

# Lý thuyết thông tin

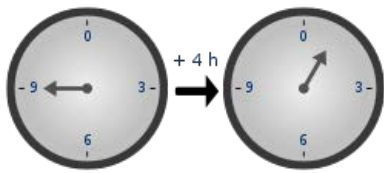
## Phần 3: Cơ sở lý thuyết mã hóa

### Bài 8 (Bài đọc bổ trợ)

## Các cấu trúc đại số



Nguyễn Quốc Dinh



# Modular arithmetic

- **modular arithmetic** is a system of arithmetic for integers
- For a positive integer  $n$ , two integers  $a$  and  $b$  are said to be **congruent modulo  $n$** , and written as

$$a \equiv b \pmod{n},$$

if their difference  $a - b$  is an integer multiple of  $n$  (or  $a - b = kn$ ).

- Let  $a$  and  $n > 0$  be integers. The set of all integers which have the same remainder as  $a$  when divided by  $n$  is called the **congruence class** of  $a$  modulo  $n$ , and is denoted by  $[a]_n$ , where

$$[a]_n = \{ x \in \mathbf{Z} \mid x \equiv a \pmod{n} \}. \quad \rightarrow x = a + k.n; \quad 0 \leq a \leq n-1$$

- The set of **congruence classes** modulo  $n$  is  $\mathbf{Z}_n = \{[0], [1], \dots, [n-1]\}$

- Let  $n$  be a positive integer, and let  $a, b$  be any integers. Then the addition and multiplication of congruence classes given below are well-defined :

$$[a]_n + [b]_n = [a+b]_n \quad ; \quad [a]_n [b]_n = [ab]_n.$$

# Modular arithmetic (cont)

*Example:* The modulo-5 addition and multiplication given by Tables:

Table 1 . Modulo-5 addition

| $\oplus$ | 0 | 1 | 2 | 3 | 4 |
|----------|---|---|---|---|---|
| 0        | 0 | 1 | 2 | 3 | 4 |
| 1        | 1 | 2 | 3 | 4 | 0 |
| 2        | 2 | 3 | 4 | 0 | 1 |
| 3        | 3 | 4 | 0 | 1 | 2 |
| 4        | 4 | 0 | 1 | 2 | 3 |

Table 2 . Modulo-5 multiplication

| $\otimes$ | 0 | 1 | 2 | 3 | 4 |
|-----------|---|---|---|---|---|
| 0         | 0 | 0 | 0 | 0 | 0 |
| 1         | 0 | 1 | 2 | 3 | 4 |
| 2         | 0 | 2 | 4 | 1 | 3 |
| 3         | 0 | 3 | 1 | 4 | 2 |
| 4         | 0 | 4 | 3 | 2 | 1 |

•Chú ý: Bảng cộng và nhân modulo 5 cũng có thể áp dụng cho phép trừ và phép chia:

$$2 - 4 = 2 + (-4) = 2 + 1 = 3.$$

(-4) là phần tử đối của 4 trong phép cộng mod 5

$$3 \div 2 = 3 \cdot (2^{-1}) = 3 \cdot 3 = 4.$$

( $2^{-1}$ ) là phần tử ngược của 2 trong phép nhân mod 5

# Nhóm

## Nhóm (Groups): $\langle G, * \rangle$

Nhóm  $G$  là một tập hợp các phần tử với một phép tính trong 2 ngôi thỏa mãn đồng thời các tính chất sau:

- $a, b \in G \Rightarrow a * b = c \in G$  (tính đóng kín)
- $(a * b) * c = a * (b * c)$  (luật kết hợp)
- Tồn tại phần tử đơn vị  $e$ :  $a * e = e * a = a$
- Tồn tại phần tử ngược  $a^{-1}$ :  $a * a^{-1} = a^{-1} * a = e$

### Chú ý:

Nhóm cộng: phần tử trung hòa kí hiệu  $0$ , phần tử ngược của  $a$  ký hiệu  $-a$

Nhóm nhân: phần tử trung hòa kí hiệu  $1$ , phần tử ngược của  $a$  ký hiệu  $a^{-1}$

$$\Rightarrow \text{Nhóm cộng: } a + (-a) = e = 0$$

$$\Rightarrow \text{Nhóm nhân: } a \cdot (a^{-1}) = e = 1$$

## Nhóm giao hoán

Nếu  $a * b = b * a$  thì nhóm được gọi là nhóm giao hoán.

