Groups

Adam Kelly

Updated November 6, 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

'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[1], 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.

[a] Some 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

[1] Apart from 'magmas' I suppose, but they don't tend to be a particularly useful notion.

$h * g = k * g = e$ follows analogously. □

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

Proposition 1.1.3 (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 1.1.4 (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 1.1.5 (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.

[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 1.1.6 (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 $0 \in Z$, 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 $\mathrm{GL}_n(\mathbb{R})$ be the set of $n \times n$ matrices with non-zero determinant. Then $(\mathrm{GL}_n(\mathbb{R}), \times)$ is the **general linear group**[a].

[a] Using matrix multiplication

Example 1.1.12 (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 1.1.13 (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 1.2.1 (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.
- $\mathrm{SL}_n(\mathbb{R}) \leq \mathrm{GL}_n(\mathbb{R})$ 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 $x, y \in H$. □

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 $n \in N$, 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 $nk_1 + nk_2 = n\left(k_1 + k_2\right) \in n\mathbb{Z}$.
- *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 1.2.5 (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 $K \subset H$, $K \leq H$. □

§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 $T = \langle X \rangle$. □

Example 1.2.8

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

[a] Note 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 $\phi : H \to G$. 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 1.3.1 (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 1.3.2 (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 1.3.3

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 1.3.4

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 $a \in \mathbb{R}^*$, $\phi(\log a) = e^{\log a} = a$.

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 $\phi : H \to G$ 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 1.3.6 (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 $H \cong H$ 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 1.3.7

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 $H = \{e^{2\pi ik/n} : 0 \leq k \leq n-1\}$ 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 $\phi : H \to G$ 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 1.3.10 (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 1.3.11 (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 1.3.12 (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 1.3.13
$\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, 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 1.3.14 (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 1.3.15 (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. □

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

$$\phi((h_1,k_1)\cdot(h_2,k_2)) = \phi(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = \phi(h_1,k_1)\phi(h_2,k_2).$$

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 1.2.9.

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 $G = \{e^{2\pi ik/n} : 0 \leq k \leq n-1\}$. 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 2.1.3 (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 2.1.4 (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 $\phi : C_n \to G$ 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 2.1.5

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 occuring 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, $n \mid k$. □

§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.

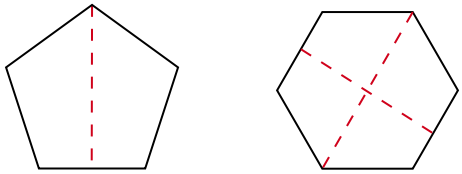
Definition 2.2.1

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.



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 2.2.3

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 $g(v_1)$ 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 2.2.4

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. □

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 rigerous 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

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

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 it's 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 $\sigma : X \to X$. The set of all permutations of X is denoted $\operatorname{Sym} X$.

Theorem 2.3.2

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 Sym X is a group. □

Definition 2.3.3 (Symmetric Group)

If $|X| = n$, we write S_n for (the isomorphism class of) 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 2.3.4

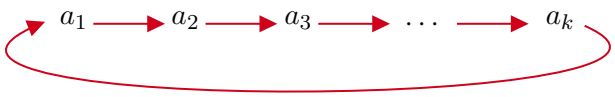
If we had some $\sigma \in S_3$ such that $\sigma(1) = 2$, $\sigma(2) = 3$, and $\sigma(3) = 1$, we would write

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

A slightly better notation for when we have a permutation that 'cycles' some elements $a_1, \cdots a_k \in \{1, 2, \ldots, n\}$ 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 2.3.5 (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

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

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

[a] This 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. □

Slightly more suprising 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.

[a] 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 $1, \sigma(1), \sigma^2(1), \dots$. 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 $1, \sigma(1), \sigma^2(1), \dots, \sigma^k(1)$ 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

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

and each $j \in \{1, 2, \dots, n\}$ 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. □

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 im as they are disjoint. By the fundamental theorem of orders, we must have $k_i \mid m$, and thus $m = \operatorname{lcm}(k_1, k_2, \dots, k_r)$ 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 2.3.13 (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

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

□

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 pairity 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 pairity is invariant with respect to σ.

Proof. Let's write $\chi(\sigma)$ for the number of cycles in σ in it's 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

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

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

Proposition 2.3.16

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

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 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 $\{1, 2, \dots, n\}$, we will restrict ourselves to functiosn that interact well with it's geometry.

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

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

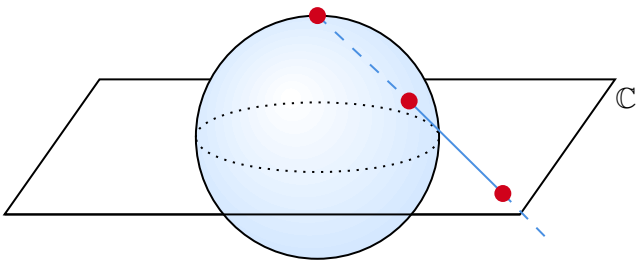
with $a, b, c, d \in \mathbb{C}$ and $ad - bc \neq 0$. We have this condition because

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

so if $ac - bc = 0$, 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 $f : \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ 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 2.4.2

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 2.4.3 (Möbius Group)

The set of Möbius maps forms a group 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.

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

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

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 $H = 2\mathbb{Z} \leq Z$. 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 $g_1 H = g_2 H$ or $g_1 \cap g_2 H = \emptyset$;

(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 $g_1 H \cap g_2 H \neq \emptyset$. Then there exists $g \in g_1 H \cap g_2 H$. So $g = g_1 h_1 = g_2 h_2$ for some $h_1, h_2 \in H$. Then $g_1 = g_2 h_2 h_1^{-1}$, so for any $h \in H$, we have $g_1 h = g_2 h_2 h_1^{-1}$, so for any $h \in H$, we have $g_1 h = g_2 h_2 h_1^{-1} h \in g_2 H$, so $g_1 H \subseteq g_2 H$. Similarity, $g_2 H \subseteq g_1 H$, thus $g_2 H = g_1 H$.

(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 3.0.5

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

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

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

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

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. □

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

Corollary 3.0.8
Groups of prime order are cyclic, and are generated by any non-idenetity 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 $\{1, 2, \dots n-1\}$ 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. □

§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 it's 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}.

Biblography

TODO: Make this proper.

- Napkin by Evan Chen – Used for a good few of the examples
- Abstract Algebra by Dummit and Foote – General Reference
- A Book of Abstract Algebra, Charles Pinter – General Reference
- 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.