

Groups

ADAM KELLY

Updated November 15, 2020

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	4
1.1 Definition of a Group	4
1.1.1 Elementary Properties of Groups	4
1.1.2 Examples of Groups	5
1.2 Subgroups	7
1.2.1 Generators	9
1.3 Homomorphisms	9
1.3.1 Kernels	12
1.3.2 Direct Products	13
2 Important Groups	15
2.1 Cyclic Groups	15
2.2 Dihedral Group	16
2.3 Permutation Groups	18
2.4 Möbius Groups	23
3 Lagrange's Theorem	26
3.1 Exploring Group Using Lagrange	29
4 Quotients of Groups	30
4.1 Normal Subgroups	30
4.2 Quotients	31
4.3 The Isomorphism Theorems	33
4.4 Simple Groups	35
5 Group Actions	37
5.1 Orbits and Stabilisers	38
5.1.1 Symmetries of the Tetrahedron	40
5.1.2 Symmetries of the Cube	41
5.1.3 Platonic Solids	43
5.2 Cauchy's Theorem	43

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 structures¹, 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 1.1.1 (Group)

A **group** is a set G with a binary operation^a $*$ 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.

^aSome texts include an additional *closure* axiom, but this is implied by $*$ being a binary operation on G .

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 1.1.2 (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.

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

¹Apart from ‘magmas’ I suppose, but they don’t tend to be a particularly useful notion.

$h * g = k * g = e$ follows analogously. \square

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

Proposition 1.1.3 (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. \square

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

Proposition 1.1.4 (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 $(g^{-1})^{-1} = g$. \square

§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 1.1.5 (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 groups². 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.

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

Example 1.1.6 (The Trivial Group)

The **trivial group** is a group whose only element is the identity, $\{e\}$.

Example 1.1.7 (Additive Group of Integers)

$(\mathbb{Z}, +)$ is an group. We have

- The identity element $0 \in \mathbb{Z}$, 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.

Example 1.1.8 (Addition Modulo n)

Let $n \in \mathbb{N}$, and let $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \dots, n-1\}$ 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 1.1.9 (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 1.1.10 (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 1.1.11 (General Linear Group)

Let $\text{GL}_n(\mathbb{R})$ be the set of $n \times n$ matrices with non-zero determinant. Then $(\text{GL}_n(\mathbb{R}), \times)$ is the **general linear group**^a.

^aUsing matrix multiplication

Example 1.1.12 (Special Linear Group)

Let $\text{SL}_n(\mathbb{R})$ be the set of $n \times n$ matrices with determinant 1. Then $(\text{SL}_n(\mathbb{R}), \times)$ 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 1.1.13 (Non-Examples of Groups)

The following 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 1.2.1 (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 1.2.2 (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.
- $\{0, 2, 4, \dots\} \leq \mathbb{Z}$ with addition.
- $\text{SL}_n(\mathbb{R}) \leq \text{GL}_n(\mathbb{R})$ with 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 1.2.3 (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 $x, y \in H$. \square

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

Theorem 1.2.4 (Subgroups of \mathbb{Z})

The subgroups of $(\mathbb{Z}, +)$ are precisely the subsets of the form $n\mathbb{Z}$ for $n \in \mathbb{N}$, 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 $H \leq \mathbb{Z}$. 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 $k \notin n\mathbb{Z}$. So, there is some integer m such that $nm < k < n(m+1)$. But then $0 \leq k - nm < n$, and $k - nm \in H$ which is a contradiction, so $H = n\mathbb{Z}$. \square

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

Proposition 1.2.5 (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 $K \subset H$, $K \leq H$. \square

§1.2.1 Generators

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

Definition 1.2.6 (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 1.2.7

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 $T = \langle X \rangle$. \square

Example 1.2.8

We have $(\mathbb{Z}, +) = \langle 1 \rangle = \langle 2, 3 \rangle^a$, and $\mathbb{Z}/5\mathbb{Z} = \langle 1 \rangle = \langle 3 \rangle$.

^aNote that we write $\langle 2, 3 \rangle$ instead of $\langle \{2, 3\} \rangle$.