# Nhóm(cont)

## Ví dụ 1:

- Tập các số nguyên  $\mathbb{Z}$  với phép toán cộng (+) tạo nên một nhóm giao hoán với phần tử đơn vị là 0.
- Nhóm  $\langle \mathbb{R}, + \rangle$  có phần tử trung hòa là 0.
- Nhóm  $\langle \mathbb{R} \setminus \{0\}, \cdot \rangle$  có phần tử trung hòa là 1.
- $\mathbb{Z}_n$  là nhóm cộng theo modulo  $n$ , nhưng không phải nhóm nhân

## Khái niệm $\mathbb{Z}_n^*$

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid (a, n) = 1\}$$

$(a, b), \gcd(a, b)$ : USCLN

- Chú ý: Nếu  $n$  là số nguyên tố thì:  $1 \leq a \leq n-1$

$$\text{exam: } \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

## Cấp của nhóm $|G|$ (hoặc $\deg G$ )

- Còn gọi là lực lượng của nhóm, là số các phần tử trong nhóm.
- Nếu  $|G|$  là hữu hạn thì ta có nhóm hữu hạn cấp  $|G|$ .

Thí dụ: Xét nhóm nhân của  $\mathbb{Z}_{11}$ :  $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

Đây là nhóm cấp 10 vì  $|\mathbb{Z}_{11}^*| = 10$ .

## Nhóm con

- Nếu  $H \in G$  và  $\langle H, * \rangle$  tạo nên một nhóm thì  $H$  là nhóm con của  $G$ .
- Cấp của  $H$  là ước của cấp của  $G$ .

## Nhóm(cont)

### Nhóm xyclic

Xét nhóm hữu hạn  $\langle G, \bullet \rangle$ . Nếu tồn tại phần tử  $\alpha \in G$  sao cho với mỗi  $b \in G$  đều có thể biểu diễn được dưới dạng  $b = \alpha^i$  ( $i$ : nguyên)

Như vậy  $G$  có thể mô tả như sau:

$$G = \{ \alpha^i, \forall i \}$$

thì  $G$  được gọi là nhóm xyclic sinh bởi  $\alpha$ .  $\alpha$  được gọi là **phần tử sinh** (hay phần tử nguyên thủy) của nhóm.

### Ví dụ:

Xét nhóm nhân của  $\mathbb{Z}_{11}^*$ :  $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

Đây là nhóm Cyclic với  $\alpha = 2$ .

Ta có:  $2^0 = 1$   $2^5 = 10$

$2^1 = 2$   $2^6 = 9$

$2^2 = 4$   $2^7 = 7$

$2^3 = 8$   $2^8 = 3$

$2^4 = 5$   $2^9 = 6$

Ta có thể viết  $\mathbb{Z}_{11}^* = \{2^i \bmod 11\}$ .

# Vành

**Vành (Rounds):**  $\langle R, +, \bullet \rangle$

Vành  $R$  là một tập hợp các phần tử với hai phép toán trong hai ngôi (Phép cộng, phép nhân) thỏa mãn các tính chất sau:

- $\langle R, + \rangle$  là một nhóm cộng giao hoán  $\Rightarrow$  phải có  $0$ , mọi phần tử  $a$  có phần tử ngược  $-a$
- $\langle R^*, \bullet \rangle$  không yêu cầu tạo thành nhóm nhân  $\Rightarrow$  Điều này có nghĩa là không nhất thiết phải có phần tử  $1$ , và không nhất thiết mọi phần tử  $a$  đều có phần tử ngược  $a^{-1}$ .

