Number Theory

Naturals        Integers        \( \mathbb{Z}_n \)
closed under +  closed under +  closed under +
\( a + b = b + a \)  \( a + b = b + a \)  \( a + n b = b + n a \)
\( (a + b) + c = a + (b + c) \) \( a + (b + c) = a + (b + c) \) \( (a + n b) + c = a + (b + c) \)
\( a + 0 = a \Rightarrow a \)  \( a + 0 = \mathbb{N} \)  \( a + n 0 = 0 + n a \)
\( a + (-a) = 0 \)  \( a + (-a) = 0 \)  \( a + n (-a) = 0 \)

Number Theory

Matrices        Integers        \( \mathbb{Z}_n \)
closed under +  closed under +  closed under +
\( A + B = B + A \)  \( a + b = b + a \)  \( a + n b = b + n a \)
\( (A + B) + C = A + (B + C) \) \( (a + b) + c = a + (b + c) \) \( (a + n b) + c = a + (b + c) \)
\( A + 0 = A \)  \( a + 0 = 0 + a \)  \( a + n 0 = 0 + n a \)
\( A + (-A) = 0 \)  \( a + (-a) = 0 \)  \( a + n (-a) = 0 \)
closed under *  closed under *  closed under *
ditto \( (a + b)^* c = a^* c + b^* c \)  ditto
\( 1/a \) may not exist \( a \neq 0 \)  \( a \neq 0 \)

Number Theory

Invertible Matrices        Rationals        \( \mathbb{Z}_n \) (n prime)
closed under +  closed under +  closed under +
\( A + B = B + A \)  \( a + b = b + a \)  \( a + n b = b + n a \)
\( (A + B) + C = A + (B + C) \) \( (a + b) + c = a + (b + c) \) \( (a + n b) + c = a + (b + c) \)
\( A + 0 = A \)  \( a + 0 = 0 + a \)  \( a + n 0 = 0 + n a \)
\( A + (-A) = 0 \)  \( a + (-a) = 0 \)  \( a + n (-a) = 0 \)
closed under *  closed under *  closed under *
ditto \( (a + b)^* c = a^* c + b^* c \)  ditto
\( 1/a \) exists if \( a = 0 \)  ditto

Abstraction:
Abstract away the inessential features of a problem
Today we are going to study the abstract properties of binary operations.

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 study the seven symmetries of the square frame.

Symmetries of the Square

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

Composition

Define the operation "\( \cdot \)" to mean "first do one symmetry, and then do the next."

For example,

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

Question: if \( a, b \in Y_{SQ} \), does \( a \cdot b \in Y_{SQ} \)? Yes!
How many symmetries for n-sided body? 2n

Some Formalism

If S is a set, S × S is:

the set of all (ordered) pairs of elements of S

S × S = {(a, b) | a ∈ S and b ∈ S}

If S has n elements, how many elements does S × S have? n²

Formally, • is a function from Y_{SQ} × Y_{SQ} to Y_{SQ}

• : Y_{SQ} × Y_{SQ} → Y_{SQ}

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

Binary Operations

“•” is called a binary operation on Y_{SQ}

Definition: A binary operation on a set S is a function • : S × S → S

Example:
The function f : N × N → N defined by

f(x, y) = xy + y

is a binary operation on N

Implicitly contains “closure”

Associativity

A binary operation • on a set S is associative if:

for all a, b, c ∈ S, (a • b) • c = a • (b • c)

Examples:

Is f : N × N → N defined by f(x, y) = xy + y associative?

(ab + b)c + c = a(bc + c) + (bc + c)? NO!

Is the operation • on the set of symmetries of the square associative? YES!

Commutativity

A binary operation • on a set S is commutative if

For all a, b ∈ S, a • b = b • a

Is the operation • on the set of symmetries of the square commutative? NO!

R₀ • F₁ ≠ F₁ • R₀

Identities

R₀ is like a null motion

Is this true: ∀a ∈ Y_{SQ}, a • R₀ = R₀ • a = a? YES!