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 1.2.9 (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 $\phi : H \rightarrow G$. 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 1.3.1 (Homomorphism)

Let $(G, *_{\mathcal{G}})$ and $(H, *_{\mathcal{H}})$ be groups. A function $\phi : H \rightarrow G$ is a **group homomorphism** if for all $a, b \in H$,

$$\phi(a *_{\mathcal{H}} b) = \phi(a) *_{\mathcal{G}} \phi(b).$$

Example 1.3.2 (Inclusion Function)

If $H \leq G$, then the function $\iota : H \rightarrow G$ that has $\iota(h) = h$ for $h \in H$ is a homomorphism. It is also injective.

Example 1.3.3

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

$$\phi(k + l) = (k + l) \pmod{n} = (k \pmod{n}) + (l \pmod{n}) = \phi(k) + \phi(l).$$

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

Example 1.3.4

The function $\phi : (\mathbb{R}, +) \rightarrow (\mathbb{R}^*, \cdot)$ where $x \mapsto e^x$ 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 $a \in \mathbb{R}^*$, $\phi(\log a) = e^{\log a} = a$.

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

Proposition 1.3.5 (Properties of Homomorphisms)

Let $\phi : H \rightarrow G$ be a homomorphism.

- (i) $\phi(e_H) = e_G$.
- (ii) $\phi(h^{-1}) = \phi(h)^{-1}$ for all $h \in H$.
- (iii) If $\psi : G \rightarrow K$ is another homomorphism, then $\psi \circ \phi : H \rightarrow K$ is also a homomorphism.

Proof.

- (i) We have $e_H *_{\mathcal{H}} e_H = e_H$, so $\phi(e_H *_{\mathcal{H}} e_H) = \phi(e_H) *_{\mathcal{G}} \phi(e_H) = \phi(e_H)$, so by the cancellation law, $\phi(e_H) = e_G$.

- (ii) Consider $\phi(h) *_{\mathcal{G}} \phi(h^{-1}) = \phi(h *_{\mathcal{H}} h^{-1}) = \phi(e_{\mathcal{H}}) = e_{\mathcal{G}}$, by (i). So $\phi(h) *_{\mathcal{G}} = \phi(h^{-1}) = e_{\mathcal{G}}$ which is the defining property of an inverse, so $\phi(h^{-1}) = \phi(h)^{-1}$.
- (iii) We have

$$\begin{aligned}
 (\psi \circ \phi)(a *_{\mathcal{H}} b) &= \psi(\phi(a *_{\mathcal{H}} b)) \\
 &= \psi(\phi(a) *_{\mathcal{G}} \phi(b)) \\
 &= \psi(\phi(a)) *_{\mathcal{K}} \psi(\phi(b)) \\
 &= (\psi \circ \phi)(a) *_{\mathcal{K}} (\psi \circ \phi)(b),
 \end{aligned}$$

so $\psi \circ \phi$ is a homomorphism from $\mathcal{H} \rightarrow \mathcal{K}$. \square

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

Definition 1.3.6 (Isomorphism)

If a function $\phi : \mathcal{H} \rightarrow \mathcal{G}$ is bijection, and ϕ is also a homomorphism from $\mathcal{H} \rightarrow \mathcal{G}$, then we say it is an **isomorphism**. We say two groups \mathcal{H}, \mathcal{G} are **isomorphic**, written $\mathcal{H} \cong \mathcal{G}$ if there is an isomorphism from $\mathcal{H} \rightarrow \mathcal{G}$.

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 1.3.7

Consider the group $\mathcal{G} = \{1, i, -1, -i\}$ with complex multiplication. Then $\mathcal{G} \cong \mathbb{Z}/4\mathbb{Z}$. This is isomorphic with the isomorphism $\phi : \mathcal{G} \rightarrow \mathbb{Z}/4\mathbb{Z}$, 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 $\mathcal{H} = \{e^{2\pi i k/n} : 0 \leq k \leq n-1\}$ with complex multiplication is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Example 1.3.8 (\mathbb{Z} ’s subgroups are isomorphic)

$\mathbb{Z} \cong n\mathbb{Z}$ for $n \in \mathbb{Z}$, as defined in [Theorem 1.2.4](#).

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

Proposition 1.3.9 (Inverses of isomorphisms are isomorphisms)

Let $\phi : H \rightarrow G$ be an isomorphism. Then $\phi^{-1} : G \rightarrow H$ is also an isomorphism.

