Groups

Adam Kelly, Lectured by Dr. A. Khukhro

Michaelmas 2020

This document is an account of the Cambridge Mathematical Tripos course 'Groups', lectured by Dr. Ana Khukhro. in Michaelmas 2020. This is a work in progress, and is likely to to contain errors, which you may assume to be my own.

Contents

§1 Groups

§1.1 Definition

In this section we will formally introduce the notion of a group, and we will consider some examples of groups along with their basic properties.

Definition 1.1

A **group** is a set G with a binary operation $*$ on G such that:

- *Identity.* G has an **identity element** e such that $e * g = g * e = g$ for all $g \in G$.
- *Inverses.* Each element $g \in G$ has an **inverse**, that is, an element $g^{-1} \in G$ such that $g * g^{-1} = g^{-1} * g = e$.
- *Associativity.* The operation $*$ is associative, that is $(g * h) * k = g * (h * k)$ for any $g, h, k \in G$.

Remark (A pedantic point)**.** In some cases, people will add an additional 'closure' axiom, stating that if $g, h \in G$ then $g * h \in G$. However, this is redundant as it is implied by stating that $*$ is a binary operation on G. You must keep it in mind however when checking if something is a group.

Remark (Bracketing)**.** The 'associativity' axiom means that we can write $g * h * k$ without specifying what order it should be done first.

Notation. It's proper to state that '$(G, *)$ is a group', but this is regularily abbreviated to saying 'G is a group', whenever the operation being used is clear.

So that's what a group is, let's dive straight into some examples.

Example 1.2 (Examples of Groups)

The following are all examples of groups.

1. $G = \{e\}$, along with the binary operation $*$ satisfying $e * e = e$ (the 'trivial group').
2. G being the set of symmetries of a shape, along with $g * h$ defined to be 'performing h followed by g' where $g, h \in G$ is a group.
3. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are all groups.
4. The nonzero[a] real numbers $\mathbb{R}\backslash\{0\}$ with multiplication is a group.
5. $(\mathbb{R}, *)$ where $r * s = r + s + 5$ for any $r, s \in \mathbb{R}$ is a group.
6. $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ with addition modulo n is a group.
7. A vector space with vector addition is a group.
8. The set of invertible 2×2 matrices with real coefficients, $GL_2(\mathbb{R})$ is a group with respect to matrix multiplication.

[a] You should consider why we need to exclude zero for $\mathbb{R}$ to be a group.

Proof Sketch. Check that each construction satisfies all of the axioms stated in the def-

inition of a group. □

Let's also look at some structures that are *not* groups.

Example 1.3 (Non-Examples of Groups)
The following are all *not* groups.

1. $G = \{0, 1, 2, \dots, n-1\}$ with addition.
2. $(\mathbb{Z}, \times)$.
3. $(\mathbb{R}, *)$ where $r * s = r^2 s$ for $r, s \in \mathbb{R}$.
4. $G = \{0, 1, 2, \dots\}$ and the operation $*$ such that $m * n = |n - m|$ for $m, n \in G$.

Notation. We often write $g \cdot h$ or gh for $g * h$, where $*$ is the group's binary operation.

§1.2 Direct Consequences of the Definition

Let's look at some easy consequences of the group axioms.

Proposition 1.4
Let G be a group, and let g be any element of G.

(i) The identity element is unique.

(ii) The inverse of g is unique.

(iii) If $g * h = g$, then $h * g = g$ and $h = e$.

(iv) If $g * h = e$, then $h * g = e$ and $e = g^{-1}$.

(v) $(gh)^{-1} = h^{-1} g^{-1}$.

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

Proof. We will prove each in order.

(i) Suppose that e and e' are both identity elements. Then

$$e * e' = e \quad \text{and} \quad e * e' = e',$$

hence $e = e * e' = e'$.

