $g_1 \cap g_2H = \emptyset$*;*

(iii) $G = \bigcup_{g \in G} gH$

In particular, defining the index of H in G *as* $|G : H|$ *to be the number of distinct cosets of* H *in* G*, then* $|G| = |G : H| \cdot |H|$.

Proof.

(i) The function $H \to gH$, $g \to gh$ defined a bijection between H and gH.

(ii) Suppose $g_1H \cap g_2H \neq \emptyset$. Then there exists $g \in g_1H \cap g_2H$. So $g = g_1h_1 = g_2h_2$ for some $h_1, h_2 \in H$. Then $g_1 = g_2h_2h_1^{-1}$, so for any $h \in H$, we have $g_1h = g_2h_2h_1^{-1}h \in g_2H$, so $g_1H \subseteq g_2H$. Similarity, $g_2H \subseteq g_1H$, thus $g_2H = g_1H$.

(iii) Given some $g \in G$, then $g \in gH$ (since $e \in H$). Thus $G \subseteq \bigcup_{g \in G} gH$, and certainly $\bigcup gH \subseteq G$, thus $G = \bigcup_{g \in G} gH$.

Finally, $|G|$ is partitioned into the number of distinct cosets of H, thus $|G| = |G : H| \cdot |G|$. □

What this theorem is saying is 'cosets pave the group', as all the paving stones (the cosets) are the same size, they don't overlap, and they cover the whole group.

Here, we used left cosets but we could have used right cosets and would have gotten an analogous result. In general, the left and right cosets are not equal: $gH \neq Hg$. When this is true, it is an interesting property of a subgroup, that we will look at later in this chapter.

So left and right cosets are not generally, the same but what about two left cosets?

Proposition 3.5. *If H is a subgroup of a group G, and $g_1, g_2 \in G$, then*

$$g_1H = g_2H \iff g_1^{-1}g_2 \in H.$$

Proof Sketch. Follows from definitions. □

In particular, taking $g' \in gH$ gives $g'H = gH$.

Let us take an element from each of the distinct cosets of a subgroup

$$g_1,\ g_2,\ \ldots,\ g_{|G:H|},$$

then

$$G = \bigcup_{i=1}^{|G:H|} g_iH,$$

where the union is the union of disjoint sets. The elements g_i are called *coset representatives* of H in G.

We can use Lagrange's theorem to immediately derive some useful results.

Corollary 3.6 (Order of an Element Divides Order of a Group)**.** *Let G be a finite group, and let $g \in G$. Then* $\text{ord}_G(g) \mid |G|$.

Proof. Notice that the subgroup $\langle g \rangle$ is a cyclic group of order $\text{ord}_G(g)$. Then $|\langle g \rangle| \mid |G|$ by Lagrange's theorem. □

Corollary 3.7. *Let G be a finite group, and $g \in G$. Then $g^{|G|} = e$.*

Proof. The order of g divides $|G|$, and thus $|G| = \text{ord}_G(g) \cdot k$ for some k. Thus $g^{|G|} = g^{\text{ord}_G(g) \cdot k} = e^k = e$. □

Corollary 3.8. *Groups of prime order are cyclic, and are generated by any non-identity element.*

Proof. Let's suppose we have a group G with $|G| = p$, for a prime p. Take $g \in G$. Then $|\langle g \rangle| \mid |G|$ by Lagrange. So $|\langle g \rangle| = 1$ or p. If $g \neq e$, then $|\langle g \rangle| \neq 1$, so it must be p. So $\langle g \rangle = G$. □

We will now see how a theorem from number theory can be proved using Lagrange's theorem. First, recall that $(\mathbb{Z}/n\mathbb{Z})^\times$ is a group made up of the elements of $\{1, 2, \ldots n-1\}$ that have an inverse. We also have $|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$, which you should recall from 'Numbers and Sets'. We will now prove the following theorem.

Theorem 3.9 (Fermat-Euler Theorem)**.** *Let $n \geq 1$, and $a \in \mathbb{Z}$ coprime to n. Then*

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

Proof Sketch. Note that $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ which is a group, then $a^{\phi(n)} = a^{|(\mathbb{Z}/n\mathbb{Z})^\times|} = e$, by the corollary we proved earlier. □

3.1 Exploring Group Using Lagrange

Recall that we have $|G| = |G : H| \cdot |H|$, so based on the order of G, we can deduce the possible orders of a subgroup H.

Remark. Just because some $k \mid |G|$, that doesn't imply that there is some subgroup of order k.

Example 3.10 (Subgroups of D_{10})**.** Consider the group D_{10}. The order of this group is 10, so its subgroups must be of order 1, 2, 5 and 10 by Lagrange's theorem. 1 does occur with the subgroup $\{e\}$. Also 10 occurs with the subgroup D_{10}.

If we want a subgroup of order 2, we need to have the identity e and some other element of order 2. There are 5 such elements in D_{10} (reflections), which gives us 5 subgroups of order 2.

If we want a subgroup of order 5, it must be cyclic by Corollary 3.8. We have 4 elements of order 5 in D_{10}.

These are all of the subgroups of D_{10}.

We will study groups of small order in this course, and we can already classify groups of order ≤ 5 using Lagrange.

- If $|G| = 1$, then $G = \{e\}$.
- If $|G| = 2$, 3, or 5, then G is the cyclic group C_2, C_3, and C_5 respectively, by Corollary 3.8.
- If $|G| = 4$, we have two possibilities, as we will see in the following proposition.

Proposition 3.11 (Groups of Order 4)**.** *If $|G| = 4$, then $G \cong C_4$ or $G \cong C_2 \times C_2$.*

Proof. By Lagrange, the possible orders of elements of G are 1, 2 or 4. If there is an element of order 4, say g, then $\langle g \rangle = G \cong C_4$. If there is no element of order 4, then all non-identity elements have order 2. We proved in Example Sheet 1 (apologies if you have not done this question) that G is abelian. We can take two distinct elements of order 2, say b, c. Then $\langle b \rangle \cap \langle c \rangle = \{e, b\} \cap \{e, c\} = \{e\}$. Also everything commutes as G is abelian, and if we have bc, then $bc \neq b$ and $bc \neq c$. Also $bc \neq e$ as otherwise $b = c^{-1} = c$. Thus bc is the fourth element of the group. Thus by the direct product theorem, $G = \langle b \rangle \times \langle c \rangle \cong C_2 \times C_2$. □

To study groups of order 6 and greater, we are going to need more algebraic machinery.

4 Quotients of Groups

Using the direct product, we have a notion of 'multiplying' groups together. We will now think about how and when it makes sense to 'divide' one group by another.

4.1 Normal Subgroups

We will also be interested in subgroups for which the left and right cosets coincide.

Definition 4.1 (Normal Subgroups)**.** A subgroup $N \leq L$ is *normal* if $\forall g \in G$, $gN = Ng$. We write $N \trianglelefteq G$.

Proposition 4.2 (Equivalent Conditions for Normal Subgroups)**.** *The following are all equivalent conditions for a subgroup being normal.*

(i) $\forall g \in G$, $gN = Ng$.

(ii) $\forall g \in G$, *and* $\forall n \in N$, $g^{-1}ng \in N$ *(or* $gng^{-1} \in N$*).*

(iii) $\forall g \in G$, $g^{-1}Ng = N$.

Proof Sketch. Follows from definitions. □

We will use all of these conditions interchangeably.

Example 4.3. The following are all normal subgroups

(i) $n\mathbb{Z} \trianglelefteq \mathbb{Z}$, as for all $a \in Z$, we have $a + n\mathbb{Z} = \{a + nk : k \in \mathbb{Z}\} = \{nk + a : k \in \mathbb{Z}\} = n\mathbb{Z} + a$.

(ii) $A_3 \trianglelefteq S_3$, where $A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$. Clearly $eA_3 = A_3e$, and $(1\ 2\ 3)A_3 = A_3(1\ 2\ 3)$, $(1\ 3\ 2)A_3 = A_3(1\ 3\ 2)$. Also $(1\ 2)A_3 = \{(1\ 2), (2\ 3), (1\ 3)\} = A_3(1\ 2)$, and similarily for $(1\ 3)$ and $(2\ 3)$.

Proposition 4.4. *Any subgroup of an abelian group is normal.*

Proof. For any subgroup N, if G is abelian, we have $g^{-1}ng = n \in N$, so N is normal. □

Proposition 4.5. *Any subgroup of index 2 is normal.*

Proof. If $H \leq G$ is a subgroup with $|G : H| = 2$, then there are only two cosets. $H = eH = He$ is one of the cosets, and since cosets are disjoint (by Lagrange), the other coset has be $G \backslash H$ both for left and right cosets. So H is normal. □

These propositions give us two rich sources of normal subgroups, and we will now see something that gives all possible normal subgroup.

Proposition 4.6. *If* $\phi : G \to H$ *is a homomorphism, then* $\ker \phi \trianglelefteq G$.

Proof. First we note that the kernel of a homomorphism is a subgroup. Then given some $k \in \ker\phi$, $g \in G$, then

$$\phi(g^{-1}kg) = \phi(g)^{-1}\phi(k)\phi(g) = \phi(g)^{-1}e\phi(g) = e,$$

so $g^{-1}kg \in \ker\phi$, for all $g \in G$ and $k \in \ker\phi$. □

Later on, we will see that normal subgroups are *exactly* kernels of homomorphisms.

Example 4.7. The following are all normal subgroups.

1. $\mathrm{SL}_2(\mathbb{R}) \trianglelefteq \mathrm{GL}_2(\mathbb{R})$, as $\mathrm{SL}_2(\mathbb{R}) = \ker(\det)$.
2. $A_n \trianglelefteq S_n$ as A_n is the kernel of the sign homomorphism. Also $|S_n : A_n| = 2$.

With the notion of normal subgroups, we can continue to classify groups of small order.

Proposition 4.8 (Groups of Order 6)**.** *If $|G| = 6$, then $G \cong C_6$ or D_6.*

Proof. By Lagrange, possible element orders are 1 (for e), 2, 3 and 6. If there is an element of order 6, then $G \cong C_6$. If there is no such element, then by one of the questions on the example sheet (again sorry), then there is an element of order 3, say r, as otherwise our group would have an order that is a power of 2. So $|\langle r\rangle| = 3$ and by Lagrange, $|G| = 6 = |G : \langle r\rangle| \cdot |\langle r\rangle| = 3|G : \langle r\rangle|$. So $\langle r\rangle \trianglelefteq G$.

There must also be an element s of order 2, since $|G|$ is even (again see the example sheet). We can now consider what $s^{-1}rs \in \langle r\rangle$ can be.

If $s^{-1}rs = e$, then $r = e$, which is not the case. If $s^{-1}rs = r$, then $sr = rs$, which implies that sr has order 6, which we assumed there wasn't. Thus we must have $s^{-1}rs = r^2$, so $G = \langle r, s\rangle$ with $r^3 = s^2 = e$, and $sr = r^2s = r^{-1}s$, which is how we define D_6. □

4.2 Quotients

We said that the goal of this chapter was to develop the notion of 'dividing' groups, but what does that actually mean? As in, why would we attempt to make sense of such an idea? In a previous chapter, we looked at how to recognize when there was some surjective homomorphism from a group G to another group H. We are now going to take this idea further, to see how we can construct *all* groups H such that there is a surjective homormorphism from a given group G to H. Using this, we will be able to select exactly the properties of G that we wish to preserve in H, and which we want to ignore. In the previous section we developed the idea of *normal* subgroups. This will be a key aspect in developing this idea.

We are first going to define how we can 'multiply' cosets.

Definition 4.9 (Coset Multiplication)**.** Let G be a group with a subgroup H. We define the multiplication of the coset of a and of b to be the coset of ab, that is,

$$aH \cdot bH = (ab)H.$$

There are some inherent problems with this definition. For one, it's not immediately clear that such a product is well defined. If we had some cosets $aH = a'H$ and $bH = b'H$, it is not necessarily the case that their product will be equal, that is

$$aH = a'H, \quad bH = b'H \quad \text{does not imply} \quad (ab)H = (a'b')H.$$

So when is such a product well defined? It turns out that the required condition is that H must be normal.