R₀ is called the identity of • on Y_{SQ}

In general, for any binary operation • on a set S, an element e ∈ S such that for all a ∈ S,

e • a = a • e = a

is called an identity of • 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:
   \[ a \cdot b = b \cdot a = e \]

To check “group-ness”

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

Commutative or “Abelian” Groups

If \( G = (S, \cdot) \) and \( \cdot \) is commutative, then \( G \) is called a commutative group.

remember,
“commutative” means
\[ a \cdot b = b \cdot a \] for all \( a, b \) in \( S \)
Some examples...

Examples

Is \((\mathbb{N},+)\) a group?
- Is \(\mathbb{N}\) closed under +? YES!
- 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 \(\mathbb{Z}\) closed under +? YES!
- 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 Odds closed under +? NO!
- Is + associative on Odds? YES!
- Is there an identity? NO!
- Does every element have an inverse? YES!

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

Examples

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

\((Y_{\text{SQ}}, \cdot)\) is a group
the “dihedral” group \(D_4\)

Examples

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

\((\mathbb{Z}_n, +_n)\) is a group
Examples
Is \((\mathbb{Z}_n, \star_n)\) a group?
(\(\mathbb{Z}_n\) is the set of integers modulo n)

- Is \(\star_n\) associative on \(\mathbb{Z}_n\)? YES!
- Is there an identity? YES: 1
- Does every element have an inverse? NO!

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

Examples
Is \((\mathbb{Z}_n, \circ_n)\) a group?
(\(\mathbb{Z}_n\) is the set of integers modulo n that are relatively prime to n)

- Is \(\circ_n\) associative on \(\mathbb{Z}_n\)? YES!
- Is there an identity? YES: 1
- Does every element have an inverse? YES!

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

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

1. \(\star\) is associative
2. (Identity) There exists an element \(e \in S\) such that:
   \[ e \star a = a \star e = a, \quad \text{for all } a \in S \]
3. (Inverses) For every \(a \in S\) there is \(b \in S\) such that: \(a \star b = b \star a = e\)

Some properties of groups...

Identity Is Unique

Theorem: A group has at most one identity element

Proof:
Suppose \(e\) and \(f\) are both identities of \(G=(S, \star)\)

Then \(f = e \star f = e \)

\(\Rightarrow\) exactly one identity

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 $b = b \star e = b \star (a \star c) = (b \star a) \star c = c$

---

Cancellation

**Theorem:** If $a \star b = a \star c$, then $b = c$

**Proof:**

\[
(a^{-1} \star (a \star b)) = (a^{-1} \star (a \star c))
\]

\[
\Rightarrow (a^{-1} \star a) \star b = (a^{-1} \star a) \star c
\]

\[
\Rightarrow e \star b = e \star c
\]

\[
\Rightarrow b = c
\]

---

Orders and Generators

**Order of a Group**

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

How many groups of order 2 are there?

- $\begin{array}{|c|c|}
  \hline
  e & f \\
  \hline
  f & e \\
  \hline
\end{array}$

**Generators**

A set $T \subseteq S$ is said to generate the group $G = (S, \star)$ if every element of $S$ can be expressed as a finite “sum” of elements in $T$

Question: Does $\{R_{90}\}$ generate $Y_{90}$? NO!

Question: Does $\{F, R_{90}\}$ generate $Y_{90}$? YES!

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

Does $Y_{90}$ have a generator? NO!
Generators For \((\mathbb{Z}_n, +)\)

Any \(a \in \mathbb{Z}_n\) such that \(\text{GCD}(a, n) = 1\) generates \((\mathbb{Z}_n, +)\)

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 \(G = (S, \ast)\), we use \(a^t\) denote \((a \ast a \ast \cdots \ast a)\) \(t\) 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 \((\mathbb{Z}, +)\) is infinite.