(ii) Suppose that $g * h = e$ and $gk = e$. Then

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

(iii) If $g * h = g$ then we have

$$\begin{aligned} & g * h = g \\ \implies & g^{-1} * g * h = g^{-1} * g \\ \implies & h = e. \end{aligned}$$

(iv) If $g * h = e$ then

$$\begin{aligned} & g * h = e \\ \implies & g^{-1} * g * h = g^{-1} * e \\ \implies & h = g^{-1}. \end{aligned}$$

(v) We have

$$(g * h) * (h^{-1}g^{-1}) = g * h * h^{-1} * g^{-1} = g * g^{-1} = e,$$

thus $(gh)^{-1} = h^{-1}g^{-1}$ by definition.

(vi) Note that $g * g^{-1} = e$, so g is the inverse of g^{-1} which is unique by (ii), so $g = (g^{-1})^{-1}$.

□

Definition 1.5

A group G is **abelian** (or commutative) if $\forall g, h \in G$, $g * h = h * g$.

Definition 1.6

A group G is **finite** if it has a finite number of elements, and it is **infinite** otherwise. The number of elements of G is the **order** of G, written $|G|$.

§1.3 Subgroups

Given any mathematical object, it's typically useful to know about its 'subobjects'.

Definition 1.7

Let $(G, *)$ be a group., A subset $H \subseteq$ is called a **subgroup** of G if $(H, *)$ is also a group. We write this as $H \leq G$.

Remark. To check if $H < G$ is a subgroup, we can just check

1. Closure (ie. $\forall h_1, h_2 \in H$, $h_1 * h_2 \in H$).
2. Identity (ie. $e \in H$).
3. Inverses (ie. $\forall h \in H$, $h^{-1} \in H$).

We note that there is no need to check that $*$ is associative, as it is inherited from the fact G is a group.

Example 1.8

The following are all subgroups.

- $\{e\} \leq G$, the 'trivial subgroup'.
- $G \leq G$.
- $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$.

- If $G = \{\text{symmetries of } \triangle\}$ then $\{e, s\} \leq G$ and $\{e, r, r^2\} \leq G$.

Lemma 1.9 (Fast Subgroup Checking)

Let G be a group. $H \leq G$ is a subgroup if and only if H is non-empty and for all $a, b \in H$, $ab^{-1} \in H$.

Proof. Exercise. □

Let's investigate some subgroups of $\mathbb{Z}$.

Proposition 1.10

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

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

- 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 $H = n\mathbb{Z}$. □

Proposition 1.11

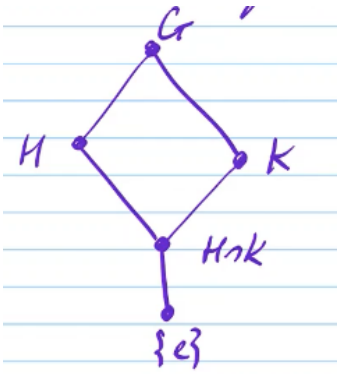
(i) Let H, K be subgroups of a group G. Then $H \cap K \leq G$.

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

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

Proof. Exercise. □

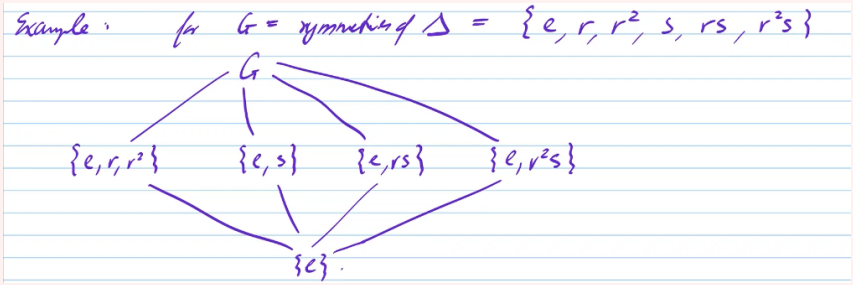
A useful way to think about subgroups is via a diagram, as follows. This is known as a "Lattice of subgroups".



An ascending edge or sequence of edges implies the lower subgroup is contained in the upper.

Example 1.12 (Subgroup Lattice for Triangle Symmetries)

We have the following lattice



Definition 1.13

Let X be a non-empty subset of a group G, then the **subgroup generated by** X, denoted $\langle X \rangle$, is the intersection of all subgroups containing X. Equivalently, it is the smallest subgroup of G containing X.