Proposition 4.10 (Coset Multiplication for Normal Subgroups)**.** *Let H be a normal subgroup of G. Then if $aH = a'H$ and $bH = b'H$, we have $(ab)H = (a'b')H$.*

Proof. If $aH = a'H$, then $a \in a'H$, so $a = a'h_1$ for some $h_1 \in H$. Also if $bH = b'H$, we have $b = b'h_2$ for $h_2 \in H$. Thus $ab = a'h_1b'h_2$. Then as H is normal, $h_1b' = b'h_3$ for some $h_3 \in H$. Then $ab = a'b'h_3h_2$, and as $h_3h_2 \in H$, this must be in $(a'b')H$. □

We now get to the central result of this section.

Proposition 4.11. *Let $N \trianglelefteq G$. The set of cosets of N in G forms a group under coset multiplication.*

Proof. This operation is well defined by the proposition above. We now check the group axioms.

- *Closure.* If g_1N and g_2N are cosets, so is g_1g_2N.
- *Identity.* $eN = N$.
- *Associativity.* This follows from the associativity of G: $(g_1N \cdot g_2N) \cdot g_3N = (g_1g_2N) \cdot g_3N = ((g_1g_2)g_3)N = (g_1(g_2g_3))N = g_1N \cdot (g_2N \cdot g_3N)$.

□

Definition 4.12 (Quotient Group)**.** If $N \trianglelefteq G$, then G/N is the group of cosets of N in G is called the *quotient group* of G by N.

Example 4.13 (Quotient Groups)**.**

(i) The group of integers modulo n is the quotient group of $n\mathbb{Z}$ in $\mathbb{Z}$ is a group, $\mathbb{Z}/n\mathbb{Z}$.

(ii) As $A_3 \trianglelefteq S_3$, we have the quotient group S_3/A_3, which has 2 elements since $|S_3 : A_3| = 2$. Thus $S_3/A_3 \cong C_2$.

(iii) If $G = H \times K$, then both H and K are normal in G, and $G/H \cong K$ and $G/K \cong H$.

(iv) If $N = \langle r^2 \rangle \leq D_8$, then it is a normal subgroup, and $D_8/N \cong C_2 \times C_2$.

Remark. In general, quotients are *not* subgroups. In general, they may not even be isomorphic to a subgroup in a group.

Theorem 4.14. *Given $N \trianglelefteq G$, the function $\pi : G \to G/N$ where $\pi(g) = gN$ is a surjective homomorphism called the* quotient map*, and* $\ker \pi = N$.

Proof. First we prove that π is a homomorphism. We have $\pi(g)\pi(h) = gN \cdot hN = ghN = \pi(gh)$. It's clearly injective, and also $\pi(g) = gN = N \iff g \in N$. Thus $\ker \pi = N$. □

This is a key result: *normal subgroups are exactly kernels of homomorphisms.*

4.3 The Isomorphism Theorems

Using the idea of quotient groups, we can prove the following theorem.

Theorem 4.15 (First Isomorphism Theorem)**.** *Let $\phi : G \to H$ be a homomorphism. Then $G/\ker \phi \cong \operatorname{img} \phi$.*

Proof. Define $\overline{\phi} : G/\ker \phi \to \operatorname{img} \phi$ via $g \ker \phi \to \phi(g)$. This is well defined, as if $g_1 \ker \phi = g_2 \ker \phi$, then $g_1 = g_2k$ for some $k \in \ker \phi$. So $\overline{\phi}(g_1 \ker \phi) = \phi(g_1) = \phi(g_2k) = \phi(g_2)\phi(k) = \phi(g_2) = \overline{\phi}(g_2 \ker \phi)$.

We can show that $\overline{\phi}$ is a homomorphism, as

$$\overline{\phi}(g \ker \phi \cdot g' \ker \phi) = \overline{\phi}(gg' \ker \phi) = \phi(gg') = \phi(g)\phi(g') = \overline{\phi}(g \ker \phi) \cdot \overline{\phi}(g' \ker \phi).$$

We now show that $\overline{\phi}$ is also an isomorphism, by showing it is a bijection. First $\overline{\phi}$ is surjective as all elements in $\operatorname{img} \phi$ are of the form $\phi(g)$ for some $g \in G$. It is also injective, as if $\overline{\phi}(g \ker \phi) = e = \phi(g)$ in $\operatorname{img} \phi$, then $g \in \ker \phi$, so $g \ker \phi = \ker \phi$. □

Example 4.16.

(i) $\det : \mathrm{GL}_2(\mathbb{R}) \to \mathbb{R}^\times$ has $\operatorname{img} \det = R^\times$, $\ker \det = \mathrm{SL}_2(\mathbb{R})$, so $\mathrm{GL}_2(\mathbb{R})/\mathrm{SL}_2(\mathbb{R}) \cong R^\times$.

(ii) Consider the map $\phi : \mathbb{R} \to \mathbb{C}^\times$, where $\phi(r) = e^{2\pi ir}$. This is a homomorphism, and its image is the circle of radius 1 in $\mathbb{C}$ (which is S^1), and the kernel is $\mathbb{Z}$. Then by the first isomorphism theorem, we have $\mathbb{R}/\mathbb{Z} \cong S^1$.

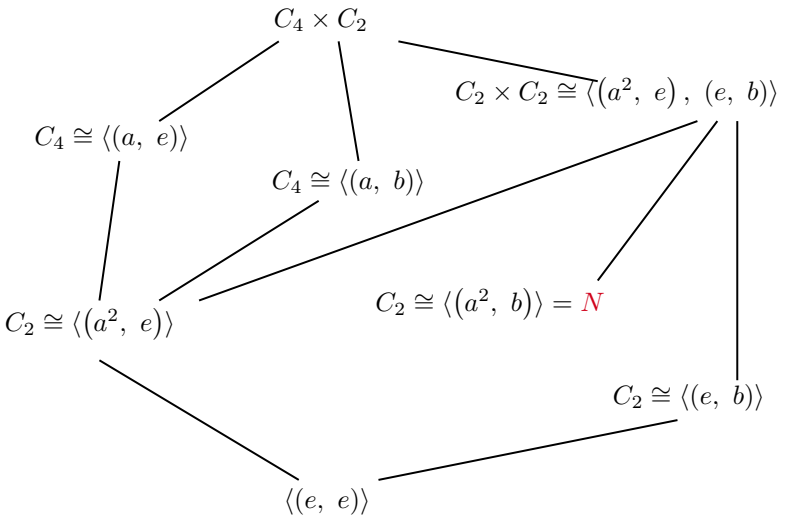
Quotient groups also have an interesting subgroup structure.

Theorem 4.17 (Correspondence Theorem)**.** *Let $N \trianglelefteq G$, then the subgroups of G/N are in bijective correspondence with subgroups of G containing N.*

Proof. If we have some $N \leq M \leq G$, with $N \trianglelefteq G$, then $N \trianglelefteq M$, and clearly $M/N \leq G/N$. Conversely, for every subgroup $H \leq G/N$, we can take the preimage of H under the quotient map $\phi G \to G/N$, that is, $\phi^{-1}(H) = \{g \in G : gN \in G\}$. We can check that this is a subgroup of G by checking the group axioms. We have closure by as $g_1, g_2 \in \pi^{-1}(H)$, then $g_1 g_2 N = g_1 N \cdot g_2 N$, so $g_1 g_2 N \in H$, and we inherit identity, inverses and associativity from the parent group. Now $\pi^{-1}(H)$ contains N, since $\forall n \in N$, $nN = N \in H$ (it's the identity coset). We can check that for $N \leq M \leq G$, $pi^{-1}(M/N) = M$, and for $H \leq G/n$, $\pi^{-1}(H)/N = H$. So this correspondence is bijective. □

This correspondence preserves lots of structure, for example indices, normality, containment.

Example 4.18. Suppose $C_4 = \{e, a, a^2, a^3\}$ and $C_2 = \{e, b\}$. Consider the group $\mathbb{C}_4 \times C_2$. Its subgroups are as follows.



We will define $N = \langle (a^2, b) \rangle$, which is normal because our group is abelian. Then if we look at $C_4 \times C_2/N$, then the correspondence theorem tells us that its subgroups are the intermediate subgroups between $C_4 \times C_2$ and N, and thus it has the following subgroup lattice.

$$C_4 \times C_2/N \quad \text{———} \quad C_2 \cong \{N,\ (e,\ b)N\} \quad \text{———} \quad \{N\}$$

This also shows us that because $C_4 \times C_2/N$ has order 4 by Lagrange, it must be isomorphic to C_4 (as otherwise it would be isomorphic to $C_2 \times C_2$, which would have a different subgroup lattice).

Now, if we had some subgroup $H \leq G$ that didn't contain $N \trianglelefteq G$, we can still make a normal subgroup of H by intersecting. This is the second isomorphism theorem.

Theorem 4.19 (Second Isomorphism Theorem)**.** *Let $H \leq G$ and $N \trianglelefteq G$. Then $H \cap N \trianglelefteq H$ and $H/(H \cap N) \cong HN/N$.*

Proof Sketch. When $N \trianglelefteq G$ and $H \leq G$, then $HN = \{hn : h \in H, n \in N\}$ is a subgroup of H, and $HN = \langle H, N \rangle$ (the smallest subgroups of G containing H and N). Then consider the function $\phi : H \to HN/N$, with $\phi(h) = hN$. We can check this is a well defined, surjective homomorphism, and its kernel is $N \cap H$, and we can apply the first isomorphism to get $H/(N \cap H) \cong HN/N \leq G/N$. □

We mentioned previously that normality is preserved. We can even say something about quotients.

Theorem 4.20 (Third Isomorphism Theorem)**.** *Let $N \leq M \leq G$ such that $N \trianglelefteq G$ and $M \trianglelefteq G$. Then $M/N \trianglelefteq G/N$ and $(G/N)/(M/N) \cong G/M$.*

Proof. We define $\phi : G/N \to G/M$ by $\phi(gN) = gM$. ϕ is well-defined since $N \leq M$, and it's a surjective homomorphism. Its kernel is M/N, and thus by the first isomorphism theorem, $(G/N)/(M/N) \cong G/M$. □

Let's have a look at some examples of the isomorphism theorems.

Example 4.21. Consider the group $\mathbb{Z}$, and define $H = 3\mathbb{Z}$ and $N = 5\mathbb{Z}$. Note that Then by the second isomorphism theorem as , $H/(H \cap N) \cong HN/N \cong \mathbb{Z}/5\mathbb{Z}$, as $\langle H, N \rangle = \mathbb{Z}$ by Bezout's lemma.

4.4 Simple Groups

We will finish this chapter with the introduction of *simple groups*.

Definition 4.22 (Simple Groups)**.** A group G is *simple* if its only normal subgroups are $\{e\}$ and G.

Example 4.23 (Examples of Simple Groups)**.** The following are simple groups:

- C_p for a prime p.
- A_5 (we will prove this later on).

Finite simple groups are important as they can be thought of as the 'building blocks' of all finite groups. If we have some finite group with a normal subgroup, we can take the quotient by that normal subgroup, and you would obtain two objects (the quotient and the normal subgroup) that are smaller than the original group. These objects can help you understand the groups more, but simple groups can't be decomposed further.

Recently, the classification of all finite simple groups was completed, and you can find a large book with all finite simple groups in it!

5 Group Actions

The next aspect of group theory we shall look at is *group actions*, where we study how groups interact with other objects. This isn't such a foreign concept – if you consider the examples of groups that we have looked at previously, we have in many cases been able to identify elements by their effect on some set. For example, we determined the elements of S_n by how it permuted elements of the set $\{1, 2, \ldots, n\}$, and we defined D_{2n} based on the symmetries of an n-gon.

Of course, using the group axioms we can somewhat forget that these were ever groups that acted on certain objects, but by introducing these objects that groups can act upon adds a certain richness to the subject.

Definition 5.1 (Group Action)**.** Let G be a group, and let X be a set. An *action* of G on X is a function $\alpha : G \times X \to X$ written $\alpha(g, x) = \alpha_g(x)$, satisfying

- $\alpha_g(x) \in X$ for all $g \in G$ and $x \in X$.
- $\alpha_e(x) = x$ for all $x \in X$.
- $\alpha_g \circ \alpha_h(x) = \alpha_{gh}(x)$ for any $g, h \in G$ and $x \in X$.

Example 5.2. The following are all examples of groups that act on various sets.

(i) The group S_n acts on X by permutation.

(ii) The group D_{2n} acts on the vertices of a regular n-gon, and if we label these vertices 1, 2, ..., n, we get an action on the set $\{1, 2, \ldots, n\}$.

(iii) The symmetries of a cube act on a set of vertices, a set of edges, a set of faces, and a set of pairs of opposite faces.

Remark. These examples show us that more than one group can act on a given set, for example in (i) and (ii). A group can also act on many sets.

