Examples of groups

Some familiar groups

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are abelian groups under $+$.

- $\mathbb{Q}^\times = \mathbb{Q}\setminus\{0\}$, $\mathbb{R}^\times = \mathbb{R}\setminus\{0\}$, and $\mathbb{C}^\times = \mathbb{C}\setminus\{0\}$ are abelian groups under $\cdot$.

- Any vector space is an abelian group under $+$.

<u>Note</u>: When the group operation is $+$, we write the inverse of $g \in G$ as $-g$, not g^{-1}!

<u>Note</u>: We'll usually refer to a group $(G, *)$ by only referencing the set G, leaving the group operation $*$ implicit.

Integers modulo n

Let $n \in \mathbb{N}$. Congruence modulo n partitions $\mathbb{Z}$ into equivalence classes $[a]$ for $a \in \mathbb{Z}$, where

$$a \in [b] \iff a \equiv b \pmod{n} \iff [a] = [b]$$

Let's define a binary operation $+$ on equivalence classes by

$$[a] + [b] = [a+b]$$

This is well-defined!

<u>From Math 3345</u>: If $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then $a+b \equiv c+d \pmod{n}$.

<u>Translates to</u>: If $[a] = [c]$ and $[b] = [d]$, then $[a]+[b] = [a+b] = [c+d] = [c]+[d]$. ✓

Let $\mathbb{Z}_n$ be the set of all equivalence classes. Then $(\mathbb{Z}_n, +)$ is a group because

1. $+$ is associative,
2. $[0]$ is the identity, and
3. the inverse of $[a]$ is $[-a]$.

Since $+$ is commutative, $\mathbb{Z}_n$ is abelian.

<u>Note</u>: A complete list of equivalence classes is $[0], [1], \ldots, [n-1]$.

When the context is clear, we drop the brackets and write

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

<u>Alternative notations</u>: $\mathbb{Z}/n$ or $\mathbb{Z}/n\mathbb{Z}$.

Ex: In $\mathbb{Z}_4 = \{0,1,2,3\}$, the addition can be visualized as

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

This is called the <u>Cayley table</u> of the group $\mathbb{Z}_4$.

From looking at the Cayley table, we can easily see that $\mathbb{Z}_4$ is abelian.

Why? It is symmetric across the main diagonal.

What else do we notice...?

Multiplication modulo n

$\mathbb{Z}_n$ is not a group under multiplication.

But $\cdot$ is associative and 1 (really, $[1]$) is the identity, so the only problem is inverses.

So, define

$$U(n) = \{[a] \in \mathbb{Z}_n \mid [a] \text{ has an inverse under } \cdot\}$$

to be the group of units in $\mathbb{Z}_n$.

(Note: "unit" means "invertible element")

Ex: In $\mathbb{Z}_4$,

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

So $U(4) = \{1, 3\}$ with Cayley table

$\cdot$	1	3
1	1	3
3	3	1