Chương 6. Nhắc lại một số kiến thức đại số liên quan

Nhóm giao hoán

ĐN: Tập G cùng với một phép toán cộng trên G, ký hiệu (G,+) là một ***nhóm giao hoán*** nếu:

i. (Kết hợp) $\forall x, y, z \in G: x + (y + z) = (x + y) + z$.

ii. (Giao hoán) $\forall x, y \in G: x + y = y + x$.

iii. (Có ptử trung hoà) $\exists 0 \in G: x + 0 = x, \forall x \in G$.

iv. (Có ptử đối) $\forall x \in G, \exists (-x) \in G: x + (-x) = 0$.

Đối với (G,*), ta viết xy thay cho x*y, ptử đơn vị là 1, ptử nghịch đảo là x^{-1}.

VD: $(\mathbf{Z},+)$, $(\mathbf{R},+)$, $(\mathbf{M}_n(\mathbf{R}),+)$, $(\mathbf{R}\backslash\{0\},*)$, $(\{0,1\}^n,+)$, $(\mathbf{Z}_p,\oplus)$.

VD1: Nhóm $(\{0,1\}^n,+)$

- $\{0,1\}^n$ là tập tất cả các chuỗi nhị phân độ dài n.
- Phép + là phép cộng bit không nhớ.
- Phần tử đối –x của $x \in \{0,1\}^n$ cũng là x.
- Phần tử trung hoà là 00…0.

VD: $\{0,1\}^2 = \{00, 01, 10, 11\}$.

- 01 + 11 = 10.
- 11 + 11 = 00.

VD2: Nhóm $(\mathbf{Z}_p, \oplus)$

- $\mathbf{Z}_p = \{0, 1, 2, \ldots, p-1\}$.
- Phép cộng: với $x, y \in \mathbf{Z}_p$,
  - Nếu $x + y < p$ thì $x \oplus y = x + y$.
  - Nếu $x + y \geq p$ thì $x \oplus y = x + y - p$.
- Phần tử trung hoà là 0.
- Phần tử đối của x là $p - x$.
- Nếu không có gì nhập nhằng ta viết + thay cho $\oplus$.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Figure 1: Addition in $\mathbf{Z}_3$

Phép trừ và phép chia

$$x - y := x + (-y).$$

$$x/y := xy^{-1}.$$

Nhóm con

ĐN: Cho G là nhóm giao hoán, và $K \subseteq G$.

1. K được gọi là ***nhóm con (subgroup)*** của G, ký hiệu $K \leq G$, nếu nó đóng với phép toán +, tức là:
   - $\forall x, y \in K: x + y \in K$.
   - $0 \in K$.
   - Nếu $x \in K$ thì $-x \in K$.
2. Lớp ***ghép (coset)*** của $x \in G$ modulo K là tập $x + K = \{x + k \mid k \in K\}$.

Ví dụ

- Tập tất cả các số nguyên chẵn $\mathbf{Z}_{even}$ là một tập con của $\mathbf{Z}$.
- Lớp ghép của 1 là tập tất cả các số lẻ:
- $1 + \mathbf{Z}_{even} = \{1 + k \mid k \text{ chẵn}\} = \mathbf{Z}_{odd}$.
- $\mathbf{Z}_{odd} = 1 + \mathbf{Z}_{even} = 3 + \mathbf{Z}_{even} = -1 + \mathbf{Z}_{even} = \ldots$
- Lớp ghép của 0 cũng chính là $\mathbf{Z}_{even}$:
- $0 + \mathbf{Z}_{even} = \mathbf{Z}_{even} = 2 + \mathbf{Z}_{even} = 4 + \mathbf{Z}_{even} = \ldots$
- Như vậy: $\mathbf{Z} = \mathbf{Z}_{odd} \cup \mathbf{Z}_{even}$.

Bài tập

1. CMR mọi nhóm con của $(\mathbf{Z},+)$ đều có dạng $p\mathbf{Z}$ với $p = 0, 1, 2, \ldots$
2. Tìm tất cả các nhóm con của $(\mathbf{Z}_{12},+)$.
3. CMR trong mọi nhóm giao hoán G:
   a) Có duy nhất một pt trung hoà/pt đơn vị.
   b) Mỗi $x \in G$, có duy nhất một phần tử đối/nghịch đảo.