Lemma 5.3. *For all $g \in G$ and an action $\alpha_g : X \to X$, the map $x \mapsto \alpha_g(x)$ is a bijection.*

Proof. We have $\alpha_g(\alpha_{g^{-1}}(x)) = \alpha_{gg^{-1}}(x) = \alpha_e(x) = x$ for all $x \in X$, and similarly, $\alpha_{g^{-1}}(\alpha_g(x)) = x$ for all $x \in X$. Hence $\alpha_g \circ \alpha_{g^{-1}}$ and $\alpha_{g^{-1}} \circ \alpha_g$ are the identity functions, so α_g is a bijection. □

We can also define actions by linking G to $\mathrm{Sym}(X)$ in the following way.

Proposition 5.4. *Let G be a group, and X be a set. Then $\alpha : G \times X \to X$ is an action if and only if the function $\rho : G \to \mathrm{Sym}(X)$ where $\rho(g) = \alpha(g)$ is a homomorphism.*

Proof. If α is an action, then by Lemma 5.3, α_g is a bijection from $X \to X$, so $\alpha_g \in \mathrm{Sym}(X)$. Now $\rho(gh) = \alpha_{gh}$ and for all $x \in X$, $\alpha_{gh}(x) = \alpha_g \circ \alpha_h(x)$, so $\rho(gh) = \alpha_{gh} = \alpha_g \circ \alpha_h = \rho(g)\rho(h)$, so ρ is a homomorphism.

Otherwise, if we have some homomorphism $\rho : G \to \mathrm{Sym}(X)$, we can define $\alpha : G \times X \to X$ by $\alpha(g, x) = \alpha_g(x) = \rho(g)(x)$. Then α is an action. This is true because $\rho(g) \in \mathrm{Sym}(X)$, so $\rho(g)(x) = \alpha_g(x) \in X$, and $\rho(e)$ is the identity in $\mathrm{Sym}(X)$ which implies $\rho(e)(x) = x$, and finally, $\rho(gh) = \rho(g)\rho(h)$ implies that $\alpha_{gh}(x) = \alpha_g \circ \alpha_g(x)$ for all $x \in X$. □

We can make the notation slightly easier. When we write $\alpha_g : X \to X$, we can really think of g as being a function on x, and we can write $g(x)$ instead.

With the above proposition in mind, we can define the *kernel* of an action.

Definition 5.5. The *kernel of an action* $\alpha : G \times X \to X$ is the kernel of the homomorphism $\rho : G \to \mathrm{Sym}(x)$ (as above).

These are all of the elements of G that act as the identity of $\mathrm{Sym}(X)$, that is, they do nothing to every $x \in X$. Note that by the first isomorphism theorem, this also implies that $G/\ker\rho \cong \mathrm{img}\,\rho \leq \mathrm{Sym}(X)$, and thus if $\ker\rho = \{e\}$, then $G \leq \mathrm{Sym}(X)$.

Example 5.6.

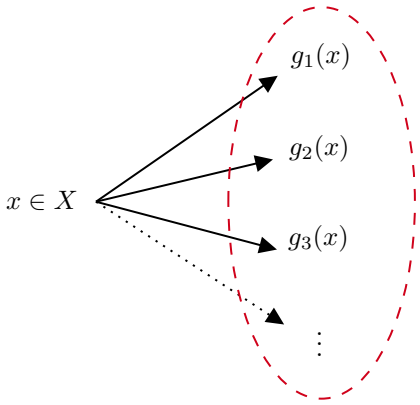
(i) D_{2n} acting on $\{1, \ldots, n\}$ (the labelled vertices on an n-gon) has $\ker\rho = \{e\}$, as every non-trivial element of D_{2n} moves at least one vertex. Thus $D_{2n} \leq S_n$.

(ii) Let G be the symmetries of a cube, and consider X to be the set of unordered pairs of opposite faces. Then $|X| = 3$. So we get a homomorphism $\rho : G \to S_3$. Clearly there are symmetries of the cube that realize all of the permutation of X, so ρ is surjective. So, $G/\ker\phi \cong S_3$.

Definition 5.7 (Faithful Actions)**.** An action of G on X is called *faithful* if $\ker\rho = \{e\}$.

5.1 Orbits and Stabilisers

Consider the following two questions: for a group G acting on a set X, what elements of X we can 'get to' from a certain $x \in X$ using the action of G? Also, which group elements leave a given $x \in X$ unchanged?



Definition 5.8 (Orbit)**.** Let G act on X, and let $x \in X$. The *orbit* of x is

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

Definition 5.9 (Stabilizer)**.** The *stabilizer* of x is

$$\mathrm{Stab}(x) = \{g \in G : g(x) = x\} \subseteq G.$$

We say that an action of *transitive* if $\mathrm{Orb}(x) = X$, that is, if we can get to any element from any other element.

Example 5.10. For $G = S_3 = \{e, (1\ 2), (2\ 3), (1\ 3), (1\ 2\ 3), (1\ 3\ 2)\} \leq S_4$. G acts on $\{1, 2, 3, 4\}$, and we have $\mathrm{Orb}(1) = \mathrm{Orb}(2) = \mathrm{Orb}(3) = \{1, 2, 3\}$, but $\mathrm{Orb}(4) = \{4\}$. Also $\mathrm{Stab}(1) = \{e, (2\ 3)\}$, $\mathrm{Stab}(2) = \{e, (1\ 3)\}$, $\mathrm{Stab}(3) = \{e, (1\ 2)\}$ and $\mathrm{Stab}(4) = G$.

Lemma 5.11. *For any $x \in X$, $\mathrm{Stab}(x)$ is a subgroup of G.*

Proof. We check the group axioms.

- *Closure.* If $g, h \in \mathrm{Stab}(x)$, then $(gh)(x) = g(h(x)) = g(x) = x$, so $gh \in \mathrm{Stab}(x)$.
- *Identity.* $e(x) = x$, so $e \in \mathrm{Stab}(x)$.
- *Inverses.* If $g \in \mathrm{Stab}(x)$ then $g(x) = x$ so $x = g^{-1}(x)$, and $g^{-1} \in \mathrm{Stab}(x)$.

□

Now recall that a partition of a set X is a set of subsets of X such that each $x \in X$ belongs to exactly one subset in the partition.

Lemma 5.12. *Let G act on X. Then the orbits partition X.*

Proof. Firstly, for any $x \in X$, $x \in \mathrm{Orb}(x)$. Secondly, if $z \in \mathrm{Orb}(x) \cap \mathrm{Orb}(y)$, then there exists $g_1 \in G$ such that $g_1(x) = z$, and there exists $g_2 \in G$ such that $g_2(y) = z$, that is, $y = g_2^{-1}(z)$. So $y = g_2^{-1}g_1(x)$, and thus for any $g \in G$, $g(y) = (gg_2^{-1}g_1)(x) \in \mathrm{Orb}(x)$. So $\mathrm{Orb}(y) \subseteq \mathrm{Orb}(x)$. Similarly, $\mathrm{Orb}(x) \subseteq \mathrm{Orb}(y)$. Thus orbits are either disjoint or equal. □

Recall the proof that any permutation could be written as the product of disjoint cycles. What we were really doing was finding the orbits in $\{1, 2, \ldots, n\}$ under $\langle\sigma\rangle$, which are disjoint.

Remark. Note that unlike cosets, the sizes of orbits can be different.

When we have an action, we can say even more about the structure of our group.

Theorem 5.13 (Orbit-Stabiliser Theorem)**.** *Let a finite group G act on X. Then for any $x \in X$,*

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

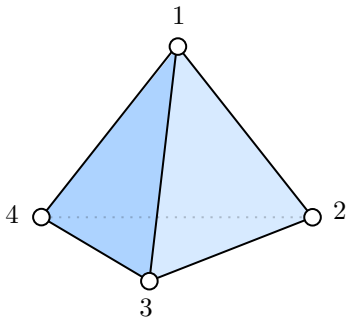
Proof. Note that $g(x) = h(x)$ occurs if and only if $h^{-1}g(x) = x$, that is, when $h^{-1}g \in \operatorname{Stab}(x)$. Then this is true iff the cosets $g\operatorname{Stab}(x) = h\operatorname{Stab}(x)$. Rephrasing, distinct points in the orbit of x are in bijection with distinct cosets of $\operatorname{Stab}(x)$. So $|\operatorname{Orb}(x)| = |G : \operatorname{Stab}(x)| = |G|/|\operatorname{Stab}(x)|$ by Lagrange, and the result follows. □

In particular, notice that all elements in a given coset $g\operatorname{Stab}(x)$ do the same thing to x as g, as an element of this coset $g\operatorname{Stab}(x)$ has the form gh, $h \in \operatorname{Stab}(x)$, so $gh(x) = g(h(x)) = g(x)$.

We can use the orbit-stabiliser theorem to investigate groups further. For example, we already know $|D_{2n}| = 2n$, but we can also show this by the orbit-stabiliser theorem. D_{2n} acts transitively on $\{1, \ldots, n\}$, so $|\operatorname{Orb}(1)| = n$, and $\operatorname{Stab}(1) = \{e, s\}$, as the first vertex is fixed by one reflection and the identity. Thus $|D_{2n}| = |\operatorname{Orb}(1)| \cdot |\operatorname{Stab}(1)| = n \cdot 2 = 2n$.

5.1.1 Symmetries of the Tetrahedron

To see the power of using Orbits and Stabilisers, we are going to consider two more involved examples, beginning with the symmetries of a tetrahedron.



The tetrahedron has

- 4 faces (all regular triangles),
- 4 vertices, labelled $\{1, 2, 3, 4\}$,
- 6 edges.

So let G be the group of symmetries of the tetrahedron. Clearly G acts transitively on the vertices, and there's no non-identity symmetry that fixes all of the vertices. So we have an injective homomorphism $\rho : G \to S_4$.

We can consider the orbit and stabiliser for a vertex of the tetrahedron, say 1. For orbits, there is a symmetry that allows us to get from 1 to any other vertex, thus $\operatorname{Orb}(1) = \{1, 2, 3, 4\}$. Then, the symmetries that leave the vertex 1 fixed are going to be the symmetries of the bottom face (the 2, 3, 4 triangle). Thus $\operatorname{Stab}(1) \cong D_6$, the symmetries of a triangle.

With this information, then orbit stabiliser tells us that

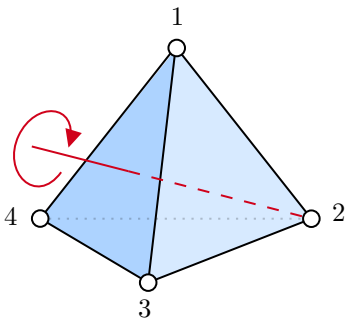
$$|G| = |\operatorname{Orb}(1)| \cdot |\operatorname{Stab}(1)| = 4 \cdot 6 = 24,$$

and as $|S_4| = 4! = 24$, and as $G \leq S_4$, we must have $G = S_4$. So just by considering the symmetries relating to one vertex, we were able to deduce the order of the group G, and also find a group that it's isomorphic to!

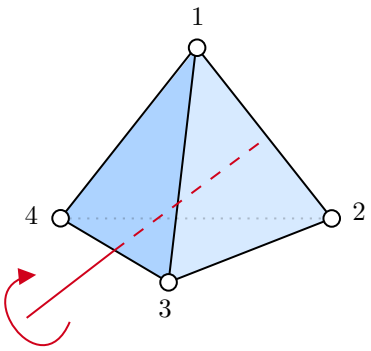
We can also consider a group G^+ of the rotations in G. Then in G^+, $\mathrm{Orb}(1) = \{1, 2, 3, 4\}$ as we can only use rotations, and then $\mathrm{Stab}(1)$ is going to be the rotations of the bottom triangle, thus $\mathrm{Stab}(1) \cong C_3$. Then again by the orbit stabiliser theorem,

$$|G^+| = |\mathrm{Orb}(1)| \cdot |\mathrm{Stab}(1)| = 4 \cdot 3 = 12,$$

and as $G^+ \leq G \cong S_4$, we must have $G^+ = A_4$! Indeed, we can check that G^+ is made up of all of the even permutations of the four vertices, that is, all of the 3-cycles and the elements of the form $(1\ 2)(3\ 4)$.



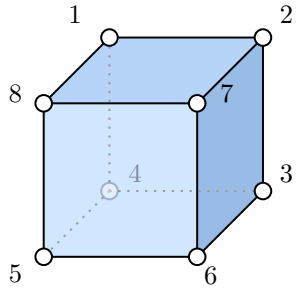
$(1\ 3\ 4)$



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

5.1.2 Symmetries of the Cube

We are now going to look at the symmetries of a cube in a similar way.

