

Chương 1

NHÓM

Đại học Khoa Học Tự Nhiên Tp. Hồ Chí Minh

Chương 1. NHÓM

- Nhóm
- Lũy thừa và cấp của phần tử
- Nhóm các số nguyên modulo n
- Nhóm con
- Nhóm con chuẩn tắc và nhóm thương
- Nhóm hoán vị
- Đồng cấu nhóm

1.1. Nhóm

- ❶ Phép toán hai ngôi
- ❷ Định nghĩa nhóm
- ❸ Các tính chất cơ bản của nhóm
- ❹ Bảng nhân
- ❺ Nửa nhóm, vị nhóm

1.1.1. Phép toán hai ngôi

Định nghĩa. Phép toán hai ngôi (gọi tắt là *phép toán*) trên tập hợp X là một ánh xạ

$$\begin{aligned} f : X \times X &\longrightarrow X \\ (x, y) &\longmapsto f(x, y). \end{aligned}$$

Ta dùng ký hiệu xfy thay cho $f(x, y)$. Như vậy, ứng với các phép toán $*, \circ, +, \cdot, \dots$ ta có các ký hiệu $x*y, x \circ y, x + y, x \cdot y, \dots$

Nhận xét. $*$ là phép toán trên X nếu thỏa *tính đóng*, nghĩa là

$$\forall x, y \in X, x*y \in X.$$

Ví dụ.

- Phép cộng và phép nhân thông thường trên các tập hợp $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ là các phép toán.
- Phép trừ thông thường là phép toán trên các tập hợp $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ nhưng *không* là phép toán trên \mathbb{N} .

Tính chất

Định nghĩa. Cho phép toán $*$ trên tập hợp X . Ta nói phép toán $*$:

- ① **giao hoán**, nếu với mọi $x, y \in X, x*y = y*x$;
- ② **kết hợp**, nếu với mọi $x, y, z \in X, (x*y)*z = x*(y*z)$;
- ③ có **phần tử trung hòa trái** (tương ứng, **phải**) là e nếu $e \in X$ và với mọi $x \in X, e*x = x$ (tương ứng, $x*e = x$).

Nếu e vừa là phần tử trung hòa trái vừa là phần tử trung hòa phải thì ta nói e là **phần tử trung hòa** của phép toán $*$.

Mệnh đề. Một phép toán có nhiều nhất một phần tử trung hòa

Chứng minh. Giả sử e' và e'' là hai phần tử trung hòa. Khi đó

$$\begin{aligned} e' &= e' * e'' && (\text{vì } e'' \text{ là trung hòa phải}) \\ &= e'' && (\text{vì } e' \text{ là trung hòa trái}) \end{aligned}$$

Định nghĩa. Cho $*$ là một phép toán trên tập hợp X có phần tử trung hòa e và x là một phần tử tùy ý của X . Ta nói

- x **khả đối xứng trái** (tương ứng, **phải**) nếu tồn tại $x' \in X$ sao cho $x' * x = e$ (tương ứng, $x * x' = e$).
- Khi đó x' được gọi là **phần tử đối xứng trái** (tương ứng, **phải**) của x .

Trường hợp x vừa khả đối xứng trái, vừa khả đối xứng phải thì ta nói x khả đối xứng và phần tử $x' \in X$ thỏa $x * x' = x' * x = e$ được gọi là **phần tử đối xứng** của x .

Mệnh đề. Nếu phép toán $*$ kết hợp thì một phần tử có nhiều nhất một phần tử đối xứng.

Chứng minh. Giả sử x' và x'' là hai phần tử đối xứng của x . Khi đó $x' * x = e$ và $x * x'' = e$. Do đó

$$x' = x' * e = x' * (x * x'') = (x' * x) * x'' = e * x'' = x''.$$

1.1.2. Định nghĩa nhóm

Định nghĩa. Cho G là tập khác rỗng và $*$ là một phép toán trên G . Khi đó G được gọi là **nhóm** với phép toán $*$ nếu thỏa 3 tính chất sau:

- i) Tính kết hợp: $\forall x, y, z \in G, (x*y)*z = x*(y*z)$;
- ii) Tính trung hòa: Tồn tại $e \in G$ sao cho $\forall x \in G, x*e = e*x = x$;
- iii) Tính khả đối xứng: $\forall x \in G$ tồn tại $x' \in G$ sao cho
$$x*x' = x'*x = e.$$

Ví dụ. Xét tập hợp $G = \mathbb{Z}$ với phép toán $*$ là phép toán cộng. Chứng minh rằng $(\mathbb{Z}, *)$ là nhóm.

Giải.

- ❶ **Tính kết hợp:** Với mọi $x, y, z \in \mathbb{Z}$, ta có

$$(x*y)*z = (x + y) + z = x + (y + z) = x*(y*z).$$

② **Tính trung hòa:** Cho $e = 0$, với mọi $x \in \mathbb{Z}$, ta có

$$x * e = x + 0 = x \text{ và } e * x = 0 + x = x.$$

Do đó tồn tại $e = 0 \in \mathbb{Z}$ sao cho

$$\forall x \in \mathbb{Z}, x * e = e * x = x.$$

③ **Tính khả đối xứng:** Với mọi $x \in \mathbb{Z}$, ta chọn $x' = -x$. Ta có

$$x * x' = x + (-x) = 0 = e \text{ và } x' * x = (-x) + x = 0 = e.$$

Do đó, $\forall x \in \mathbb{Z}$ tồn tại $x' = -x \in \mathbb{Z}$ sao cho $x * x' = x' * x = e$.

Như vậy $(\mathbb{Z}, +)$ là nhóm. Tương tự

$$(\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Q}^*, .), (\mathbb{R}^*, .), (\mathbb{C}^*, .)$$

là các nhóm.

Định nghĩa. Nếu với mọi $x, y \in G$ ta có $x*y = y*x$, thì G được gọi là nhóm *giao hoán* hay nhóm *Abel*.

Ví dụ.(tự làm) Trên \mathbb{Z} , ta định nghĩa phép toán như sau

$$\forall x, y \in \mathbb{Z}, x*y = x + y - 2.$$

Chứng minh $(\mathbb{Z}, *)$ là nhóm Abel.

Ví dụ.(tự làm) Chứng tỏ rằng các tập sau với phép toán tương ứng không là nhóm

- a \mathbb{N} với phép cộng
- b \mathbb{Z} với phép trừ
- c \mathbb{R} với phép nhân
- d $M_2(\mathbb{R})$ với phép nhân ma trận

Chú ý. Để đơn giản trong trình bày, phép toán $*$ có thể được ngầm hiểu và ký hiệu xy (đọc là “ x nhân y ”) được thay cho $x*y$.

Đồng thời, ta có thể nói G là nhóm thay vì $(G, *)$ là nhóm.

Định nghĩa. Số phần tử của nhóm G được gọi là **cấp** của G , ký hiệu bởi $|G|$

- Nếu G có hữu hạn phần tử thì G được gọi là **nhóm hữu hạn**.
- Nếu nhóm G có vô hạn phần tử thì G được gọi là **nhóm vô hạn** và ta ký hiệu $|G| = \infty$.

Ví dụ. Xét $G = \{1, -1\}$ với phép nhân thông thường. Khi đó, G là nhóm Abel hữu hạn (cấp 2).

Ví dụ. Xét $G = \{1, -1, i, -i\}$ với phép nhân thông thường. Khi đó, G là nhóm Abel hữu hạn (cấp 4).

Ví dụ. $(\mathbb{Z}, +)$ là nhóm vô hạn.

1.1.3. Các tính chất cơ bản của nhóm

Mệnh đề. Cho G là nhóm. Khi đó

- ❶ Phần tử e (trong tính chất ii)) xác định duy nhất, được gọi là **phần tử đơn vị** hay phần tử trung hòa của G .
- ❷ Với mọi $x \in G$, phần tử x' (trong tính chất iii)) xác định duy nhất, được gọi là **phần tử nghịch đảo** hay phần tử đối xứng của x , ký hiệu x^{-1} .

Ví dụ. Đặt $GL_n(\mathbb{R})$ là tập hợp tất cả các ma trận vuông khả nghịch cấp n với hệ số thuộc \mathbb{R} , nghĩa là

$$GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det(A) \neq 0\}.$$

Khi đó $GL_n(\mathbb{R})$ là nhóm với phép toán nhân ma trận.

Phần tử đơn vị của $GL_n(\mathbb{R})$ là ma trận đơn vị I_n , và phần tử nghịch đảo của ma trận $A \in GL_n(\mathbb{R})$ là ma trận A^{-1} .

Nhóm $GL_n(\mathbb{R})$ được gọi là **nhóm tuyến tính tổng quát** bậc n trên \mathbb{R} .

Mệnh đề. Giả sử G là một nhóm với phần tử đơn vị e . Khi đó, với mọi $x, y, z \in G$, ta có:

i) $(x^{-1})^{-1} = x.$

ii) $(xy)^{-1} = y^{-1}x^{-1}.$

iii) $xy = e$ khi và chỉ khi $yx = e$. Hơn nữa khi đó $y = x^{-1}.$

iv) Phép toán có tính giản ước, nghĩa là $\forall x, y, z \in G$, nếu $xy = xz$ hay $yx = zx$ thì $y = z.$

Chứng minh. i) Ta có

$$(x^{-1})^{-1} = (x^{-1})^{-1}e = (x^{-1})^{-1}(x^{-1}x) = ((x^{-1})^{-1}x^{-1})x = ex = x.$$

ii) Ta có

$$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xex^{-1} = (xe)x^{-1} = xx^{-1} = e.$$

Nhân trái hai vế cho $(xy)^{-1}$ ta được $(xy)^{-1} = y^{-1}x^{-1}.$

iii) Giả sử $xy = e$. Ta có

$$x^{-1} = x^{-1}e = x^{-1}(xy) = (x^{-1}x)y = ey = y.$$

Nhân phải hai vế cho x , ta $yx = x^{-1}x = e$. Tương tự cho chiều đảo.

iv) Giả sử $xy = xz$. Ta nhân trái hai vế cho x^{-1} ta có

$$\begin{aligned}x^{-1}(xy) &= x^{-1}(xz) \\ \Leftrightarrow (x^{-1}x)y &= (x^{-1}x)z \\ \Leftrightarrow ey &= ez \\ \Leftrightarrow y &= z.\end{aligned}$$

Tương tự nếu $yx = zx$ thì bằng cách nhân phải hai vế cho x^{-1} ta được $y = z$.

1.1.4. Bảng nhân

Giả sử $G = \{x_1, x_2, \dots, x_n\}$ là nhóm hữu hạn cấp n . Khi đó **bảng nhân** của nhóm G là một bảng gồm n^2 vị trí, trong đó phần tử ở vị trí dòng thứ i và cột thứ j là tích $x_i x_j$.

	x_1	x_2	\dots	x_n
x_1	$x_1 x_1$	$x_1 x_2$	\dots	$x_1 x_n$
x_2	$x_2 x_1$	$x_2 x_2$	\dots	$x_2 x_n$
\vdots	\vdots	\vdots	\ddots	\vdots
x_n	$x_n x_1$	$x_n x_2$	\dots	$x_n x_n$

Nhận xét. Các phần tử trên một dòng hay một cột đều khác nhau, và là một sự hoán vị các phần tử của G .

