Tổng quan Lý thuyết nhóm

Ngày 23 tháng 4 năm 2021

Nội dung

Lý thuyết tập hợp

Tập hợp (Set): một tập hợp bao gồm các phần tử, mỗi phần tử đều khác nhau.

Lý thuyết tập hợp

Tập hợp (Set): một tập hợp bao gồm các phần tử, mỗi phần tử đều khác nhau.
Biểu diễn tập hợp: có 2 cách biểu diễn tập hợp

1. Liệt kê. Ví dụ $A = \{1, 2, 3, 6\}$
2. Dùng tính chất đặc trưng của các phần tử. Ví dụ $A = \{x \in \mathbb{N} \mid 6 \vdots x\}$

Lý thuyết tập hợp

Tập hợp (Set): một tập hợp bao gồm các phần tử, mỗi phần tử đều khác nhau.

Biểu diễn tập hợp: có 2 cách biểu diễn tập hợp

1. Liệt kê. Ví dụ $A = \{1, 2, 3, 6\}$
2. Dùng tính chất đặc trưng của các phần tử. Ví dụ $A = \{x \in \mathbb{N} \mid 6 \vdots x\}$

Tập hợp rỗng (Empty set): tập hợp không có phần tử nào. Ký hiệu $\varnothing$

Lý thuyết tập hợp

Tập hợp (Set): một tập hợp bao gồm các phần tử, mỗi phần tử đều khác nhau.
Biểu diễn tập hợp: có 2 cách biểu diễn tập hợp

1. Liệt kê. Ví dụ $A = \{1, 2, 3, 6\}$
2. Dùng tính chất đặc trưng của các phần tử. Ví dụ $A = \{x \in \mathbb{N} \mid 6 \vdots x\}$

Tập hợp rỗng (Empty set): tập hợp không có phần tử nào. Ký hiệu $\varnothing$
Tập hợp con (Subset): tập hợp B được gọi là tập hợp con của tập hợp A nếu tất cả phần tử của B đều thuộc A
Ví dụ: $B = \{1, 2, 3\}$, $A = \{1, 2, 3, 4\}$. Ta ký hiệu $B \subset A$
Như vậy tập hợp rỗng là tập hợp con của mọi tập hợp.

Lý thuyết tập hợp

Tập hợp (Set): một tập hợp bao gồm các phần tử, mỗi phần tử đều khác nhau.
Biểu diễn tập hợp: có 2 cách biểu diễn tập hợp

1. Liệt kê. Ví dụ $A = \{1, 2, 3, 6\}$
2. Dùng tính chất đặc trưng của các phần tử. Ví dụ $A = \{x \in \mathbb{N} \mid 6 \vdots x\}$

Tập hợp rỗng (Empty set): tập hợp không có phần tử nào. Ký hiệu $\varnothing$
Tập hợp con (Subset): tập hợp B được gọi là tập hợp con của tập hợp A nếu tất cả phần tử của B đều thuộc A
Ví dụ: $B = \{1, 2, 3\}$, $A = \{1, 2, 3, 4\}$. Ta ký hiệu $B \subset A$
Như vậy tập hợp rỗng là tập hợp con của mọi tập hợp.
Lực lượng của tập hợp: là số phần tử của tập hợp. Ký hiệu là $|A|$. Ví dụ với $A = \{1, 2, 3, 4\}$ thì $|A| = 4$

Lý thuyết số (Number theory)

Chia hết (Divisibility). số nguyên *a chia hết cho/bị chia hết bởi* số nguyên b, nếu tồn tại số nguyên c sao cho $a = bc$. Ký hiệu $a \vdots b$ hoặc $b|a$. Khi đó b gọi là ước của a và a gọi là bội của b

Lý thuyết số (Number theory)

Chia hết (Divisibility). số nguyên *a chia hết cho/bị chia hết bởi* số nguyên b, nếu tồn tại số nguyên c sao cho $a = bc$. Ký hiệu $a \vdots b$ hoặc $b|a$. Khi đó b gọi là ước của a và a gọi là bội của b

Ước chung. Bội chung.