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

§1.3.1 Kernels

When dealing with homomorphisms, say $\phi : H \rightarrow G$, 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 1.3.10 (Image)

Let $\phi : H \rightarrow G$ 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 1.3.11 (Kernel)

Let $\phi : H \rightarrow G$ 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 1.3.12 (The Image and Kernel are Subgroups)

Let H and G be groups and let $\phi : H \rightarrow G$ 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 1.3.13

$\phi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$, 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 1.3.14 (Surjectivity and Injectivity Criterion)

Let $\phi : H \rightarrow G$ 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. \square

§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 1.3.15 (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 1.3.16

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

Proof Sketch. Check everything component-wise. \square

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 1.3.17 (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 $\phi : H \times K \rightarrow G$, 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 injectivity criterion. \square

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 1.2.9](#).

Definition 2.1.1 (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 2.1.2 (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 $G = \{e^{2\pi i k/n} : 0 \leq k \leq n-1\}$. Then (G, \cdot) is generated by $\langle e^{2\pi i/n} \rangle$ 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 2.1.3 (Cyclic Group C_n)

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

Theorem 2.1.4 (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 $\phi : C_n \rightarrow G$ 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 $\phi(a^j a^k) = \phi(a^{j+k}) = b^{j+k} = b^j b^k = \phi(a^j) \phi(a^k)$. 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 $\phi : \mathbb{Z} \rightarrow G$ 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 $G \cong \mathbb{Z}$. \square

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

Proposition 2.1.5

Cyclic groups are abelian.

Proof Sketch. Check definitions. \square

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

Definition 2.1.6 (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 2.1.7 (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, $n \mid k$. \square

§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.

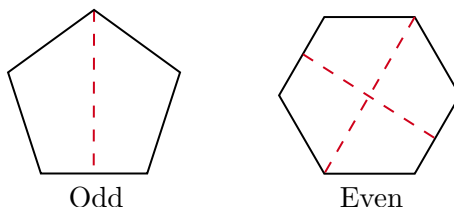
Definition 2.2.1

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 2.2.2

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.



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 2.2.3

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 $g(v_2)$ 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. \square

Proposition 2.2.4

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. \square

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 2.2.5

The group

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

but the group

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

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 2.3.1 (Permutations)

Given a set X , a **permutation** of X is a bijective function $\sigma : X \rightarrow X$. The set of all permutations of X is denoted $\text{Sym } X$.

Theorem 2.3.2

For any set X , $\text{Sym } X$ is a group with respect to composition.

Proof. We check the group axioms individually.

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

Thus $\text{Sym } X$ is a group. □

Definition 2.3.3 (Symmetric Group)

If $|X| = n$, we write S_n for (the isomorphism class of) $\text{Sym } X$. 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 $X = \{1, 2, 3, \dots, n\}$ 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 2.3.4

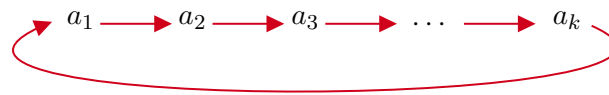
If we had some $\sigma \in S_3$ such that $\sigma(1) = 2$, $\sigma(2) = 3$, and $\sigma(3) = 1$, we would write

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

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

$$\sigma = (a_1 \ a_2 \ \cdots \ a_k)$$

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

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

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

Definition 2.3.5 (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 2.3.6 (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

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

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

^aThis is, in general, not the case

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 2.3.7 (Disjoint Cycles)

We say that two cycles are **disjoint** if no number appears in both cycles.

Lemma 2.3.8

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 $x \in \{1, 2, \dots, n\}$, 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. \square

Slightly more surprising is the following theorem

Theorem 2.3.9 (Writing Permutations with Cycles)

Any $\sigma \in S_n$ can be written uniquely^a as the composition of disjoint cycles.

^aUp 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 $1, \sigma(1), \sigma^2(1), \dots$. Since $\{1, 2, \dots, n\}$ 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 $1, \sigma(1), \sigma^2(1), \dots, \sigma^{k-1}(1)$ 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 $\{1, 2, \dots, n\}$ 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

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

and each $j \in \{1, 2, \dots, n\}$ 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 $\sigma(a_1), \sigma^2(a_1), \dots$. 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. \square

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

Definition 2.3.10

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

Example 2.3.11

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

Theorem 2.3.12

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 i as they are disjoint. By the fundamental theorem of orders, we must have $k_i \mid m$, and thus $m = \text{lcm}(k_1, k_2, \dots, k_r)$ by minimality. \square

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 2.3.13 (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

$$(a_1 \ a_2 \ \cdots \ a_k) = (a_1 \ a_2)(a_2 \ a_3) \cdots (a_{k-1} \ a_k).$$

□

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 parity of the number of transpositions *is* invariant among decompositions.

