Today we are going to study the abstract properties of binary operations.

Rotating a Square in Space

Imagine we can pick up the square, rotate it in any way we want, and then put it back on the white frame.

We will now study these 8 motions, called symmetries of the square:

Symmetries of the Square

\[ Y_{SQ} = \{ R_0, R_{90}, R_{180}, R_{270}, F_\uparrow, F_\downarrow, F_\rightarrow, F_\leftarrow \} \]
Composition
Define the operation \( \ast \) to mean “first do one symmetry, and then do the next”

For example,
- \( R_{90} \ast R_{180} \) means “first rotate 90˚ clockwise and then 180˚”
  \[ R_{270} \]
- \( F_l \ast R_{90} \) means “first flip horizontally and then rotate 90˚”
  \[ F / \]

Question: if \( a, b \in Y_{SQ} \), does \( a \ast b \in Y_{SQ} \)?

Some Formalism
If \( S \) is a set, \( S \times S \) is:
- the set of all (ordered) pairs of elements of \( S \)

\[ S \times S = \{ (a, b) \mid a \in S \text{ and } b \in S \} \]

If \( S \) has \( n \) elements, how many elements does \( S \times S \) have? \( n^2 \)

Formally, \( \ast \) is a function from \( Y_{SQ} \times Y_{SQ} \) to \( Y_{SQ} \)

\[ \ast : Y_{SQ} \times Y_{SQ} \rightarrow Y_{SQ} \]

As shorthand, we write \( \ast(a, b) \) as “\( a \ast b \)”

Binary Operations
“\( \ast \)” is called a binary operation on \( Y_{SQ} \)

Definition: A binary operation on a set \( S \) is a function \( \ast : S \times S \rightarrow S \)

Example:
The function \( f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} \) defined by
\[ f(x, y) = xy + y \]
is a binary operation on \( \mathbb{N} \)

Associativity
A binary operation \( \ast \) on a set \( S \) is associative if:

- for all \( a, b, c \in S \), \( (a \ast b) \ast c = a \ast (b \ast c) \)

Examples:
- Is \( f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} \) defined by \( f(x, y) = xy + y \) associative?
  \( (ab + b)c + c = a(bc + c) + (bc + c) \)? NO!
- Is the operation \( \ast \) on the set of symmetries of the square associative? YES!

Commutativity
A binary operation \( \ast \) on a set \( S \) is commutative if

- for all \( a, b \in S \), \( a \ast b = b \ast a \)

Is the operation \( \ast \) on the set of symmetries of the square commutative? NO!

\[ R_{90} \ast F_l \neq F_l \ast R_{90} \]
Identities

$R_0$ is like a null motion

Is this true: $\forall a \in Y_{SQ}, \ a \bullet R_0 = R_0 \bullet a = a$? YES!

$R_0$ is called the identity of $\bullet$ on $Y_{SQ}$

In general, for any binary operation $\bullet$ on a set $S$, an element $e \in S$ such that for all $a \in S$, $e \bullet a = a \bullet e = a$ is called an identity of $\bullet$ on $S$

Inverses

Definition: The inverse of an element $a \in Y_{SQ}$ is an element $b$ such that:

$a \bullet b = b \bullet a = R_0$

Examples:

- $R_{90}$ inverse: $R_{270}$
- $R_{180}$ inverse: $R_{180}$
- $F_\|$ inverse: $F_\|$
To check “group-ness”

Given $(S, *)$
1. Check “closure” for $(S, *)$ (i.e., for any $a, b$ in $S$, check $a * b$ also in $S$).
2. Check that associativity holds.
3. Check there is a identity
4. Check every element has an inverse

Examples
Is $(\mathbb{N}, +)$ a group?
- Is $+$ associative on $\mathbb{N}$? YES!
- Is there an identity? YES: 0
- Does every element have an inverse? NO!

$(\mathbb{N}, +)$ is NOT a group

Examples
Is $(\mathbb{Z}, +)$ a group?
- Is $+$ associative on $\mathbb{Z}$? YES!
- Is there an identity? YES: 0
- Does every element have an inverse? YES!

$(\mathbb{Z}, +)$ is a group

Examples
Is $(\text{Odds}, +)$ a group?
- Is $+$ associative on Odds? YES!
- Is there an identity? YES: 0
- Does every element have an inverse? YES!
- Are the Odds closed under addition NO!

