Introduction to Groups

Definition. A **group** is a set G with a **binary operation** $\circ : G \times G \to G$ satisfying the following three properties.

(Associative) $(a \circ b) \circ c = a \circ (b \circ c) \qquad = a \circ b \circ c$

(Identity Exists) There is an **identity element** $e \in G$ with $e \circ g = g \circ e = g$ for all $g \in G$.

(Inverses Exist) Every element $g \in G$ has in **inverse** $g^{-1} \in G$ with $g^{-1} \circ g = g \circ g^{-1} = e$.

Comments:

We'll usually write $\circ$ as either multiplication or addition.
e.g. Instead of "$a \circ b$" we'll write "$a + b$" or "$a \cdot b$" or just "ab".

Using "e" for the identity element comes from German *Einheit* meaning "unit" or "identity".
If we write $\circ$ as multiplication, then we will *usually* write "1" for the identity (instead of e).
If we write $\circ$ as addition, then we will *usually* write "0" for the identity (instead of e).
If we write $\circ$ as addition, then we *usually* write "$-g$" for inverse instead of g^{-1}.

Definition. If $a \circ b = b \circ a$ for all $a, b \in G$ then we say G is "**commutative**" or "**abelian**".

If a group is commutative, then we will often use the "+" sign to denote the group operation. If a group is not commutative, then please do not use the "+" sign. Sometimes people like to use weird symbols for the group operation like $\otimes$, $\boxtimes$, $\oplus$, etc. That's fine, too.

If you have something like a group but not associative, that's called a **magma**. If you have something like a group but without inverses, that's called a **monoid**. Those are all cool, but we aren't studying them here.

Basic properties of groups.

There can be only one identity element in a group!
Proposition. *If two elements satisfy the property to be a group identity, then they are equal.*

There can be only one inverse for each group element!
Proposition. *If two elements satisfy the property to be the inverse of g then they are equal.*

Inverses satisfy a universal property. The inverse of g is **the** element which composes with g to give e. If you use mysterious means to find such an element, then it is the inverse of g. Congratulations.

The inverse of a composition is the composition of inverses, in reverse order.
Proposition. $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$

Double inverse undoes itself.
Proposition. $(a^{-1})^{-1} = a$

Identity is its own inverse.
Proposition. $e^{-1} = e$

Division is unique (on either side).
Proposition. *Given elements $a, b \in G$ there are unique $x, y \in G$ with $ax = b$ and $ya = b$.*

Since multiplication is often not commutative ($ab \neq ba$), division could be different on the two sides! Computer algebra systems write $x = b \backslash a$ for "a divided by b on the left" and $y = a/b$ for "a divided by b on the right"

We can cancel on left and right.
Proposition. *Given $a, b, c \in G$, if $ba = ca$ then $b = c$; similarly if $ab = ac$ then $b = c$.*

Definition. We use the following **exponential notation** where $n \in \mathbb{N}$ is a positive integer.

- $g^0 = e$
- $g^n = \underbrace{g \circ g \circ \cdots \circ g}_{n \text{ times}}$
- $g^{-n} = \underbrace{g^{-1} \circ g^{-1} \circ \cdots \circ g^{-1}}_{n \text{ times}}$

If G is commutative, and we are using "+" for the group operation, then we will instead write multiplicatively $0g = 0$, $ng = g + g + \cdots + g$, $-ng = (-g) + (-g) + \cdots + (-g)$.

Integer powers all make sense.
Proposition. *The expected exponential laws are true.*

- $g^n \circ g^m = g^{n+m}$
- $\left(g^n\right)^m = g^{nm}$
- $\left(g^{-1}\right)^n = \left(g^n\right)^{-1}$

Other interesting properties.

I'm going to stop writing $\circ$ for the group operation, because it takes too much space.

Definition. The product $[a, b] = aba^{-1}b^{-1}$ is called the **commutator** of a and b.

Commutators measure whether elements commute.
Proposition. *$aba^{-1}b^{-1} = e$ if and only if $ab = ba$.*

Inverses reverse the order of commutators.
Proposition. $[a, b]^{-1} = [b, a]$

Definition. The product aba^{-1} is called the **conjugate** of b by a.

Powers of conjugates are conjugates of powers.
Proposition. $\left(aba^{-1}\right)^n = ab^n a^{-1}$

Conjugates of commutators are commutators of conjugates.
Proposition. $g\,[a, b]\,g^{-1} = [gag^{-1}, gbg^{-1}]$

Definition. An element $g \in G$ which commutes with all other elements is called **central**.

We can find central elements using conjugation!
Proposition. *An element is central if and only if $ghg^{-1} = h$ for all $h \in G$*

The **center** of G is the set of popular guys that get along with everyone. (Z is for German: "*Zentrum*"!)
Definition. The **center** of a group is $Z(G) = \{g \mid g \text{ commutes with all elements of } G\}$