Mã tuyến tính nhị phân

Mệnh đề: Mọi mã tuyến tính nhị phân K độ dài n đều là một nhóm con của nhóm $\{0, 1\}^n$.

Chứng minh: Thực vậy, nó thoả 3 tính chất của nhóm con:

- Đóng với phép cộng
- Có phần tử trung hoà
- Có phần tử đối.

Tính chất của lớp ghép

Mệnh đề: các lớp ghép modulo K trong một nhóm G thoả các tính chất sau:

- Mỗi phần tử của G đều nằm trong một lớp nào đó.
- Hai lớp phân biệt thì không có phần tử chung.
- Hai phần tử x, y cùng nằm trong một lớp khi và chỉ khi hiệu của chúng x – y thuộc nhóm con K.
- Nếu |K| = r thì các lớp có cùng r phần tử.

Chứng minh: (bài tập)

Nhận xét

- Một nhóm G có thể phân hoạch thành các lớp rời nhau cùng kích thước.
- Nếu G là một nhóm hữu hạn n phần tử, K là một nhóm con r phần tử của G thì số các lớp là n/r.
- Mỗi lớp ghép ta chọn một phần tử đại diện, gọi là ***coset leader***.
- Tập tất cả các coset leader ký hiệu là G/K.

Lớp $\mathbf{Z}/p\mathbf{Z}$

- Với mỗi số tự nhiên p, đặt $p\mathbf{Z} = \{pn \mid n \in \mathbf{Z}\}$.
- $p\mathbf{Z}$ là một nhóm con của $(\mathbf{Z},+)$
- Có đúng p lớp ghép của $(\mathbf{Z},+)$ modulo $p\mathbf{Z}$: $0 + p\mathbf{Z}$, $1 + p\mathbf{Z}$, …, $p - 1 + p\mathbf{Z}$.
- Ta chọn 0, 1, …, p – 1 làm các coset leader cho các lớp ghép này
- Vậy $\mathbf{Z}/p\mathbf{Z} = \mathbf{Z}_p$.

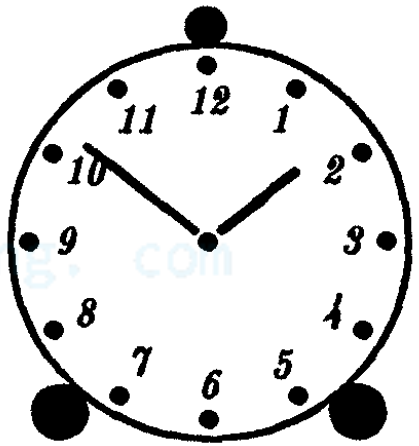


Figure 2: Z_{12}

Đồng dư

ĐN: hai số nguyên x, y được gọi là ***đồng dư modulo p***, ký hiệu $\mathbf{x \equiv y \pmod{p}}$, nếu chúng cùng nằm trong một lớp ghép modulo p**Z**. Nói cách khác x – y chia hết cho p.

VD: $1 \equiv -1 \pmod{2}$.

- $14 \equiv 2 \pmod{12}$.

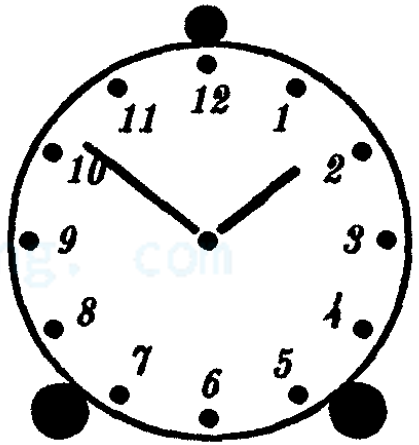


Figure 2: Z_{12}

Dãy chuẩn trong mã nhị phân tuyến tính

- K là nhóm con của $\{0, 1\}^n$.
- → K phân hoạch được thành các coset
- Với mỗi coset, ta chọn coset leader c có w(c) nhỏ nhất.