Theorem 2.3.14 (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 parity 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

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

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

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

$$\begin{aligned} \chi(\sigma) &\equiv \chi(e) + k \equiv n + k \pmod{2} \\ \chi(\sigma) &\equiv \chi(e) + l \equiv n + l \pmod{2}, \end{aligned}$$

and thus $k \equiv l \pmod{2}$. □

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

Definition 2.3.15 (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 $\text{sign}(\sigma) = (-1)^k$. If k is even, we say that σ is **even**, and if k is odd, we say that σ is **odd**.

Proposition 2.3.16

For $n \geq 2$, $\text{sign} : S_n \rightarrow \{\pm 1\}$ 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 $\text{sign}(\sigma\sigma') = (-1)^{k+l} = (-1)^k(-1)^l = \text{sign}(\sigma)\text{sign}(\sigma')$, so sign is a homomorphism. It is also surjective since $\text{sign}(e) = 1$ and $\text{sign}(1\ 2) = -1$. \square

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

Definition 2.3.17 (Alternating Group)

The **alternating group** A_n is the kernel of the homomorphism $\text{sign} : S_n \rightarrow \{\pm 1\}$, 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 $\mathbb{C} \rightarrow \mathbb{C}$ - but since \mathbb{C} has some intrinsic geometric properties (lines, circles, etc) unlike $\{1, 2, \dots, n\}$, we will restrict ourselves to functions that interact well with its geometry.

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

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

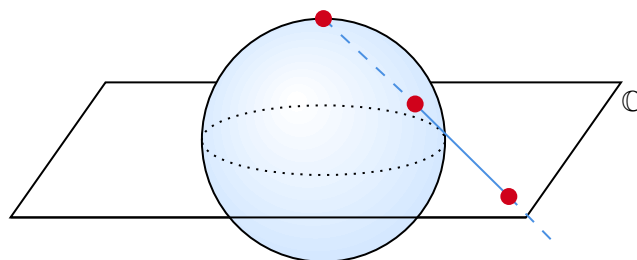
with $a, b, c, d \in \mathbb{C}$ and $ad - bc \neq 0$. We have this condition because

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

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 2.4.1 (Möbius Maps)

A **Möbius map** is a function $f : \hat{\mathbb{C}} \rightarrow \hat{\mathbb{C}}$ 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 2.4.2

Möbius maps are bijections $\hat{\mathbb{C}} \rightarrow \hat{\mathbb{C}}$.

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 2.4.3 (Möbius Group)

The set of Möbius maps forms a group under composition.

Proof.

- *Closure.* Let $f_1(z) = \frac{a_1z+b_1}{c_1z+d_1}$ and $f_2(z) = \frac{a_2z+b_2}{c_2z+d_2}$. Then

$$f_2(f_1(z)) = \frac{(a_1a_2 + b_2c_1)z + (a_2b_1 + b_2d_1)}{(c_2a_1 + d_2c_1)z + (c_2b_1 + d_2d_1)} = \frac{a'z + b'}{c'z + d'},$$

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.

To see what Möbius maps actually do to the extended complex plane, consider the following theorem.

Theorem 2.4.4

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

$$\begin{aligned} z &\mapsto z + \frac{d}{c} \mapsto \frac{1}{z + \frac{d}{c}} \mapsto \frac{(-ad + bc)c^{-2}}{z + \frac{d}{c}} \\ &\mapsto \frac{a}{c} + \frac{(-ad + bc)c^{-2}}{z + \frac{d}{c}} = \frac{az + b}{cz + d}. \end{aligned}$$

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 3.0.1 (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 3.0.2 (Cosets of $2\mathbb{Z}$)

Let $H = 2\mathbb{Z} \leq \mathbb{Z}$. 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 3.0.3

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 3.0.4 (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 $g_1H \cap g_2H = \emptyset$;
- (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 $H \rightarrow gH, h \rightarrow gh$ 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 $g_1h = g_2h_2h_1^{-1}h$, so for any $h \in H$, we have $g_1h \in g_2H$, 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 $\bigcup_{g \in G} gH \subseteq G$, thus $G = \bigcup_{g \in G} gH$.