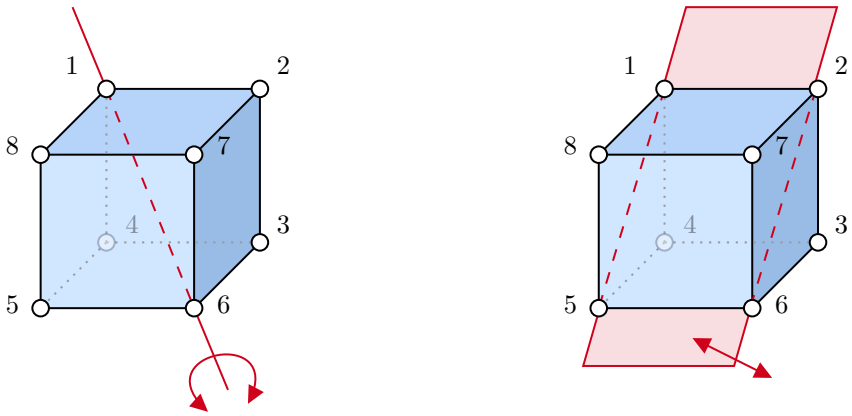


We have

- 6 faces (all square),
- 8 vertices, labelled $\{1, 2, 3, 4, 5, 6, 7, 8\}$,
- 12 edges.

Let G be the group of symmetries of the cube. In this example, we will find that it is interesting to consider either acting on the vertices or on the faces.

When G acts on the vertices of the cube, we can find the size of the orbit and stabiliser of a vertex geometrically. G is transitive, hence $|\mathrm{Orb}(1)| = 8$. Then the elements that stabilize the vertex 1 are going to be the identity, the rotations about an axis through 1, and the reflections about planes through 1 and an outgoing edge. These are shown below.



So $|\operatorname{Stab}(1)| = 6$. Then by the orbit-stabiliser theorem,

$$|G| = |\operatorname{Orb}(1)| \cdot |\operatorname{Stab}(1)| = 8 \cdot 6 = 48.$$

We will determine this group completely later.

Now let's look at the group of rotations, G^+, acting on the 8 vertices. We have $|\operatorname{Orb}(1)| = 8$ as before, but the stabilisers of 1 are only going to be the rotations, so $|\operatorname{Stab}(1)| = 3$. Thus

$$|G^+| = |\operatorname{Orb}(1)| \cdot |\operatorname{Stab}(1)| = 8 \cdot 3 = 24.$$

Now if we let G^+ act on the four diagonals of the cube, giving $\rho : G^+ \to S_4$. We will have all 4-cycles in $\operatorname{img} \rho$, and also all transpositions[7]. So we have $(1\ 2)$ and $(1\ 2\ 3\ 4)$, but we found previously (in Example Sheet 2) that this generates S_4, so ρ is surjective. Then as $|G^+| = 24 = |S_4|$, so we must have $G^+ \cong S_4$.

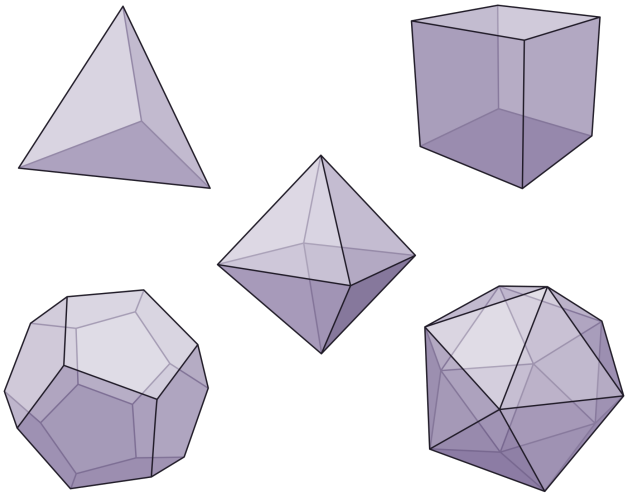
5.1.3 Platonic Solids

The last two shapes were two of the five *platonic solids*.

Definition 5.14 (Platonic Solid)**.** A *platonic solid* is a solid shape in $\mathbb{R}^3$ that has polygonal faces, straight edges and vertices such that the group of the shape's symmetries acts transitively on triples of the form $(\text{vertex}, \text{incident edge}, \text{incident face})$.

So these solids are particularly symmetric. The other platonic solids are the *octohedron*, *dodecahedron* and *icosahedron*.

[7] If you don't see why, I encourage you to draw a cube with a diagonal elongated, and see what the rotations do to it.



There are also links between the symmetries of these shapes - the cube and octahedron are *dual*, that is, they can be inscribed in each other with vertices in the middle of faces. The icosahedron and dodecahedron are also duel. In fact, this duel property implies that they have the same symmetry groups. So there is only 3 distinct symmetry groups of platonic solids.

5.2 Cauchy's Theorem

We are now going to see how group actions can be used to prove a beautiful theorem. Back in Example Sheet 1, we had the following problem.

Problem. Let G be a group of even order. Show that G contains an element of order two.

It is *not true* in general that if $k \mid |G|$, then there is an element of order k – but it is true for primes. This result is *Cauchy's theorem*.

Theorem 5.15 (Cauchy's Theorem)**.** *Let G be a finite group, and let p be a prime such that $p \mid |G|$. Then G has an element of order p.*

Proof. Consider the group $G^p = \underbrace{G \times G \times \cdots \times G}_{p \text{ times}}$, that is, the group formed of p-tuples of elements of G, with component wise composition. Consider the subset $X \subseteq G$,

$$X = \{(g_1, \ldots, g_p) \in G^p : g_1 g_2 \cdots g_p = e\},$$

Informally, 'p-tuples multiplying to e'. Note that $g \in G$ has order p if and only if $(g, \ldots, g) \in X$ where g is not the identity.

Now take a cyclic group $C_p = \langle a \rangle$, and let C_p act on X by 'cycling', where $a(g_1, g_2, \ldots, g_p) = (g_2, \ldots, g_p, g_1)$. It is easily checked that this is an action. Since orbits partition X, the sum of the sizes of distinct orbits must be $|X|$, but $|X| = |G|^{p-1}$, since we can choose anything to put in the $p-1$ entries, and set the last entry to the inverse of their product. So since $p \mid |G|$, $p \mid |X|$. We have by the orbit-stabiliser theorem that

$$|\operatorname{Orb}(g_1, \ldots, g_p)| \cdot |\operatorname{Stab}(g_1, \ldots, g_p)| = |C_p| = p.$$

So any orbit has size 1 or p, and they sum to $|X|$, so

$$|X| = \sum_{\text{orbits of size } 1} 1 + \sum_{\text{orbits of size } p} p.$$

Clearly $|\operatorname{Orb}(e, e, \ldots, e)| = 1$, and thus as $p \mid |X|$, there must be some other orbits of size 1. But orbits of size 1 must be of the form $(g, g, \ldots, g)$, so there exists some $g \neq e \in G$ such that $g^p = e$. □

5.3 Important Actions

Once you have recovered from how nice the previous theorem was, we will look at some important examples of group actions. We will begin with left multiplication actions.

Lemma 5.16 (Left Multiplication is an Action)**.** *Let G be a group. Then G acts on itself by left multiplication. This action is faithful and transitive.*

Proof. For any $g \in G$ and $x \in G$, then $gx \in G$. Also, $ex = x$ for any $x \in G$, and lastly, $(gh)x = g(h(x))$ is true by the associativity of G, so it is an action. It is faithful as if $gx = x$ then $g = e$ by the uniqueness of the identity. It's also transitive as given $x, y \in G$, set $g = yx^{-1}$, then $g(x) = gx = yx^1x = y$. □

Definition 5.17 (Left Regular Action)**.** The left multiplication action of a group on itself is called the *left regular action.*

With this group action, we can finally prove a result that we have been vaguely alluding to (and which should make intuitive sense).

Theorem 5.18 (Cayley's Theorem)**.** *Every group is isomorphic to a subgroup of a symmetric group.*

Proof. Let G act on itself by the left regular action. This gives a homomorphism $\rho : G \to \operatorname{Sym}(G)$, with $\ker \phi = \{e\}$ since the action is faithful. Hence by the first isomorphism theorem, $G/\ker \phi \cong \operatorname{img} \phi \leq \operatorname{Sym}(G)$. □

Proposition 5.19 (Left-Coset Action)**.** *Let $H \leq G$. Then G acts on the set of left-cosets by left multiplication, and the action is transitive. This is the* left-coset action.

Proof. We have $g(g_1H) = gg_1H$, so $g(g_1H)$ is a left coset. Also $e(g_1H) = eg_1H = g_1H$. Finally, $(gg')(g_1H) = gg'g_1H = g(g'(g_1H))$, so this is an action. Also given g_1H and g_2H, we have $(g_1g_2^{-1})(g_2H) = g_1g_2^{-1}g_2H = g_1H$, so this action is transitive. □

Remark. For $H = \{e\}$, then this is the left-regular action, as the cosets are just the elements of G.

This action gives us a way to induce actions of G onto its quotient groups G/N.

5.3.1 Conjugation

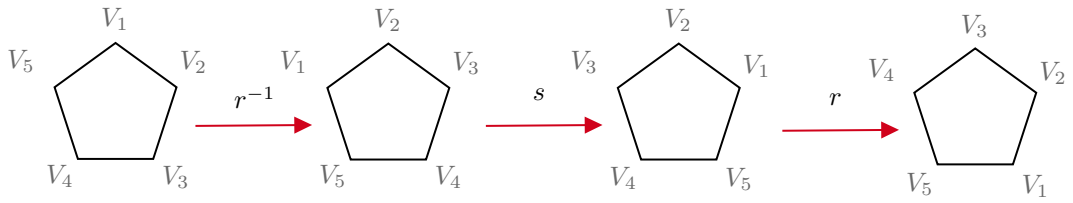
The next idea we will discuss is *conjugation.*

Definition 5.20 (Conugation)**.** Given $g, h \in G$, the element $hgh^{-1} \in G$ is the conjugate of g by h.

Conjugate elements should be thought of as doing the 'same thing' but from 'different points of view'. The exact meaning of this will be more clear as we look at some examples later on.

Example 5.21. Consider the group D_{10}, and consider the conjugate s and rsr^{-1}, where s is reflection through the vertex v_1, and r is a clockwise rotation sending v_1 to v_2 and so on.

What rsr^{-1} does is rotating so that the reflection can be done through a different axis.



So in this example, we are still performing an action, just from a different point of view.

Example 5.22. In the group $\mathrm{GL}_n \mathbb{R}$, the conjugate of a matrix represents the same transformation but written with respect to a different basis.

So it's natural to expect that conjugate elements have similar properties. Let's prove some facts about conjugation.

Proposition 5.23 (Conjugation is an Action)**.** *A group G acts on itself by conjugation.*

Proof. We have $g(x) = gxg^{-1} \in G$ for all $g, x \in G$. Also, $e(x) = exe^{-1} = x$ for all x, and finally, $g(h(x)) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = (gh)(x)$, for all $g, h, x \in G$. So this is an action. □

This action's kernel, orbits and stabilisers even have their own names.

Definition 5.24 (Center)**.** The kernel of the conjugation action of G on itself is the *center* $Z(G)$ of G:

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

Equivalently, the center of a group is the set of all elements that commute with every element in the group.

Definition 5.25 (Conjugacy Class)**.** An orbit of the conjugation action is a *conjugacy class*:

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

Definition 5.26 (centralizers)**.** The stabilisers of the conjugation action are the *centralizers*:

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

Equivalently, $C(h)$ is the set of elements that commute with h.

There is a connection between the center and the centralizers, namely

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

Definition 5.27 (Subgroup Conjugation)**.** If $H \leq G$, $g \in G$, then the *conjugate of H by g* is

$$gHg^{-1} = \{ghg^{-1} : h \in H\}.$$

Proposition 5.28. *Let $H \leq G$ and $g \in G$. Then gHg^{-1} is also a subgroup of G.*

Proof. Clearly $e \in gHg^{-1}$, so it is nonempty. Thus we can apply the subgroup criterion. Let gxg^{-1} and $gyg^{-1} \in gHg^{-1}$. Then

$$(gxg^{-1})(gyg^{-1})^{-1} = (gxg^{-1}gy^{-1}g^{-1}) = g(xy^{-1})g^{-1},$$

and as $H \leq G$, we have $xy^{-1} \in H$ so $g(xy^{-1})g^{-1} \in gHg^{-1}$, so it is a subgroup. □

In fact, $gHg^{-1} \cong H$, which should match our intuition about how conjugate elements act.