Ví dụ. Lập bảng nhân của nhóm $G = \{1, -1\}$ với phép toán nhân thông thường.

$$G = \{1, -1\}$$

Giải.

	1	-1
1	1	-1
-1	-1	1

Ví dụ.(tự làm) Lập bảng nhân của nhóm $G = \{1, -1, i, -i\}$ với phép toán nhân thông thường.

Đáp án.

	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

1.1.5. Nửa nhóm, vị nhóm

Định nghĩa. Cho $G \neq \emptyset$ và $*$ là một phép toán trên G . Khi đó $(G, *)$ được gọi là

- ① **nửa nhóm** nếu $*$ có tính chất kết hợp.
- ② **vị nhóm** nếu $*$ có tính chất kết hợp và có phần tử đơn vị.

Nhận xét. Mọi nhóm đều là nửa nhóm, nhưng điều ngược lại không đúng.

Ví dụ.

- ① $(\mathbb{N}, +)$, (\mathbb{N}, \cdot) là nửa nhóm, vị nhóm nhưng không là nhóm.
- ② $(\mathbb{Z}, -)$ không là nửa nhóm.
- ③ $(\mathbb{N}^*, +)$ là nửa nhóm, nhưng không là vị nhóm.

Định lý. Cho $(G, .)$ là một nửa nhóm khác rỗng. Các mệnh đề sau tương đương:

- (i) $(G, .)$ là một nhóm.
- (ii) Với mọi $a, b \in G$, các phương trình $ax = b$ và $ya = b$ đều có nghiệm trong G .
- (iii) Trong G có phần tử đơn vị trái e' và với mọi $x \in G$, tồn tại $x' \in G$ sao cho $x'x = e'$.
- (iv) Trong G có phần tử đơn vị phải e'' và với mọi $x \in G$, tồn tại $x'' \in G$ sao cho $xx'' = e''$.

Chứng minh. (i) \Rightarrow (ii) Ta có $x = a^{-1}b$ và $y = ba^{-1}$ lần lượt là các nghiệm của phương trình $ax = b$ và $ya = b$.

(ii) \Rightarrow (iii) Do $G \neq \emptyset$ nên tồn tại $a_0 \in G$. Gọi e' là nghiệm của phương trình $ya_0 = a_0$, nghĩa là $e'a_0 = a_0$. Khi đó e' là phần tử đơn vị trái. Thật vậy, với b là một phần tử tùy ý của G , gọi c là nghiệm của phương trình $a_0x = b$, khi đó $a_0c = b$ nên

$$e'b = e'(a_0c) = (e'a_0)c = a_0c = b.$$

Vậy e' là phần tử đơn vị trái. Tính chất sau cùng trong (iii) được suy từ giả thiết mọi phương trình dạng $ya = e'$ đều có nghiệm trong G .

(iii) \Rightarrow (i) Giả sử trong G có phần tử đơn vị trái e' và với mọi $x \in G$, tồn tại $x' \in G$ sao cho $x'x = e'$. Ta chứng minh e' là phần tử đơn vị và x' là phần tử nghịch đảo của x .

Theo giả thiết, với x' như trên tồn tại $x'' \in G$ sao cho $x''x' = e'$. Do đó

$$xx' = e'(xx') = (x''x')(xx') = x''(x'x)x' = x''e'x' = x''x' = e'.$$

Suy ra

$$xe' = x(x'x) = (xx')x = e'x = x.$$

Các kết quả trên chứng tỏ e' là phần tử đơn vị và $x' = x^{-1}$. Do đó $(G, .)$ là một nhóm.

Tương tự ta cũng có (i) \Rightarrow (ii); (ii) \Rightarrow (iv) và (iv) \Rightarrow (i).

1.2. Lũy thừa và cấp của phần tử

- ❶ Lũy thừa của một phần tử
- ❷ Cấp của một phần tử

1.2.1. Lũy thừa của một phần tử

Định nghĩa. Cho G là nhóm với phần tử đơn vị e và $x \in G$. **Lũy thừa** bậc $k \in \mathbb{N}$ của x (ký hiệu bởi x^k) được định nghĩa bằng quy nạp như sau:

$$x^0 = e; \quad x^1 = x; \quad x^2 = xx; \dots; \quad x^k = (x^{k-1})x.$$

Với mọi k nguyên dương, ta ký hiệu x^{-k} để chỉ phần tử $(x^{-1})^k$.

Mệnh đề. Cho G là một nhóm và $x \in G$. Khi đó, với mọi $m, n \in \mathbb{Z}$ ta có:

i) $x^m x^n = x^{m+n} = x^n x^m.$

ii) $(x^m)^n = x^{mn}.$

Mệnh đề. Cho G là nhóm và $x, y \in G$ sao cho $xy = yx$. Khi đó, với mọi $n \in \mathbb{Z}$, ta có $(xy)^n = x^n y^n.$

Chú ý. Tùy theo phép toán chúng ta đang xét trên nhóm G mà tên gọi, ký hiệu các phần tử trên G thay đổi. Cụ thể

Nhóm $(G, .)$	Nhóm $(G, +)$
tích của a với b : ab phần tử đơn vị: $e; 1$ phần tử nghịch đảo của a : a^{-1} lũy thừa bậc n của a : a^n	tổng của a với b : $a + b$ phần tử không: 0 phần tử đối của a : $-a$ n lần a : na

1.2.2. Cấp của một phần tử

Hỏi. Cho G là nhóm và $x \in G$. Hỏi tồn tại số nguyên dương n sao cho $x^n = e$ không?

Ví dụ. Cho nhóm $(\mathbb{R}^*, .)$, tìm phần tử thỏa mãn câu hỏi trên.

Định nghĩa. **Cấp** của x là số nguyên dương n nhỏ nhất sao cho $x^n = e$, ký hiệu là $|x|$ hay $\text{ord}(x)$.

Nếu không tồn tại như vậy thì x được gọi là phần tử có **cấp vô hạn**, và ta ký hiệu $|x| = \infty$.

Ví dụ.

- ❶ Trong nhóm $(\mathbb{R}, +)$, mọi phần tử khác 0 đều có cấp vô hạn.
- ❷ Trong nhóm $G = \{1, -1, i, -i\}$, mọi phần tử đều có cấp hữu hạn, cụ thể: phần tử 1 có cấp 1; phần tử -1 có cấp 2; các phần tử i và $-i$ có cấp 4.

Mệnh đề. Cho G là một nhóm và $x \in G$. Khi đó:

i) $|x| = 1 \Leftrightarrow x = e$.

ii) Nếu $|x| = n$ thì $\forall m \in \mathbb{Z}, x^m = e \Leftrightarrow n \mid m$.

Chứng minh. i) Hiển nhiên.

ii) Gọi p, r lần lượt là phần thương và phần dư trong phép chia m cho n , nghĩa là

$$m = np + r, \quad 0 \leq r < n.$$

Khi đó

$$x^m = x^{np+r} = (x^n)^p x^r = x^r.$$

(\Rightarrow) Nếu $x^m = e$ thì $x^r = e$. Mà n là số nguyên dương nhỏ nhất sao cho $x^n = e$ và $0 \leq r < n$ nên $r = 0$. Do đó $n \mid m$.

(\Leftarrow) Nếu $n \mid m$ thì $r = 0$ nên $x^m = e$.

Mệnh đề. Cho G là nhóm và $x, y \in G$. Khi đó:

❶ $|xy| = |yx|$

❷ $|x^{-1}| = |x|$

Chứng minh. i) Với mỗi n nguyên dương, ta có

$$\begin{aligned}(xy)^n &= \underbrace{(xy)(xy) \dots (xy)}_{n \text{ lần}} \\&= \underbrace{(xy)(xy) \dots (xy)}_{n \text{ lần}} (xx^{-1}) \\&= x \underbrace{(yx)(yx) \dots (yx)}_{n \text{ lần}} x^{-1} \\&= x(yx)^n x^{-1}\end{aligned}$$

Do đó, nếu $|xy| = n$ thì $(xy)^n = e$ và $(xy)^k \neq e$ với mọi $0 < k < n$. Suy ra $(yx)^n = e$ và $(yx)^k \neq e$ với mọi $0 < k < n$. Do đó $|yx| = n$.

ii) Ta có $(x^{-1})^n = (x^n)^{-1}$ nên lý luận tương tự trên ta cũng được $|x^{-1}| = |x|$.

1.3. Nhóm các số nguyên modulo n

- ❶ Nhóm $(\mathbb{Z}_n, +)$
- ❷ Phép nhân trong \mathbb{Z}_n

1.3.1. Nhóm $(\mathbb{Z}_n, +)$

Nhắc lại. Cho n là một số nguyên dương và \sim là một quan hệ trên \mathbb{Z} xác định bởi:

$$\forall x, y \in \mathbb{Z}, x \sim y \Leftrightarrow x \text{ và } y \text{ có cùng phần dư khi chia cho } n.$$

hay

$$\forall x, y \in \mathbb{Z}, x \sim y \Leftrightarrow (x - y) \vdots n.$$

Khi đó \sim là một quan hệ tương đương trên \mathbb{Z} . Quan hệ này được gọi là *quan hệ đồng dư theo modulo n* .

Với mỗi $x \in \mathbb{Z}$, ta có

$$\bar{x} = \{x + kn \mid k \in \mathbb{Z}\} = \{x, x \pm n, x \pm 2n, x \pm 3n, \dots\}.$$

Ta đặt

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$$

Định nghĩa.

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}.$$

Trên \mathbb{Z}_n , ta định nghĩa phép toán $+$ như sau:

$$\forall \bar{x}, \bar{y} \in \mathbb{Z}_n, \quad \bar{x} + \bar{y} = \overline{x + y}.$$

Khi đó $(\mathbb{Z}_n, +)$ là nhóm Abel hữu hạn. Nhóm này được gọi là *nhóm cộng các số nguyên modulo n* .

Ví dụ. Bảng cộng của nhóm \mathbb{Z}_4

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Nhận xét. Với mọi $\bar{x} \in \mathbb{Z}_n$ và mọi $m \in \mathbb{Z}$, ta có $m \cdot \bar{x} = \overline{mx}$.

1.3.2. Phép nhân trong \mathbb{Z}_n

Định nghĩa. Với $\bar{x}, \bar{y} \in \mathbb{Z}_n$, ta đặt

$$\bar{x} \cdot \bar{y} = \overline{xy}.$$

Khi đó (\mathbb{Z}_n, \cdot) là nửa nhóm.

Ví dụ. Trong \mathbb{Z}_8 ta có $\bar{2} \cdot \bar{4} = \bar{0}$; $\bar{4} \cdot \bar{5} = \bar{4}$.

