2. Groups

2.1 Definitions

There are many situations where we encounter seemingly different objects, but where the same set of "rules" is obeyed. So even though they may appear different, there will be certain properties shared.

Definition

A **group** is a set $G$ together with an operation $*$ on $G$ (a way of combining elements) of $G$ together such that:

1. **G is closed under this operation:**

   $a * b \in G$ for all $a, b \in G$

2. The operation is associative:

   $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$

3. **G contains an identity element:**

   $\exists e \in G \text{ s.t. } a * e = a = e * a$ for all $a \in G$.

4. **G is closed under inverses:**

   For each $a \in G$ there exists some element $a^{-1} \in G$ s.t.

   $a * a^{-1} = e = a^{-1} * a$. 
Often the operation is understood, & we write simply \( ab \) instead of \( a \times b \).

Sometimes, we might need to be clear what operation is being used, then we might write it out.

**IF** the operation is commutative, i.e.,

\[
ab = ba \text{ for all } a, b \in G,
\]

then \( G \) is said to be an abelian group or a commutative group.

**Ex:** The group of symmetries of a square.

- \( G \) is a set of 8 functions.
- The operation is composition of functions.

**Definition**

The order of a group is \( \# \) of elements in the group (or cardinality of the group if it is infinite).

Write: \( \# G \) or \( |G| \) or \( o(G) \)

**Ex:** If \( G \) = symmetries of a square then \( \# G = 8 \).
Generic group notations

When talking about a generic group, we usually use a "multiplicative-type" notation for group operation, i.e., write

\( ab \) for \( a \cdot b \)
\( a^{-1} \) for inverse element
\( e \) for identity element

On the other hand, when talking specifically about an abelian group, we often use an "additive-type" notation, i.e., write

\( a + b \) for \( a + b \)
\( -a \) for inverse element
\( 0 \) for identity element

In either case, this is just a notation to denote an operation. The actual operation might be an actual kind of multiplication or addition, or something much more exotic, like composition of functions.
Examples

a. \( \mathbb{Z} = \{ \ldots, -1, 0, 1, \ldots \} \) under + (abelian)

b. \( \mathbb{R} \) (real line) under + (abelian)

Example
Consider \( \mathbb{Z} \) under multiplication:

1. Closed under multiplication \( \checkmark \)
2. Multiplication is associative \( \checkmark \)
3. \( \exists \) identity: \( 1 \cdot n = n \cdot 1 = n \) \( \forall n \) \( \checkmark \)
4. Inverses: NO.

\( \not\exists \) integer \( n \) s.t. \( 2n = 1 \).

Not a group.
Example
Try \( \mathbb{R} \) under multiplication.

Now 2 has an inverse: \( 2 \cdot \frac{1}{2} = 1 \)

But 0 does not: \( \forall x \text{ s.t. } 0x = 1 \)

Example
\( \mathbb{R}^* = \mathbb{R} \setminus \{0\} = \{ x \in \mathbb{R} : x \neq 0 \} \) under multiplication.

Exercise: This is a group (\& is abelian)
Example

Set $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$.

Define $m \ast n = mn \mod 5$

where $k \mod 5 = \text{remainder when } k \text{ is divided by } 5$.

\[
12 \mod 5 = 2 \\
28 \mod 5 = 3 \\
30 \mod 5 = 0 \quad \text{etc}
\]

This operation $\ast$ is a "multiplicative-like" operation.

Exercise: $\mathbb{Z}_5^*$ is a group under $\ast$.

(i.e. abelian)
Example: An abelian group that contains 6 elements.

\[ \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\} \] (This is not exactly the def of \( \mathbb{Z}_6 \) that we'll use later.

Operation: \( m \oplus n = m + n \mod 6 \).

"Multiplication" (Addition) table:

\[
\begin{array}{cccccc}
\oplus & 0 & 1 & 2 & 3 & 4 & 5 \\
\hline
0 & 0 & 1 & 2 & 3 & 4 & 5 \\
1 & 1 & 2 & 3 & 4 & 5 & 0 \\
2 & 2 & 3 & 4 & 5 & 0 & 1 \\
3 & 3 & 4 & 5 & 0 & 1 & 2 \\
4 & 4 & 5 & 0 & 1 & 2 & 3 \\
5 & 5 & 0 & 1 & 2 & 3 & 4 \\
\end{array}
\]

Commutative!

\[ 3 \oplus 3 = 0 \] so the inverse of 3 is 3.

We are writing "additively," so we denote inverses by

\[ -3 = 3 \]

Similarly:

\[ -1 = 5 \]
\[ -2 = 4 \]
\[ -3 = 3 \]
\[ -4 = 2 \]
\[ -5 = 1 \]
\[ -0 = 0 \]

Exercise: Show \( \oplus \) is associative \((m \oplus n) \oplus k = m \oplus (n \oplus k)\) Not trivial.
Example

Let

\[ GL_n(\mathbb{R}) = \{ A : A \text{ is an invertible } n \times n \text{ matrix} \} \]

(we'll assume matrices have real entries, but this works for complex entries as well).

Exercise: \( GL_n(\mathbb{R}) \) is a group under matrix multiplication.

Show that \( GL_1(\mathbb{R}) = \mathbb{R}^* \), the set of nonzero real nos. under ordinary multiplication.

