Abelian Groups and Subgroups

AMP Day 3

Jonathan Alcaraz

Mike mentioned that we sometimes denote groups by just the set G without specifying exactly the binary operation. In this vain, we often drop the operation all together. For example in the group $(G, \star)$, we often write gh instead of $g \star h$. This notation should evoke the feeling of multiplication of real numbers. In that vain, we also use the notation:

$$g^k = \underbrace{g\, g \cdots g}_{k \text{ times}}$$

and $g^{-k} = (g^{-1})^k$.

Toy Example

Consider the following subset of $\mathbb{C}$:

$$\{1, i, -1, -i\}$$

This forms a group under the operation of **complex multiplication**. Explicitly, we can make a table for the operation as:

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

From this table, we can observe that the element 1 is the identity and every element has an inverse. Moreover, we know that the operation is associative since we know that complex multiplication is associative.

One further observation is that we can get to every element in this group by taking powers of i:

$$\begin{aligned} i^0 &= 1 \\ i^1 &= i \\ i^2 &= -1 \\ i^3 &= -i \\ i^4 &= 1 \\ &\vdots \end{aligned}$$

Definition

We say a group G is **cyclic** if there is some element $g \in G$ such that for any element $h \in G$, we can write:

$$h = g^k$$

for some integer k. We say G is **generated by** g.

Examples — Cyclic Groups

Some cyclic groups we've seen before:

- $\mathbb{Z}$ is generated by 1.
- The group above is generated by i.

Our new favorite examples:

Consider the set

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

endowed with the operation known as **modular arithmetic**. Explicitly,

$$m +_n k = \begin{cases} m + k & \text{if } m + k < n \\ m + k - n & \text{if } m + k \geqslant n \end{cases}$$

We call this group the **integers modulo** n. $\mathbb{Z}_n$ is a cyclic group generated by 1.

Definition

A group G is said to be **abelian** if for any $a, b \in G$,

$$ab = ba$$

This is named after Norwegian mathematician **Niels Henrik Abel**, but we don't capitalize it for some reason.

Most of the groups we've seen so far have this property. Including the toy example above. Later, we'll see a non-example. For now:

Exercise

Prove that any cyclic group must abelian.

You proved that cyclic groups are abelian. You might ask whether all abelian groups are cyclic. Here's an example to show that's not true.

Example — Non-cyclic abelian group

Consider the set

$$K = \{e, a, b, c\}$$

and we can define the operation with the table:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

This group is called the **Klein 4-group**. K is not cyclic since any element squares to the identity.

You might be starting to think that all groups are abelian. Here's an example:

Examples — Non-abelian

- Consider the set

  $$Q = \{\pm 1, \pm i, \pm j, \pm k\}$$

  These elements have the property:

  $$i^2 = j^2 = k^2 = ijk = -1$$

  From this, we *could* write up a whole table, but that would take a lot of time. We call this group the **quaternian group**.

- The so-called **Rubik's group** which is the group of moves you can make on a Rubik's cube.

Definition

Given a group $(G, \star)$, a subset $H \subseteq G$ is a **subgroup** of G if $(H, \star)$ is a group. That is

- The identity $e \in H$.
- Given $h_1, h_2 \in H$, the product $h_1 h_2 \in H$.
- If $h \in H$, then $h^{-1} \in H$.

Notice, we don't need to check associativity, since that's inherited from the ambient group G.

Example

$\{1, i, -1, -1\}$ is a subgroup of Q.

Exercise

Let G be any group and g any element of G. Consider the following set:

$$\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$$

Prove that $\langle g \rangle$ is a subgroup of G. We call $\langle g \rangle$ the **cyclic subgroup** of G generated by g.