Định nghĩa. Phần tử \bar{x} trong \mathbb{Z}_n được gọi là **khả nghịch** nếu tồn tại $\bar{y} \in \mathbb{Z}_n$ sao cho $\bar{x} \cdot \bar{y} = \bar{1}$.

Khi đó \bar{y} được gọi là nghịch đảo của \bar{x} , ký hiệu $\bar{y} = \bar{x}^{-1}$.

Ví dụ. Trong \mathbb{Z}_9 ta có:

- ❶ $\bar{3}$ không khả nghịch, vì $\bar{3} \cdot \bar{3} = \bar{0}$.
- ❷ $\bar{4}$ khả nghịch và $\bar{4}^{-1} = \bar{7}$, vì $\bar{4} \cdot \bar{7} = \bar{1}$.

Mệnh đề. Cho $\bar{x} \in \mathbb{Z}_n$, ta có \bar{x} khả nghịch khi và chỉ khi $(x; n) = 1$.

Chứng minh. (\Rightarrow) Nếu \bar{x} khả nghịch thì tồn tại $\bar{y} \in \mathbb{Z}_n$ sao cho

$$\bar{x}.\bar{y} = \bar{1} \Leftrightarrow \overline{xy} = \bar{1}.$$

Do đó tồn tại $p \in \mathbb{Z}$ sao cho $xy = 1 + np$, nghĩa là

$$x.y + n(-p) = 1.$$

Như vậy $(x; n) = 1$.

(\Leftarrow) Nếu $(x; n) = 1$ thì tồn tại $p, q \in \mathbb{Z}$ sao cho

$$xp + nq = 1.$$

Suy ra $\overline{x.p} = \bar{1}$, do đó \bar{x} khả nghịch và $\bar{x}^{-1} = \bar{p}$.

Kiểm tra tính khả nghịch và tìm nghịch đảo của $\bar{x} \in \mathbb{Z}_n$

Tìm d là ước số chung lớn nhất của x và n .

- Nếu $d = 1$ thì dùng thuật chia Euclid để biểu diễn

$$1 = xp + nq.$$

Khi đó $\bar{x}.\bar{p} = \bar{1}$ nên \bar{x} khả nghịch và $\bar{x}^{-1} = \bar{p}$.

- Nếu $d > 1$ thì ta biểu diễn $x = dp$ và $n = dq$. Khi đó

$$xq = dpq = pn,$$

nên $\bar{x}.\bar{p} = \bar{0}$. Do đó \bar{x} không khả nghịch.

Ví dụ. Trong \mathbb{Z}_{24} , tìm tất cả các phần tử khả nghịch và tìm phần tử nghịch đảo tương ứng.

1.4 Nhóm con

- ① Định nghĩa nhóm con
- ② Tính chất của nhóm con
- ③ Nhóm con cyclic
- ④ Nhóm con sinh bởi một tập hợp

1.4.1. Định nghĩa nhóm con

Định nghĩa. Cho G là nhóm và $\emptyset \neq H \subseteq G$. Khi đó H được gọi là **nhóm con** của G , ký hiệu $H \leq G$, nếu H là nhóm đối với phép toán đã được trang bị trên G .

Ví dụ. Cho G là nhóm. Khi đó $\{e\}$ và G đều là các nhóm con của G . Ta gọi các nhóm này là các **nhóm con tầm thường** của G .

Ví dụ.

- 1 Nhóm cộng: $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.
- 2 Nhóm nhân: $Q^* \leq R^* \leq C^*$.

Ví dụ. Cho n là một số nguyên dương, ta đặt $n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$. Khi đó $n\mathbb{Z} \leq \mathbb{Z}$.

1.4.2. Tính chất của nhóm con

Định lý. Cho H là một tập con khác rỗng của nhóm G . Khi đó các mệnh đề sau tương đương:

- (i) $H \leq G$;
- (ii) Với mọi $x, y \in H, xy \in H$ và $x^{-1} \in H$;
- (iii) Với mọi $x, y \in H, x^{-1}y \in H$;
- (iv) Với mọi $x, y \in H, xy^{-1} \in H$.

Chứng minh. (i) \Rightarrow (ii). Với mọi $x, y \in H$, vì H là nhóm nên $xy \in H$.

Gọi e' là phần tử đơn vị của nhóm con H . Ta có $xe' = x$. Nhân trái hai vế cho x^{-1} trong G ta được $e' = e$.

Giả sử x' là phần tử nghịch đảo của x trong nhóm con H , ta có $x'x = e$ nên $x^{-1} = x' \in H$.

(ii) \Rightarrow (iii). Với mọi $x, y \in H$, theo giả thiết (ii) cho ta $x^{-1} \in H$. Do đó $x^{-1}y \in H$.

(iii) \Rightarrow (i) Vì $H \neq \emptyset$ nên tồn tại $a \in H$. Do đó $e = a^{-1}a \in H$.

Với mọi $x \in H$, $x^{-1} = x^{-1}e \in H$.

Cuối cùng, với mọi $x, y \in H$, do $x^{-1} \in H$ nên $xy = (x^{-1})^{-1}y \in H$. Suy ra $H \leq G$.

Tương tự cho trường hợp (ii) \Rightarrow (iv) và (iv) \Rightarrow (i).

Ví dụ. Xét G là nhóm $(\mathbb{Z}, +)$ và H là tập hợp tất cả các số nguyên chẵn. Kiểm tra $H \leq G$.

Giải.

- ❶ Rõ ràng $H \neq \emptyset$ và $H \subseteq G$.
- ❷ Với mọi $x, y \in H$, nghĩa là x, y là những số chẵn, ta có
 - ❶ $x + y$ chẵn, suy ra $x + y \in H$
 - ❷ $-x$ chẵn, suy ra $-x \in H$

Vậy $H \leq G$.

Ví dụ. (tự làm) Cho G là nhóm $(\mathbb{Z}, +)$ và n là số nguyên dương. Đặt

$$H = \{na \mid a \in \mathbb{Z}\}$$

Kiểm tra $H \leq G$.

Nhắc lại. $GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det(A) \neq 0\}$.

Ví dụ. Với $n \geq 2$, ta đặt

$$SL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det(A) = 1\}.$$

Chứng minh $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$.

Giải.

- 1 Ta có $\det(I_n) = 1$ nên $I_n \in SL_n(\mathbb{R})$. Do đó $SL_n(\mathbb{R}) \neq \emptyset$.
- 2 Với mọi $A \in SL_n(\mathbb{R})$ ta có $\det(A) = 1 \neq 0$ nên A khả nghịch, nghĩa là $A \in GL_n(\mathbb{R})$. Do đó $SL_n(\mathbb{R}) \subseteq GL_n(\mathbb{R})$.

③ Với mọi $A, B \in SL_n(\mathbb{R})$, ta có $\det(A) = \det(B) = 1$. Khi đó

- $\det(AB) = \det(A)\det(B) = 1$. Do đó $AB \in SL_n(\mathbb{R})$.
- $\det(A^{-1}) = \frac{1}{\det(A)} = 1$. Do đó $A^{-1} \in SL_n(\mathbb{R})$.

Vậy $SL_n(\mathbb{R})$ là nhóm con của $GL_n(\mathbb{R})$. Nhóm này được gọi là **nhóm tuyến tính đặc biệt bậc n** trên \mathbb{R} .

Mệnh đề. Nếu H và K là hai nhóm con của nhóm G thì $H \cap K$ cũng là nhóm con của G .

Chứng minh. • Vì H, K là các nhóm con của G nên $H \cap K \subseteq G$. Hơn nữa, $e \in H \cap K$ nên $H \cap K \neq \emptyset$.

- Với mọi $x, y \in H \cap K$, ta có $x, y \in H$ và $x, y \in K$ nên
 - $xy \in H$ và $xy \in K$. Do đó $xy \in H \cap K$.
 - $x^{-1}y \in H$ và $x^{-1}y \in K$. Do đó $x^{-1}y \in H \cap K$.

Suy ra $H \cap K \leq G$.

1.4.3. Nhóm con cyclic

Ví dụ. (tự làm) Cho G là nhóm và $a \in G$. Ta đặt H là tập hợp tất cả các lũy thừa nguyên của a , nghĩa là

$$H = \{a^n \mid n \in \mathbb{Z}\}.$$

Chứng minh rằng $H \leq G$.

Định nghĩa. Cho G là nhóm và $a \in G$. Ta đặt

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}.$$

Khi đó $\langle a \rangle$ được gọi là **nhóm con cyclic** sinh bởi a . Suy ra, nếu $|a| = n$ thì

$$\langle a \rangle = \{e, a, \dots, a^{n-1}\}.$$

Nếu $\langle a \rangle = G$ thì ta nói G là **nhóm cyclic** và a được gọi là **phần tử sinh** của G .

Ví dụ.

- ① Nhóm $(\mathbb{Z}, +)$ là nhóm cyclic sinh bởi 1.
- ② Với mỗi $n \in \mathbb{Z}$, nhóm con cyclic sinh bởi n trong nhóm $(\mathbb{Z}, +)$ là

$$\langle n \rangle = \{nx \mid x \in \mathbb{Z}\}.$$

Nhóm này được ký hiệu bởi $n\mathbb{Z}$.

- ③ Nhóm nhân $G = \{1, -1\}$ là nhóm cyclic sinh bởi -1 .
- ④ Nhóm nhân $G = \{1, -1, i, -i\}$ là nhóm cyclic sinh bởi i .

Định lý. Mọi nhóm con của nhóm cyclic đều là nhóm cyclic. Hơn nữa, nếu $H \leq \langle a \rangle$ và $H \neq \{e\}$ thì $H = \langle a^n \rangle$ trong đó n là số nguyên dương nhỏ nhất sao cho $a^n \in H$.

Chứng minh. Giả sử $G = \langle a \rangle$ và $H \leq G$.

- Nếu $H = \{e\}$ thì hiển nhiên H là nhóm con cyclic sinh bởi e .

• Nếu $H \neq \{e\}$ tồn tại k nguyên dương sao cho $a^k \in H$. Gọi n là số nguyên dương nhỏ nhất sao cho $a^n \in H$. Ta cần chứng minh $H = \langle a^n \rangle$.

Thật vậy, hiển nhiên $\langle a^n \rangle \subseteq H$.

Ngược lại, cho $x = a^m \in H$. Chia m cho n ta tìm được $q, r \in \mathbb{Z}$ sao cho

$$m = qn + r, \quad 0 \leq r < n.$$

Vì $a^r = a^m(a^n)^{-q} \in H$ mà n là số nguyên dương nhỏ nhất sao cho $a^n \in H$ nên ta phải có $r = 0$, nghĩa là $m = qn$. Do đó

$$x = a^m = (a^n)^q \in \langle a^n \rangle.$$

Điều này chứng tỏ $H \subseteq \langle a^n \rangle$. Vậy $H = \langle a^n \rangle$.

Hệ quả. Mọi nhóm con của nhóm cộng \mathbb{Z} đều có dạng $n\mathbb{Z}$ với n là số nguyên không âm.

