What is "abstract algebra"?

The study of:

① Sets with "algebraic structure" satisfying certain properties.

ex: "addition", "multiplication", or some other binary operation

to be specified in a later lecture

Exs: • Groups

$(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, $(\mathbb{Q}^{+},\cdot)$, $(\mathbb{R}^{+},\cdot)$

(Integers modulo 10, +)

(Polynomials with real coefficients, +)

$(\{2\times 2 \text{ real matrices } A \text{ with } \det(A)\neq 0\},\cdot)$

$(\mathcal{P}(S),\Delta)$

symmetric difference

power set of a set S

• Rings

$(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$

(Integers modulo 10, + , ·)

(Polynomials with real coefficients, + , ·)

• Fields

$(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$

(Integers modulo 11, + , ·)

② Maps between these sets which respect the algebraic structure. (<u>homomorphisms</u>)

Exs: 1) Define $\psi : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^+, \cdot)$

by $\psi(x) = e^x$.

Then $\forall x, y \in \mathbb{R}$,

$$\psi(x+y) = e^{x+y} \quad \text{(def. of } \psi\text{)}$$

binary oper. in $(\mathbb{R}, +)$

$$= e^x e^y \quad \text{(props. of exponentials)}$$

$$= \psi(x) \cdot \psi(y) \quad \text{(def. of } \psi\text{)}$$

binary oper. in $(\mathbb{R}^+, \cdot)$

2) Define $\varphi : (\mathbb{Z}, +) \longrightarrow$ (Integers modulo 10, +)

by $\varphi(n) = n \bmod 10$.

Then $\forall n, m \in \mathbb{Z}$,

$$\varphi(n+m) = (n+m) \bmod 10$$

addition in $\mathbb{Z}$

$$= (n \bmod 10) + (m \bmod 10)$$

$$= \varphi(n) + \varphi(m)$$

addition in the integers modulo 10

Historical motivations:

Two main categories of problems:

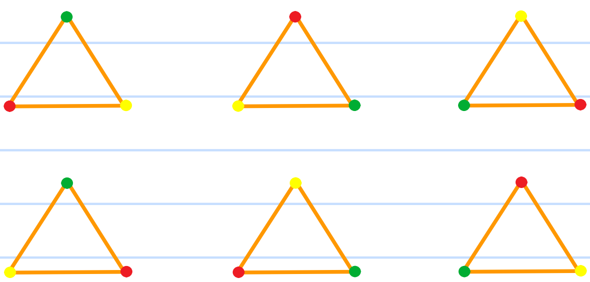
① Symmetries of sets of objeets

- Galois's study of symmetries of roots of polynomials.

  (insolvability of the quintic)

- Symmetries of geometric objects

  Ex: Rigid motions of regular polygons in the plane.



② Number theory: Integers modulo n and related groups.

Ex: What is the units digit of 3^{2023}?

Solution:

Working modulo 10:

n	$3^n \bmod 10$
1	3
2	9
3	7
4	1
5	3
6	9
7	7
8	1
$\vdots$	$\vdots$

Group theory explanation:

(working in $(\mathbb{Z}/10\mathbb{Z})^\times$)

(multiplicative order of 3 divides $|(\mathbb{Z}/10\mathbb{Z})^\times| = 4$)

$$\begin{aligned} \text{So } 3^{2023} &= 3^{4\cdot 505+3} \\ &= (3^4)^{505}\cdot 3^3 \\ &= 1^{505}\cdot 7 \\ &= 7 \bmod 10. \end{aligned}$$

Therefore the units digit of 3^{2023} is 7.

→ applications to cryptography, computer science, and many other parts of mathematics.