Show that \( GL_n(\mathbb{R}) \) is nonabelian \( \forall n \geq 2 \).
Examples: The affine group ("ax+b group")

Given $a, b \in \mathbb{R}$, $a \neq 0$, define

$$T_{a,b} : \mathbb{R} \rightarrow \mathbb{R} \text{ by } T_{a,b}(x) = ax + b$$

Let

$$G = \{ T_{a,b} : a, b \in \mathbb{R}, a \neq 0 \}$$

Claim: $G$ is a group under composition of functions.

Closure under composition

$$(T_{a,b} \circ T_{c,d})(x) = T_{a,b}(T_{c,d}(x))$$

$$= T_{a,b}(cx + d)$$

$$= a(cx + d) + b$$

$$= acx + ad + b$$

$$= T_{ac, ad+b}(x).$$

So

$$T_{a,b} \circ T_{c,d} = T_{ac, ad+b} \in G.$$
Exercise: Show \( T_{1,0} \) is an identity element.

Find \( (T_{a,b})^{-1} \)

Why don't we have to worry about associativity?

Thus, \( G \) is a group.

Exercise: Show \( G \) is nonabelian.

Remark
Not every operation is associative!

Example
Consider subtraction on \( \mathbb{R} \):

\[
(a-b) - c \neq a - (b-c)
\]
Power of an element

Let \( a \in G \). Then we set

\[
a^n = a \cdots a \quad \text{for } n \geq 1
\]

\[
a^0 = e
\]

\[
a^{-n} = a^{-1} \cdots a^{-1} \quad \text{for } n \geq 1
\]

\[
= (a^{-1})^n.
\]

Note: We use "multiplicative" notation when we are talking about general groups. If we know the operation is more like "addition" then we use an additive notation.

\[
a + \cdots + a = na \quad \text{instead of } a^n, \text{ call these multiples instead of powers}
\]

\[
-\ a \text{ instead of } a^{-1}
\]

\[
-\ a - \cdots - a = -na \text{ instead of } a^{-n}
\]
Ex. In the group $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ under multiplication.

Powers of 2:

\[
\begin{align*}
2^0 &= 1 & 2^{-1} &= \frac{1}{2} \\
2^1 &= 2 & 2^{-2} &= \frac{1}{4} \\
2^2 &= 4 &= 2 \cdot 2 \\
2^3 &= 8 &= 2 \cdot 2 \cdot 2 \\
\vdots & & \vdots
\end{align*}
\]

In the group $\mathbb{Z}$ under addition

"Powers" of 2:

Multiples

\[
\begin{align*}
0 \cdot 2 &= 0 \\
1 \cdot 2 &= 2 \\
2 \cdot 2 &= 4 = 2 + 2 \\
3 \cdot 2 &= 6 = 2 + 2 + 2 \\
-1 \cdot 2 &= -2 \\
-2 \cdot 2 &= -4 = -2 + -2 \\
\vdots & & \vdots
\end{align*}
\]
Ex. In the group $\mathbb{Z}_7 = \{0, 1, \ldots, 6\}$ under $+ \mod 7$

\[
\begin{align*}
0 \cdot 2 &= 0 \\
1 \cdot 2 &= 2 \\
2 \cdot 2 &= 4 \\
3 \cdot 2 &= 6 \\
4 \cdot 2 &= 1 \\
5 \cdot 2 &= 3 \\
6 \cdot 2 &= 5 \\
7 \cdot 2 &= 0 & \text{then they repeat!}
\end{align*}
\]

-2 = 5 because 2 + 5 = 0
-4 = -2 - 2 = 5 + 5 = 3

Ex. In the group $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ under $\cdot \mod 7$

\[
\begin{align*}
2^0 &= 1 \\
2^1 &= 2 \\
2^2 &= 4 \\
2^3 &= 8 \equiv 1 \\
\end{align*}
\]

Then the powers repeat. There are only 3 possible powers!

\[
\{2^n \mod 7 : n \in \mathbb{Z}\} = \{1, 2, 4\}
\]
2.2 Some Simple Remarks

Theorem
Let $G$ be a group. Then the following statements hold.

a. Cancellation Laws: $xa = xb \Rightarrow a = b$
and $ax = bx \Rightarrow a = b$

b. The identity element is unique.

c. Each $a$ in $G$ has a unique inverse $a^{-1} \in G$.

d. $(a^{-1})^{-1} = a$

e. $(ab)^{-1} = b^{-1}a^{-1}$.

Proof:
a. If $xa = xb$, then

$$x^{-1}(xa) = (x^{-1}x)a = e a = a$$

$$x^{-1}(xb) = (x^{-1}x)b = e b = a$$

The other cancellation law is similar.
b. Suppose $e$ & $f$ were both identity elements. Then

$$\forall a \in G, \ ae = a = ea \quad \& \quad af = f = fa$$

(*)

Hence

$$fe = f \quad \text{by (*)}$$

$$fe = e \quad \text{by (**)}$$

So $e = f.$

c. Suppose $b$ & $c$ were both inverses of $a$. Then

$$ba = e = ab \quad \& \quad ca = e = ac$$

So

$$b(ac) = be = b$$

$$= (ba)c = ec = c.$$

d. Since $a^{-1}a = e = aa^{-1}$, the inverse of $a^{-1}$ is $a$, i.e., $(a^{-1})^{-1} = a.$
5. We want to show that \( b^{-1}a^{-1} \) is the inverse of \( ab \).

If we multiply them together, we get:

\[
(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}
\]
\[
= aea^{-1}
\]
\[
= aa^{-1}
\]
\[
= e
\]

and \((b^{-1}a^{-1})(ab) = e\) similarly. Hence \( b^{-1}a^{-1} \) is the inverse of \( ab \).