Chứng minh. Áp dụng định lý trên với $\mathbb{Z} = \langle 1 \rangle$.

1.4.4. Nhóm con sinh bởi một tập hợp

Định nghĩa. Cho G là nhóm và $S \subseteq G$. Khi đó, nhóm con nhỏ nhất của G chứa S được gọi là **nhóm con sinh bởi S** , ký hiệu là $\langle S \rangle$.

Tập hợp S được gọi là **tập sinh** của nhóm $\langle S \rangle$. Nếu S hữu hạn thì ta nói $\langle S \rangle$ là nhóm hữu hạn sinh.

Nhận xét. Nếu $S = \emptyset$ thì $\langle S \rangle = \{e\}$.

Định lý. Cho G là một nhóm và $\emptyset \neq S \subseteq G$ là một tập hợp con khác rỗng của G . Khi đó:

$$\langle S \rangle = \{x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n} \mid n \in \mathbb{N}^*, x_i \in S, \varepsilon_i = \pm 1\}. \quad (1)$$

Chứng minh.

$$\langle S \rangle = \{x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n} \mid n \in \mathbb{N}^*, x_i \in S, \varepsilon_i = 1\}.$$

Ta gọi ký hiệu vế phải của đẳng thức là H .

Vì nhóm con $\langle S \rangle$ chứa tất cả các phần tử x_i của S nên $H \subseteq \langle S \rangle$.

Mặt khác, do cách đặt H ta thấy: nếu $x, y \in H$ thì $xy \in H$ và $x^{-1} \in H$ nên $H \leq G$. Từ đây, do $S \subseteq H$ nên $\langle S \rangle \subseteq H$. Vậy $H = \langle S \rangle$.

1.5. Nhóm con chuẩn tắc và nhóm thương

- ❶ Lớp ghép trái
- ❷ Chỉ số của một nhóm con
- ❸ Nhóm con chuẩn tắc
- ❹ Nhóm thương

1.5.1. Lớp ghép trái

Định nghĩa. Cho G là nhóm và H là nhóm con của G . Với mỗi $x \in G$, ta đặt

$$xH = \{xh \mid h \in H\} \text{ và } Hx = \{hx \mid h \in H\}.$$

Ta gọi xH và Hx lần lượt là **lớp ghép trái** và **phải** của H (sinh bởi phần tử x).

Mệnh đề. Cho G là nhóm, H là nhóm con của G , và $x, y \in G$. Khi đó:

$$\textcircled{i} \quad y \in xH \Leftrightarrow x^{-1}y \in H \Leftrightarrow xH = yH.$$

$$\textcircled{ii} \quad y \in Hx \Leftrightarrow yx^{-1} \in H \Leftrightarrow Hx = Hy.$$

Chứng minh. i) • Nếu $y \in xH$ thì tồn tại $h \in H$ sao cho $y = xh$. Do đó $x^{-1}y = h \in H$.

- Nếu $x^{-1}y \in H$ thì với mọi $xh \in xH$, ta có

$$xh = (yy^{-1})xh = y(y^{-1}x)h = y(x^{-1}y)^{-1}h = y[(x^{-1}y)^{-1}h] \in yH,$$

do đó $xH \subseteq yH$. Tương tự, với mọi $yh \in yH$, ta có

$$yh = (xx^{-1})yh = x(x^{-1}y)h = x[(x^{-1}y)h] \in xH,$$

do đó $yH \subseteq xH$. Vậy $xH = yH$.

- Nếu $xH = yH$ thì do $y = ye \in yH$ nên $y \in xH$.

ii) Chứng minh tương tự. ■

Định lý. Cho G là nhóm, $H \leq G$. Trên G ta định nghĩa quan hệ \sim như sau:

$$\forall x, y \in G, x \sim y \Leftrightarrow x^{-1}y \in H.$$

Khi đó \sim là quan hệ tương đương trên G . Đồng thời, với mọi $x \in G$, lớp tương đương của x là $\bar{x} = xH$.

$$\forall x, y \in G, x \sim y \Leftrightarrow x^{-1}y \in H.$$

Chứng minh. Tính phản xạ. Với mọi $x \in G$, ta có $x^{-1}x = e \in H$. Do đó $x \sim x$.

Tính đối xứng. Với mọi $x, y \in G$, nếu $x \sim y$, nghĩa là $x^{-1}y \in H$, thì $y^{-1}x = (x^{-1}y)^{-1} \in H$, suy ra $y \sim x$.

Tính bắc cầu. Với mọi $x, y, z \in G$, nếu $x \sim y$ và $y \sim z$, nghĩa là $x^{-1}y \in H$ và $y^{-1}z \in H$, thì

$$x^{-1}z = x^{-1}(yy^{-1})z = (x^{-1}y)(y^{-1}z) \in H,$$

suy ra $x \sim z$.

Vậy \sim là một quan hệ tương đương trên G .

Theo định nghĩa

$$\bar{x} = \{g \in G \mid g \sim x\}.$$

Do đó, với mọi $g \in \bar{x}$ ta có $g^{-1}x \in H$. Suy ra $x^{-1}g \in H$. Theo Mệnh đề trên ta có $g \in xH$. Do đó $\bar{x} = xH$.

1.5.2. Chỉ số của một nhóm con

Nhận xét. Cho H là nhóm con của nhóm G thì quan hệ tương đương - xác định

$$\forall x, y \in G, x \sim y \Leftrightarrow x^{-1}y \in H.$$

sẽ phân hoạch G thành hợp của các lớp ghép trái rời nhau của H .

Định nghĩa. Tập hợp tất cả các lớp ghép trái của H được gọi là **tập thương** của G trên H , ký hiệu là G/H . Số phần tử của tập hợp này được gọi là **chỉ số** của H trong G , ký hiệu là $[G : H]$.

Định lý. [Định lý Lagrange] Cho G là nhóm hữu hạn và H là nhóm con của G . Khi đó

$$|G| = |H|[G : H].$$

Chứng minh. Nếu xH là một lớp ghép trái của H , ta xét ánh xạ

$$\begin{aligned}\varphi : H &\longrightarrow xH \\ h &\longmapsto xh\end{aligned}$$

Dễ dàng chứng minh φ là song ánh. Suy ra, $|xH| = |H|$. Do đó số phần tử của các lớp ghép trái đều bằng nhau và bằng $|H|$. Hơn nữa số lớp ghép là $[G : H]$, nên

$$|G| = |H|[G : H].$$

Hệ quả. Cho G là một nhóm hữu hạn cấp n . Khi đó:

- i) Cấp của mỗi nhóm con của G là một ước số n .
- ii) Cấp của mỗi phần tử thuộc G là một ước số n .
- iii) Nếu n nguyên tố thì G là nhóm cyclic và mọi phần tử khác e trong G đều là phần tử sinh của G .

Chứng minh. iii) Với mọi $a \in G$, nếu $a \neq e$ thì $|a| \neq 1$, mà $|a|$ là ước của n và n nguyên tố nên $|a| = n$, suy ra $|G| = |\langle a \rangle|$. Do đó $G = \langle a \rangle$.

1.5.3. Nhóm con chuẩn tắc

Định nghĩa. Cho G là nhóm và H là nhóm con của G . Khi đó H được gọi là **nhóm con chuẩn tắc** của G , ký hiệu $H \trianglelefteq G$, nếu

$$\forall x \in G, \forall h \in H, \text{ ta có } x^{-1}hx \in H.$$

Ví dụ. Ta có

● $GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det(A) \neq 0\}$

● $SL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det(A) = 1\}$

Chứng minh rằng $SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$.

Chứng minh. Với mọi $X \in GL_n(\mathbb{R})$ và $A \in SL_n(\mathbb{R})$, ta có

$$\det(X^{-1}AX) = (\det X)^{-1}(\det A)(\det X) = \det(A) = 1,$$

nghĩa là $X^{-1}AX \in SL(n, \mathbb{R})$. Suy ra $SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$.

Mệnh đề. Cho G là nhóm và H là nhóm con của G . Khi đó các điều sau tương đương:

- (i) $H \trianglelefteq G$.
- (ii) $\forall x \in G, x^{-1}Hx \subseteq H$, trong đó $x^{-1}Hx = \{x^{-1}hx \mid h \in H\}$.
- (iii) $\forall x \in G, x^{-1}Hx = H$.
- (iv) $\forall x \in G, xH = Hx$.

Chứng minh. (i) \Rightarrow (ii). Hiển nhiên từ định nghĩa.

(ii) \Rightarrow (iii). Giả sử $\forall x \in G, x^{-1}Hx \subseteq H$. Ta có

$$xHx^{-1} = (x^{-1})^{-1}H(x^{-1}) \subseteq H.$$

Nhân trái cho x^{-1} và phải cho x , ta có $H \subseteq x^{-1}Hx$. Từ đó ta có $x^{-1}Hx = H$.

(iii) \Rightarrow (iv). Giả sử $\forall x \in G, x^{-1}Hx = H$, khi đó

$$xH = x(x^{-1}Hx) = Hx.$$

(iv) \Rightarrow (i). Giả sử $\forall x \in G, xH = Hx$. Khi đó, với mọi $x \in G$ và $h \in H$ ta có

$$hx \in Hx = xH$$

nên tồn tại $k \in H$ sao cho $hx = xk$. Suy ra $x^{-1}hx = k \in H$. Điều này chứng tỏ $H \trianglelefteq G$.

Nhận xét.

- ❶ Các nhóm con tầm thường $\{e\}$ và G của G đều chuẩn tắc trong G .
- ❷ Nếu G là nhóm Abel thì mọi nhóm con của G đều chuẩn tắc trong G .

1.5.4. Nhóm thương

Định lý. Cho G là một nhóm và H là nhóm con chuẩn tắc của G .
Khi đó:

- i) Lớp xyH chỉ phụ thuộc vào các lớp xH và yH mà không phụ thuộc vào sự lựa chọn của các phần tử đại diện x, y của các lớp đó.
- ii) Tập thương G/H cùng với phép toán nhân định bởi

$$(xH)(yH) = xyH$$

là một nhóm, gọi là **nhóm thương** của G trên H .

Chứng minh. i) Giả sử $x'H = xH$ và $y'H = yH$, nghĩa là

$$x^{-1}x' \in H \text{ và } y^{-1}y' \in H.$$

Ta cần chứng minh $x'y'H = xyH$, nghĩa là $(xy)^{-1}(x'y') \in H$.

Ta có

$$(xy)^{-1}(x'y') = y^{-1}x^{-1}x'y' = y^{-1}x^{-1}x'(yy^{-1})y' = [y^{-1}(x^{-1}x')y][y^{-1}y'].$$

Mặt khác, $x^{-1}x' \in H$. Do đó

$$y^{-1}(x^{-1}x')y \in H \text{ (vì } H \trianglelefteq G\text{)}.$$

Hơn nữa $y^{-1}y' \in H$. Suy ra $(xy)^{-1}(x'y') \in H$.

ii) Do i) nên phép toán nhân được định nghĩa như trong (ii) được hoàn toàn xác định. Hơn nữa

- Tính kết hợp của phép toán nhân trên G/H được suy từ tính kết hợp của phép toán nhân trên G .
- Phần tử đơn vị trong G/H chính là lớp $eH = H$.
- Phần tử nghịch đảo của lớp xH chính là $x^{-1}H$.