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

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 3.0.5

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. \square

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

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

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

then

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

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 3.0.6 (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. \square

Corollary 3.0.7

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 $g^{|G|} = g^{\text{ord}_G(g) \cdot k} = e^k = e$. \square

Corollary 3.0.8

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 $\langle g \rangle = G$. \square

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 $\{1, 2, \dots, n-1\}$ 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 3.0.9 (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. \square

§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 3.1.1 (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 3.0.8](#). 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 3.0.8](#).
- If $|G| = 4$, we have two possibilities, as we will see in the following proposition.

Proposition 3.1.2 (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, $G = \langle b \rangle \times \langle c \rangle \cong C_2 \times C_2$. \square

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 4.1.1 (Normal Subgroups)

A subgroup $N \leq G$ is **normal** if $\forall g \in G, gN = Ng$. We write $N \trianglelefteq G$.

Proposition 4.1.2 (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 4.1.3

The following are all normal subgroups

- (i) $n\mathbb{Z} \trianglelefteq \mathbb{Z}$, as for all $a \in \mathbb{Z}$, 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 similarly for $(1\ 3)$ and $(2\ 3)$.

Proposition 4.1.4

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 4.1.5

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 to be $G \setminus H$ both for left and right cosets. So H is normal. \square

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

Proposition 4.1.6

If $\phi : G \rightarrow H$ 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 $k \in \ker \phi$. \square

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

Example 4.1.7

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 4.1.8 (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 . \square

§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 homomorphism 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 4.2.1 (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 4.2.2 (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 $(a'b')H$. \square

We now get to the central result of this section.

Proposition 4.2.3

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 : $(g_1N \cdot g_2N) \cdot g_3N = (g_1g_2N) \cdot g_3N = ((g_1g_2)g_3)N = (g_1(g_2g_3))N = g_1N \cdot (g_2N \cdot g_3N)$.

\square

Definition 4.2.4

If $N \trianglelefteq G$, then N/G is the group of cosets of N in G is called the **quotient group** of G by N .

Example 4.2.5 (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 4.2.6

Given $N \trianglelefteq G$, the function $\pi : G \rightarrow G/N$ 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 $\ker \pi = N$. \square

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 4.3.1 (First Isomorphism Theorem)

Let $\phi : G \rightarrow H$ be a homomorphism. Then $G/\ker \phi \cong \text{img } \phi$.

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

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

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

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

Example 4.3.2

- (i) $\det : \mathrm{GL}_2(\mathbb{R}) \rightarrow \mathbb{R}^\times$ has $\mathrm{img} \det = \mathbb{R}^\times$, $\ker \det = \mathrm{SL}_2(\mathbb{R})$, so $\mathrm{GL}_2(\mathbb{R})/\mathrm{SL}_2(\mathbb{R}) \cong \mathbb{R}^\times$.
- (ii) Consider the map $\phi : \mathbb{R} \rightarrow \mathbb{C}^\times$, where $\phi(r) = e^{2\pi i r}$. 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 4.3.3 (Correspondence Theorem)

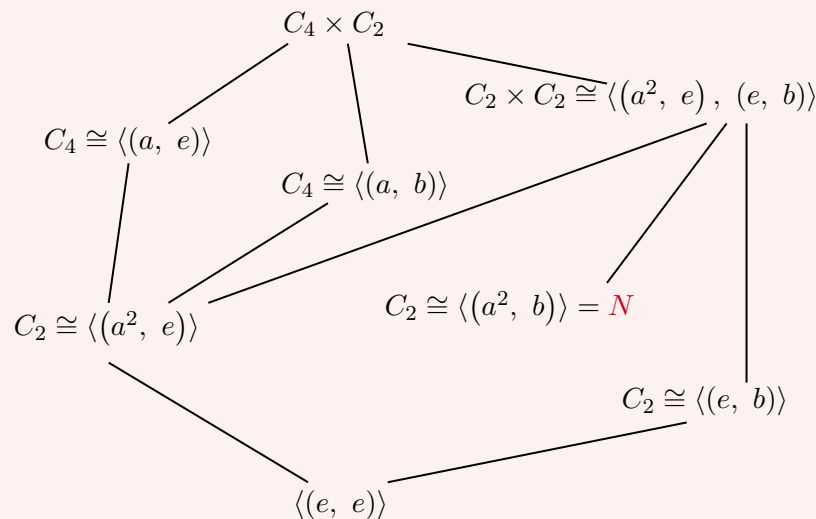
Let $N \trianglelefteq G$, then the subgroups of G/N are in bijective correspondence with subgroups of G containing N .