Trong đó:  $R^* = R \setminus \{0\}$

- Tính chất phân phối:  $(a + b) c = a c + b c$

Vành  $R$  được gọi là vành giao hoán nếu ta có  $a b = b a$

# Vành(cont)

## Thí dụ vành:

- Tập  $\mathbb{Z}$  với phép cộng và nhân thông thường là một vành giao hoán
- Tập  $\mathbb{Z}_n$  với phép cộng và nhân modulo  $n$  là một vành giao hoán

cuu duong than cong . com

## Ideal:

Ideal  $I$  là một tập con trong vành  $R$  có các tính chất sau:

- $a, b \in I$  :  $a + b \in I$ ,  $\langle I, + \rangle$  là một nhóm con đối với nhóm cộng của  $R$ .
- $c \in R$  :  $c \cdot a \in I$

cuu duong than cong . com



# Trường

## Trường (Fields) $\langle F, +, \cdot \rangle$

Trường  $F$  là một tập hợp các phần tử với hai phép toán trong hai ngôi thỏa mãn:

- $\langle F, + \rangle$  là một nhóm cộng giao hoán  $\Rightarrow$  có phần tử 0
- $\langle F^*, \cdot \rangle$  là một nhóm đối với phép nhân  $\Rightarrow$  có phần tử 1.

Trong đó:  $F^* = F \setminus \{0\}$

### Thí dụ:

- Tập  $\mathbb{R}$  với phép cộng và nhân thông thường là một trường
- Tập  $\mathbb{C}$  với phép cộng và nhân số phức là một trường
- Tập  $\mathbb{Z}_n$  với phép cộng và nhân modulo  $n$  chỉ là một trường nếu  $n$  là số nguyên tố
- Tập  $\mathbb{Z}$  với phép cộng và nhân thông thường là một vành giao hoán, nhưng không phải là một trường.

**Nhận xét:** Trường chặt chẽ hơn vành.

# Trường(cont)

## finite fields:

- A finite field with  $q$  elements is called  $GF(q)$ . “Galois field” Evariste Galois (1811–1832).  
 $q$  is called order of finite field, and must be a power of a prime  $p$ .
- If  $p$  is a prime number, the set of integers,  $\{0, 1, \dots, p - 1\}$ , forms a prime field  $GF(p)$  with  $p$  elements under modulo- $p$  addition and multiplication, where 0 and 1 are the zero and unit elements of the field, respectively.

## Example:

Consider the special case for which  $p = 2$ . For this case, forms a field of two elements  $\{0, 1\}$ , called a *binary field*, denoted by  $GF(2)$  under modulo-2 addition and multiplication as given by tables:

$$F = GF(2) = \{0, 1 \mid +, *\}$$

| + | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

| * | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

- Chú ý: Trường  $GF(2)$ , trong cả phép cộng và nhân, phần tử ngược của 1 là chính nó.

# Không gian vector (vector spaces)

## Không gian vector trên trường $F$

Giả sử  $F$  là một trường với các phần tử coi là các vô hướng. Một không gian vector  $V$  trên trường  $F$  là một tập hợp  $V$  mà trên đó phép tính cộng vector và phép tính nhân vector với số vô hướng được định nghĩa sao cho các tính chất cơ bản sau đây được thỏa mãn:

- i.  $V$  là một nhóm giao hoán với phép (+)
- ii. Với  $a$  thuộc  $F$ ,  $v$  thuộc  $V$ , thì  $a.v$  thuộc  $V$ .
- iii.  $a.(u+v) = a.u+a.v$ ;  $(a+b)v = a.v+b.v$
- iv.  $(a.b).v = a.(b.v)$
- v. Với  $1$  là phần tử đơn vị của  $F$ :  $1.v = v$