ĐN: ***standard array*** của K là bảng tất cả các từ mã độ dài n được sắp như sau:

Coset leaders			
$Leader_1$ = $codeword_1$ = 00…0	**$Codeword_2$**	**…**	**$Codeword_m$**
$Leader_2$ …	$Codeword_2 + leader_2$	…	$Codeword_m + leader_2$
$Leader_i$	$Codeword_2 + leader_i$	…	$Codeword_m + leader_i$

K

Chọn coset leader? → Xem giáo trình

VD: Mã K_5

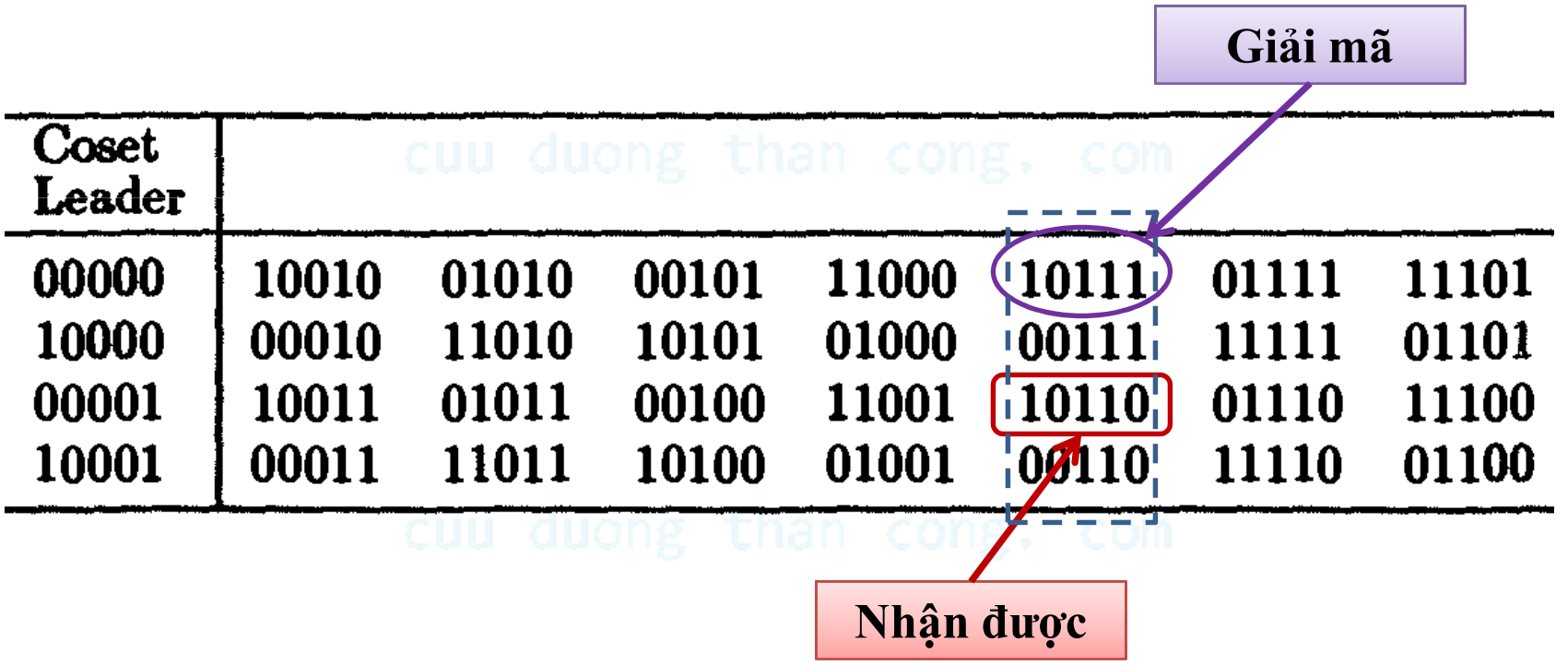
$$x_4 = x_1 + x_2,$$
$$x_5 = x_1 + x_2 + x_3 + x_4.$$

00000	10010	01010	00101	11000	10111	01111	11101

Coset Leader							
00000	10010	01010	00101	11000	10111	01111	11101
10000	00010	11010	10101	01000	00111	11111	01101
00001	10011	01011	00100	11001	10110	01110	11100
10001	00011	11011	10100	01001	00110	11110	01100

Figure 5: A standard array of the code K_5

Giải mã bằng các dãy chuẩn



Bài tập

1. Tìm một dãy chuẩn cho
   a) mã lặp $K_ả$.
   b) Mã Hamming (7,4).
2. Gọi K là mã tuyến tính tạo bởi các tổng của các từ 101011, 011101, 011010.
   a) Tìm ma trận parity check H của K.
   b) Tìm một dãy chuẩn của K. Giải mã chuỗi nhận được 111011.

