High School Math

attribute — 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 ~~this~~ that "implement" the abstract class.

First abstract class : Group $(G, \oplus, \ominus)$

G = set : possible attribute values

Abstract class with 2 operations: addition ($\oplus$) and inverse ($\neg$). 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 $a \in G$
   e: 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.

$(G$, integer addition, $-)$ is a group.

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

$\oplus$ = 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 ✗ $S \cap \bigcirc = \{1,\dots,n\}$ The result of $S \cap \bigcirc$ if 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.

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

   Group except inverse property.

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

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

   distributivity

Example 3 G = Set of integer $\mathbb{Z}$

$\oplus$ = addition on integer inverse of a is $-a$

$\otimes$ = 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 : $(G, \oplus, \neg)$

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

$0 \cdot P = e.$

Property For all $P \in G$, $\|G\| \cdot P = e$

Fourth abstract class $(G, \oplus, \neg, \otimes, 1/)$

Four operations - addition, additive inverse, multiplication, multiplicative inverse
subtraction division

1. $(G, \oplus, \neg)$ is an abelian group
with identity e
2. $(G - \{e\}, \otimes, 1/)$ is also an ablian 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 $a \in G - \{e\}$ $\mathbb{Z} - \{0\}$ such that $2 \cdot a = e' = 1$
[Inverse property of the group $(G - \{e\}, \otimes, 1/)$]

There is not such an integer. $(G - \{e\}, \otimes, 1/)$ is not an ~~alb~~ abelian group.

$(\mathbb{Z}, +, -, \times, 1/)$ 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

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

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

$(\mathbb{Q}, +, -, 1/)$ is a field.

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

$a \oplus b = (a+b) \bmod 7$ $\quad$ ~~for~~ $\quad e = 0$ because $(a+0) \bmod 7 = a$

integer addition

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

For $a \geq 1$, $\quad a \oplus \neg a = (a + (7-a)) \bmod 7 = 7 \bmod 7 = 0$

For $a = 0$, $\quad a \oplus \neg a = (0+0) \bmod 7 = 0$

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

$a \otimes b = (ab) \bmod 7$ $\qquad e' = 1$ because $(a \cdot 1) \bmod 7 = a$

integer multiplication

$a = 1$	$1/1 = 1$	because	$(1 \cdot 1) \bmod 7 = 1$
$a = 2$	$1/2 = 4$	because	$(2 \cdot 4) \bmod 7 = 1$
$a = 3$	$1/3 = 5$	because	$(3 \cdot 5) \bmod 7 = 1$
$a = 4$	$1/4 = 2$	because	$(2 \cdot 4) \bmod 7 = 1$
$a = 5$	$1/5 = 3$	because	$(3 \cdot 5) \bmod 7 = 1$
$a = 6$	$1/6 = 6$	because	$(6 \cdot 6) \bmod 7 = 1$

Prime Field $\quad p$: positive prime number

$\mathbb{F}_p = G = \{0, 1, \dots, p-1\}$ $\qquad a \oplus b = (a+b) \bmod p$ $\qquad a \otimes b = (ab) \bmod p$

$e = 0$ $\qquad e' = 1$

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

Theorem $\quad$ For all $a \in \{1, \dots, p-1\}$, there exists exactly one $b \in \{1, \dots, p-1\}$ such that $(ab) \bmod p = 1$. [Fermat's little theorem]

How to find $1/a$? $\qquad$ Diophantine's algorithm

Example $p = 179$ $a = 7$ Find b such that $(ab) \bmod 179 = 1$

$ab = 179n + 1$ for some integer n when $(ab) \bmod 179 = 1$

$7b = 179n + 1$

$\boxed{7b - 179n = 1}$

$179 = 7 \cdot 25 + 4$

$7 = 4 \cdot 1 + 3$

$4 = 3 \cdot 1 + 1$

~~$3 = 1 \cdot 3 + 0$~~

$1 \cdot 179 - 7 \cdot 25 = 4$

$1 \cdot 7 - 4 \cdot 1 = 3$

$1 \cdot 4 - 3 \cdot 1 = 1$

$1 \cdot 4 - (1 \cdot 7 - 4 \cdot 1) = 1$

$2 \cdot 4 - 1 \cdot 7 = 1$

$2 \cdot [1 \cdot 179 - 7 \cdot 25] - 1 \cdot 7 = 1$

$\boxed{2 \cdot 179 - 51 \cdot 7 = 1}$

$b = -51$ $n = -2$

$\boxed{O(\log^3 n)}$

$b = -51 \longrightarrow$ ~~$b = 179 - 51 = 128$~~

$7 \cdot (-51) \bmod 179 = 1$

$[7 \cdot (-51) + 7 \cdot 179] \bmod 179 = 1$

$7 \cdot (128) \bmod 179 = 1$

$\hookrightarrow 1/7$

Bonus Question

What is $1/58$ for the same field?

Extension Field : Consider $\mathbb{F}_2 = \{0, 1\}$.

No member can be a solution of $x^3 + x + 1 = 0$.

Denoting x with 0 or 1, we will have 1.

We will extend the set $\mathbb{F}_2$ to $\mathbb{F}_2 / x^3 + x + 1$, $\subseteq \{$ polynomial of x with coefficient 0, 1 $\}$

$\oplus$ (Addition mod 2) mod x^3+x+1 $\otimes$ (Multiplication mod 2) mod x^3+x+1 $= \{0, 1, x, x+1, x^2, x^2+1, \dots\}$

Ex

$$(x^2) \otimes (x+1) = [(x^3 + x^2) \bmod (x^3 + x + 1)] \bmod 2$$

$$= [(x^3 + x^2 - x^3 - x - 1) \bmod (x^3 + x + 1)] \bmod 2$$

$$= [[(x^2 - x - 1)] \bmod 2] \bmod (x^3 + x + 1)$$

$$= [[(x^2 + x + 1) + (-2x - 2)] \bmod 2] \bmod (x^3 + x + 1)$$

$$= x^2 + x + 1$$

$$\mathbb{F}_2 / x^3+x+1 = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$$

$$= \{000, 001, 010, 011, 100, 101, 110, 111\} = \mathbb{F}_{2^3}$$

coordinate for x^2

coordinate for x

coordinate for 1

Conclusion

- Group — Addition and Subtraction
- Ring — Addition, Subtraction, Multiplication
- Field — 〃, division.
- Field Extension — Larger Field.