$u, v$  thuộc  $V$  gọi là các vec tơ. Vec tơ  $0$  là phần tử đơn vị của  $V$

$a, b$  thuộc  $F$  gọi là các vô hướng

$u + v$  : vector addition

$a.v$ : Scalar multiplication

# Không gian vectơ (cont)

Nói cách khác, Không gian vectơ trên trường  $F$  có các tính chất sau

- Nếu  $\mathbf{u}, \mathbf{v} \in V$ , thì  $\mathbf{u} + \mathbf{v} \in V$ .
- Nếu  $a \in F, \mathbf{v} \in V$ , thì  $a \mathbf{v} \in V$ .
- Với mọi  $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ , ta có  $\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$ .
- Với mọi  $\mathbf{v}, \mathbf{w} \in V$ , ta có  $\mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v}$ .
- Có một phần tử  $\mathbf{0} \in V$ , gọi là vectơ không, sao cho  $\mathbf{v} + \mathbf{0} = \mathbf{v}$  với mọi  $\mathbf{v} \in V$ .
- Với mọi  $\mathbf{v} \in V$ , có một phần tử  $\mathbf{w} \in V$ , gọi là phần ngược của  $\mathbf{v}$ , sao cho  $\mathbf{v} + \mathbf{w} = \mathbf{0}$ .
- Với mọi  $a \in F$  và  $\mathbf{v}, \mathbf{w} \in V$ , ta có  $a(\mathbf{v} + \mathbf{w}) = a \mathbf{v} + a \mathbf{w}$ .
- Với mọi  $a, b \in F$  và  $\mathbf{v} \in V$ , ta có  $(a + b) \mathbf{v} = a \mathbf{v} + b \mathbf{v}$ .
- Với mọi  $a, b \in F$  và  $\mathbf{v} \in V$ , ta có  $a(b \mathbf{v}) = (ab) \mathbf{v}$ .
- Với mọi  $\mathbf{v} \in V$ , ta có  $1 \mathbf{v} = \mathbf{v}$ ,  $1$  là phần tử đơn vị của phép nhân trong  $F$ .

# Không gian vectơ (cont)

## Không gian tuyến tính $V_n$ trên $GF(2)$

Xét tập  $V_n$  gồm các phần tử có khuôn dạng là một bộ tọa độ  $n$  thành phần ( $n$ -tuple):

$$v = (v_0, v_1, \dots, v_{n-1}) \quad \text{with } v_i \in F$$

- Người ta định nghĩa phép cộng các phần tử của  $V_n$ :

$$u = (u_0, \dots, u_{n-1}) \quad v = (v_0, \dots, v_{n-1})$$

$$u + v = (u_0 + v_0, u_1 + v_1, \dots, u_{n-1} + v_{n-1}) \quad \text{with } u_i + v_i \in F \text{ in mod - 2 addition}$$

- Người ta định nghĩa phép nhân  $n$ -tuple với vô hướng  $a \in F$ :

$$a.v = (av_0, av_1, \dots, av_{n-1}) \quad \text{with } av_i \text{ in mod - 2 multiplication}$$

Nhận xét: Bằng việc chứng minh các tính chất cho thấy  $V_n$  là một không gian vectơ dưới phép cộng và phép nhân với vô hướng như định nghĩa trên. Các  $n$ -tuples được gọi là các vectơ  $n$  chiều trong không gian  $V_n$ .

# Không gian vectơ (cont)

- **Exam:**

- Let  $n = 5$ . The vector space  $V_5$  of all the 5-tuples over  $GF(2)$  consists of the following  $2^5$  binary 5-tuples:

$(00000), (00001), \dots, (11111)$ .