- Nếu số nguyên d vừa là ước của a, vừa là ước của b thì d được gọi là ước chung của a và b. Ví dụ: $\{1, 2\}$ là tập các ước chung của 2 và 4
  Trong tất cả ước chung ta quan tâm tới ước chung lớn nhất.
- Nếu số nguyên c vừa là bội của a, vừa là bội của b thì c được gọi là bội chung của a và b. Ví dụ các số $\{15, 30, 45, \cdots\}$ là các bội chung của 3 và 5
  Trong tất cả bội chung ta quan tâm bội chung nhỏ nhất

Lý thuyết số (Number theory)

Chia hết (Divisibility). số nguyên *a chia hết cho/bị chia hết bởi* số nguyên b, nếu tồn tại số nguyên c sao cho $a = bc$. Ký hiệu $a \vdots b$ hoặc $b|a$. Khi đó b gọi là ước của a và a gọi là bội của b

Ước chung. Bội chung.

- Nếu số nguyên d vừa là ước của a, vừa là ước của b thì d được gọi là ước chung của a và b. Ví dụ: $\{1, 2\}$ là tập các ước chung của 2 và 4
  Trong tất cả ước chung ta quan tâm tới ước chung lớn nhất.
- Nếu số nguyên c vừa là bội của a, vừa là bội của b thì c được gọi là bội chung của a và b. Ví dụ các số $\{15, 30, 45, \cdots\}$ là các bội chung của 3 và 5
  Trong tất cả bội chung ta quan tâm bội chung nhỏ nhất

Số nguyên tố (Prime number). Nếu số nguyên dương p chỉ đúng 2 ước là 1 và chính nó thì p gọi là số nguyên tố. Nếu không thì là **hợp số**. Ví dụ các số nguyên tố: {2, 3, 5, 7, 11, 13, 17, 19, ...}

Nội dung

Lý thuyết nhóm (Group theory)

Định nghĩa. *Nhóm (Group)* $(G, \star)$ gồm một tập hợp G các phần tử và phép toán 2 ngôi $\star$ trên các phần tử thuộc G.

Lý thuyết nhóm (Group theory)

Định nghĩa. *Nhóm (Group)* $(G, \star)$ gồm một tập hợp G các phần tử và phép toán 2 ngôi $\star$ trên các phần tử thuộc G.
Một nhóm thỏa mãn các tính chất sau:

- Tính đóng (Closure): với 2 phần tử a, b bất kì thuộc G, $a \star b \in G$
- Phần tử đơn vị (Identity Law): tồn tại phần tử e sao cho với mọi phần tử $a \in G$, $a \star e = e \star a = a$
- Phần tử nghịch đảo (Inverse Law): với mọi phần tử $a \in G$, tồn tại phần tử $a' \in G$ sao cho $a \star a' = a' \star a = e$
- Tính kết hợp (Associative Law): với mọi $a, b, c \in G$, $(a \star b) \star c = a \star (b \star c)$

Lý thuyết nhóm. Ví dụ

Ví dụ 1. Tập hợp số nguyên $\mathbb{Z}$ và $\star$ là phép cộng $(+)$ thông thường trên tập số nguyên

Lý thuyết nhóm. Ví dụ

Ví dụ 1. Tập hợp số nguyên $\mathbb{Z}$ và $\star$ là phép cộng $(+)$ thông thường trên tập số nguyên

- Với $a, b \in \mathbb{Z}$, $a + b \in \mathbb{Z}$
- Phần tử đơn vị là 0. Với mọi $a \in \mathbb{Z}$ thì $a + 0 = 0 + a = a$
- Phần tử nghịch đảo của a là $-a$, vì $a + (-a) = (-a) + a = 0$
- Tính kết hợp: $(a + b) + c = a + (b + c)$

Lý thuyết nhóm. Ví dụ

Ví dụ 2. Tập hợp số thực $\mathbb{R}\backslash\{0\}$ và $\star$ là phép nhân $(\times)$ thông thường

