

class

function, operation

- Set $\{1, 2, 3\}$ → Union, intersection, complement
- Logic true, false → and, or, not
- Integer $1, 2, 3, \dots$ → add, subtract, multiplication
- Complex Number $1 + 2i$ → add, subtract, ...

class

interface / abstract class

add, subtraction, negation.

We will work on the properties of "the abstract class" → abstract algebra.



properties of all classes that "implement" the abstract class.

First abstract class: Group (G, \oplus, \ominus)
 set: possible attribute values

Abstract class with 2 operations: addition and inverse. They must have the following properties.

1. closure For all $a, b \in G$, $a \oplus b \in G$

2. Associativity For all $a, b, c \in G$, $(a \oplus b) \oplus c = a \oplus (b \oplus c)$

3. Identity There exists $e \in G$ such that $a \oplus e = e \oplus a = a$ for all $a \in G$
 identity of

4. Inverse For all a , there exist $\neg a$ such that $a \oplus \neg a = e = \neg a \oplus a$

Example 1 $G =$ set of integer \mathbb{Z}

inverse of a is $-a$.

$\oplus =$ addition on integer

1. closure $a + b$ is integer

2. Associativity $a + (b + c) = (a + b) + c$

3. Identity $e = 0$ as $a + 0 = a = 0 + a$ for all a .

4. Inverse $a + -a = 0$ for all a .

$(G, \text{integer addition}, -)$ is a group.

Example 2 $G = \text{coproduct of } \{1, \dots, n\}$ inverse of S is $\{1, \dots, n\} - S$

$\oplus = \text{intersection}$

1. closure $S \cap P$ is a subset of $\{1, \dots, n\}$

2. Associativity $(S \cap P) \cap Q = S \cap (P \cap Q)$

3. Identity $e = \{1, \dots, n\}$ $S \cap \{1, \dots, n\} = S$

4. Inverse \times $S \cap \emptyset = \{1, \dots, n\}$ The result of $S \cap \emptyset$ is a subset of S if $S \neq \{1, \dots, n\}$

(superset of $\{1, \dots, n\}$, intersection, complement) is not a group.

First Second abstract class: Abelian group (G, \oplus, \neg)

Group with one more property.

5. commutativity For all $a, b \in G$, $a \oplus b = b \oplus a$.

Third abstract class: $(G, \oplus, \neg, \otimes)$

Three operations - addition, additive inverse, multiplication

1. (G, \oplus, \neg) is an abelian group

2. For all $a, b, c \in G$, $(a \otimes b) \otimes c = a \otimes (b \otimes c)$

There exists $e' \in G$ such that $a \otimes e' = a = e' \otimes a$ for all $a \in G$.

For all a, b , $a \otimes b \in G$

3. For all $a, b, c \in G$, $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

$(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$

Group except inverse property.

distributivity

Example 3

$G = \text{Set of integer } \mathbb{Z}$

inverse of a is $-a$

$\oplus = \text{addition on integer}$

$\otimes = \text{multiplication on integer}$

1. (G, \oplus, \neg) is an abelian group [example 1]

2. $a \cdot b \in \mathbb{Z}$

$a \cdot 1 = a = 1 \cdot a$

[$e' = 1$]

$(a \cdot b) \cdot c = a \cdot (b \cdot c)$

3. $a \cdot (b + c) = a \cdot b + a \cdot c$

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

Scalar Multiplication : (G, \oplus, \ominus)

Let $P, Q \in G$, and $n \in \mathbb{Z}_{\geq 0}$, $n \cdot P = \underbrace{(P \oplus P \oplus \dots \oplus P)}_{n \text{ times}}$

$$0 \cdot P = e.$$

Property For all $P \in G$, $1 \cdot P = P$

Fourth abstract class $(G, \oplus, \ominus, \otimes, \oslash, 1)$

Four operations — addition, additive inverse (subtraction), multiplication, multiplicative inverse (division)

1. (G, \oplus, \ominus) is an abelian group with identity e

2. $(G - \{e\}, \otimes, \oslash, 1)$ is also an abelian group

3. Distributivity For all a, b, c , $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

Example 4 $G =$ Set of integer \mathbb{Z}

\oplus = addition on integer — inverse of a is $-a$ $e = 0$ (identity on addition)

\otimes = multiplication on integer — $e' = 1$ (identity on multiplication)

There must be $a \in \mathbb{Z} - \{0\}$ such that $2 \cdot a = e' = 1$

[Inverse property of the group $(\mathbb{Z} - \{0\}, \otimes, \oslash, 1)$]

There is not such an integer. $(\mathbb{Z} - \{0\}, \otimes, \oslash, 1)$ is not an ~~ab~~ abelian group.

$(\mathbb{Z}, +, -, \times, /)$ is not a field.

Example 5 \mathbb{Q} = set of rational number

\oplus = addition on rational number — inverse of a is $-a$

\otimes = multiplication on rational number — inverse of $\frac{a}{b}$ is $\frac{b}{a}$

$(\mathbb{Q}, \oplus, -)$ is an abelian group

$(\mathbb{Q} - \{0\}, \otimes, \oslash, 1)$ is an abelian group

For all $a, b, c \in \mathbb{Q}$, $a \cdot (b + c) = a \cdot b + a \cdot c$

$(\mathbb{Q}, +, -, \cdot, /)$ is a field.

Example 6

$$G = \{0, 1, 2, 3, 4, 5, 6\}$$

$$a \oplus b = (a + b) \pmod 7$$

integer addition

$$\text{for } e = 0 \text{ because } (a + 0) \pmod 7 = a$$

$$\neg a = \begin{cases} (7-a) & \text{when } a > 1 \\ 0 & \text{otherwise} \end{cases}$$

$$\text{For } a > 1, a \oplus \neg a = (a + (7-a)) \pmod 7 = 7 \pmod 7 = 0$$

$$\text{For } a = 0, a \oplus \neg a = (0 + 0) \pmod 7 = 0$$

(G, \oplus, \neg) is an abelian group.

$$a \otimes b = (ab) \pmod 7$$

integer multiplication

$$e' = 1 \text{ because } (a \cdot 1) \pmod 7 = a$$

$$a = 1 \quad 1/1 = 1 \quad \text{because } (1 \cdot 1) \pmod 7 = 1$$

$$a = 2 \quad 1/2 = 4 \quad \text{because } (2 \cdot 4) \pmod 7 = 1$$

$$a = 3 \quad 1/3 = 5 \quad \text{because } (3 \cdot 5) \pmod 7 = 1$$

$$a = 4 \quad 1/4 = 2 \quad \text{because } (2 \cdot 4) \pmod 7 = 1$$

$$a = 5 \quad 1/5 = 3 \quad \text{because } (3 \cdot 5) \pmod 7 = 1$$

$$a = 6 \quad 1/6 = 6 \quad \text{because } (6 \cdot 6) \pmod 7 = 1$$

Prime Field p : positive prime number

$$\mathbb{F}_p = G = \{0, 1, \dots, p-1\}$$

$$a \oplus b = (a + b) \pmod p$$

$$e = 0$$

$$\neg a = \begin{cases} (p-a) & \text{when } a > 1 \\ 0 & \text{otherwise} \end{cases}$$

$$a \otimes b = (ab) \pmod p$$

$$e' = 1$$

$$1/a = ?$$

Theorem

For all $a \in \{1, \dots, p-1\}$, there exists exactly one $b \in \{1, \dots, p-1\}$ such that

$$(ab) \pmod p = 1. \quad [\text{Fermat's Little theorem}]$$

How to find $1/a$?

Diophantine's algorithm