- The vector sum of  $(01010)$  and  $(10110)$  is

$$(01110) + (10110) = (0 + 1, 1 + 0, 1 + 1, 1 + 1, 0 + 0) = (11000) \in V_5.$$

- Using the rule of scalar multiplication, we obtain

$$0.(01110) = (0.0, 0.1, 0.1, 0.1, 0.0) = (00000) \in V_5.$$

$$1.(01110) = (1.0, 1.1, 1.1, 1.1, 1.0) = (01110) \in V_5.$$

# Không gian vectơ (cont)

- **Linear combination** của các vectơ  $\mathbf{v}_0, \dots, \mathbf{v}_{k-1} \in V_n$  là :  $a_0 \mathbf{v}_0 + \dots + a_{k-1} \mathbf{v}_{k-1}$  với các hệ số  $a_0, \dots, a_{k-1} \in F$ .
- Các vectơ  $\mathbf{v}_0, \dots, \mathbf{v}_{k-1} \in V_n$  trên trường  $F$  được gọi là độc lập tuyến tính nếu tổ hợp:  $a_0 \mathbf{v}_0 + \dots + a_{k-1} \mathbf{v}_{k-1}$  chỉ bằng 0 khi và chỉ khi
$$a_0 = a_1 = \dots = a_{k-1} = 0$$

## Hệ quả:

For  $0 \leq k \leq n$ , a set of  $k$  linearly independent vectors in  $V_n$  spans a *k-dimensional subspace* of  $V_n$  (Nghĩa là, Với  $k \leq n$ , và hệ  $G$  gồm  $k$  vectơ độc lập tuyến tính  $\mathbf{g}_0, \dots, \mathbf{g}_{k-1} \in V_n$ . Thì tập  $C$  gồm tất cả các tổ hợp tuyến tính của  $G$  là một **k-dimensional subspace** of  $V_n$ ).

- Hệ  $G$  là một cơ sở (basic) của  $C$ ;  **$G$  spans  $C$** ;  $G$  không chứa vector 0.
- Vì các vectơ của  $C$  có dạng  $c = a_0 \mathbf{g}_0 + \dots + a_{k-1} \mathbf{g}_{k-1}$ ,  $a_i$  thuộc  $GF(2)$ , do đó tương ứng sẽ có  $2^k$  vectơ phân biệt trong  $C$ .
- Một Không gian có tối thiểu một cơ sở, chúng đều có số vectơ bằng nhau.

# Không gian vectơ (cont)

- **Return exam:**

- Let  $n = 5$ . The vector space  $V_5$  of all the 5-tuples over  $GF(2)$  consists of the following 32 binary 5-tuples: (00000), (00001), ..... , (11111).
- The five vectors (10000), (01000), (00100), (00010), and (00001) are linearly independent (dạng chính tắc) and they form a basis of  $V_5$ . This basic spans the  $V_5$  over  $GF(2)$ .
- The basic of 3 linearly independent vectors {(10001), (00111), (11100)} spans a three-dimensional subspace with the following eight vectors:

(00000), (01010), (11100), (10001), (10110), (01101), (11011), (00111).

Ta có thể tìm thấy một cơ sở khác của không gian con này gồm ba vector độc lập tuyến tính {(11100), (01010), (10001)}.



# Không gian vector (cont)

## G-matrix over GF(2)

- Mỗi cơ sở  $G$  của không gian con  $k$  chiều  $C \in V_n$  có thể ánh xạ thành ma trận sinh, trong đó mỗi hàng là một  $n$ -tuple over GF(2).  $G$  có hai cách biểu diễn: **k hàng** hoặc **mảng  $k \times n$** :

$$G = \begin{pmatrix} g_0 \\ g_1 \\ \dots \\ g_{k-1} \end{pmatrix} = \begin{pmatrix} g_{0,0} & g_{0,1} & \dots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & \dots & g_{1,n-1} \\ \dots & \dots & \dots & \dots \\ g_{k-1,0} & g_{k-1,1} & \dots & g_{k-1,n-1} \end{pmatrix}$$

- Không gian con  $k$  chiều  $C$  (gồm  $2^k$  vector sinh bởi  $G$ ) gọi là *row space* của  $G$ .
- Bằng sự thực hiện các phép toán hàng sơ cấp (đổi chỗ hai hàng bất kỳ, cộng một hàng vào một hàng khác) ta sẽ được một ma trận  $G'$ . Cả  $G$  và  $G'$  cùng sinh ra cùng một không gian hàng  $C$ .
- Xét một bộ các vô hướng  $a = (a_0 a_1 \dots a_{k-1})$ . Phép nhân ma trận  $a.G$  sẽ cho 1 vector  $n$  chiều  $v \in C$ :

$$v = (v_0 v_1 \dots v_{n-1}) = a.G = (a_0 a_1 \dots a_{k-1}) \begin{pmatrix} g_0 \\ g_1 \\ \dots \\ g_{k-1} \end{pmatrix} = a_0 g_0 + a_1 g_1 + \dots + a_{k-1} g_{k-1}$$

