Groups

Adam Kelly

October 13, 2020

1 What is a Group?

'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. A *group* is a set G with a binary operation[2] $*$ which satisfies the axioms:

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

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

In the next 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).

[1]Apart from 'magmas' I suppose, but they don't tend to be a particularly useful notion.
[2]Some texts include an additional *closure* axiom, but this is implied by $*$ being a binary operation on G.

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.

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 $(g^{-1})^{-1} = g$. □

Theorem 1.5 (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* $b = c$.

It is worth noting though that we cannot (in general) cancel $a * b = c * a$.

With the notion of a group now defined, we can consider some non-trivial examples of groups.

Example 1.6 (Non-Examples of Groups)**.**

- The pair $(\mathbb{Q}, \cdot)$ is *not* a group. The element $0 \in \mathbb{Q}$ does not have an inverse.

Example 1.7 (Examples of Groups)**.** The following are all groups.

1. The additive group of integers, $(\mathbb{Z}, +)$.
2. $(Z, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$