Proposition 5.29 (Subgroup Conjugation is an Action)**.** *A group G acts by conjugation on the set of its subgroups. The singleton orbits are the normal subgroups.*

Proof. Let G act on the set of subsets by conjugation, that is, for $H \leq G$, we define $g(H) = gHg^{-1}$. We will check that this is a group action.

We have closure by the argument above. We have identity, as $eHe^{-1} = H$ for any subgroup H. Also for $g, k \in G$, we have $g \circ k(H) = g(kHk^{-1}) = gkHk^{-1}g^{-1} = (gk)H(gk)^{-1} = (gk)(H)$, so this is indeed an action.

The singleton orbits are the normal subgroups, as a subgroup N is normal if $gNg^{-1} = N$ for any $g \in G$ (which corresponds to every element in G stabilising N). □

Another way to look at normal subgroup is using conjugation. We already established that if and only if N is normal in G, we have $gNg^{-1} = N$, for any $g \in G$.

Proposition 5.30. *Normal subgroups are unions of conjugacy classes.*

Proof. Let $N \trianglelefteq G$. Then if $h \in N$, then $ghg^{-1} \in N$ for any $g \in G$. Hence $\mathrm{ccl}(h) \subseteq N$. So N is a union of conjugacy classes of its elements, that is, $N = \bigcup_{h \in N} \mathrm{ccl}(h)$. Conversely, suppose that we have a subgroup H that is the union of conjugacy classes. Then taking any $g \in G$ and $h \in H$, ,then $ghg^{-1} \in H$, so $H \trianglelefteq G$. □

Example 5.31. Consider the group $A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\} \trianglelefteq S_3$. We can write this as $A_3 = \{e\} \cup \{(1\ 2\ 3), (1\ 3\ 2)\}$, which are both conjugacy classes.

Conjugation in S_n and A_n is rather interesting. Let's begin with a lemma.

Lemma 5.32 (Conjugation Permutes Elements in a Cycle)**.** *Given k-cycle $(a_1\ \cdots\ a_k)$ and $\sigma \in S_n$, we have*

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

which is also a k-cycle.

Proof. Note that if we consider the action of $\sigma(a_1\ \cdots\ a_k)\sigma^{-1}$ on a_i, we have

$$\sigma(a_i) \mapsto a_i \mapsto a_{i+1} \mapsto \sigma(a_{i+1}).$$

So $\sigma(a_1\ \cdots\ a_k)\sigma^{-1}$ does the same thing as $(\sigma(a_1)\ \sigma(a_2)\ \cdots\ \sigma(a_k))$ on the set $\{\sigma(a_1), \ldots, \sigma(a_k)\}$. Then for any $a \notin \{\sigma(a_1), \ldots, \sigma(a_k)\}$, then $\sigma(a_1\ \cdots\ a_k)\sigma^{-1}$ and $(\sigma(a_1)\ \sigma(a_2)\ \cdots\ \sigma(a_k))$ both leave a unchanged. □

Proposition 5.33. *Two elements of S_n are conjugate in S_n if and only if they have the same cycle type.*

Proof. Two elements that are conjugate will certaintly gave the same cycle type, as given $\sigma \in S_n$, we can write σ as the product of disjoint cycles $\sigma = \sigma_1\sigma_2 \cdots \sigma_m$. Then if $\rho \in S_n$, $\rho\sigma\rho^{-1} = (\rho\sigma_1\rho^{-1})(\rho\sigma_2\rho^{-1}) \cdots (\rho\sigma_m\rho^{-1})$, and by our previous lemma, $\rho\sigma_i\rho^{-1}$ us a cycle of the same length as σ_i, and $\rho\sigma_i\rho^{-1}$ are all disjoint (as ρ is a bijection). Conversely, if we have σ and τ that are the same cycle type, then we can write

$$\sigma = (a_1\ a_2\ \cdots\ a_{k_1})(a_{k_1+1}\ a_{k_1+2}\ \cdots\ a_{k_2}) \cdots$$
$$\tau = (b_1\ b_2\ \cdots\ b_{k_1})(b_{k_1+1}\ b_{k_1+2}\ \cdots\ b_{k_2}) \cdots$$

in disjoint cycle notation, including any singletons (those fixed by σ and τ) so that all of $\{1, \ldots, n\}$ appears in both σ and τ. Then setting ρ to be $\rho(a_i) = b_i$, we will have $\rho\sigma\rho^{-1} = \tau$. □

Let's have a look at an example: the conjugacy classes of S_4.

Example 5.34 (Normal subgroups of S_4)**.** Consider the following table of conjugacy classes of S_4.

Cycle Type	Example Element	Size of ccl	Size of C_{S_4}	Sign
$1, 1, 1, 1$	e	1	24	$+1$
$2, 1, 1$	$(1\ 2)$	$4 \cdot 3/2 = 6$	4	-1
$2, 2$	$(1\ 2)(3\ 4)$	$4 \cdot 3/(2 \cdot 2) = 3$	8	$+1$
$3, 1$	$(1\ 2\ 3)$	$4 \cdot 3 \cdot 2/3 = 8$	3	$+1$
4	$(1\ 2\ 3\ 4)$	$4 \cdot 3 \cdot 2/4 = 6$	4	-1

From this table, we can work out the normal subgroups of S_4. Each normal subgroup must contain e, and must be the union of conjugacy classes, and we must have the order of the subgroup dividing the order of the group. We can check what combinations of conjugacy classes satisfies these.

We can consider these possibilities by considering the divisors of 24, the order of the group: $1, 2, 3, 4, 6, 8, 12, 24$. From these, we have

- Order 1: $\{e\}$
- Order 4: $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$, which is $C_2 \times C_2$, also known as V_4, the Klein four group.
- Order 12: A_4.
- Order 24: S_4.

Now because we have all of the normal subgroups, we can also get all of the possible quotients of S_4, as

- $S_4/\{e\} \cong S_4$.
- $S_4/V_4 \cong S_3$.
- $S_4/A_4 \cong C_2$.
- $S_4/S_4 \cong \{e\}$.

Now let's look at conjugation in the alternating group. Note that $\operatorname{ccl}_{S_n}(\sigma) = \{\tau\sigma\tau^{-1} : \tau \in S_n\}$ and $\operatorname{ccl}_{A_n}(\sigma) = \{\tau\sigma\tau^{-1} : \tau \in A_n\}$, so $\operatorname{ccl}_{A_n}(\sigma) \subseteq \operatorname{ccl}_{S_n}(\sigma)$. But elements that are conjugate in S_n may not be conjugate in A_n. For eample, $(2\ 3)(1\ 2\ 3)(2\ 3) = (1\ 3\ 2) \in S_3$, but $(2\ 3) \notin A_3$, and there are no elements $\tau \in A_3$ such that $\tau(1\ 2\ 3)\tau^{-1} = (1\ 3\ 2)$.

Some conjugacy classes of S_n will split into smaller conjugacy classes in A_n. By orbit-stabiliser, $|S_n| = |\operatorname{ccl}_{S_n}(\sigma)| \cdot |C_{S_n}(\sigma)|$, and $|A_n| = |\operatorname{ccl}_{A_n}(\sigma)| \cdot |C_{A_n}(\sigma)|$. But $|S_n| = 2 \cdot |A_n|$ and $|\operatorname{ccl}_{A_n}(\sigma)| \leq |\operatorname{ccl}_{S_n}(\sigma)|$, so either $\operatorname{ccl}_{A_n}(\sigma) = \operatorname{ccl}_{S_n}(\sigma)$ and $|C_{A_n}(\sigma)| = \frac{1}{2}|C_{S_n}(\sigma)|$, or $|\operatorname{ccl}_{A_n}(\sigma)| = \frac{1}{2}|\operatorname{ccl}_{S_n}(\sigma)|$ and $|C_{A_n}(\sigma)| = |C_{S_n}(\sigma)|$.

To consider this further, we will introduce a natural definition.

Definition 5.35 (Splitting Conjugacy Classes)**.** When $|\operatorname{ccl}_{A_n}(\sigma)| = \frac{1}{2}|\operatorname{ccl}_{S_n}(\sigma)|$, we say that the conjugacy class of σ *splits* in A_n.

So when does this happen?

Proposition 5.36. *The conjugacy class of $\sigma \in A_n$ splits in A_n if and only if no odd permutations commute with σ.*

Proof. $|\operatorname{ccl}_{A_n}(\sigma)| = \frac{1}{2}|\operatorname{ccl}_{S_n}(\sigma)| \iff C_{A_n}(\sigma) = C_{S_n}(\sigma)$. Now $C_{A_n}(\sigma) = A_n \cap C_{S_n}(\sigma)$, and $A_n \cap C_{S_n}(\sigma) = C_{S_n}(\sigma)$ if and only if $C_{S_n}(\sigma)$ doesn't contain any odd elements, that is, when no odd permutations commute with σ. □

Example 5.37 (Conjugacy classes in A_4)**.** We will consider the conjugacy classes in A_4.

Cycle Type	Example Element	Odd Element in C_{S_4}?	Size of ccl_{S_4}	Size of ccl_{A_4}
$1, 1, 1, 1$	e	yes, eg. $(1\ 2)$	1	1
$2, 2$	$(1\ 2)(3\ 4)$	yes, eg. $(1\ 2)$	3	3
$3, 1$	$(1\ 2\ 3)$	no	8	4

Example 5.38 (Conjugacy classes in A_5)**.** We will consider the conjugacy classes in A_5.

Cycle Type	Example Element	Odd Element in C_{S_5}?	Size of ccl_{S_5}	Size of ccl_{A_5}
$1, 1, 1, 1$	e	yes, eg. $(1\ 2)$	1	1
$2, 2, 1$	$(1\ 2)(3\ 4)$	yes, eg. $(1\ 2)$	15	15
$3, 1, 1$	$(1\ 2\ 3)$	yes, eg. $(4\ 5)$	20	20
5	$(1\ 2\ 3\ 4\ 5)$	no	24	12

We can use this result to prove something that was mentioned earlier.

Theorem 5.39. *A_5 is simple.*

Proof. Normal subgroups must be unions of conjugacy classes, must contain e and must divide $|A_5| = 60$. The size of conjugacy classes in A_5 are $1, 15, 20, 12$ and 12. To sum these to get a divisor of 60, we can only have 1, and $1 + 15 + 20 + 12 + 12 = 60$, so the only normal subgroups are $\{e\}$ and A_5. □

Remark. All A_n for $n \geq 5$ are simple.

6 The Möbius Group, Revisited

With group actions, we now have more tools to study the Möbius group M. Recall that we defined the Möbius group as the set of Möbius maps, under composition.

Definition (Möbius Maps)**.** A *Möbius map* is a function $f : \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ of the form

$$f(z) = \frac{az + b}{cz + d},$$

with $a, b, c, d \in \mathbb{C}$ and $ad - bc \neq 0$, and with $f(-d/c) = \infty$ and

$$f(\infty) = \begin{cases} \frac{a}{c} & \text{if } c \neq 0 \\ \infty & \text{if } c = 0 \end{cases}.$$

This definition defined an action of the Möbius group on the extended complex plane. This action is faithful.

Proposition 6.1. *The action of the Möbius group $\mathcal{M}$ on the extended complex plane is faithful, and so $\mathcal{M} \leq \mathrm{Sym}(\hat{\mathbb{C}})$.*

Proof. Consider $\rho : M \to \mathrm{Sym}(\hat{\mathbb{C}})$ given by $\rho(f)(z) = f(z)$. Then if $\rho(f)$ is the identity permutation, then f is the identity in M. So ρ is injective and the action is faithful. □

We can think about points that are invariant under Möbius map.

Definition 6.2 (Fixed Point)**.** A *fixed point* of a Möbius map $f : \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ is a point $z \in \hat{\mathbb{C}}$ such that $f(z) = z$.

