Introduction to Algebraic Structure

Doan Nhat Quang

doan-nhat.quang@usth.edu.vn
University of Science and Technology of Hanoi
ICT department

Introduction

- Algebra (*meaning: reunion of broken parts*):
  - Algebra is the study of mathematical symbols and the rules for manipulating these symbols
  - It includes everything from elementary equation solving to the study of abstractions such as **groups, rings,** and **fields**.

Introduction

Why Study Algebra?

- Algebra is a powerful tool, its use is widely applied in many domains.
- All modern technology relies on mathematics and algebra.
  - Numerical Methods, Image Processing, Machine Learning, etc.
- Studying algebra helps your mind to think logically and break down and solve problems.

Applications with Algebra

Information

The values of the variables are the boolean values, true and false, usually denoted 1 and 0, respectively (or bit in computer).

The basic operations:

- AND (conjunction)
- OR (disjunction)
- NOT (negation)

bit → byte

Applications with Algebra

Information

Applications:

- Data Transfer: Bits and bytes are transmitted one at a time in serial transmission
- Storage: Bits and bytes are used to store data in digital devices
- Bar code: Barcode is a visual, machine-readable representation of data

Applications with Algebra

Cryptography

Cryptography is the study of sending and receiving secret messages.

- The message to be sent is called the **plaintext** message. The disguised message is called the **ciphertext**.
- The plaintext and the ciphertext are both written in an **alphabet**, consisting of **letters** or **characters**.

Applications with Algebra

Cryptography

A cryptosystem, or cipher:

- **encryption**, the process of transforming a plaintext message to a ciphertext message
- **decryption**, the reverse transformation of changing a ciphertext message into a plaintext message.

Applications with Algebra

Cryptography

One of the first and most famous private key cryptosystems was the shift code used by Julius Caesar

- digitize the alphabet by letting $A = 00, B = 01, .., Z = 25$.
- encoding function $f(p) = p + 3 \bmod 26$
- that is, $A \to D, B \to E, .., Z \to C$.

Applications with Algebra

Cryptography

Suppose we receive the encoded message DOJHEUD. To decode this message, we have to digitize it:

$$3; 14; 9; 7; 4; 20; 3;$$

Applications with Algebra

Cryptography

Suppose we receive the encoded message DOJHEUD. To decode this message, we have to digitize it:

$$3; 14; 9; 7; 4; 20; 3;$$

Next we apply the inverse transformation to get

$$0; 11; 6; 4; 1; 17; 0;$$

$\rightarrow$ RSA Cryptosystem.

Applications with Algebra

Coding theory

- A problem is raised when sending a message over a channel that could be affected by **noise**.
- The task is to encode and decode the information in a the manner that will allow the detection, and possibly the correction, of errors caused by noise.

Applications with Algebra

Coding theory

- Suppose that the message to be encoded is a binary n-tuple $(x_1, x_2, ..., x_n)$
- The message is encoded into a binary 3n-tuple by simply repeating the message three times: $(x_1, x_2, ..., x_n) \rightarrow (x_1, x_2, ..., x_n; x_1, x_2, ..., x_n; x_1, x_2, ..., x_n)$

- The original message is (0110), then the transmitted message will be (0110 0110 0110).
- If the received codeword will be (0110 1110 0110), which will be correctly decoded as (0110).

Terminology

A **statement** in logic or mathematics is an assertion that is either true or false.

- 5 + 3 - 1 * 0
- All cats are black
- $5 < 0$
- $f(x) = x^3 + 2x + 10$

Terminology

A **mathematical proof** is nothing more than a convincing **argument** about the accuracy of a statement.

Often a complex statement: *If p, then q* where p and q are both statements.

- p - **hypothesis**
- q - **conclusion**

Terminology

Consider the following example: if $ax^2 + bx + c = 0$ and $a \neq 0$, then

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

is the solution of the function

Terminology

Consider the following example: if $ax^2 + bx + c = 0$ and $a \neq 0$, then

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

is the solution of the function

if this entire statement is **true** and we can show that the hypothesis $ax^2 + bx + c = 0$ with $a \neq 0$ is true, then the conclusion must be true.

Terminology

- **Definition**: a precise and unambiguous description of the meaning of a mathematical term. It characterizes the meaning of a word by giving all the properties and only those properties that must be true.
- **Axiom**: a statement that is assumed to be true without proof. These are the basic building blocks from which all theorems are proved.

Terminology

- **Theorem**: a mathematical statement that is proved using rigorous mathematical reasoning. In a mathematical paper, the term theorem is often reserved for the most important results.
- **Lemma**: a minor result whose sole purpose is to help in proving a theorem. It is a stepping stone on the path to proving a theorem.
- **Proposition**: a proved and often interesting result, but generally less important than a theorem.