Trường

ĐN: Tập F với hai phép toán + và * được gọi là ***trường (field)*** nếu thoả các tính chất sau:

1) (F,+) là một nhóm giao hoán với pt trung hoà 0.
2) (F - {0},*) là một nhóm giao hoán với pt đơn vị 1.
3) $x(y + z) = xy + xz$ với mọi $x, y, z \in F$.

VD: **R**, **Q**, **C**, $\mathbf{Z}_2$, $\mathbf{Z}_p$ (với p nguyên tố).

Z không là một trường (mà là một ***vành***).

Lưu ý

1. $xy = 0 \Rightarrow x = 0$ hoặc $y = 0$.
2. $x0 = 0$ với mọi x.
3. với $a \neq 0$: $ax = ay \Rightarrow x = y$.

Bài tập:

1. ả hắc lại Đả của *vành (ring)*.
2. CM: $(x^{-1})^{-1} = x$ với mọi x khác 0.

Trường Z_p

ĐN: $(Z_p,+)$ đã được Đẩ . $(Z_p,*)$ được Đẩ như sau:

x*y = số dư của phép chia xy cho p.

- *Nếu p là số nguyên tố thì Z_p là một trường.*

VD

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Figure 1: Operations of Z_3

Bài tập

1. Viết bảng phép toán cho Z_5. Tìm x^{-1} cho các x khác 0 thuộc Z_5.
2. CMR tập sau cùng với hai phép toán lập thành một trường

+	0	1	p	q
0	0	1	p	q
1	1	0	q	p
p	p	q	0	1
q	q	p	1	0

·	0	1	p	q
0	0	0	0	0
1	0	1	p	q
p	0	p	q	1
q	0	q	1	p

Không gian vector

ĐN: Cho F là một trường, các phần tử $\in$ F gọi là các ***scalar (vô hướng)***. Tập L gồm các phần tử gọi là ***vector***, cùng với phép cộng vector và phép nhân với vô hướng được gọi là một ***không gian vector (vector space)*** nếu:

- (L,+) là một nhóm giao hoán.
- st(a) = s(ta) với mọi a $\in$ L, s, t $\in$ F.
- t(a + b) = ta + tb và (s + t)a = sa + ta với mọi s, t $\in$ F, a, b $\in$ L.

- 1a = a với mọi a.

VD: $\mathbf{Z_2^n}$ = {từ nhị phân độ dài n} là một KGVT

Lưu ý

1. $0a = 0$ với mọi $a \in L$.
2. $(-1)a = -a$ với mọi $a \in L$.
3. $t\mathbf{0} = \mathbf{0}$ với mọi $t \in F$.

Bài tập:

1. Có bao nhiêu vector trong KGVT $\mathbf{Z}_2^n$, $\mathbf{Z}_3^n$
2. CM tập các ma trận với phép toán cộng và nhân vô hướng lập thành một KGVT.

KGVT con

ĐN: Tập $K \subset L$ được gọi là ***KGVT con (subspace)*** nếu nó đóng với phép cộng và nhân:

- $a + b \in K$ với mọi $a, b \in K$.
- $ta \in K$ với mọi $a \in K, t \in F$.

VD: Một mã nhị phân tuyến tính độ dài n là một KGVT con của $\mathbf{Z}_2^n$

Tổ hợp tuyến tính

ĐN: ***Tổ hợp tuyến tính (linear combination)***
của các vector $a_1, a_2, \ldots, a_m \in L$ là tổng

$$t_1a_1 + t_2a_2 + \ldots + t_ma_m$$

với $t_1, \ldots, t_m \in F$.