Lý thuyết nhóm. Ví dụ

Ví dụ 2. Tập hợp số thực $\mathbb{R}\backslash\{0\}$ và $\star$ là phép nhân $(\times)$ thông thường

- Với $a, b \in \mathbb{R}\backslash\{0\}$, $a \times b \in \mathbb{R}\backslash\{0\}$
- Phần tử đơn vị là 1. Với mọi $a \in \mathbb{R}\backslash\{0\}, a \times 1 = 1 \times a = a$
- Phần tử nghịch đảo của a là $\frac{1}{a}$, vì $a \times \frac{1}{a} = \frac{1}{a} \times a = 1$
- Tính kết hợp: $(a \times b) \times c = a \times (b \times c)$

Nhóm Abel. Nhóm vòng

Nếu nhóm có tính giao hoán (Commutative Law): $a \star b = b \star a$, $\forall a, b \in G$, thì nhóm được gọi là **nhóm Abel**

Nhóm Abel. Nhóm vòng

Nếu nhóm có tính giao hoán (Commutative Law): $a \star b = b \star a$, $\forall a, b \in G$, thì nhóm được gọi là **nhóm Abel**

Phép lũy thừa: với nhóm $(G, \star)$ ta định nghĩa phép lũy thừa

- $g^k = \underbrace{g \star g \star \cdots \star g}_{k \text{ lần}}$ với g là phần tử thuộc G và $k \in \mathbb{N}$
- $g^{-k} = (g')^k$
- $g^0 = e$

Nhóm Abel. Nhóm vòng

Nếu nhóm có tính giao hoán (Commutative Law): $a \star b = b \star a$, $\forall a, b \in G$, thì nhóm được gọi là **nhóm Abel**

Phép lũy thừa: với nhóm $(G, \star)$ ta định nghĩa phép lũy thừa

- $g^k = \underbrace{g \star g \star \cdots \star g}_{k \text{ lần}}$ với g là phần tử thuộc G và $k \in \mathbb{N}$
- $g^{-k} = (g')^k$
- $g^0 = e$

Ta gọi G là **nhóm vòng (cyclic group)** nếu mọi phần tử trong G đều có thể biểu diễn dưới dạng g^k với $g \in G$ và $k \in \mathbb{N}$.
Khi đó g được gọi là **phần tử sinh** (generator) của nhóm.

Nhóm Abel. Nhóm vòng

Nếu nhóm có tính giao hoán (Commutative Law): $a \star b = b \star a$, $\forall a, b \in G$, thì nhóm được gọi là **nhóm Abel**

Phép lũy thừa: với nhóm $(G, \star)$ ta định nghĩa phép lũy thừa

- $g^k = \underbrace{g \star g \star \cdots \star g}_{k \text{ lần}}$ với g là phần tử thuộc G và $k \in \mathbb{N}$
- $g^{-k} = (g')^k$
- $g^0 = e$

Ta gọi G là **nhóm vòng (cyclic group)** nếu mọi phần tử trong G đều có thể biểu diễn dưới dạng g^k với $g \in G$ và $k \in \mathbb{N}$.
Khi đó g được gọi là **phần tử sinh** (generator) của nhóm.
Ví dụ: nhóm $(\mathbb{Z}, +)$ với phần tử sinh là 1. Vì với mọi $a \in \mathbb{Z}^+$, ta có
$a = \underbrace{1 + 1 + \cdots + 1}_{a \text{ lần}}$

Lý thuyết nhóm. Bài tập

Bài tập 1. Các tập hợp và toán tử sau có tạo thành nhóm hay không?

1. $(\mathbb{Z}, \times)$
2. $(S, \times)$. Với S là tập hợp các số phức có mô đun là 1, tức là $S = \{z \in \mathbb{C} \mid |z| = 1\}$
3. $((\mathbb{Z}/p\mathbb{Z})^\times, \times)$. Với $(\mathbb{Z}/p\mathbb{Z})^\times$ là tập hợp các thặng dư khác 0 modulo p, trong đó p là số nguyên tố. (tập hợp $\{1, 2, \cdots, p-1\}$)

Lý thuyết nhóm. Bài tập

Bài tập 1. Các tập hợp và toán tử sau có tạo thành nhóm hay không?