Nhận xét. Nếu G là một nhóm giao hoán thì rõ ràng nhóm thương G/H cũng giao hoán. Nhưng chiều đảo không đúng.

Ví dụ. Ta có $(\mathbb{Z}, +)$ giao hoán nên với mỗi số nguyên dương n , nhóm con $n\mathbb{Z}$ chuẩn tắc trong \mathbb{Z} , và nhóm thương $\mathbb{Z}/n\mathbb{Z}$ là nhóm cộng \mathbb{Z}_n các số nguyên modulo n .

1.6. Nhóm hoán vị

- ❶ Định nghĩa
- ❷ Chu trình
- ❸ Tính chẵn, lẻ của hoán vị
- ❹ Nhóm thay phiên

1.6.1. Định nghĩa

Định nghĩa. Cho tập hợp $X \neq \emptyset$ gồm n phần tử (ta có thể đồng nhất X với $\{1, 2, \dots, n\}$). Đặt S_n là tập hợp gồm tất cả các song ánh từ X vào X . Khi đó S_n là một nhóm với phép hợp nối ánh xạ. Ta gọi S_n là **nhóm hoán vị** bậc n .

Mỗi phần tử $\sigma \in S_n$ được gọi là một **phép hoán vị** (hay một **phép thế**) bậc n và có thể được biểu diễn bởi một ma trận cấp $2 \times n$

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Nhận xét. Nhóm hoán vị S_n là nhóm hữu hạn có cấp $n!$, và

- có phần tử trung hòa là ánh xạ đồng nhất id_X
- phần tử nghịch đảo của $\sigma \in S_n$ là ánh xạ ngược σ^{-1} .
- không giao hoán nếu $n > 2$.

Ví dụ. Trong S_5 , phép hoán vị σ được xác định bởi

$$\sigma(1) = 4, \sigma(2) = 5, \sigma(3) = 3, \sigma(4) = 2, \sigma(5) = 1.$$

Khi đó σ được biểu diễn là

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix}.$$

Giả sử

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}.$$

Hãy tìm dạng biểu diễn của $\sigma\tau$ và $\tau\sigma$?

Đáp án.

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix} \text{ và } \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix}.$$

1.6.2. Chu trình

Định nghĩa. Phép hoán vị $\sigma \in S_n$ được gọi **chu trình** có chiều dài r (hay **r -chu trình**) nếu tồn tại các phần tử phân biệt $i_1, i_2, \dots, i_r \in X$ sao cho

$$\sigma(i_1) = i_2, \dots, \sigma(i_{r-1}) = i_r, \sigma(i_r) = i_1$$

và

$$\sigma(i) = i, \forall i \in X \setminus \{i_1, i_2, \dots, i_r\}.$$

Khi đó ta viết

$$\sigma = (i_1 \ i_2 \ \dots \ i_r).$$

► Mỗi 2-chu trình trong S_n được gọi là một **chuyển vị**.

► Hai chu trình $\sigma = (i_1 \ i_2 \ \dots \ i_r)$, $\tau = (j_1 \ j_2 \ \dots \ j_s)$ được gọi là **rời nhau** hay **độc lập** nếu $\{i_1, i_2, \dots, i_r\} \cap \{j_1, j_2, \dots, j_s\} = \emptyset$.

Ví dụ. a) Trong nhóm hoán vị S_7 , chu trình $\sigma = (1\ 3\ 4\ 7)$ có chiều dài 4, và

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 7 & 5 & 6 & 1 \end{pmatrix}.$$

b) Trong nhóm hoán vị S_8 , chuyển vị $(2\ 5)$ là phép hoán vị

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 5 & 3 & 4 & 2 & 6 & 7 & 8 \end{pmatrix}.$$

c) Trong nhóm hoán vị S_5 , cho

$$\sigma = (1\ 2\ 5\ 3) \quad \text{và} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix}.$$

Ta có

$$\begin{aligned} \sigma\tau &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix} = (1\ 4\ 2); \\ \tau\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix} = (1\ 3\ 4); \end{aligned}$$

Mệnh đề.

- i) Nếu σ là một r -chu trình thì cấp của σ là r .
- ii) Nghịch đảo của một r -chu trình cũng là một r -chu trình. Hơn nữa, nếu $\sigma = (i_1 i_2 \cdots i_r)$ thì $\sigma^{-1} = (i_r \cdots i_2 i_1)$.
- iii) Hai chu trình σ và τ rời nhau thì chúng giao hoán, nghĩa là $\sigma\tau = \tau\sigma$.

Ví dụ. a) Nếu $\sigma = (1\ 3\ 2\ 5\ 4)$ thì σ có cấp 5 và

$$\sigma^{-1} = (4\ 5\ 2\ 3\ 1).$$

b) Ta có

$$(1\ 2\ 4\ 7)(5\ 3\ 6) = (5\ 3\ 6)(1\ 2\ 4\ 7).$$

Định lý. Mọi hoán vị σ khác ánh xạ đồng nhất đều được phân tích thành tích các chu trình rời nhau có độ dài lớn hơn hay bằng 2. Sự phân tích là duy nhất sai khác một sự đổi chỗ các chu trình.

Ví dụ. Trong nhóm hoán vị S_{10} , cho

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 2 & 7 & 9 & 1 & 4 & 8 & 5 & 6 & 10 \end{pmatrix}.$$

Hãy phân tích σ thành tích các chu trình rời nhau.

Giải. Ta bắt đầu từ phần tử 1. Ta có

$$\sigma(1) = 3, \sigma(3) = 7, \sigma(7) = 8, \sigma(8) = 5, \sigma(5) = 1.$$

Do đó ta được chu trình $(1\ 3\ 7\ 8\ 5)$. Tiếp tục với phần tử 2, ta có $\sigma(2) = 2$ nên ta chuyển sang phần tử 4. Ta có

$$\sigma(4) = 9, \sigma(9) = 6, \sigma(6) = 4.$$

Do đó ta được chu trình $(4\ 9\ 6)$.

Cuối cùng, $\sigma(10) = 10$ nên quá trình phân tích σ thành tích các chu trình rời nhau kết thúc. Như vậy

$$\sigma = (1\ 3\ 7\ 8\ 5)(4\ 9\ 6).$$

Ví dụ. (tự làm) Trong nhóm hoán vị S_{12} , cho

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 4 & 3 & 1 & 7 & 9 & 11 & 12 & 5 & 8 & 6 & 10 \end{pmatrix}.$$

Hãy phân tích σ thành tích các chu trình rời nhau.

Đáp án. $(1\ 2\ 4)(5\ 7\ 11\ 6\ 9)(8\ 12\ 10)$

Hệ quả. Cho $\sigma \in S_n$. Nếu σ được viết dưới dạng tích của các chu trình rời nhau thì cấp của σ là bội chung nhỏ nhất của cấp các chu trình đó.

Ví dụ. Trong nhóm hoán vị S_{10} , cho

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 2 & 7 & 9 & 1 & 4 & 8 & 5 & 6 & 10 \end{pmatrix}.$$

Hãy tìm cấp của σ .

Giải. Ta có $\sigma = (1\ 3\ 7\ 8\ 5)(4\ 9\ 6)$. Do đó cấp của σ là 15.

Bổ đề. Mọi chu trình trong S_n đều được phân tích thành tích của các chuyển vị.

Chứng minh. Cho $\sigma = (i_1 i_2 \dots i_r)$ là một chu trình. Khi đó

$$\sigma = (i_1 i_r)(i_1 i_{r-1}) \dots (i_1 i_2).$$

Mệnh đề. Mọi phép hoán vị trong S_n đều được phân tích thành tích của các chuyển vị.

Ví dụ. Trong nhóm hoán vị S_{10} , cho

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 2 & 7 & 9 & 1 & 4 & 8 & 5 & 6 & 10 \end{pmatrix}.$$

Hãy phân tích σ thành tích các chuyển vị.

Giải. Ta có

$$\sigma = (1\ 3\ 7\ 8\ 5)(4\ 9\ 6) = (1\ 5)(1\ 8)(1\ 7)(1\ 3)(4\ 6)(4\ 9)$$

1.6.3. Tính chẵn, lẻ của hoán vị

Định nghĩa. Cho $\sigma \in S_n$. Ta nói rằng $\{i, j\}$ tạo thành một *nghịch thế* đối với σ nếu

$$(i - j)[\sigma(i) - \sigma(j)] < 0,$$

nghĩa là khi $i < j$ ta có $\sigma(i) > \sigma(j)$.

Ví dụ. Trong S_4 , cho hoán vị $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$. Tìm các nghịch thế của σ .

Đáp án. $\{1, 4\}$, $\{2, 3\}$, $\{2, 4\}$, $\{3, 4\}$

Ví dụ.(tự làm) Trong S_5 , cho hoán vị $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$. Tìm các nghịch thế của σ .

Định nghĩa. Nếu số các nghịch thế đối với σ là k thì **dấu** của σ , ký hiệu $\text{sgn}(\sigma)$, là hàm được định nghĩa bởi

$$\text{sgn}(\sigma) = (-1)^k.$$

- Nếu $\text{sgn}(\sigma) = 1$ thì σ được gọi là **hoán vị chẵn**.
- Nếu $\text{sgn}(\sigma) = -1$ thì σ được gọi là **hoán vị lẻ**.

Nhận xét.

- i) $\text{sgn}(\text{id}_X) = 1$.
- ii) $\text{sgn}(\sigma) = \text{sgn}(\sigma^{-1})$.
- iii) Nếu σ là một chuyển vị thì $\text{sgn}(\sigma) = -1$.

Định lý. Với mọi $\sigma, \tau \in S_n$ thì

$$\text{sgn}(\sigma\tau) = \text{sgn}(\sigma)\text{sgn}(\tau).$$

Ví dụ. Xét tính chẵn lẻ của hoán vị

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 6 & 4 & 8 & 1 & 7 & 10 & 2 & 9 \end{pmatrix}$$

Giải. Ta có

$$\begin{aligned}\sigma &= (1\ 3\ 6)(2\ 5\ 8\ 10\ 9) \\ &= (1\ 6)(1\ 3)(2\ 9)(2\ 10)(2\ 8)(2\ 5).\end{aligned}$$

Vì σ được viết dưới dạng tích của 6 chuyển vị (mỗi chuyển vị có dấu bằng -1) nên $\text{sgn}(\sigma) = 1$ nghĩa là σ là một hoán vị chẵn.

Hệ quả. Cho $\sigma \in S_n$. Khi đó:

- ❶ Nếu σ là tích của k chuyển vị thì $\text{sgn}(\sigma) = (-1)^k$.
- ❷ Nếu σ là r -chu trình thì $\text{sgn}(\sigma) = (-1)^{r-1}$. Suy ra, σ chẵn $\Leftrightarrow r$ lẻ; σ lẻ $\Leftrightarrow r$ chẵn.