$(\text{Odds}, +)$ is NOT a group

Examples
Is $(\text{Y} \text{SQ}, \cdot)$ a group?
- Is $\cdot$ associative on $\text{Y} \text{SQ}$? YES!
- Is there an identity? YES: $R_0$
- Does every element have an inverse? YES!

$(\text{Y} \text{SQ}, \cdot)$ is a group
Examples

Is \((\mathbb{Z}_n, +)\) a group?
\((\mathbb{Z}_n \text{ is the set of integers modulo } n)\)
- Is \(+\) associative on \(\mathbb{Z}_n\)? YES!
- Is there an identity? YES: 0
- Does every element have an inverse? YES!

\((\mathbb{Z}_n, +)\) is a group

Examples

Is \((\mathbb{Z}_n, *)\) a group?
\((\mathbb{Z}_n \text{ is the set of integers modulo } n)\)
- Is \(*\) associative on \(\mathbb{Z}_n\)? YES!
- Is there an identity? YES: 1
- Does every element have an inverse? NO!

\((\mathbb{Z}_n, *)\) is NOT a group

Examples

Is \((\mathbb{Z}_n^*, \cdot)\) a group?
\((\mathbb{Z}_n^* \text{ is the set of integers modulo } n \text{ that are relatively prime to } n)\)
- Is \(*\) associative on \(\mathbb{Z}_n^*\)? YES!
- Is there an identity? YES: 1
- Does every element have an inverse? YES!

\((\mathbb{Z}_n^*, \cdot)\) is a group

And some properties...

Identity Is Unique

Theorem: A group has at most one identity element
Proof:
Suppose \(e\) and \(f\) are both identities of \(G=(S, \cdot)\)
Then \(f = e \cdot f = e\)
We denote this identity by “\(e\)”

Inverses Are Unique

Theorem: Every element in a group has a unique inverse
Proof:
Suppose \(b\) and \(c\) are both inverses of \(a\)
Then \(b \cdot e = b \cdot (a \cdot c) = (b \cdot a) \cdot c = c\)
Orders and generators

Order of a group
A group \( G = (S, *) \) is finite if \( S \) is a finite set
Define \( |G| = |S| \) to be the order of the group (i.e. the number of elements in the group)
What is the group with the least number of elements?
\( G = (\{e\}, *) \) where \( e \ast e = e \)
How many groups of order 2 are there?

\[
\begin{array}{ccc}
  e & f & f \\
  e & f & e \\
\end{array}
\]

Generators
A set \( T \subseteq S \) is said to generate the group \( G = (S, *) \) if every element of \( S \) can be expressed as a finite product of elements in \( T \)

Question: Does \( \{R_{90}\} \) generate \( Y_{SQ} \)? NO!
Question: Does \( \{F, R_{90}\} \) generate \( Y_{SQ} \)? YES!

Generators For \((Z_n, +)\)
Any \( a \in Z_n \) such that \( \text{GCD}(a, n) = 1 \) generates \((Z_n, +)\)

Claim: If \( \text{GCD}(a, n) = 1 \), then the numbers \( a, 2a, \ldots, (n-1)a \), \( na \) are all distinct modulo \( n \)
Proof (by contradiction):
Suppose \( xa = ya \pmod{n} \) for \( x, y \in \{1, \ldots, n\} \) and \( x \neq y \)
Then \( n \mid a(x-y) \)
Since \( \text{GCD}(a, n) = 1 \), then \( n \mid (x-y) \), which cannot happen

Order of an element
If \( G = (S, *) \), we use \( a^n \) denote \( (a \ast a \ast \ldots \ast a) \) \( n \) times

Definition: The order of an element \( a \) of \( G \) is the smallest positive integer \( n \) such that \( a^n = e \)
The order of an element can be infinite!
Example: The order of 1 in the group \((Z, +)\) is infinite
What is the order of \( F \) in \( Y_{SQ} \)? 2
What is the order of \( R_{90} \) in \( Y_{SQ} \)? 4

Orders
Theorem: If \( G \) is a finite group, then for \( g \) in \( G \), \( \text{order}(g) \) is finite.