What is the order of \(F_1\) in \(Y_{sp}\)? 2

What is the order of \(R_{90}\) in \(Y_{sp}\)? 4

Orders

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

Proof: Consider \(g, g \ast g, g \ast g \ast g = g^3, g^4, \ldots\)

Since \(G\) is finite, \(g^i = g^j\) for some \(j < k\)

\[\Rightarrow g^i = g^j \Rightarrow g^{i-j} = e\]

Multiplying both sides by \((g^j)^{-1}\)

\[\Rightarrow e = g^0\]

Remember

order of a group \(G\) = size of the group \(G\)

order of an element \(g\) in group \(G\)

\[= (\text{smallest } n > 0 \text{ s.t. } g^n = e)\]

\(\Rightarrow g\) is a generator of group \(G\)

if \(\text{order}(g) = \text{order}(G)\)
Orders

What is order($\mathbb{Z}_n$, $+$)? $n$

For $x$ in ($\mathbb{Z}_n$, $+$), what is order($x$)?

$$\text{order}(x) = n/\text{GCD}(x,n)$$

Orders

order($\mathbb{Z}_n^\ast$, $\ast$)? $\phi(n)$

For $x$ in ($\mathbb{Z}_n^\ast$, $\ast$), what is order($x$)?

$$\text{At most } \phi(n)$$

(Euler’s theorem)

Orders

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

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

(remember, this is Fermat’s Little Theorem)

What group did we use for the corollary?

$G = (\mathbb{Z}_p^\ast, \ast)$, 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.

In fact, $(\text{Multiples of } k, +)$ is also a subgroup.

Is $(\text{Odds}, +)$ a subgroup of $(\mathbb{Z}, +)$?

No! $(\text{Odds}, +)$ is not even a group!
Examples

\((\mathbb{Z}_n, +_n)\) is a group and if \(k \mid n\),
Is \(((0, k, 2k, 3k, \ldots, (n/k-1)k), +_n)\) subgroup of \((\mathbb{Z}_n, +_n)\)?
Only if \(k\) is a divisor of \(n\).

Is \((\mathbb{Z}_n, +_n)\) a subgroup of \((\mathbb{Z}_n, +_n)\)?
No! it doesn’t even have the same operation
Is \((\mathbb{Z}_n, +_n)\) a subgroup of \((\mathbb{Z}_n, +_n)\)?
No! \((\mathbb{Z}_n, +_n)\) is not a group! (not closed)

Subgroup facts (identity)

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

\(e\)

Proof: Clearly, \(e\) satisfies
\(e \cdot a = a \cdot e = a\) for all \(a\) in \(T\).
But we saw there is a unique such element in any group.

Subgroup facts (inverse)

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

\(b\)

Proof: let \(c\) be a’s inverse in \(H\).
Then \(c \cdot a = e\)
\[\Rightarrow c \cdot a \cdot b = e \cdot b\]
\[\Rightarrow c \cdot e = b\]
\[\Rightarrow c = b\]

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 \(G = (S, \cdot)\).
Order(\(H\)) = Order(\(x\)). (check!)

“Right” way of looking at primality testing

Fermat: if \(n\) prime, then \(a^{n-1} = 1 \pmod n\)
for all \(0 < a < n\).

Suppose the converse was also true:
“If \(n\) composite, then exists \(g\) with \(0 < g < n\).
\(g^{n-1} \neq 1 \pmod n\)"

Then consider “bad elements” for this \(n\):
elements \(b\) such that \(b^{n-1} \neq 1 \pmod n\)
Bad elements form a subgroup of \(\mathbb{Z}_n\) \(\Rightarrow |\text{Bad}| < \frac{1}{2}n\)
Picking random element, it is good with probability \(\frac{1}{2}\).
Sadly, converse not true. Fixing that gives Miller-Rabin.
Symmetries of the Square
Compositions

Groups
Binary Operation
Identity and Inverses
Basic Facts: Inverses Are Unique
Generators
Order of element, group

Subgroups
Lagrange’s theorem

Here’s What You Need to Know...