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 $\phi : G \rightarrow G/N$, that is, $\phi^{-1}(H) = \{g \in G : gN \in H\}$. We can check that this is a subgroup of G by checking the group axioms. We have closure by as $g_1, g_2 \in \phi^{-1}(H)$, 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 $\phi^{-1}(H)$ contains N , since $\forall n \in N$, $nN = N \in H$ (it's the identity coset). We can check that for $N \leq M \leq G$, $\phi^{-1}(M/N) = M$, and for $H \leq G/N$, $\phi^{-1}(H)/N = H$. So this correspondence is bijective. \square

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

Example 4.3.4

Suppose $C_4 = \{e, a, a^2, a^3\}$ and $C_2 = \{e, b\}$. Consider the group $C_4 \times C_2$. 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.

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

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 4.3.5 (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 G , and $HN = \langle H, N \rangle$ (the smallest subgroups of G containing H and N). Then consider the function $\phi : H \rightarrow HN/N$, with $\phi(h) = hN$. We can check this is a well defined, surjective homomorphism, and it's kernel is $N \cap H$, and we can apply the first isomorphism to get $H/(N \cap H) \cong HN/N \leq G/N$. \square

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

Theorem 4.3.6 (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 $\phi : G/N \rightarrow G/M$ by $\phi(gN) = gM$. ϕ is well-defined since $N \leq M$, and it's a surjective homomorphism. It's kernel is M/N , and thus by the first isomorphism theorem, $(G/N)/(M/N) \cong G/M$. \square

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

Example 4.3.7

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 4.4.1 (Simple Groups)

A group G is **simple** if its only normal subgroups are $\{e\}$ and G .

Example 4.4.2 (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 $\{1, 2, \dots, n\}$, 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 5.0.1 (Group Action)

Let G be a group, and let X be a set. An **action** of G on X is a function $\alpha : G \times X \rightarrow X$ 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 5.0.2

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 $1, 2, \dots, n$, we get an action on the set $\{1, 2, \dots, n\}$.
- (iii) The group D_{2n} acts on the vertices of a regular n -gon, and if we label these vertices $1, 2, \dots, n$, we get an action on the set $\{1, 2, \dots, n\}$.
- (iv) 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 5.0.3

For all $g \in G$ and an action $\alpha_g : X \rightarrow X$, 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. \square

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

Proposition 5.0.4

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

Proof. If α is an action, then by [Lemma 5.0.3](#), α_g is a bijection from $X \rightarrow X$, so $\alpha_g \in \text{Sym}(X)$. 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 $\rho : G \rightarrow \text{Sym}(X)$, we can define $\alpha : G \times X \rightarrow X$ by $\alpha(g, x) = \alpha_g(x) = \rho(g)(x)$. Then α is an action. This is true because $\rho(g) \in \text{Sym}(X)$, so $\rho(g)(x) = \alpha_g(x) \in X$, and $\rho(e)$ is the identity in $\text{Sym}(X)$ which implies $\rho(e)(x) = x$, and finally, $\rho(gh) = \rho(g)\rho(h)$ implies that $\alpha_{gh}(x) = \alpha_g \circ \alpha_h(x)$ for all $x \in X$. \square

We can make the notation slightly easier. When we write $\alpha_g : X \rightarrow X$, 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 5.0.5

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

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

Example 5.0.6

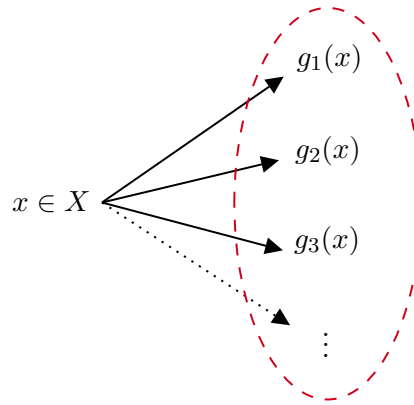
- (i) D_{2n} acting on $\{1, \dots, n\}$ (the labelled vertices on an n -gon) has $\ker \rho = \{e\}$, as every non-trivial element of D_{2n} moves at least one vertex. Thus $D_{2n} \leq S_n$.
- (ii) Let G be the symmetries of a cube, and consider X to be the set of unordered pairs of opposite faces. Then $|X| = 3$. So we get a homomorphism $\rho : G \rightarrow S_3$. 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 5.0.7 (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 5.1.1 (Orbit)**