For \((Z_n, +)\), recall that
\( \text{order}(g) = n/\text{GCD}(n, g) \)
Orders

What about \( (\mathbb{Z}_n^*, \ast) \)?

\[ \text{order}(\mathbb{Z}_n^*, \ast) = \phi(n) \]

What about the order of its elements?

Non-trivial theorem:
There are \( \phi(n-1) \) generators of \( (\mathbb{Z}_n^*, \ast) \)

Orders

Theorem: Let \( x \) be an element of \( G \). The order of \( x \) divides the order of \( G \)

Corollary: If \( p \) is prime, \( a^{p-1} \equiv 1 \pmod{p} \)
(remember, this is Fermat’s Little Theorem)

BTW, what group did we apply the theorem to?

\[ G = (\mathbb{Z}_n^*, \ast), \text{order}(G) = p-1 \]

Groups and Subgroups

Subgroups

Suppose \( G = (S, \ast) \) is a group.

If \( T \subseteq S \), and if \( H = (T, \ast) \) is also a group, then \( H \) is called a subgroup of \( G \).

Examples

\( (\mathbb{Z}, +) \) is a group
and \( (\text{Evens}, +) \) is a subgroup.

Also, \( (\mathbb{Z}, +) \) is a subgroup of \( (\mathbb{Z}, +) \). (Duh!)

What about \( (\text{Odds}, +) \)?
Examples

\((\mathbb{Z}_n, +_n)\) is a group and if \(k \mid n\), what about \(((0, k, 2k, 3k, \ldots, (n/k)k), +_n)\)?

Is \((\mathbb{Z}_n, +_n)\) a subgroup of \((\mathbb{Z}_n, +_n)\)?

Quick facts (identity)

If \(e\) is the identity in \(G = (S, \cdot)\), what is the identity in \(H = (T, \cdot)\)?

Quick facts (inverse)

If \(b\) is \(a\)'s inverse in \(G = (S, \cdot)\), what is \(a\)'s inverse in \(H = (T, \cdot)\)?

Lagrange's Theorem

Theorem: If \(G\) is a finite group, and \(H\) is a subgroup then the order of \(H\) divides the order of \(G\).

In symbols, \(|H|\) divides \(|G|\).

Corollary: If \(x\) in \(G\), then \(\text{order}(x)\) divides \(|G|\).

Proof of Corollary:
Consider the set \(T_x = \{x, x^2 = x \cdot x, x^3, \ldots\}\)
\(H = (T_x, \cdot)\) is a group. (check!)
Hence it is a subgroup of \(G = (S, \cdot)\).
\(\text{Order}(H) = \text{order}(x)\). (check!)

On to other algebraic definitions

Lord Of The Rings

We often define more than one operation on a set

For example, in \(\mathbb{Z}_n\) we can do both addition and multiplication modulo \(n\)

A ring is a set together with two operations
**Definition:**
A ring $R$ is a set together with two binary operations $+$ and $\times$, satisfying the following properties:

1. $(R, +)$ is a commutative group
2. $\times$ is associative
3. The distributive laws hold in $R$:
   
   $$(a + b) \times c = (a \times c) + (b \times c)$$
   $$c \times (a + b) = (c \times a) + (c \times b)$$

**Examples:**
Is $(Z, +, \times)$ a ring?

How about $(Z, +, \min)$?

---

**Fields**

**Definition:**
A field $F$ is a set together with two binary operations $+$ and $\times$, satisfying the following properties:

1. $(F, +)$ is a commutative group
2. $(F \setminus \{0\}, \times)$ is a commutative group
3. The distributive law holds in $F$:

   $$(a + b) \times c = (a \times c) + (b \times c)$$

**Examples:**
Is $(Z, +, \times)$ a field?

How about $(R, +, \times)$?

How about $(Z_n, +_n, \times_n)$?

---

**In The End...**

Why should I care about any of this?

Groups, Rings and Fields are examples of the principle of abstraction: the particulars of the objects are abstracted into a few simple properties.

If you prove results from some group, check if the results carry over to any group.
Symmetries of the Square
Compositions

Groups
Binary Operation
Identity and Inverses
Basic Facts: Inverses Are Unique
Generators

Here’s What You Need to Know...

Rings and Fields
Definition