1. $(\mathbb{Z}, \times)$
2. $(S, \times)$. Với S là tập hợp các số phức có mô đun là 1, tức là $S = \{z \in \mathbb{C} \mid |z| = 1\}$
3. $((\mathbb{Z}/p\mathbb{Z})^\times, \times)$. Với $(\mathbb{Z}/p\mathbb{Z})^\times$ là tập hợp các thặng dư khác 0 modulo p, trong đó p là số nguyên tố. (tập hợp $\{1, 2, \cdots, p-1\}$)

Bài tập 1 (Đáp án)

1. Không phải vì phần tử đơn vị là 1 nhưng không tồn tại nghịch đảo với mọi $a \in \mathbb{Z}$
2. $(S, \times)$ là một nhóm
3. $((\mathbb{Z}/p\mathbb{Z})^\times, \times$ là nhóm

Lý thuyết nhóm. Bài tập

Bài tập 2. Cho nhóm S_3 bao gồm các phần tử sau

$$e,\ \sigma,\ \sigma^2,\ \tau,\ \sigma\tau,\ \sigma^2\tau$$

với e là phần tử đơn vị và phép nhân được thực hiện theo quy tắc sau

$$\sigma^3 = e,\ \tau^2 = e,\ \tau\sigma = \sigma^2\tau$$

Tính

(a) $\tau\sigma^2$

(b) $\tau(\sigma\tau)$

(c) $(\sigma\tau)(\sigma\tau)$

(d) $(\sigma\tau)(\sigma^2\tau)$

Câu hỏi phụ: S_3 có tính giao hoán không? Vì sao?

Lý thuyết nhóm. Bài tập

Bài tập 2 (Đáp án)

(a) $\tau\sigma^2 = (\tau\sigma)\sigma = (\sigma^2\tau)\sigma = (\sigma^2)(\tau\sigma) = (\sigma^2)(\sigma^2\tau) = \sigma^4\tau = \sigma\tau$

(b) $\tau(\sigma\tau) = (\tau\sigma)\tau = (\sigma^2\tau)\tau = (\sigma^2)(\tau^2) = (\sigma^2)e = \sigma^2$

(c) $(\sigma\tau)(\sigma\tau) = \sigma(\tau\sigma)\tau = \sigma(\sigma^2\tau)\tau = (\sigma^3)(\tau^2) = ee = e$

(d) $(\sigma\tau)(\sigma^2\tau) = (\sigma\tau)(\tau\sigma) = \sigma(\tau^2)\sigma = \sigma e\sigma = \sigma\sigma = \sigma^2$

Dễ thấy, $\tau\sigma = \sigma^2\tau \Rightarrow \tau\sigma \neq \sigma\tau$

Do đó S_3 không giao hoán

Đọc thêm. Nhóm như trên là nhóm Dihedral D_{2n} (ở đây $n = 3$)

Nhóm con (Subgroup)

Số lượng phần tử của nhóm G (order) được ký hiệu là $\#G$

Nhóm con (Subgroup)

Số lượng phần tử của nhóm G (order) được ký hiệu là $\#G$
Cấp của một phần tử (order): với phần tử $g \in G$, số nguyên dương k nhỏ nhất để $g^k = e$ được gọi là *cấp* của phần tử g.

Nhóm con (Subgroup)

Số lượng phần tử của nhóm G (order) được ký hiệu là $\#G$
Cấp của một phần tử (order): với phần tử $g \in G$, số nguyên dương k nhỏ nhất để $g^k = e$ được gọi là *cấp* của phần tử g.
Tính chất: Đặt $n = \#G$

- Với mọi $g \in G$, $g^n = e$
- Nếu phần tử $g \in G$ có order là k, khi đó $k|n$

Nhóm con (Subgroup)

Số lượng phần tử của nhóm G (order) được ký hiệu là $\#G$
Cấp của một phần tử (order): với phần tử $g \in G$, số nguyên dương k nhỏ nhất để $g^k = e$ được gọi là *cấp* của phần tử g.
Tính chất: Đặt $n = \#G$

- Với mọi $g \in G$, $g^n = e$
- Nếu phần tử $g \in G$ có order là k, khi đó $k|n$

Nếu $k = n$, g là phần tử sinh (generator) của nhóm G.