Theorem 6.3. *A Möbius map with at least three fixed points is the identity.*

Proof. Let $f(z) = \frac{az+b}{cz+d}$ have at least 3 fixed points. If ∞ is not a fixed point of f, then $\frac{az+b}{cz+d} = z$ for more than three complex numbers z, that is, $cz^2 + (d - a)z - b = 0$ has more than three roots in $\mathbb{C}$. But this is quadratic, so we can't have more than two roots, unless $c = b = 0$, $d = a$ for all z. But then $f(z) = z$. If ∞ is a fixed point of f, then we have $a/c = \infty \implies c = 0$, and thus $z = \frac{az+b}{d}$ for more than two complex numbers z, which can only occur when $a = d, b = 0$, so $f(z) = z$. □

What this theorem really tells us is that knowing what a Möbius map does on 3 points in $\hat{\mathbb{C}}$ uniquely determines it.

Corollary 6.4. *If two Möbius maps coincide on three distinct points in $\hat{\mathbb{C}}$, then they are equal.*

Proof. Let $f, g \in \mathcal{M}$ be such that $f(z_1) = g(z_1)$, $f(z_2) = g(z_2)$ and $f(z_3) = g(z_3)$ for three distinct points z_1, z_2 and $z_3 \in \hat{\mathbb{C}}$. Then $g^{-1}f(z_i) = g^{-1}g(z_i) = z_i$ for $i = 1, 2, 3$, and thus $g^{-1}f$ fixed more than 3 points, and it must be the identity. So $f = g$. □

Theorem 6.5 (Existence of Unique Möbius Maps)**.** *There is a unique Möbius map sending any three distinct points of $\hat{\mathbb{C}}$ to any three distinct points of $\hat{\mathbb{C}}$. That is, given $z_1, z_2, z_3 \in \hat{\mathbb{C}}$ and $w_1, w_2, w_3 \in \hat{\mathbb{C}}$ all distinct then there's a unique $f \in \mathcal{M}$ such that $f(z_i) = w_i$ for $i = 1, 2, 3$.*

Proof. Note that uniqueness follows from existence by the previous corollary. We will construct the map by supposing that $w_1 = 0$, $w_2 = 1$ and $w_3 = \infty$, and then we will use the group structure. Define $f(z) = \frac{(z_2 - z_3)(z - z_1)}{(z_2 - z_1)(z - z_3)}$. This satisfies $f(z_i) = w_i$ for all i. There are some special cases. If $z_1 = \infty$ use $f(z) = \frac{z_2 - z_3}{z - z_3}$, if $z_2 = \infty$ use $f(z) = \frac{z - z_1}{z - z_3}$, and if $z_3 = \infty$ use $f(z) = \frac{z - z_1}{z_2 - z_1}$.

Thus we can find some f_1 sending (z_1, z_2, z_3) to $(0, 1, \infty)$. But then in the same way we can find some f_2 sending (w_1, w_2, w_3) to $(0, 1, \infty)$. But then we can use the group structure, considering $f = f_2^{-1} \circ f_1$, this will send (z_1, z_2, z_3) to (w_1, w_2, w_3), as required. □

6.1 Conjugation

For two Möbius maps f and h, we can consider what happens when we conjugate hfh^{-1}. This acts in much the same way that any conjugate in a group structure does. For example, $\text{ord}(hfh^{-1}) = \text{ord}(f)$, since $(hfh^{-1})^n = hf^n h^{-1}$. Also, If f fixes z, then hfh^{-1} fixes z. In particular, the number of fixed points of a conjugate is the same as that of the original Möbius map. This observation has a partial converse.

Theorem 6.6. *Every non-identity $f \in \mathcal{M}$ has either 1 or 2 fixed points. If f has 1 fixed point, then it will be conjugate to the map $z \mapsto z + 1$, and if f has 2 fixed points, it will be conjugate to a map of the form $z \mapsto az$ for some non-zero $a \in \mathbb{C}$.*

Proof. We know that a non-identity Möbius map has at most 2 fixed points, but we show that there can't be zero fixed points. If $f(z) = \frac{az + b}{cz + d}$, then considering the quadratic $cz^2 + (d - a)z - b = 0$, formed by considering $f(z) = z$, this must have at least one solution.

Now we consider the two cases. If f has exactly 1 fixed point, say z_0, then choose some $z_1 \in \mathbb{C}$ which is not fixed by f. Then consider the triple $(z_1, f(z_1), z_0)$, which are all distinct points. So there is some $g \in \mathcal{M}$ so that $(z_1, f(z_1), z_0) \mapsto (0, 1, \infty)$. Then we can consider the conjugate of f by g. Then gfg^{-1} sends $0 \mapsto z_1 \mapsto f(z_1) \mapsto 1$, and $\infty \mapsto z_0 \mapsto z_0 \mapsto \infty$, so $gfg^{-1}(0) = 1$, $gfg^{-1}(\infty) = \infty$, so gfg^{-1} must be equal to $z \mapsto az + 1$ for $a \in \mathbb{C}$. If $a \neq 1$, then there is a non-infinity fixed point, $1/(1 - a)$, but this is a contradiction, so $a = 1$. Thus f is conjugate via g to the map $z \mapsto z + 1$, as required.

If f has exactly 2 fixed points, z_0 and z_1, then let g be any Möbius map sending $(z_0, z_1) \mapsto (0, \infty)$. So gfg^{-1} sends $0 \mapsto z_0 \mapsto z_0 \mapsto 0$, and $\infty \mapsto z_1 \mapsto z_1 \mapsto \infty$. So this conjugate fixes 0 and ∞. We can deduce that gfg^{-1} must have the form $z \mapsto az$, where $a = gfg^{-1}(1)$. □

We can use this to efficiently compute powers of Möbius maps, f^n for all $f \in \mathcal{M}$. We can see that $(gfg^{-1})^m = gf^m g^{-1}$, but this will be easy to compute, because the conjugate can have a nice form. Then we can conjugate back to get f^m.

6.2 Circles and Lines – Geometric Properties of Möbius Maps

We've seen that the image of 3 points in $\mathbb{C}$ under a given Möbius map uniquely determines that map. We also know (from geometry) that 3 points determine lines or circles.

In the complex plane, the a circle with center $b \in C$ and radius $r > 0 \in \mathbb{C}$ is the locus of points satisfying

$$|z - b| = r.$$

We can then write this as $|z - b|^2 - r^2 = 0$, or $(z - b)(\overline{z - b}) - r^2 = 0$, which we can write as

$$z\overline{z} - \overline{b}z - b\overline{z} + b\overline{b} - r^2 = 0. \qquad (*)$$

Also, the equation of a straight line in the complex plane (for $a, b, c \in \mathbb{R}$) is

$$a \cdot \text{re}(z) + bi \cdot \text{im}(z) = c,$$

that is

$$\frac{\overline{a+ib}}{2}z + \frac{a+ib}{2}\overline{z} - c = 0. \tag{†}$$

The form of these equations is slightly unusual but they are put in this form to emphasize the following definition. While we require three points in $\mathbb{C}$ to determine a circle, we only need two points to determine a line. But if we work in $\hat{\mathbb{C}}$, we consider the point at infinity, ∞ to be on *every* line. In this way, a line is determined by exactly 3 points in $\hat{\mathbb{C}}$, namely two points on the complex plane and a point at infinity.

Thinking in this way, we can unify the concepts of circles and lines in the extended complex plane, by introducing *clines*, a neologism covering both circles and lines.

Definition 6.7 (Clines in $\hat{\mathbb{C}}$)**.** A *cline* in $\hat{\mathbb{C}}$ is the set of points satisfying the equation

$$Az\overline{z} + \overline{B}z + B\overline{z} + C = 0,$$

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

Any equation of the form in the definition will match with exactly one of equation (∗) or (†).

Looking back at Möbius maps, we get the rather interesting result.

Theorem 6.8 (Möbius Maps Preserve Clines)**.** *Möbius send clines in $\hat{\mathbb{C}}$ to clines in $\hat{\mathbb{C}}$.*

Proof. Recall that the Möbius group $\mathcal{M}$ is generated by a composition of dilations/rotations, translations and inversions. That is, $z \mapsto az$, $z \mapsto z + b$ and $z \mapsto 1/z$.

Writing $S(A, B, C)$ for the circle satisfying $Az\overline{z} + \overline{B}z + B\overline{z} + C = 0$, we can check what happens under the various maps.

Under $z \mapsto az$, we have $S(A, B, C) \mapsto S\left(\frac{A}{\overline{a}a}, \frac{B}{\overline{A}}, C\right)$. Under $z \mapsto z + b$, $S(A, B, C) \mapsto S(A, B - Ab, C + Ab\overline{b} - B\overline{b} - \overline{B}b)$. Finally, under $z \mapsto 1/z$, we have $S(A, B, C) \mapsto S(C, \overline{B}, A)$. □

In practice, because both clines and Möbius maps are determined by 3 points (or where they send 3 points), it is quite straightforward to find a Möbius map which sends a given cline to another cline.

Example 6.9. Let's say we wanted to find $f \in \mathcal{M}$ which send the unit circle to the real line.

If we pick three points on the unit circle, say $\{-1, i1\}$, and three points on $\mathbb{R}$, say $\{-1, 0, 1\}$, then we could find a map f such that -1 and 1 are fixed, but so that i is sent to 0. For example,

$$f(z) = \frac{z - i}{1 - iz}$$

works.

6.3 Cross Ratios

Recall that given three points $z_1, z_2, z_3 \in \hat{\mathbb{C}}$, we have a unique Möbius map f such that $f(z_1) = 0$, $f(z_2) = 1$ and $f(z_3) = \infty$.

Definition 6.10 (Cross Ratio)**.** If we have four distinct points $z_1, z_2, z_3, z_4 \in \hat{\mathbb{C}}$, then their *cross-ratio* (z_1, z_2, z_3, z_4) is defined to be $f(z_4)$, where f is the unique Möbius map such that $f(z_1) = 0$, $f(z_2) = 1$ and $f(z_3) = \infty$.

In particular, the cross ratio of $(0, 1, \infty, w) = w$, for all $w \in \hat{\mathbb{C}}$. This is because f is forced to be the identity. There is a way to compute the cross ratio.

Theorem 6.11 (Computing Cross Ratios)**.** *For points z_1, z_2, z_3 and $z_4 \in \hat{\mathbb{C}}$, we have*

$$(z_1, z_2, z_3, z_4) = \frac{(z_4 - z_1)(z_2 - z_3)}{(z_2 - z_1)(z_4 - z_3)}.$$

Proof Sketch. This follows from the construction of the unique Möbius map. □

Remark. There are many conventions for the cross-ratio, depending on the order of 0, 1 and ∞. Some of these will be the same.

Proposition 6.12. *Double transpositions of the z_i fix the cross-ratio, that is,*

$$(z_1, z_2, z_3, z_4) = (z_2, z_1, z_4, z_3) = (z_3, z_4, z_1, z_2) = (z_4, z_3, z_2, z_1).$$

Proof Sketch. Note that this follows from the previous theorem. □

There is a connection between cross ratios and Möbius maps.

Theorem 6.13. *Möbius maps preserve cross-ratio.*

Proof. Let $f \in \mathcal{M}$ be the unique Möbius map such that $f : (z_1, z_2, z_3) \mapsto (0, 1, \infty)$, so that $f(z_4) = (z_1, z_2, z_3, z_4)$. Then for any Möbius map $g \in \mathcal{M}$, we have $f \circ g^{-1}$ sends $g(z_1) \mapsto 0$, $g(z_2) \mapsto 1$, and $g(z_3) \mapsto \infty$. Also $f \circ g^{-1}$ is unique, as Möbius maps are uniquely determined by how they transform three points. So, if we have $(g(z_1), g(z_2), g(z_3), g(z_4)) = (f \circ g^{-1})(g(z_4)) = f(z_4) = (z_1, z_2, z_3, z_4)$. □

This has an interesting geometric corollary.

Theorem 6.14. *Four distinct points $z_1, z_2, z_3, z_4 \in \hat{\mathbb{C}}$ lie on a cline if and only if $(z_1, z_2, z_3, z_4) \in \mathbb{R}$.*

Proof. Let f be the unique Möbius map sending $(z_1, z_2, z_3) \to (0, 1, \infty)$, so that $f(z_4) = (z_1, z_2, z_3, z_4)$. The cline C passing through z_1, z_2, z_3 is sent to the cline through $0, 1, \infty$ (the real axis), and so z_4 lies on C if and only if $f(z_4)$ lies on the real axis, that is, $f(z_4) \in \mathbb{R} \cup \{\infty\}$. But $f(z_3) = \infty$, so $f(z_4) \neq \infty$. Thus z_4 lies on C if and only if $z_4 \in \mathbb{R}$. □

7 Matrix Groups

In this chapter we will look at various groups of matrices. We will look at the actions of matrix groups on related actions, and we will study distance preserving maps (or *isometries*) on $\mathbb{R}^2$ and $\mathbb{R}^3$.