Ví dụ.(tự làm) Trong nhóm hoán vị S_{10} , xét các phép hoán vị

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 3 & 5 & 7 & 6 & 1 & 8 & 4 & 10 & 9 \end{pmatrix};$$

$$\sigma_2 = (1\ 3\ 4\ 7)(2\ 5)(1\ 2\ 4\ 3).$$

- a) Viết σ_1 và σ_2 dưới dạng tích các chu trình rời nhau và dưới dạng tích các chuyển vị. Suy ra tính chẵn, lẻ và cấp của chúng.
- b) Viết $\sigma_1\sigma_2; \sigma_2^2; \sigma_2^{-1}; \sigma_2^{-2}; \sigma_1^2\sigma_2; \sigma_1\sigma_2^2$ dưới dạng tích các chu trình rời nhau. Xét tính chẵn, lẻ và cấp của chúng.
- c) Tìm $\sigma \in S_n$ thỏa $\sigma_1\sigma\sigma_2^{-2} = \sigma_1^3$.

1.6.4. Nhóm thay phiên

Ví dụ. Trong nhóm S_n , ta đặt A_n là tập hợp tất cả các hoán vị chẵn trong S_n , nghĩa là

$$A_n = \{\sigma \in S_n \mid \text{sgn}(\sigma) = 1\}.$$

Chúng minh $A_n \trianglelefteq S_n$.

Giải. • Rõ ràng $\text{id}_X \in A_n$. Suy ra $A_n \neq \emptyset$.

• Với mọi $\sigma, \tau \in A_n$, nghĩa là $\text{sgn}(\sigma) = 1$; $\text{sgn}(\tau) = 1$, ta có

$$\text{sgn}(\sigma^{-1}\tau) = \text{sgn}(\sigma^{-1})\text{sgn}(\tau) = \text{sgn}(\sigma)\text{sgn}(\tau) = 1.1 = 1.$$

Vậy $\sigma^{-1}\tau \in A_n$. Suy ra $A_n \leq S_n$.

• Với mọi $\sigma \in A_n$ và $\rho \in S_n$, ta có

$$\text{sgn}(\rho^{-1}\sigma\rho) = \text{sgn}(\rho^{-1})\text{sgn}(\sigma)\text{sgn}(\rho) = \text{sgn}(\rho).1.\text{sgn}(\rho) = \text{sgn}^2(\rho) = 1.$$

Vậy $\rho^{-1}\sigma\rho \in A_n$. Suy ra $A_n \trianglelefteq S_n$.

Định nghĩa. Nhóm A_n được gọi là *nhóm thay phiên* bậc n

1.7. Đồng cấu nhóm

- ① Định nghĩa
- ② Tính chất
- ③ Nhân và ảnh đồng cấu
- ④ Định lý đẳng cấu

1.7.1 Định nghĩa

Định nghĩa. Một ánh xạ f từ nhóm $(G, *)$ vào nhóm (G', \circ) được gọi là một **đồng cấu** (**nhóm**) nếu f bảo toàn phép toán, nghĩa là

$$\forall x, y \in G, f(x * y) = f(x) \circ f(y).$$

- ▶ Một đồng cấu từ G vào G được gọi là một **tự đồng cấu** của G .
- ▶ Một đồng cấu đồng thời là đơn ánh, toàn ánh hay song ánh được gọi lần lượt là **đơn cấu**, **toàn cấu** hay **đẳng cấu**.
- ▶ Một tự đồng cấu song ánh được gọi là một **tự đẳng cấu**.
- ▶ Nếu tồn tại một đẳng cấu từ nhóm G vào nhóm G' thì ta nói G **đẳng cấu** với G' , ký hiệu $G \simeq G'$.

Ví dụ. Ánh xạ

$$\begin{array}{ccc} \text{id}_G : & G & \longrightarrow G \\ & x & \longmapsto x \end{array}$$

được gọi là **tự đẳng cấu đồng nhất** của G .

Ví dụ.

- ① Cho $H \leq G$. Khi đó ánh xạ

$$\begin{aligned} i_H : H &\longrightarrow G \\ x &\longmapsto x \end{aligned}$$

là một đơn cấu, gọi là *đơn cấu chính tắc*.

- ② Cho $H \trianglelefteq G$. Khi đó ánh xạ

$$\begin{aligned} \pi : G &\longrightarrow G/H \\ x &\longmapsto xH \end{aligned}$$

là một toàn cấu, gọi là *toàn cấu chính tắc*.

- ③ Giả sử G và G' là hai nhóm tùy ý. Khi đó ánh xạ $f : G \longrightarrow G'$ định bởi $f(x) = e'$ là một đồng cấu, gọi là *đồng cấu tầm thường*.

Ví dụ.

- ① Ánh xạ $x \mapsto e^x$ là một đẳng cấu từ nhóm cộng các số thực \mathbb{R} lên nhóm nhân \mathbb{R}^+ các số thực dương.
- ② Ánh xạ $\det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$ là một toàn cấu.

Ví dụ. Cho G là một nhóm và $a \in G$. Xét ánh xạ $\varphi_a : G \longrightarrow G$ được định bởi $\varphi_a(x) = axa^{-1}$. Chứng tỏ φ_a là một tự đẳng cấu của G .

Chứng minh.

- $\forall x, y \in G$, ta có

$$\varphi_a(xy) = a(xy)a^{-1} = (axa^{-1})(aya^{-1}) = \varphi_a(x)\varphi_a(y).$$

Suy ra, φ_a là một đồng cấu.

- Với mỗi $y \in G$, tồn tại duy nhất $x = a^{-1}ya \in G$ sao cho $y = \varphi_a(x)$. Do đó φ_a là một song ánh.

Như vậy φ_a là một tự đẳng cấu của nhóm G .

1.7.2. Tính chất

Mệnh đề. Cho $f : G \rightarrow G'$ là đồng cấu nhóm và e, e' lần lượt là phần tử đơn vị của G và G' . Khi đó:

- i) $f(e) = e'$
- ii) Với mọi $x \in G$, $f(x^{-1}) = (f(x))^{-1}$
- iii) Với mọi $x \in G$ và $n \in \mathbb{Z}$, $f(x^n) = (f(x))^n$

Chứng minh.

i) Ta có $ee = e$, do đó $f(e)f(e) = f(e)$. Từ tính giản ước của phép nhân trong G' cho ta $f(e) = e'$.

ii) Với mọi $x \in G$, ta có $x^{-1}x = e$, do đó $f(x^{-1})f(x) = e'$. Suy ra

$$f(x^{-1}) = (f(x))^{-1}.$$

iii) Hiển nhiên từ định nghĩa đồng cấu và bằng quy nạp.

Mệnh đề. Tích của hai đồng cấu nhóm là một đồng cấu nhóm. Đặc biệt, tích của hai đơn cấu (tương ứng: toàn cấu, đẳng cấu) là một đơn cấu (tương ứng: toàn cấu, đẳng cấu).

Chứng minh. Giả sử $f : G \longrightarrow G'$ và $g : G' \longrightarrow G''$ là các đồng cấu nhóm. Xét ánh xạ tích $g \circ f$, ta có với mọi $x, y \in G$,

$$\begin{aligned}(g \circ f)(xy) &= g(f(xy)) \\ &= g(f(x)f(y)) \\ &= g(f(x))g(f(y)) \\ &= (g \circ f)(x) (g \circ f)(y).\end{aligned}$$


nên $g \circ f$ vẫn còn là đồng cấu nhóm. ■

Mệnh đề. Ánh xạ ngược của một đẳng cấu nhóm là một đẳng cấu nhóm.

Chứng minh. Giả sử $f : G \rightarrow G'$ là một đẳng cấu. Vì $f^{-1} : G' \rightarrow G$ cũng là song ánh nên ta chỉ cần chứng minh f^{-1} là đồng cấu.

Thật vậy, với mọi $x', y' \in G'$, tồn tại $x, y \in G$ sao cho $x' = f(x)$ và $y' = f(y)$ nên

$$\begin{aligned} f^{-1}(x'y') &= f^{-1}(f(x)f(y)) \\ &= f^{-1}(f(xy)) \\ &= (f^{-1}f)(xy) \\ &= \text{Id}_G(xy) \\ &= xy = f^{-1}(x')f^{-1}(y'). \end{aligned}$$

Vậy f^{-1} là đồng cấu và do đó f^{-1} là đẳng cấu. 

1.7.3. Nhân và ảnh của đồng cấu

Định lý. Cho đồng cấu nhóm $f : G \longrightarrow G'$, H là nhóm con của G và H' là nhóm con của G' . Khi đó:

- i) $f(H)$ là một nhóm con của G' .
- ii) $f^{-1}(H')$ là một nhóm con của G . Hơn nữa, nếu H' là nhóm con chuẩn tắc của G' thì $f^{-1}(H')$ là nhóm con chuẩn tắc của G .

Đặc biệt, $\text{Im} f = f(G)$ là nhóm con của G' và $\text{Ker} f = f^{-1}(\{e'\})$ là nhóm con chuẩn tắc của G .

Ta gọi $\text{Im} f$ là **ảnh** của f và $\text{Ker} f$ là **nhân** của f .

Chứng minh. i)

- Vì $e \in H$ nên $e' = f(e) \in f(H)$.
- Với mọi $x', y' \in f(H)$, tồn tại $x, y \in H$ sao cho $x' = f(x), y' = f(y)$. Ta có

$$\begin{aligned}
 (x')^{-1}y' &= f(x)^{-1}f(y) \\
 &= f(x^{-1})f(y) \\
 &= f(x^{-1}y) \in f(H) \text{ do } x^{-1}y \in H.
 \end{aligned}$$

Vậy $f(H) \leq G'$.

ii) • Vì $f(e) = e' \in H'$ nên $e \in f^{-1}(H')$. Suy ra $f^{-1}(H') \neq \emptyset$.

• Với mọi $x, y \in f^{-1}(H')$ ta có $f(x) \in H'$ và $f(y) \in H'$ nên

$$f(x^{-1}y) = (f(x))^{-1}f(y) \in H',$$

nghĩa là $x^{-1}y \in f^{-1}(H')$.

Vậy $f^{-1}(H') \leq G$.

Bây giờ giả sử $H' \trianglelefteq G'$. Khi đó với mọi $x \in G$ và $h \in f^{-1}(H')$ ta có $f(h) \in H'$ nên

$$f(x^{-1}hx) = (f(x))^{-1}f(h)f(x) \in H' \quad (\text{do } H' \trianglelefteq G')$$

Từ đó $x^{-1}hx \in f^{-1}(H')$. Do đó $f^{-1}(H') \trianglelefteq G$.

Cuối cùng nhận xét rằng $G \leq G$ và $\{e'\} \trianglelefteq G'$ nên theo kết quả trên ta có khẳng định sau cùng của định lý. ■

Mệnh đề. Cho đồng cấu nhóm $f : G \rightarrow G'$. Khi đó, f là đơn cấu khi và chỉ khi $\text{Ker } f = \{e\}$.

