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.
In how many different ways can we put the square back on the frame?

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

Symmetries of the Square

\[ Y_{SQ} = \{ R_0, R_{90}, R_{180}, R_{270}, F|, F\, , F, F \} \]

Composition

Define the operation “•” to mean “first do one symmetry, and then do the next”.

For example,

- \( R_{90} \circ R_{180} \) means “first rotate 90° clockwise and then 180°”
  \[ = R_{270} \]
- \( F| \circ R_{90} \) means “first flip horizontally and then rotate 90°”
  \[ = F\] 

Question: if \( a,b \in Y_{SQ} \), does \( a \circ b \in Y_{SQ} \)? Yes!
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, $\cdot$ is a function from $Y_{SQ} \times Y_{SQ}$ to $Y_{SQ}$

$\cdot : Y_{SQ} \times Y_{SQ} \rightarrow Y_{SQ}$

As shorthand, we write $\cdot (a,b)$ as "$a \cdot b$"

Binary Operations

"$\cdot$" is called a binary operation on $Y_{SQ}$

Definition: A binary operation on a set $S$ is a function $\cdot : S \times S \rightarrow S$

Example:

The function $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ defined by $f(x,y) = xy + y$

is a binary operation on $\mathbb{N}$

Assciativity

A binary operation $\cdot$ on a set $S$ is associative if:

for all $a,b,c \in S$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

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 $\cdot$ on the set of symmetries of the square associative? YES!

Commutativity

A binary operation $\cdot$ on a set $S$ is commutative if

For all $a,b \in S$, $a \cdot b = b \cdot a$

Is the operation $\cdot$ on the set of symmetries of the square commutative? NO!

$R_{90} \cdot F_1 \neq F_1 \cdot R_{90}$
**Identities**

$R_0$ is like a null motion

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

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

In general, for any binary operation $\cdot$ on a set $S$, an element $e \in S$ such that for all $a \in S$,

$$e \cdot a = a \quad e \cdot e = a$$

is called an identity of $\cdot$ on $S$

---

**Inverses**

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

$$a \cdot b = b \cdot a = R_0$$

Examples:

- $R_{90}$ inverse: $R_{270}$
- $R_{180}$ inverse: $R_{180}$
- $F_\|$ inverse: $F_\|$  

Every element in $Y_{SQ}$ has a unique inverse
Groups

A group $G$ is a pair $(S, \cdot)$, where $S$ is a set and $\cdot$ is a binary operation on $S$ such that:

1. $\cdot$ is associative
2. (Identity) There exists an element $e \in S$ such that:
   $e \cdot a = a \cdot e = a$, for all $a \in S$
3. (Inverses) For every $a \in S$ there is $b \in S$ such that: $a \cdot b = b \cdot a = e$

If $\cdot$ is commutative, then $G$ is called a commutative group

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 $(\mathbb{Y}_\text{SQ}, \bullet)$ a group?

- Is $\bullet$ associative on $\mathbb{Y}_\text{SQ}$? YES!
- Is there an identity? YES: $R_0$
- Does every element have an inverse? YES!

$(\mathbb{Y}_\text{SQ}, \bullet)$ is a group
Examples

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

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 \(f = e \cdot f = e\)

Inverses Are Unique

Theorem: Every element in a group has a unique inverse

Proof:
Suppose \(b\) and \(c\) are both inverses of \(a\)

Then \(b = b \cdot e = b \cdot (a \cdot c) = (b \cdot a) \cdot c = c\)

A group \(G = (S, \cdot)\) 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? \(G = \{(e), \cdot\}\) where \(e \cdot e = e\)

How many groups of order 2 are there?

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

A set $T \subseteq S$ is said to generate the group $G = (S, \ast)$ 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 $\{S_1, R_{90}\}$ generate $Y_{SQ}$? YES!

An element $g \in S$ is called a generator of $G=(S, \ast)$ if $\{g\}$ generates $G$.

Does $Y_{SQ}$ have a generator? NO!

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 $n | a(x-y)$.

Since $\text{GCD}(a,n) = 1$, then $n | (x-y)$, which cannot happen.

Orders

Theorem: Let $x$ be an element of $G$. The order of $x$ divides the order of $G$.

Corollary: If $p$ is prime, $a^{p-1} = 1 \pmod{p}$.

(This is called Fermat’s Little Theorem).

$\{1, \ldots, p-1\}$ is a group under multiplication modulo $p$.
Lord Of The Rings

We can define more than one operation on a set
For example, in \( \mathbb{Z}_n \), we can do 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 \( R \):
   \[
   (a + b) \times c = (a \times c) + (b \times c)
   a \times (b + c) = (a \times b) + (a \times c)
   \]

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. \( (F-\{0\},\times) \) is a commutative group
3. The distributive law holds in \( F \):
   \[
   (a + b) \times c = (a \times c) + (b \times c)
   \]

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
All the results carry over to any group
Symmetries of the Square
Compositions

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

Rings and Fields
Definition

Here’s What You Need to Know…