# Không gian vector (cont)

- Inner Products

- Let  $\mathbf{u} = (u_0, u_1, \dots, u_{n-1})$  and  $\mathbf{v} = (v_0, v_1, \dots, v_{n-1})$  be two  $n$ -tuples over  $\text{GF}(2)$ . We define the *inner product* of  $\mathbf{u}$  and  $\mathbf{v}$  as the following sum:

$$\mathbf{u} \cdot \mathbf{v} = u_0 v_0 + u_1 v_1 + \dots + u_{n-1} v_{n-1}$$

where the multiplications and additions in the sum are carried out with multiplication and addition of  $\text{GF}(2)$ . So the inner product of two  $n$ -tuples over  $\text{GF}(2)$  is an element of  $\text{GF}(2)$ , i.e., a scalar.

- If  $\mathbf{u} \cdot \mathbf{v} = 0$ , we say that  $\mathbf{u}$  and  $\mathbf{v}$  are *orthogonal* (*trực giao*) to each other.
- **Example:** Consider the two 5-tuples, (10111) and (11010). The inner product of these two binary 5-tuples is

$$(10111) \cdot (11010) = 1.1 + 0.1 + 1.0 + 1.1 + 1.0 = 1 + 0 + 0 + 1 + 0 = 0.$$

Since their inner product is 0, they are orthogonal to each other.

# Không gian vector (cont)

## Dual Spaces

- For  $0 \leq k < n$ , let  $C$  be a  $k$ -dimensional subspace of the vector space  $V_n$ .  
Let  $C_d$  be the set of  $n$ -tuples in  $V_n$  such that, for any  $\mathbf{u} \in C$  and  $\mathbf{v} \in C_d$ ,  
inner product:  $\mathbf{u} \cdot \mathbf{v} = 0$ 
  - $C_d$  contains at least the vector  $0$  and hence is non-empty
  - $C_d$  is a subspace of the vector space  $V_n$ .
  - $C_d$  is called the *dual* (or *null*) space of  $C$  and vice versa.
- Theorem:** For  $0 \leq k \leq n$ , let  $C$  be a  $k$ -dimensional subspace of the vector space  $V_n$ . The dimension of its dual space  $C_d$  is  $n - k$ . i.e.,  $\dim(C_d) = n - k$ .
- Note:** Nếu  $C$  có ma trận sinh  $G$ , và  $C_d$  có ma trận sinh  $H$

$$G = \begin{pmatrix} g_0 \\ g_1 \\ \dots \\ g_{k-1} \end{pmatrix} = \begin{pmatrix} g_{0,0} & g_{0,1} & \dots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & \dots & g_{1,n-1} \\ \dots & \dots & \dots & \dots \\ g_{k-1,0} & g_{k-1,1} & \dots & g_{k-1,n-1} \end{pmatrix} \quad H = \begin{pmatrix} h_0 \\ h_1 \\ \dots \\ h_{n-k-1} \end{pmatrix} = \begin{pmatrix} h_{0,0} & h_{0,1} & \dots & h_{0,n-1} \\ h_{1,0} & h_{1,1} & \dots & h_{1,n-1} \\ \dots & \dots & \dots & \dots \\ h_{n-k-1,0} & h_{n-k-1,1} & \dots & h_{n-k-1,n-1} \end{pmatrix}$$

thì bất kỳ hàng  $g_i$  nào và bất kỳ hàng  $h_j$  nào cũng trực giao với nhau, tức là tích vô hướng  $g_i \cdot h_j = 0$ .