Some things that you can do in a group: (let $G$ be a group).

1. **Cancel:** If $a * b = a * c$, then $b = c$.
   
   **Proof:** Multiply on the left by $a^{-1}$:
   
   $a^{-1} * (a * b) = (a^{-1} * a) * b = e * b = b$
   
   Likewise, if $b * a = c * a$, then $b = c$.

   **Caution:** $a * b = c * a$ does not imply $b = c$ (unless the group is abelian).

2. Solve for $x$ in $a * x = b$:
   
   Multiply both sides on the left by $a^{-1}$:
   
   $a^{-1} * (a * x) = (a^{-1} * a) * x = e * x = x$
   
   $a * x = b$
   
   $x = a^{-1} * b$.

   **Converse:** for $(a^{-1} * x = b)$.

**Useful Facts in Groups:**

1. $e * e = e$
   
   **Proof:** $e^{-1} * e = e$

2. $(x^{-1})^{-1} = x$ \( \forall x \in G \)
   
   **Proof:** $(x^{-1}) * x^{-1} = e = x * x^{-1}$, Now cancel $x^{-1}$ to get $(x^{-1})^{-1} = x$.

3. $(x * y)^{-1} = y^{-1} * x^{-1}$ \( \forall x, y \in G \)
   
   **Proof:** $(x * y) * (y^{-1} * x^{-1}) = (x * (y * y^{-1})) * x^{-1} = (x * e) * x^{-1} = x * x^{-1} = e$

   Also $(x * y) * (x * y)^{-1} = e$

   $(x * y) * (x * y)^{-1} = (x * y) * (y^{-1} * x^{-1})$. Now cancel $x * y$ from the left,

   **Follows from the assoc. law:**

   $(x * y) * (y^{-1} * x^{-1}) = ((x * y) * y^{-1}) * x^{-1} = (x * (y * y^{-1})) * x^{-1}$

   **There is a general associative law:** $x_1 * x_2 * \ldots * x_n$ is the same
Two More Examples of Groups

(1) \( \forall n \in \mathbb{Z}^+ \), \( \mathbb{Z}_n = \{ z \in \mathbb{C} : z^n = 1 \} \) is a group, under multiplication of complex numbers. It is closed under multiplication because

\[ \mathbb{Z}_n \times \mathbb{Z}_n \Rightarrow z^n w^n = 1 \Rightarrow (z w)^n = z^n w^n = 1 \cdot 1 = 1 \Rightarrow z w \in \mathbb{Z}_n \]

It is associative (inherited from properties of \( \mathbb{C} \)). It has an identity element \( 1 \in \mathbb{Z}_n \), and it is closed under taking inverse: \( z \in \mathbb{Z}_n^* \Rightarrow z^{-1} : \)

\[ (z^{-1})^n = \frac{1}{z^n} = \frac{1}{1} = 1 \Rightarrow z^{-1} \in \mathbb{Z}_n \]

(2) \( \forall n \in \mathbb{Z}^+ \), \( \mathbb{Z}_n \) is a group.

Proof: \( \mathbb{Z}_n \cong \mathbb{U}_n \) (p. 18 middle & bottom).

as binary structures.

Since \( \mathbb{U}_n \) is a group, so is \( \mathbb{Z}_n \). (See end of Example 9.2.)

(\( Y_1, Y_2, Y_3 \) are structural properties.)

Def: Two groups are isomorphic if they are isomorphic as binary structures. An isomorphism of groups is an isomorphism of binary structures. A bijection that has the homomorphism property.

Def: The order of a group \( G \) (or \( \langle G, * \rangle \)) is the number of elements of \( G \), denoted \( |G| \) (as with cardinalities).

Example: \( \mathbb{Z}_n \) is a group of order \( n \), \( \forall n \in \mathbb{Z}^+ \).

Def: A group \( G \) is finite if the set \( G \) is finite, and infinite otherwise.
Groups via Tables

For a (small) finite group, we can give its group operation by listing its value for each pair of elements, usually in the form of a table.

Example: Groups of order 3.

Let $G$ be a group of order 3. Call the identity element $e$, and call the other $a$ and $b$, so $G = \{e, a, b\}$.

1. The row & column for $e$ must be filled in as indicated, since $x \cdot e = e \cdot x = x$ for all $x \in G$.

Since equations $c \cdot x = d$ can be solved uniquely for each $d$, the row labeled $c$ must contain each element of $G$ exactly once.

Likewise for columns (using $x \cdot c = d$). Can only have a here because $b \cdot e$ already appear in that column.

These two entries can be filled in by looking at what's missing in each of their rows.

Is this a group? Isomorphic to $\mathbb{Z}_3$, with:

- $e \leftrightarrow 0$
- $a \leftrightarrow 1$
- $b \leftrightarrow 2$.

...it's a group.

In general, you would need to check associativity by hand. (Very tedious!)

Since the table is symmetric (about its diagonal, as in matrices), the group is abelian.
A Word on Notation.

Up until now we've been using a variant of multiplicative notation. We've called written the group operation "x" and inverse of x is written x⁻¹ (both uses x⁻).

Multiplicative notation: Write the binary operation as x or • or nothing (a x b or a b or just ab), write the inverse of a as a⁻¹, and the identity element as e or 1.

This is handy for \( (\mathbb{Q}^+, \times) \), \( (\mathbb{R}^+, \times) \), \( (\mathbb{C}^+, \times) \), \( U_1 \) on \( \mathbb{Cn} \), or \( \text{GL}_n(\mathbb{R}) \) (~ \( \text{GL}(n, \mathbb{R}) \)).

Additive notation: Write the binary operation as +, write the inverse of a as -a, and the identity element as 0.

This is handy for \( (\mathbb{Z}, +) \), \( (\mathbb{Q}, +) \), etc., and \( (\mathbb{Z}_n, +n) \).

Additive notation can only be used for abelian groups.

Next: Subgroups.