Nhóm con (Subgroup)

Số lượng phần tử của nhóm G (order) được ký hiệu là $\#G$
Cấp của một phần tử (order): với phần tử $g \in G$, số nguyên dương k nhỏ nhất để $g^k = e$ được gọi là *cấp* của phần tử g.
Tính chất: Đặt $n = \#G$

- Với mọi $g \in G$, $g^n = e$
- Nếu phần tử $g \in G$ có order là k, khi đó $k|n$

Nếu $k = n$, g là phần tử sinh (generator) của nhóm G.
Nhóm con của nhóm $(G, \star)$ là nhóm $(G', \star)$, với $G' \subset G$. Khi đó,

- Với mọi $a, b \in G'$, $a \star b \in G'$
- Phần tử đơn vị là e chính là phần tử đơn vị của G
- Phần tử nghịch đảo là $a' \in G'$
- Tính kết hợp: với mọi $a, b, c \in G'$, $(a \star b) \star c = a \star (b \star c)$

Nhóm con. RSA

Tại sao cần nhóm con? Vì việc tính toán trên nhóm con thường nhanh hơn (nhiều lần) do miền giá trị nhỏ hơn.

Nhóm con. RSA

Tại sao cần nhóm con? Vì việc tính toán trên nhóm con thường nhanh hơn (nhiều lần) do miền giá trị nhỏ hơn.
Ví dụ: trong thuật toán RSA, quá trình giải mã $m = c^d \pmod N$, chúng ta thường chọn $e = 65537$ nên d tìm được sẽ rất lớn. Do đó việc giải mã sẽ rất chậm.
Do $N = pq$ với p và q là 2 số nguyên tố phân biệt, ta có thể dùng định lý số dư Trung Hoa để tăng tốc độ tính lên 4 lần.

Nhóm con. RSA

Ngoài p và q để tính $N = pq$, ta cần thêm các tham số dP, dQ và $qInv$ như sau:

- $dP.e = 1 \bmod p$
- $dQ.e = 1 \bmod q$
- $qInv.q = 1 \bmod p$ (với giả định $p > q$)

Nhóm con. RSA

Ngoài p và q để tính $N = pq$, ta cần thêm các tham số dP, dQ và $qInv$ như sau:

- $dP.e = 1 \bmod p$
- $dQ.e = 1 \bmod q$
- $qInv.q = 1 \bmod p$ (với giả định $p > q$)

Áp dụng định lý số dư Trung Hoa theo phương pháp Garner, thay vì tính $m = c^d \pmod N$ ta có thể tính m như sau:

- $m_1 = c^{dP} \bmod p$
- $m_2 = c^{dQ} \bmod q$
- $h = qInv(m_1 - m_2) \pmod p$
- $m = m_2 + qh$

Với cách thực hiện như trên ta chỉ cần tính phép modulo p và q nhỏ hơn rất nhiều so với modulo N

Nội dung

Vành

Định nghĩa. *Vành (Ring)* $(R, +, \times)$ gồm tập hợp R các phần tử và hai phép toán 2 ngôi là phép cộng $(+)$ và phép nhân $(\times)$ thỏa mãn các tính chất sau:

Vành

Định nghĩa. *Vành (Ring)* $(R, +, \times)$ gồm tập hợp R các phần tử và hai phép toán 2 ngôi là phép cộng $(+)$ và phép nhân $(\times)$ thỏa mãn các tính chất sau:

- R là nhóm Abel đối với phép cộng. Ta ký hiệu phần tử đơn vị của phép cộng là 0 và phần tử nghịch đảo của a trong phép cộng là $-a$. Phép trừ $a - b = a + (-b)$
- Tính đóng đối với phép nhân: với 2 phần tử a, b bất kì thuộc R, $a \times b \in R$
- Tính kết hợp đối với phép nhân: với mọi $a, b, c \in R$, $(a \times b) \times c = a \times (b \times c)$
- Tính phân phối giữa phép cộng và phép nhân: với mọi $a, b, c \in$

$$(a + b) \times c = a \times c + b \times c$$
$$a \times (b + c) = a \times b + a \times c$$