Chứng minh. (\Rightarrow) Nếu f là đơn cấu thì với mọi $x \in G$,

$$\begin{aligned}x \in \text{Ker } f &\Leftrightarrow f(x) = e' \\&\Leftrightarrow f(x) = f(e) \\&\Leftrightarrow x = e.\end{aligned}$$

Do đó $\text{Ker } f = \{e\}$.

(\Leftarrow) Nếu $\text{Ker } f = \{e\}$ thì với mọi $x, y \in G$,

$$\begin{aligned}f(x) = f(y) &\Leftrightarrow f(x^{-1}y) = (f(x))^{-1}f(y) = e' \\&\Leftrightarrow x^{-1}y \in \text{Ker } f \\&\Leftrightarrow x^{-1}y = e \Leftrightarrow x = y.\end{aligned}$$

Do đó f là đơn ánh.

1.7.4. Định lý đẳng cấu

Định lý. [Định lý đẳng cấu 1] Cho đồng cấu nhóm $f : G \rightarrow G'$. Khi đó ánh xạ

$$\bar{f} : G/\text{Ker } f \rightarrow G' \text{ định bởi } \bar{f}(x \text{ Ker } f) = f(x)$$

là một đơn cấu. Đặc biệt,

$$G/\text{Ker } f \simeq \text{Im } f.$$

Chứng minh. Đặt $H := \text{Ker } f$. Vì $H \trianglelefteq G$ nên ta lập được nhóm thương G/H . Xét tương ứng $\bar{f} : G/H \rightarrow G'$ định bởi $\bar{f}(xH) = f(x)$, ta có với mọi $x, y \in G$:

$$\begin{aligned}\bar{f}(xH) = \bar{f}(yH) &\Leftrightarrow f(x) = f(y) \Leftrightarrow (f(x))^{-1}f(y) = e' \\ &\Leftrightarrow f(x^{-1})f(y) = e' \Leftrightarrow f(x^{-1}y) = e' \\ &\Leftrightarrow x^{-1}y \in H \\ &\Leftrightarrow xH = yH.\end{aligned}$$

Như vậy với mọi $x, y \in G$,

$$\overline{f}(xH) = \overline{f}(yH) \Leftrightarrow xH = yH.$$

Chiều (\Leftarrow) chứng tỏ \overline{f} là một ánh xạ, chiều (\Rightarrow) chứng tỏ \overline{f} là một đơn ánh.

Bây giờ ta kiểm chứng \overline{f} là một đồng cấu. Thật vậy, với mọi $x, y \in G$:

$$\overline{f}((xH)(yH)) = \overline{f}(xyH) = f(xy) = f(x)f(y) = \overline{f}(xH)\overline{f}(yH).$$

Vậy \overline{f} là đồng cấu.

Ta có $\text{Im } \overline{f} = \text{Im } f$. Do đó


$$G/\text{Ker } f \simeq \text{Im } f.$$

Hệ quả. Mọi nhóm cyclic vô hạn đều đẳng cấu với nhóm $(\mathbb{Z}, +)$.
Mọi nhóm cyclic hữu hạn cấp n đều đẳng cấu với nhóm cộng $(\mathbb{Z}_n, +)$.

Chứng minh. Giả sử G là nhóm cyclic sinh bởi x . Xét ánh xạ

$$f : (\mathbb{Z}, +) \longrightarrow G \text{ định bởi } f(m) = x^m.$$

Dễ thấy f là một toàn cấu từ nhóm $(\mathbb{Z}, +)$ vào G . Vì $\text{Ker } f \leq \mathbb{Z}$ nên $\text{Ker } f$ có dạng $\text{Ker } f = n\mathbb{Z}$ với $n \in \mathbb{N}$.

- Nếu $n = 0$ thì $\text{Ker } f = \{0\}$ nên f là đơn cấu. Hơn nữa f là toàn cấu nên f là đẳng cấu. Trong trường hợp này G vô hạn và $G \simeq \mathbb{Z}$.
- Nếu $n > 0$ thì theo Định lý trên $\mathbb{Z}/n\mathbb{Z} \simeq G$. Vì nhóm thương $\mathbb{Z}/n\mathbb{Z}$ chính là nhóm \mathbb{Z}_n nên trong trường hợp này G hữu hạn cấp n và $G \simeq \mathbb{Z}_n$. 

Ví dụ. Đồng cấu $f : (\mathbb{R}, +) \longrightarrow (\mathbb{C}^*, .)$ định bởi $f(x) = \cos 2\pi x + i \sin 2\pi x$. Khi đó

$$\text{Ker } f = \mathbb{Z} \text{ và } \text{Im } f = U$$

với $U = \{z \in \mathbb{C}^* \mid |z| = 1\}$. Do đó $\mathbb{R}/\mathbb{Z} \simeq U$.

Ví dụ. Đồng cấu $f = \text{sgn} : S_n \longrightarrow (\{-1; 1\}, .)$ có $\text{Ker } f = A_n$ và $\text{Im } f = \{\pm 1\}$ nên $S_n/A_n \simeq \{\pm 1\}$.

Ví dụ. Toàn cấu $f : GL(n, \mathbb{R}) \longrightarrow \mathbb{R}^*$ định bởi $f(A) = \det A$ có

$$\text{Ker } f = \{A \in GL(n, \mathbb{R}) | \det A = 1\} = SL(n, \mathbb{R})$$

nên $GL(n, \mathbb{R})/SL(n, \mathbb{R}) \simeq \mathbb{R}^*$.

Chương 2

VÀNH, MIỀN NGUYÊN, TRƯỜNG

Đại học Khoa Học Tự Nhiên Tp. Hồ Chí Minh

Chương 2. Vành, miền nguyên, trường

- Vành
- Vành con, ideal và vành thương
- Đồng cấu vành và định lý đẳng cấu
- Miền nguyên và trường

2.1. Vành

Định nghĩa. **Vành** là một tập hợp R cùng với hai phép toán **cộng** và **nhân** thỏa các tính chất sau:

- ① $(R, +)$ là nhóm giao hoán;
- ② (R, \cdot) là nửa nhóm (có tính chất kết hợp);
- ③ Phép nhân phân phối đối với phép cộng, nghĩa là với mọi $x, y, z \in R$, ta có

$$x \cdot (y + z) = x \cdot y + x \cdot z;$$

$$(y + z) \cdot x = y \cdot x + z \cdot x.$$

Nếu phép nhân giao hoán thì ta nói vành R **giao hoán**; nếu phép nhân có phần tử đơn vị thì vành R được gọi là **vành có đơn vị**.

Ví dụ.

- $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$ là vành giao hoán có đơn vị.
- $(M_n(\mathbb{R}), +, \cdot)$ ($n \geq 2$) là vành không giao hoán có đơn vị.

Ví dụ. Cho $(G, +)$ là một nhóm Abel. Tập hợp $\text{End}(G)$ các *tự đồng cấu của nhóm* G là vành có đơn vị với phép cộng định bởi:

$$(f+g)(x)=f(x)+g(x), \quad \forall f, g \in \text{End}(G), \forall x \in G,$$

và phép nhân là phép hợp nối ánh xạ.

Ví dụ. Giả sử R_1, R_2, \dots, R_n là các vành. Khi đó tích Descartes

$$\prod_{i=1}^n R_i = \{(x_1, x_2, \dots, x_n) \mid x_1 \in R_1, x_2 \in R_2, \dots, x_n \in R_n\}$$

cùng với phép cộng

$$(x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n) = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)$$

và phép nhân

$$(x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n) = (x_1 y_1, x_2 y_2, \dots, x_n y_n)$$

là một vành, gọi là *vành tích trực tiếp* của R_1, R_2, \dots, R_n .

Nhận xét. Cho R là vành có đơn vị e . Ta đặt

$$R^* = \{x \in R \mid x \text{ khả nghịch}\}.$$

Khi đó R^* là một nhóm đối với phép nhân, gọi là **nhóm các phần tử khả nghịch** của R .

Ký hiệu. $x - y := x + (-y)$ trong đó $-y$ là phần tử đối của y .

Mệnh đề. Cho R là một vành. Khi đó với mọi $x, y, z \in R$ và $n \in \mathbb{Z}$ ta có

i) $x(y - z) = xy - xz$ và $(y - z)x = yx - zx$.

ii) $0x = x0 = 0$.

iii) $x(-y) = (-x)y = -(xy)$ và $(-x)(-y) = xy$.

iv) $(nx)y = x(ny) = n(xy)$. Đặc biệt, nếu R có đơn vị e thì

$$nx = (ne)x = x(ne).$$

Chứng minh. (i) Do tính phân phối của phép nhân đối với phép cộng ta có

$$xy = x[(y - z) + z] = x(y - z) + xz.$$

Suy ra $x(y - z) = xy - xz$. Đẳng thức còn lại được chứng minh tương tự.

(ii) Từ (i) ta có

$$0x = (y - y)x = yx - yx = 0.$$

Tương tự cho $x0 = 0$.

(iii) Từ (i) và (ii) ta có

$$x(-y) = x(0 - y) = x0 - xy = -xy.$$

Tương tự $(-x)y = -(xy)$. Hơn nữa,

$$(-x)(-y) = -(-xy) = xy.$$

(iv) Ta chứng minh $(nx)y = n(xy)$. Với $n = 0$, đẳng thức hiển nhiên đúng. Xét $n > 0$, ta có

$$(nx)y = (x + x + \dots + x)y = xy + xy + \dots + xy = n(xy).$$

Với $n < 0$, đặt $m = -n > 0$, ta có

$$(nx)y = [m(-x)]y = m[(-x)y] = m(-xy) = (-m)(xy) = n(xy).$$

Vậy $(nx)y = n(xy)$ với mọi $n \in \mathbb{Z}$. Tương tự $x(ny) = n(xy)$.

2.2. Vành con, ideal và vành thương

Định nghĩa. Cho R là một vành và A là tập con khác rỗng của R . Khi đó

- ❶ A được gọi là một **vành con** của R nếu A và hai phép toán cảm sinh từ R là vành.
- ❷ Vành con I của R được gọi là một **ideal trái** (tương ứng, **ideal phải**) của R nếu với mọi $r \in R$ và $x \in I$ ta có $rx \in I$ (tương ứng, $xr \in I$).

Ta nói I là một **ideal** của R nếu I vừa là ideal trái vừa là ideal phải của R .

Nhận xét.

- ❶ Các tập con $\{0\}$ và R đều là các ideal của R , gọi là các **ideal tầm thường**.
- ❷ Nếu vành R giao hoán thì các khái niệm ideal trái, ideal phải và ideal là trùng nhau.

Ví dụ.

- ❶ $M(n, \mathbb{Z})$ là vành con của $M(n, \mathbb{Q})$ nhưng không là ideal.
- ❷ $M(n, 2\mathbb{Z})$ là ideal của $M(n, \mathbb{Z})$
- ❸ I là ideal của \mathbb{Z} khi và chỉ khi I có dạng $n\mathbb{Z}$ với $n \in \mathbb{Z}$.