Let G act on X , and let $x \in X$. The **orbit** of x is

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

Definition 5.1.2 (Stabilizer)

The **stabilizer** of x is

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

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

Example 5.1.3

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 $\text{Orb}(1) = \text{Orb}(2) = \text{Orb}(3) = \{1, 2, 3\}$, but $\text{Orb}(4) = \{4\}$. Also $\text{Stab}(1) = \{e, (2\ 3)\}$, $\text{Stab}(2) = \{e, (1\ 3)\}$, $\text{Stab}(3) = \{e, (1\ 2)\}$ and $\text{Stab}(4) = G$.

Lemma 5.1.4

For any $x \in X$, $\text{Stab}(x)$ is a subgroup of G .

Proof. We check the group axioms.

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

□

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 5.1.5

Let G act on X . Then the orbits partition X .

Proof. Firstly, for any $x \in X$, $x \in \text{Orb}(x)$. Secondly, if $z \in \text{Orb}(x) \cap \text{Orb}(y)$, 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 $g \in G$, $g(y) = (gg_2^{-1}g_1)(x) \in \text{Orb}(x)$. So $\text{Orb}(y) \subseteq \text{Orb}(x)$. Similarly, $\text{Orb}(x) \subseteq \text{Orb}(y)$. Thus orbits are either disjoint or equal. \square

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 $\{1, 2, \dots, n\}$ 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 5.1.6 (Orbit-Stabiliser Theorem)

Let a finite group G act on X . Then for any $x \in X$,

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

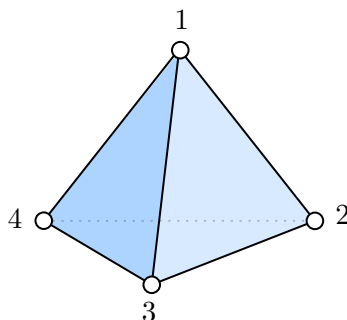
Proof. Note that $g(x) = h(x)$ occurs if and only if $h^{-1}g(x) = x$, that is, when $h^{-1}g \in \text{Stab}(x)$. Then this is true iff the cosets $g\text{Stab}(x) = h\text{Stab}(x)$. Rephrasing, distinct points in the orbit of x are in bijection with distinct cosets of $\text{Stab}(x)$. So $|\text{Orb}(x)|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

In particular, notice that all elements in a given coset $g\text{Stab}(x)$ do the same thing to x as g , as an element of this coset $g\text{Stab}(x)$ has the form gh , $h \in \text{Stab}(x)$, 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 $\{1, \dots, n\}$, so $|\text{Orb}(1)| = n$, and $\text{Stab}(1) = \{e, s\}$, as the first vertex is fixed by one reflection and the identity. Thus $|D_{2n}| = |\text{Orb}(1)| \cdot |\text{Stab}(1)| = n \cdot 2 = 2n$.

§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 $\rho : G \rightarrow S_4$.

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 $\text{Orb}(1) = \{1, 2, 3, 4\}$. 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 $\text{Stab}(1) \cong D_6$, the symmetries of a triangle.

With this information, then orbit stabiliser tells us that

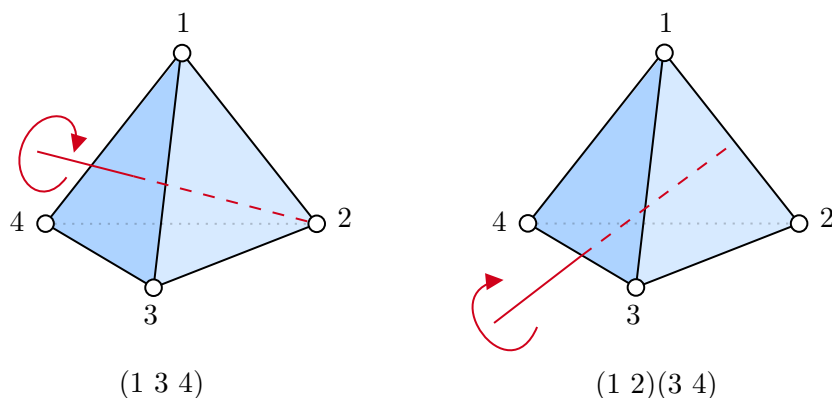
$$|G| = |\text{Orb}(1)| \cdot |\text{Stab}(1)| = 4 \cdot 6 = 24,$$