Algebraic Structures

Common Axioms

- An operation ∘ is commutative if x ∘ y = y ∘ x for every x, y in the algebraic structure
- An operation ∘ is associative if (x∘y)∘z = x ∘ (y ∘ z)
- An operation ∘ is distributive with respect to another operation ⋆

$$x \circ (y \star z) = x \circ y \star x \circ z$$

$$(x \star y) \circ z = x \circ z \star y \circ z$$

Algebraic Structures

Structures

- Group structures: one binary operation.
- Ring structures: Ring, Integral Domain, Fields, two binary operations.
- Lattice structures: two or more binary operations.

Number Systems

Consider the traditional number systems

$\mathbb{N} = \{0, 1, 2, ...\}$	the natural numbers
$\mathbb{Z} = \{m - n \mid m, n \in \mathbb{N}\}$	**the integers**
$\mathbb{Q} = \{m/n \mid m, n \in \mathbb{N}, n \neq 0\}$	the rational numbers
$\mathbb{R}$	the real numbers
$\mathbb{C}$	the complex numbers

and

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

Number Systems: Properties of $\mathbb{R}$

Addition for each pair of real numbers a and b there exists a unique real number $a + b$ such that

- $+$ is a commutative and associative operation;
- there exists in $\mathbb{R}$ a zero, 0, for addition: $a + 0 = 0 + a = a$ for all $a \in \mathbb{R}$;
- for each $a \in \mathbb{R}$ there exists an additive inverse $-a \in \mathbb{R}$ such that $a+(-a) = (-a)+a = 0$.

Number Systems: Properties of $\mathbb{R}$

Multiplication for each pair of real numbers a and b there exists a unique real number a . b such that such that

- . is a commutative and associative operation;
- there exists in $\mathbb{R}$ an identity, 1, for multiplication: $a.1 = 1.a = a$ for all a $\in \mathbb{R}^* = \mathbb{R} \backslash 0$;
- for each a $\in \mathbb{R}^*$ there exists a mulplicative inverse $a^{-1} \in \mathbb{R}$ such that $a.a^{-1} = a^{-1}.a = 1$

Number Systems: Properties of $\mathbb{R}$

Order properties: $\mathbb{R}$ come with an order relation: for all $a, b \in \mathbb{R}$, we have exactly one possibility of $a > b$, $a < b$ or $a = b$

Completeness axiom: equivalent to the statement that any infinite string of decimal digits.

Number Systems: Properties of $\mathbb{C}$

$\mathbb{C}$ has arithmetic properties just the same as those for $\mathbb{R}$ except order.

polynomials (with real or complex coefficients) always have a full complement of roots in $\mathbb{C}$ (working for quadratic polynomial function when $\Delta < 0$).

Number Systems

Properties of $\mathbb{Q}$

$\mathbb{Q}$ has the same arithmetic properties and order as those for $\mathbb{R}$ except completeness order.

Properties of $\mathbb{Z}$

In $\mathbb{Z}$, multiplication does not have the same properties, e.g. there is no $n \in \mathbb{Z}$ such that $2.n = 1$

The Integers

The integers mod n also partition $\mathbb{Z}$ into n different equivalence classes; we will denote the set of these equivalence classes by $\mathbb{Z}_n$. We can have a table called a Cayley table

Multiplication table for $\mathbb{Z}_8$

$\cdot$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

The Integers

Build a Cayley table for addition in $\mathbb{Z}_5$

The Integers

The following examples illustrate integer arithmetic modulo n

$$7 + 1 \equiv 3 \pmod{5}$$

$$7 + 1 \equiv 0 \pmod{8}$$

$$7 + 1 \equiv 8 \pmod{9}$$

Mathematical Induction

A mathematical proof technique requires:

- The **base case** proves that the property holds for a certain number (often n = 0 or 1).
- The **induction step**, proves that, if the property holds for one natural number n, then it holds for the next natural number n + 1.

Mathematical Induction

Example 1

We wish to prove that:

$$1 + 2 + ... + n = \frac{n(n+1)}{2}$$

This formula is true for n = 1 since

$$1 = \frac{1(1+1)}{2}$$

We suppose that it is true for the first n cases,

$$1 + 2 + ... + n = \frac{n(n+1)}{2}$$

Mathematical Induction

Example 1

then we have to prove that it is true for (n + 1)th case

$$\begin{aligned}1+2+...+n+(n+1) &= \frac{n(n+1)}{2}+n+1\\ &= \frac{n^2+3n+2}{2}\\ &= \frac{(n+1)((n+1)+1)}{2}\end{aligned}$$