- $\text{Span}(a_1,\ldots, a_m) := \{t_1a_1 + t_2a_2 + \ldots + t_ma_m \mid t_1, \ldots, t_m \in F\}$ là ***KGVT sinh*** bởi $\{a_1, \ldots, a_m\}$

ĐL: *Span($a_1, \ldots, a_m$) là KGVT con nhỏ nhất chứa $\{a_1, \ldots, a_m\}$.*

Ví dụ

1. Vector (1,0,-1) trong $\mathbf{R}^3$ sinh đường thẳng K = t(1,0,-1) gồm các vector (t,0,-t) với $t \in \mathbf{R}$.

2. Hai vector (1,0,-1) và (0,1,1) sinh mặt phẳng P = t(1,0,-1) + s(0,1,1).

3. Mã kiểm chẵn lẻ độ dài 4 có thể sinh bởi ba vector 1100, 1010, 1001!

Độc lập tuyến tính

ĐN: các vector $a_1, \ldots, a_m$ được gọi là ***độc lập tuyến tính (linearly independent)*** nếu không vector nào là tổ hợp tuyến tính của các vector còn lại.

- Một tập các vector độc lập tuyến tính sinh ra được chính L được gọi là ***cơ sở (basis)*** của KGVT L. Số vector trong một cơ sở của L được gọi là ***số chiều (dimension)*** của L.

Ví dụ

1. $\mathbf{R}^2$ là một KGVT 2 chiều. Một cơ sở là {(0,1),(1,0)}.

2. $\{0,1\}^n$ = {từ nhị phân độ dài n} có n chiều. Một cơ sở là tập tất cả các từ có w(e) = 1.

3. Mã kiểm chẵn lẻ độ dài 4 có thể sinh bởi ba vector 1100, 1010, 1001 độc lập tuyến tính. → số chiều = 3.

Tổ hợp tuyến tính của cơ sở

ĐL: *Cho $\{e_1, e_2, ..., e_m\}$ là một cơ sở của L. Với mỗi vector $a \in L$, tồn tại duy nhất các vô hướng $t_1, ..., t_m$ sao cho*

$$a = t_1e_1 + t_2e_2 + ... + t_me_m.$$

VD: Một từ mã kiểm chẵn lẻ độ dài 4 bất kỳ, chẳn hạn 0110 có thể viết dưới tổ hợp tuyến tính của tập sinh {1100, 1010, 1001} là 0110 = 1100 + 1010.

Tính chất của cơ sở

MĐ: *trong mọi KGVT k-chiều L:*

1) *Mọi cơ sở của L có k vector*
2) *Mọi bộ k vector độc lập tuyến tính tạo thành một cơ sở.*
3) *k là số phần tử lớn nhất của một tập độc lập tuyến tính các vector trong L.*
4) *Các KGVT con của L có số chiều nhỏ hơn k.*

Tích vô hướng

ĐN: ***Tích vô hướng (inner product)*** của hai vector $a = (a_1, a_2, \ldots, a_n)$ và $b = (b_1, b_2, \ldots, b_n)$ là:

$$a \cdot b = a_1b_1 + a_2b_2 + \ldots + a_nb_n.$$

- Hai vector được gọi là ***trực giao (orthogonal)*** nếu tích vô hướng của chúng = 0.

VD: Cho L là một

Bù trực giao

ĐN: Cho L là một KGVT con của F^n. ***Phần bù trực giao*** của L, ký hiệu $L^\perp$ là tập các vector của F^n trực giao với tất cả các vector trong L.

$$L^\perp = \{a \in F^n \mid a \cdot b = 0 \text{ với mọi } b \in L\}.$$

VD: Cho L là một đường thẳng trong $\mathbf{R}^2$. Khi đó, $L^\perp$ là đường thẳng vuông góc với L và đi qua gốc toạ độ

Tính chất của phần bù trực giao

1. $L^{\perp}$ cũng là một KGVT con.
2. ả ếu dim(L) = k thì dim($L^{\perp}$)= n – k.
3. $(L^{\perp})^{\perp} = L$.

Tóm tắt

- Đả nhóm, nhóm con, lớp ghép, trường.
- ả hóm Z_p, Z/pZ.
- Standard array
- Coset leader
- Trường Z_p.
- ĐLập TT, Tổ Hợp TT, Cơ Sở
- Tích vô hướng
- Bù trực giao

Homework

- Đọc và làm Chương 6+7 [1]
- Đọc trước chương 8 [1]