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

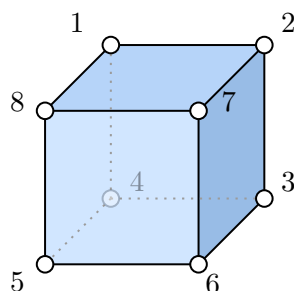
$$|G^+| = |\text{Orb}(1)| \cdot |\text{Stab}(1)| = 4 \cdot 3 = 12,$$

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



§5.1.2 Symmetries of the Cube

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

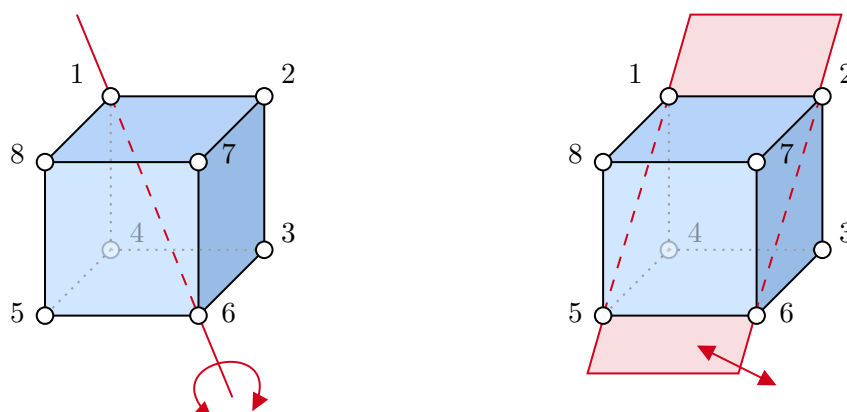


We have

- 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 $|\text{Orb}(1)| = 8$. 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 $|\text{Stab}(1)| = 6$. Then by the orbit-stabiliser theorem,

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

We will determine this group completely later.

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

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

Now if we let G^+ act on the four diagonals of the cube, giving $\rho : G^+ \rightarrow S_4$. We will have all 4-cycles in $\text{img } \rho$, and also all transpositions¹. 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 $G^+ \cong S_4$.

¹If you don't see why, I encourage you to draw a cube with a diagonal elongated, and see what the rotations do to it.

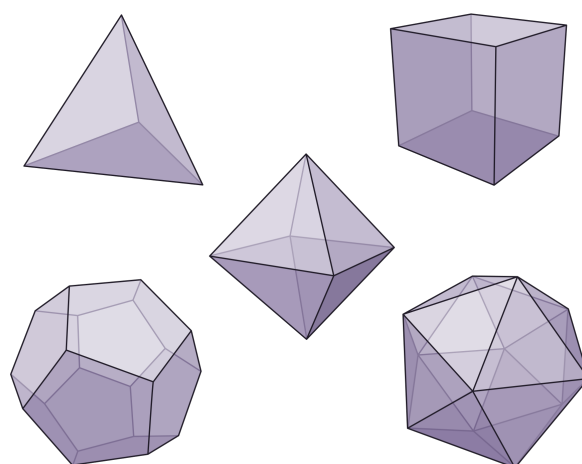
§5.1.3 Platonic Solids

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

Definition 5.1.7 (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 (vertex, incident edge, incident face).

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



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 dual. In fact, this dual 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 5.2.1 (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 $X \subseteq G^p$,

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

Informally, ‘ p -tuples multiplying to e ’. Note that $g \in G$ has order p if and only if $(g, \dots, g) \in X$ 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 $a(g_1, g_2, \dots, g_p) = (g_2, \dots, g_p, g_1)$. 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

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

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 $|\text{Orb}(e, e, \dots, e)| = 1$, 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, \dots, g) , so there exists some $g \neq e \in G$ such that $g^p = e$. \square

Bibliography

TODO: Make this proper.

- Napkin by Evan Chen – Used for a good few of the examples
- Abstract Algebra by Dummit and Foote – General Reference
- Undergraduate Algebra, Serge Lang – General Reference
- A Book of Abstract Algebra, Charles Pinter – General Reference and used in the development of Quotient Groups
- Dexter Chua and David Bai's notes – For a general view on the course structure before the lectures were completed, along with some of the proofs that were omitted from our lectures.