# Groups

Adam Kelly

Michaelmas 2020, Updated October 14, 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.

During the creation of this document, I consulted a number of other books and resources. All of these are listed in the bibliography.

## Contents

**1 Groups** **2**
1.1 Definition of a Group . . . . . 2
1.2 Elementary Properties of Groups . . . . . 2
1.3 Examples of Groups . . . . . 3
1.4 Subgroups . . . . . 5
1.5 Generators . . . . . 6
1.6 Homomorphisms . . . . . 7

# §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** (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.

## §1.2 Elementary Properties of Groups

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

**Proposition 1.2** (Uniqueness of the Identity and Inverse)

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

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

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

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

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

**Proposition 1.3** (Cancellation Law)

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

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

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

**Proposition 1.4** (Computing Inverses)

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

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

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

*Proof.*

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

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

## §1.3 Examples of Groups

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

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

**Definition 1.5** (Abelian Groups)

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

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

**Example 1.6** (The Trivial Group)

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

**Example 1.7** (Additive Group of Integers)

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

$(\mathbb{Z}, +)$ 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 1.8** (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 1.9** (Non-zero Rationals)

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

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

**Example 1.10** (Multiplication Modulo $p$)

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

**Example 1.11** (General Linear Group)

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

[a] Using matrix multiplication

**Example 1.12** (Special Linear Group)

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

### Non-Examples of Groups

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

**Example 1.13** (Non-Examples of Groups)

The following are are all *not* groups.

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

## §1.4 Subgroups

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

**Definition 1.14** (Subgroups)

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

**Example 1.15** (Examples of Subgroups)

The following are subgroups.

- For any group $G$, we have the **trivial subgroups** $\{e\} \leq G$ and $G \leq G$.
- $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ with addition.
- $\{0, 2, 4, \dots\} \leq \mathbb{Z}$ with addition.
- $\mathrm{SL}_n(\mathbb{R}) \leq GL_n(\mathbb{R})$ 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 1.16** (Subgroup Criterion)

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

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

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

**Theorem 1.17** (Subgroups of $\mathbb{Z}$)

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

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

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

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

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

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

We can use the definition of a subgroup to proof some elementary facts about subgroups.

**Proposition 1.18** (Elementary Properties of Subgroups)

Let $G$ be a group.

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

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

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

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

(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 $K \subset H$, $K \leq H$. □

## §1.5 Generators

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

**Definition 1.19** (Subgroup Generated By A Subset)

For some set $X \subseteq G$, we define the **subgroup generated by** $X$, $\langle X \rangle$, to be the smallest subgroup of $G$ which contains $X$.

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

**Proposition 1.20**

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

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

**Example 1.21**

We have $(\mathbb{Z}, +) = \langle 1 \rangle = \langle 2, 3 \rangle$[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 1.22** (Generators)

If $X$ is a subset of $G$ such that $\langle X \rangle = G$, then we call $X$ a **generator** of $G$.

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

## §1.6 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 $\phi$ 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 $\phi$ would indeed preserve some of the structure of the group. This motivates the introduction of *homomorphisms*.

**Definition 1.23** (Homomorphism)

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

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

**Example 1.24** (Inclusion Function)

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

**Example 1.25**

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

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

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

**Example 1.26**

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

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

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

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

**Proposition 1.27** (Properties of Homomorphisms)

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

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

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

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

*Proof.*

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

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

(iii) We have

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

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

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

**Definition 1.28** (Isomorphism)

If a function $\phi : H \to G$ is bijection, and $\phi$ 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 1.29**

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

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

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

**Example 1.30** ($\mathbb{Z}$'s subgroups are isomorphic)

$\mathbb{Z} \cong n\mathbb{Z}$ for $n \in \mathbb{Z}$, as defined in Theorem 1.17.

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

**Proposition 1.31** (Inverses of isomorphisms are isomorphisms)

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

*Proof Sketch.* Check that $\phi^{-1}$ is a homomorphism. □

## 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.