7.1 Examples of Matrix Groups

We are going to write $M_{n\times n}(\mathbb{F})$ to denote the set of $n \times n$ matrices over the field $\mathbb{F}$, which will typically be either $\mathbb{R}$ or $\mathbb{C}$.

Definition 7.1 (General Linear Group)**.** $\mathrm{GL}_n(\mathbb{F}) = \{A \in M_{n\times n}(\mathbb{F}) \mid A \text{ is invertible}\}$ is the *general linear group* over $\mathbb{F}$.

This is indeed a group, and the determinant is a surjective homomorphism, namely $\det : \mathrm{GL}_n(\mathbb{F}) \to \mathbb{F}^*$, the set of non-zero elements in $\mathbb{F}$.

Definition 7.2 (Special Linear Group)**.** The *special linear group* $\mathrm{SL}_n(\mathbb{F}) \leq \mathrm{GL}_n(\mathbb{F})$ is the kernel of the det homomorphism, that is, the set of elements of $\mathrm{GL}_n(\mathbb{F})$ with determinant 1.

Recall the following facts about matrices. Gives $A, B \in \mathrm{GL}_n(\mathbb{R})$,

- $(AB)^T = B^T A^T$,
- $(A^{-1})^T = (A^T)^{-1}$,
- $AA^T = I \iff A^T A = I \iff A^T = A^{-1}$,
- $(A^T)^T = A$,

- $\det(A^T) = \det(A)$.

With these we can define some groups.

Definition 7.3 (Orthogonal Group)**.** The *orthogonal group* is the group $\mathrm{O}_n = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid A^T A = I\}$.

Proposition 7.4. $\det : \mathrm{O}_n \to \{\pm 1\}$ *is a surjective homomorphism.*

Proof. This is a homomorphism as the determinant is a homomorphism in $\mathrm{GL}_n(\mathbb{R})$, and for $A \in \mathrm{O}_n$, then $A^T A = I$, and $1 = \det(AA^T) = \det(A)\det(A^T) = \det(A)^2$, so $\det(A) = \pm 1$. It is surjective as $\det I = 1$, and $\det(\mathrm{diag}(-1, 1, 1, \ldots, 1)) = -1$. □

Definition 7.5 (Special Orthogonal Group)**.** The *special orthogonal group* SO_n is the kernel of the determinant homomorphism, that is, $\mathrm{SO}_n = \{A \in \mathrm{O}_n \mid \det A = 1\}$.

These groups of matrices will be the main focus of this chapter. All of the matrix groups defined above act on the corresponding vector spaces. For example, $\mathrm{GL}_n(\mathbb{F})$ and $\mathrm{SL}_n(\mathbb{F})$ act on $\mathbb{F}^n$, and O_n, SO_n acts on $\mathbb{R}^n$.

Example 7.6. Let $G \leq \mathrm{GL}_2(\mathbb{R})$ act on $\mathbb{R}^2$. We will find the orbits. Note that $\{\mathbf{0}\}$ is always a singleton orbit, since we are acting by linear maps.

- If $G = \mathrm{GL}_2(\mathbb{R})$, then G acts transitively on $\mathbb{R}^2 \backslash \{\mathbf{0}\}$ since we can complete any $\mathbf{v} \neq \mathbf{0}$ to a basis, and we have an invertible change of basis matrix sending any basis to an other basis.
- If $G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \right\} = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, d \neq 0 \right\}$, then $\mathrm{Orb}(\mathbf{0}) = \{\mathbf{0}\}$, $\mathrm{Orb}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \left\{ \begin{pmatrix} a \\ 0 \end{pmatrix} \mid a \neq 0 \right\}$, and $\mathrm{Orb}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \left\{ \begin{pmatrix} b \\ d \end{pmatrix} \mid d \neq 0 \right\}$. This is all of the orbits, since the union gives all of $\mathbb{R}^2$.

7.2 Möbius Maps as Matrices

Let's first examine the connection between Möbius maps and matrices.

Proposition 7.7. *The function* $\phi : \mathrm{SL}_2(\mathbb{C}) \to \mathcal{M}$ *where*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto f, \quad \text{where } f(z) = \frac{az + b}{cz + d}$$

is a surjective homomorphism, with kernel $\{\pm I\}$.

Proof. First we show that ϕ is a homomorphism. If $f_1(z) = \frac{a_1 z + b_1}{c_1 z + d_1}$ and $f_2(z) = \frac{a_2 z + b_2}{c_2 z + d_2}$, then we have $f_2 \circ f_1(z) = \frac{az+b}{cz+d}$, where

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}.$$

It follows directly that ϕ is a homomorphism.

To see that it is surjective, we note that if $\frac{az+b}{cz+d}$ is a Möbius map, then the matrix

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C}),$$

since $ad - bc \neq 0$. But the determinant may not be zero, so letting $D^2 = \det M$, consider the matrix

$$\frac{M}{D^2} = \begin{pmatrix} \frac{a}{D} & \frac{b}{D} \\ \frac{c}{D} & \frac{d}{D} \end{pmatrix},$$

this has determinant one (and thus is in $\mathrm{SL}_2(\mathbb{C})$) and $\frac{\frac{a}{D}z+\frac{b}{D}}{\frac{c}{D}z+\frac{d}{D}} = \frac{az+b}{cz+d}$, so this homomorphism is surjective.

As for the kernel of ϕ, If $\phi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = Id \in \mathcal{M}$, then $\frac{az+b}{cz+d} = z$, for all $z \in \hat{\mathbb{C}}$. That is, $c = b = 0$ and $a = d$, and thus $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$. Since this has determinant 1, we also need $a = \pm 1$. Thus $\ker\phi = \{I, -I\}$. □

Corollary 7.8. $\mathcal{M} \cong \mathrm{SL}_2(\mathbb{C})/\{\pm I\}$.

Proof. Follows from the first isomorphism theorem. □

This quotient $\mathrm{SL}_2(\mathbb{C})/\{\pm I\}$ is the *projective special linear group*, $\mathrm{PSL}_2(\mathbb{C})$.

7.3 Conjugation and Changes of Basis

We can look at how the conjugation action of $\mathrm{GL}_n(\mathbb{F})$ on $M_{n\times n}(\mathbb{F})$ using the idea of changes of basis.

Recall that if we have some linear map $\alpha : \mathbb{F}^n \to \mathbb{F}^n$, we can represent α as a matrix A with respect to a basis $\{e_1, e_2, \ldots, e_n\}$ of $\mathbb{F}^n$. se a different basis $\{f_1, f_2, \ldots, f_n\}$, then α will be represented with respect to this basis by the matrix $P^{-1}AP$, where P is the *change of basis matrix*, defined by

$$f_j = \sum_{i=1}^{n} P_{ij} e_i.$$

This is an example of conjugation.

Proposition 7.9. $\mathrm{GL}_n(\mathbb{F})$ *acts on* $M_{n\times n}$ *by conjugation. The orbit of a matrix* $A \in M_{n\times n}(\mathbb{F})$ *is the set of matrices representing the same linear map as* A *with respect to different bases.*

Proof. To see that this is an action, if we have a matrix $A \in M_{n\times n}(\mathbb{F})$, then $P(A) = PAP^{-1} \in M_{n\times n}(\mathbb{F})$ for any $P \in \mathrm{GL}_n(\mathbb{F})$. Also, $I(A) = IAI^{-1} = A$, for any matrix A, and finally, if we have $Q, P \in \mathrm{GL}_n(\mathbb{F})$, then $(QP)(A) = QPA(QP)^{-1} = Q(PAP^{-1})Q^{-1} = Q(P(A))$, for any matrix A. So $\mathrm{GL}_n(\mathbb{F})$ acts on $M_{n\times n}(\mathbb{F})$.

By the argument above, we have that A and B are in the same orbit if and only if $A = PBP^{-1}$ for some $P \in \mathrm{GL}_n(\mathbb{F})$, which is true if and only if $B = P^{-1}AP$. That is, B represents the same linear map as A with respect to a different basis. Precisely, this is the basis obtained by the change of basis corresponding to P. □

Let's look at a example of this action.

Example 7.10 (Jordan Normal Form)**.** Recall that any matrix in $M_{2\times 2}(\mathbb{C})$ is conjugate to a matrix in Jordan Normal Form (JNF). That is, it's conjugate to one of the following types of matrices:

$$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} (\text{where } \lambda_1 \neq \lambda 2), \quad \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}, \quad \text{or} \quad \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}.$$

In the case of the first type of matrix, the values λ_1 and λ_2 are uniquely determined by the matrix (look at the eigenvalues), but the order is not determined uniquely. Other than that, no two matrices on this list are conjugate.

This gives us a complete description of the orbits of the action of $\mathrm{GL}_2(\mathbb{C})$ on $M_{2\times 2}(\mathbb{C})$ via conjugation.

7.4 Geometry of Orthogonal Groups

We are now going to look more closely at the orthogonal and special orthogonal group, and also the symmetries of $\mathbb{R}^2$ and $\mathbb{R}^3$.

Consider the standard inner product in $\mathbb{R}^n$: $x \cdot y = \sum_{i=1}^n x_i y_i$. Thinking of these as column vectors, we can write this as $x^T y$. If we consider the columns $p_1, \dots, p_n$ of $P \in \mathrm{O}_n$, we have $(P^T P)_{ij} = p_i^T p_j = p_i \cdot p_j$. So since $P \in \mathrm{O}_n$ if and only if $P^T P = I$, we have that

$$P \in \mathrm{O}_n \iff p_i \cdot p_j = \delta_{ij},$$

using the kronecker delta. This proves the following proposition.

Proposition 7.11. *$P \in \mathrm{O}_n$ if and only if the columns of P form an orthonormal basis.*

Thinking of $P \in \mathrm{O}_n$ as a change of basis matrix, we get the following result.

Proposition 7.12. *Consider O_n acting on $M_{n\times n}(\mathbb{R})$ by conjugation[8]. Then two matrices will be in the same orbit if and only if they represent the same linear map with respect to two orthonormal bases.*

Another characterization of O_n is that it is inner-product preserving.

Proposition 7.13 (O_n preserves inner products)**.** *$P \in \mathrm{O}_n$ if and only of $(Px) \cdot (Py) = x \cdot y$ for any $x, y \in \mathbb{R}^n$.*

Proof. If $P \in \mathrm{O}_n$, then

$$(Px) \cdot (Py) = (Px)^T (Py) = x^T P^T P y = x^T I y = x^T y = x \cdot y.$$

If $(Px) \cdot (Py) = x \cdot y$ for all $x, y \in \mathbb{R}^n$, then taking the basis vectors e_i and e_j, we have

$$Pe_i \cdot Pe_j = e_i \cdot e_j = \delta_{ij}.$$

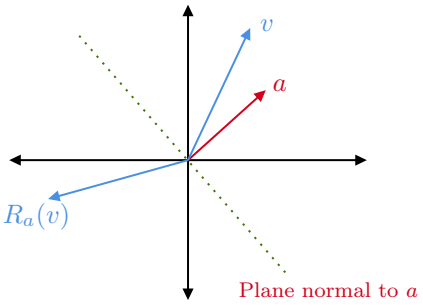
so the vectors $Pe_1, \dots, Pe_n$ are orthonormal. Then the columns of P are orthonormal, so $P \in \mathrm{O}_n$ by our previous proposition. □

Corollary 7.14. *For $P \in \mathrm{O}_n$, P preserves the length of vectors and the angle between vectors.*

Proof. This follows directly from the preservation of inner product. □

Let's investigate what the elements of O_n and SO_n look like. First, a bit of background.

Definition 7.15. If $a \in \mathbb{R}^n$ with $|a| = 1$, then the *reflection* in the plane normal to a is the linear map $R_a : \mathbb{R}^n \to \mathbb{R}^n$ such that $x \to x - 2(x \cdot a)a$.



Lemma 7.16. *R_a lies in O_n.*

[8] This is an action as O_n is a subgroup of GL_n

Proof. Let $x, y \in \mathbb{R}^n$. Then

$$\begin{aligned} R_a(x) \cdot R_a(y) &= (x - 2(x \cdot a)a) \cdot (y - 2(y \cdot a)a) \\ &= x \cdot y - 2(x \cdot a)(a \cdot y) - 2(y \cdot a)(x \cdot a) + 4(x \cdot a)(y \cdot a)(a \cdot a) \\ &= x \cdot y, \end{aligned}$$

so $R_a \in \mathrm{O}_n$, as it preserves inner products. □

As we might expect, conjugates of reflections are also reflections.