Vành

Khi vành có tính giao hoán đối với phép nhân, vành được gọi là **vành giao hoán**

- với mọi $a, b \in R$, $a \times b = b \times a$

Vành

Khi vành có tính giao hoán đối với phép nhân, vành được gọi là **vành giao hoán**

- với mọi $a, b \in R$, $a \times b = b \times a$

Một vành được gọi là **miền nguyên (integral domain)** nếu nó là vành giao hoán và có thêm 2 tính chất sau

- Phần tử đơn vị đối với phép nhân, ký hiệu là 1: $1 \times a = a \times 1 = a$
- Liên quan giữa phép nhân và phần tử đơn vị của phép cộng: nếu $a \times b = 0$ thì $a = 0$ hoặc $b = 0$

Vành. Ví dụ

Ví dụ 1. Các tập $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ với phép cộng và nhân thông thường tạo thành vành.

Vành. Ví dụ

Ví dụ 1. Các tập $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ với phép cộng và nhân thông thường tạo thành vành.

Ví dụ 2 (vành đa thức). Tập hợp các đa thức

$$P = \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \mid a_i \in \mathbb{R}\}$$

với phép cộng và nhân đa thức tạo thành một vành.

Vành. Ví dụ

Ví dụ 1. Các tập $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ với phép cộng và nhân thông thường tạo thành vành.

Ví dụ 2 (vành đa thức). Tập hợp các đa thức

$$P = \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \mid a_i \in \mathbb{R}\}$$

với phép cộng và nhân đa thức tạo thành một vành.
Nếu giới hạn lại hệ số đa thức thành $a_i \in \mathbb{Q}$ hoặc $a_i \in \mathbb{Z}$ thì P vẫn là vành

Nội dung

Trường

Định nghĩa. *Trường (Field)* $(F, +, \times)$ gồm tập hợp F các phần tử và hai phép toán 2 ngôi là phép cộng $(+)$ và phép nhân $(\times)$ thoả mãn các tính chất sau:

- $(F, +, \times)$ là miền nguyên
- Tồn tại phần tử nghịch đảo của phép nhân: với mọi $a \in F$, $a \neq 0$, tồn tại $a^{-1} \in F$ sao cho $a \times a^{-1} = 1$

Trường. Ví dụ

Ta thường làm việc trên các trường hữu hạn như:
Ví dụ 1. Trường hữu hạn $GF(p)$: Với p là số nguyên tố, trường hữu hạn $GF(p)$ tính toán trên tập hợp các thặng dư modulo p (tập hợp $\{0, 1, \cdots, p-1\}$)
Ví dụ 2. Trường hữu hạn $GF(p^n)$: Với p là số nguyên tố và n là số nguyên dương, trường hữu hạn tính toán trên tập hợp

$$P = \{(a_1, a_2, \cdots, a_n) \mid a_i \in GF(p)\}$$

cùng với các quy tắc nhất định khác.

Bài tập tổng kết

Số nguyên Gauss (Gaussian integer) là số phức có dạng

$$z = a + bi$$

với $a, b \in \mathbb{Z}$, $i^2 = -1$. Phép cộng và phép nhân 2 số nguyên Gauss được thực hiện như số phức thông thường.
Ví dụ với 2 số nguyên Gauss $z_1 = a_1 + b_1 i$ và $z_2 = a_2 + b_2 i$ thì

$$z_1 + z_2 = (a_1 + b_1) + (a_2 + b_2)i$$
$$z_1 z_2 = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i$$

Câu hỏi: Tập hợp các số nguyên Gauss với phép cộng và nhân như trên không phải là trường, vì sao? Để trở thành trường cần điều kiện gì?

Cám ơn mọi người đã lắng nghe.
Chúc buổi tối vui vẻ.