Lemma 7.17 (Conjugates of Reflections are Reflections)**.** *Given $P \in \mathrm{O}_n$, $PR_aP^{-1} = R_{Pa}$.*

Proof. We have

$$\begin{aligned} PR_aP^{-1}(x) &= P(P^{-1}(x) - 2(P^{-1}(x) \cdot a)a) \\ &= x - 2(P^{-1}(x) \cdot a)(Pa), \end{aligned}$$

but $P^{-1} = P^T$, so $P^{-1}(x) \cdot a = P^T x \cdot a = x^T Pa$, which is just $x \cdot Pa$. So $PR_aP^{-1}(x) = x - 2(x \cdot Pa)(P_a) = R_{Pa}(x)$. □

So reflections lie in O_n, but do they lie in SO_n? We need to know the determinant of a reflection R_a. We know that the determinant of a matrix is the product of its eigenvalues, so eigenvalues of R_a might be a helpful thing to find.

We can spot some straightforward eigenvectors:

$$R_a(a) = a - 2(a \cdot a)a = -a,$$

so a is an eigenvector with eigenvalue -1. And, for x in the plane normal to a, we get

$$R_a(x) = x - 2(x \cdot a)a = x.$$

so x is an eigenvector with eigenvalue 1. This is all of the eigenvalues, as the eigenvalue 1 has multiplicity $n - 1$, as we can find $n - 1$ linearly independent eigenvectors in the plane normal to a. Thus we have

$$\det(R_a) = (-1) \cdot (1)^{n-1} = -1.$$

This proves the following proposition.

Proposition 7.18 (Reflections are not in SO_n)**.** *$R_a \in \mathrm{O}_n \setminus \mathrm{SO}_n$.*

To think about the elements that *are* in SO_n, we will begin by thinking about SO_2.

Theorem 7.19 (Elements of SO_2)**.** *Every element of SO_2 is of the form*

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

for some $\theta \in [0, 2\pi)$.[9] *Conversely every such element lies in SO_2.*

Proof. Consider the matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SO}_2\,.$$

We have $A^T A = I$, and $\det A = 1$. Thus $A^T = A^{-1}$, so

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix},$$

and $a = d$, $b = -c$. Also since $ad - bc = 1$, so $a^2 + c^2 = 1$. So we can write $a = \cos\theta$ and $c = \sin\theta$ for a unique $\theta \in [0, 2\pi)$. Hence every matrix in SO_2 has the form as claimed. Conversely, the determinant of the matrix given is always one, and is in O_2, and hence lies in SO_2. □

[9] This is an anticlockwise rotation of $\mathbb{R}^2$ about the origin by angle θ.

Theorem 7.20. *The elements of* $\mathrm{O}_2 \setminus \mathrm{SO}_2$ *are the reflections in lines through the origin.*

Proof. Consider the matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{O}_2 \setminus \mathrm{SO}_2 \,.$$

Then $A^T A = I$, and $\det A = -1$. Then we have

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

and so $a = -d$, $b = c$. Since $ad - bc = -1$, we have $a^2 + c^2 = 1$, so $a = \cos\theta$, $c = \sin\theta$ for unique $\theta \in [0, 2\pi)$, and

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

We can check that

$$A \begin{pmatrix} \sin\theta/2 \\ -\cos\theta/2 \end{pmatrix} = - \begin{pmatrix} \sin\theta/2 \\ -\cos\theta/2 \end{pmatrix}, \quad \text{and} \quad A \begin{pmatrix} \cos\theta/2 \\ \sin\theta/2 \end{pmatrix} = - \begin{pmatrix} \cos\theta/2 \\ \sin\theta/2 \end{pmatrix},$$

so A is the reflection in the plane orthogonal the unit vector $\begin{pmatrix} \sin\theta/2 & -\cos\theta/2 \end{pmatrix}$.

Conversely any reflection in a line through the original will have this form, and so is in $\mathrm{O}_2 \setminus \mathrm{SO}_2$. □

Corollary 7.21. *Every element of* O_2 *is the composition of at most two reflections.*

Proof. Every element in $\mathrm{O}_2 \setminus \mathrm{SO}_2$ is a reflection, so if $A \in \mathrm{SO}_2$, then

$$A = \left[A \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right] \left[\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right],$$

and each of the matrices on the right is in $\mathrm{O}_2 \setminus \mathrm{SO}_2$, and is thus a reflection. □

Moving from two to three dimensions, we have the following theorem.

Theorem 7.22. *If* $A \in \mathrm{SO}_3$*, then there exists a vector* $v \in \mathbb{R}^3$ *such that* $|v| = 1$ *and* $Av = v$.

Proof. Such a v is an eigenvector for the eigenvalue 1, so it suffices to show 1 is an eigenvalue of A. This is equivalent to showing the determinant $\det(A - I) = 0$. We have

$$\begin{aligned} \det(A - I) &= \det(A - AA^T) \\ &= \det(A(I - A^T)) \\ &= \det A \cdot \det(I - A^T) \\ &= \det(I - A^T) \\ &= \det((I - A)^T) \\ &= \det(I - A) \\ &= \det(-I) \cdot \det(A - I) = -\det(A - I), \end{aligned}$$

so $\det(A - I) = 0$, as required. □

Corollary 7.23. *Every* $A \in \mathrm{SO}_3$ *is conjugate in* SO_3 *to a matrix of the form*

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

Proof. By the previous theorem, there exists $v_1 \in \mathbb{R}^3$ such that $|v_1| = 1$, and $Av_1 = v_1$. We can extend this to an orthonormal basis $\{v_1, v_2, v_3\}$ of $\mathbb{R}^3$. Then for $i = 2, 3$, we have

$$Av_i \cdot v_1 = Av_i \cdot Av_1 = v_i \cdot v_1 = 0,$$

so Av_2 and Av_3 lie in $\langle v_2, v_3 \rangle$. So A maps $\langle v_2, v_3 \rangle$ to itself. Now consider the restriction of A to $\langle v_2, v_3 \rangle$. This still has determinant 1, so A is an element of SO_2, and its matrix must therefore be of the form

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

So A has the matrix

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix},$$

with respect to the basis $\{v_1, v_2, v_3\}$. The change of basis matrix P lies in O_3 since $\{v_1, v_2, v_3\}$ is an orthonormal basis, and if P does not lie in SO_3, then instead we can use the basis $\{-v_1, v_2, v_3\}$. □

Geometrically, this tells us in particular that every element in SO_3 is a rotation about some axis.

Corollary 7.24. *Every element of* O_3 *is the composition of at most 3 reflections.*

Proof. If $A \in \mathrm{SO}_3$, then there exists $P \in \mathrm{SO}_3$ such that $PAP^{-1} = B$, with

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

Since this matrix is the composition of at most 2 reflections by our result in two dimensions, so $B = B_1 B_2$. Thus A also is, as the conjugate of a reflection is a reflection.

If $A \in \mathrm{O}_3 \setminus \mathrm{SO}_3$, then $\det A = -1$, then we can write

$$A = \left[A \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right] \left[\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right],$$

and the first lies in SO_3 and is thus the product of at most 2 reflections, and second matrix is a reflection. □

7.5 Symmetries of the Cube Revisited

We will finish our discussion of matrix groups by again considering the symmetries of the cube. We can think of the symmetry groups of any of the platonic solids as subgroups of O_3. We can do this by placing our solid at the origin, and then any symmetry of the solid will be an element of O_3.

One fact about O_3 is that we can write it as a direct product.

Lemma 7.25. $\mathrm{O}_3 \cong \mathrm{SO}_3 \times C_2$.

Proof Sketch. Apply the direct product theorem. □

Here, the subgroup C_2 is generated by the map $v \mapsto -v$. So if $v \mapsto -v$ is a symmetry of our platonic solid, then its group of symmetries will also split as the direct product $G^+ \times C_2$. Now this is a symmetry of the cube, so we have that the symmetry group of the cube is the group of its rotational symmetries with C_2, so

$$G^+ \times C_2 \cong S_4 \times C_2,$$

which matches our result from Chapter 5.

8 Groups of Small Order

We are going to finish off by characterizing all groups up to order 8. We have already found some of these, which we will review.

8.1 Groups of Order Up To 7

So far we have established the following classifications.

1. *Prime Order.* Then we only have the cyclic group.
2. *Order 4.* We have C_4 or $C_2 \times C_2$.
3. *Order 6.* We have C_6 and D_6.

8.2 Groups of Order 8

To study groups of order 8, we'll need to introduce a new group.

Definition 8.1 (Quaternions)**.** Consider the subset of matrices in $\mathrm{GL}_2(\mathbb{C})$ given by

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

The set $\{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$ forms the *quaternion group*, Q_8.

The elements of this group satisfy the following relations:

(i) $g^4 = \mathbf{1}$ for any $g \in Q_8$.

(ii) $(-\mathbf{1})^2 = \mathbf{1}$.

(iii) $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -\mathbf{1}$.

With that defined, let's get on to classifying groups of order 8. First, a little lemma.

Lemma 8.2. *If a finite group has all non-identity elements of order 2, then it is isomorphic to* $C_2 \times C_2 \times \cdots \times C_2$.

Proof. Recall from example sheet 1 that G must be abelian, and $|G| = 2^n$. If $|G| = 2$, then $G \cong C_2$, and if $|G| > 2$, then choose a_1 of order 2 in G. Then there exists $a_2 \notin \langle a_1 \rangle$, and by the direct product theorem, $\langle a_1, a_2 \rangle \cong \langle a_1 \rangle \times \langle a_2 \rangle \cong C_2 \times C_2$. If this is isomorphic to G, then we are done. Otherwise, pick $a_3 \notin \langle a_1, a_2 \rangle$, and we get $\langle a_1, a_2, a_3 \rangle = \langle a_1 \rangle \times \langle a_2 \rangle \times \langle a_3 \rangle \cong C_2 \times C_2 \times C_2$. Continuing in this way, we get $G \cong C_2 \times C_2 \times \cdots \times C_2$. □

And now we can get to the heart of the matter.

Theorem 8.3 (Groups of order 8)**.** *A group of order 8 is isomorphic to exactly one of* C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_8, *or* Q_8.

Proof. Note that $C_8, C_4 \times C_2$ and $C_2 \times C_2 \times C_2$ are all abelian and are distinguished by the maximal order of an element in the group. Then D_8 and Q_8 are non-abelian, and are distinguished from each other by the number of elements of order 2.

Not let G be a group such that $|G| = 8$. Then every element has order $1, 2, 4$ or 8 by Lagrange. If there is an element of order 8, then $G \cong C_8$. If every element has order 2, then $G \cong C_2 \times C_2 \times C_2$ by our lemma. Now let's assume that G has at least one element g of order 4, and no element of order 8.

Now $|G : \langle g \rangle| = 2$, and thus if $h \notin \langle g \rangle$, $G = \langle g \rangle \cup h\langle g \rangle$. If $h^2 \in h\langle g \rangle$, we would have $h \in \langle g \rangle$, which is a contradiction. Thus $h^2 \in \langle g \rangle$.

Now if $h^2 = g$ or g^3, then g would have order 8, which is a contradiction. So $h^2 = e$ or g^2. We have $\langle g \rangle \trianglelefteq G$, thus $hgh^{-1} = g^k$, for some k. We also have $g = h^2gh^{-2} = hg^kh^{-1} = (hgh^{-1})^k = g^{k^2}$, as g and h^2 commute. This implies $k^2 \equiv 1 \pmod 4$, giving two cases.

If $k \equiv 1 \pmod 4$, then $hgh^{-1} = g$, implying G is abelian. If $h^2 = e$, then $G = \langle g \rangle \times \langle h \rangle \cong C_4 \times C_2$ by the direct product theorem. If $h^2 = g^2$, then $(hg^{-1})^2 = e$, so $G = \langle g, hg^{-1} \rangle \cong C_4 \times C_2$.

If $k \equiv -1 \pmod 4$, then $hgh^{-1} = g^{-1}$. Then if $h^2 = e$, we have $G = \langle g, h \mid g^4 = h^2 = e, gh = hg^{-1} \rangle \cong D_8$. Otherwise, $h^2 = g^2$, and $G \cong Q_8$. $\square$

Remark. We know that in an abelian group, every subgroup is normal. The converse is not true, and Q_8 is a counterexample.