Định lý. [Đặc trưng của vành con] Cho A là một tập con khác rỗng của vành R . Các mệnh đề sau tương đương:

- ❶ A là một vành con của R ;
- ❷ Với mọi $x, y \in A$, $x + y \in A$, $xy \in A$, $-x \in A$;
- ❸ Với mọi $x, y \in A$, $x - y \in A$ và $xy \in A$.

Chứng minh.

(i) \Rightarrow (ii). Hiển nhiên.

(ii) \Rightarrow (iii). Với mọi $x, y \in A$, ta có $x, -y \in A$ nên

$$x - y = x + (-y) \in A.$$

(iii) \Rightarrow (i). Ta có $(A, +)$ là nhóm con của $(R, +)$. Mặt khác, các phép toán cảm sinh cũng có tính chất kết hợp và phân phối nên A là một vành, nghĩa là A là một vành con của R . ■

Định lý. [Đặc trưng của ideal] Cho I là một tập con khác rỗng của vành R . Các mệnh đề sau tương đương:

- i) I là một ideal của R ;
- ii) Với mọi $x, y \in I$ và $r \in R, x + y \in I, -x \in I, rx \in I$ và $xr \in I$;
- iii) Với mọi $x, y \in I$ và $r \in R, x - y \in I, xr \in I$ và $rx \in I$.

Mệnh đề. Giả sử R là vành có đơn vị và I là một ideal trái (hay phải) của R . Khi đó các điều sau tương đương

- i) $I = R$.
- ii) I chứa ít nhất một phần tử khả nghịch.
- iii) I chứa phần tử đơn vị.

Chứng minh. Dễ dàng.

Mệnh đề. Với I, J là hai ideal của R , đặt

$$I + J = \{x + y \mid x \in I, y \in J\};$$

$$IJ = \left\{ \sum_{i=1}^n x_i y_i \mid x_i \in I, y_i \in J, n \in \mathbb{N}^* \right\}.$$

Khi đó $I + J$ và IJ cũng là các ideal của R , gọi là **tổng** và **tích** của các ideal I và J .

Mệnh đề. Giao của một họ khác rỗng các vành con (tương ứng, ideal) của một vành R cũng là một vành con (tương ứng, ideal) của vành R .

Chứng minh. Tự chứng minh.

Vành con và ideal sinh bởi tập hợp

Định nghĩa. Cho S là một tập con khác rỗng của vành R . Ta định nghĩa:

- i) Giao của tất cả các vành con của R có chứa S là *vành con sinh bởi S* .
- ii) Giao của tất cả các ideal của R có chứa S là *ideal sinh bởi S* , ký hiệu là $\langle S \rangle$.

Từ định nghĩa ta thấy vành con (tương ứng, ideal) của R sinh bởi tập hợp S chính là vành con (tương ứng, ideal) nhỏ nhất của R có chứa S .

Đặc biệt $\{0\}$ là vành con và cũng là ideal sinh bởi tập rỗng.

Định lý. Cho S là một tập con khác rỗng của vành R . Khi đó

❶ Vành con của R sinh bởi S là tập hợp

$$\left\{ \sum_{\text{hữu hạn}} s_1 s_2 \dots s_n \mid s_i \in S \text{ hay } -s_i \in S, n \in \mathbb{N}^* \right\}.$$

❷ Nếu R có đơn vị thì ideal sinh bởi S là tập hợp

$$\langle S \rangle = \left\{ \sum_{i=1}^n x_i s_i y_i \mid x_i, y_i \in R, s_i \in S, n \in \mathbb{N}^* \right\}.$$

❸ Nếu R giao hoán có đơn vị thì

$$\langle S \rangle = \left\{ \sum_{i=1}^n x_i s_i \mid x_i \in R, s_i \in S, n \in \mathbb{N}^* \right\}.$$

Chứng minh. Ta chứng minh (ii). Các phần còn lại hoàn toàn tương tự. Đặt


$$I = \left\{ \sum_{i=1}^n x_i s_i y_i \mid x_i, y_i \in R, s_i \in S, n \in \mathbb{N}^* \right\}.$$

Ta có $S \subseteq I$ vì mọi phần tử $s \in S$ đều được viết dưới dạng $s = ese \in I$.

Hơn nữa, do cách đặt I , ta có ngay I là ideal của R .

Mặt khác, mọi ideal chứa S đều chứa tất cả các phần tử có dạng

$$\sum_{i=1}^n x_i s_i y_i \quad (\text{với } x_i, y_i \in R, s_i \in S)$$

nên phải chứa I . Điều này cho thấy I là ideal nhỏ nhất của R có chứa S , nghĩa là $I = \langle S \rangle$. 

Định nghĩa. Cho S là một tập con của vành R và $I = \langle S \rangle$. Ta nói

- ❶ I **được sinh ra bởi** S và S là **tập sinh** của I .
- ❷ Nếu S hữu hạn thì ta nói I **hữu hạn sinh**.

Đặc biệt, nếu $S = \{a\}$ thì ta viết $I = \langle a \rangle$, gọi là **ideal chính sinh bởi** a .

Nhận xét. Nếu vành R giao hoán, có đơn vị thì ideal chính sinh bởi a là:

$$\langle a \rangle = \{xa \mid x \in R\}.$$

Ta còn ký hiệu tập hợp trên là Ra .

Định lý. Giả sử I là một ideal của vành $(R, +, \cdot)$. Trên nhóm thương $(R/I, +)$ ta định nghĩa phép toán nhân như sau:

$$(x + I)(y + I) = xy + I.$$

Khi đó $(R/I, +, \cdot)$ là một vành, gọi là **vành thương** của R trên ideal I .

Chứng minh. Trước hết ta chứng minh phép toán nhân được xác định. Thật vậy, giả sử $x + I = x' + I$ và $y + I = y' + I$, nghĩa là $x - x' \in I$ và $y - y' \in I$, hay $x = x' + a$ và $y = y' + b$ với $a, b \in I$ nào đó. Khi đó

$$\begin{aligned} xy &= (x' + a)(y' + b) \\ &= x'y' + x'b + ay' + ab. \end{aligned}$$

Chú ý rằng $x'b$, ay' và ab đều thuộc I vì I là ideal của vành R . Do đó $xy - x'y' \in I$ hay $xy + I = x'y' + I$.

Như vậy phép nhân trên R/I được xác định.

Tính kết hợp và phân phối đối với phép cộng trên R/I được suy ra từ tính kết hợp và phân phối đối với phép cộng trên R . Điều này chứng tỏ $(R/I, +, \cdot)$ là một vành. ■

Nhận xét.

- Nếu vành R giao hoán thì vành thương R/I cũng giao hoán. Chiều ngược lại không đúng.
- Nếu vành R có đơn vị e thì vành thương R/I có đơn vị là $e + I$. Chiều ngược lại không đúng.

Ví dụ. Vành thương $\mathbb{Z}/n\mathbb{Z}$ là vành \mathbb{Z}_n , trong đó ngoài phép cộng đã biết, ta có phép toán nhân định bởi

$$(x + n\mathbb{Z})(y + n\mathbb{Z}) = xy + n\mathbb{Z}.$$

2.3. Đồng cấu vành và định lý đẳng cấu

Định nghĩa. Một ánh xạ f từ vành $R \rightarrow R'$ được gọi là một **đồng cấu vành** nếu f bảo toàn các phép toán, nghĩa là với mọi $x, y \in R$,

$$f(x + y) = f(x) + f(y),$$

$$f(xy) = f(x)f(y).$$

- Một đồng cấu từ R vào R được gọi là một **tự đồng cấu** của R .
- Một đồng cấu đồng thời là đơn ánh, toàn ánh, song ánh được gọi lần lượt là **đơn cấu**, **toàn cấu**, **đẳng cấu**.
- Một tự đồng cấu song ánh được gọi là một **tự đẳng cấu**. Nếu tồn tại một đẳng cấu từ R vào R' thì ta nói R đẳng cấu với R' , ký hiệu là $R \simeq R'$.

Ví dụ.

- ❶ Ánh xạ đồng nhất id_R của vành R là một tự đẳng cấu, gọi là **tự đẳng cấu đồng nhất** của R .
- ❷ Giả sử A là một vành con của vành R . Khi đó ánh xạ: $i_A : A \longrightarrow R$ định bởi $i_A(x) = x$ là một đơn cấu, gọi là **đơn cấu chính tắc**.
- ❸ Giả sử I là một ideal của vành R . Khi đó ánh xạ $\pi : R \longrightarrow R/I$ định bởi $\pi(x) = x + I$ là một toàn cấu, gọi là **toàn cấu chính tắc**.
- ❹ Giả sử R, R' là hai vành. Khi đó ánh xạ $f : R \longrightarrow R'$ định bởi $f(x) = 0_{R'}$ ($0_{R'}$ là phần tử không của vành R') là một đồng cấu, gọi là **đồng cấu tầm thường**.

Ví dụ. Xét ánh xạ $f : \mathbb{Z}_6 \longrightarrow \mathbb{Z}_6$ định bởi $f(\bar{x}) = 4\bar{x}$. Khi đó f là đồng cấu vành vì

$$f(\bar{x} + \bar{y}) = f(\overline{x + y}) = 4\overline{(x + y)} = 4\bar{x} + 4\bar{y} = f(\bar{x}) + f(\bar{y}),$$

$$f(\bar{x} \bar{y}) = f(\overline{xy}) = 4\overline{xy} = 4\bar{x} \bar{y} + 12\bar{x} \bar{y} = 16\bar{x} \bar{y} = (4\bar{x})(4\bar{y}) = f(\bar{x})f(\bar{y}).$$

Ví dụ. Cho R là một vành có đơn vị và $a \in R$ khả nghịch. Khi đó ánh xạ $f : R \rightarrow R$ định bởi $f(x) = axa^{-1}$ là một tự đẳng cấu của R .

Thật vậy, dễ thấy f là một song ánh, hơn nữa f là đồng cấu vì

$$f(x + y) = a(x + y)a^{-1} = axa^{-1} + aya^{-1} = f(x) + f(y),$$

$$f(xy) = a(xy)a^{-1} = (axa^{-1})(aya^{-1}) = f(x)f(y).$$

Vậy f là đẳng cấu.

Mệnh đề. Nếu $f : R \rightarrow R'$ là một đồng cấu vành thì $f(0_R) = 0_{R'}$ và $f(-x) = -f(x)$ với mọi $x \in R$. Hơn nữa $f(x - y) = f(x) - f(y)$ với mọi $x, y \in R$.

Mệnh đề. Tích của hai đồng cấu vành là một đồng cấu vành. Đặc biệt, tích của hai đơn cấu (tương ứng, toàn cấu, đẳng cấu) vành cũng là đơn cấu (tương ứng, toàn cấu, đẳng cấu) vành.

Mệnh đề. Ánh xạ ngược của một đẳng cấu vành cũng là đẳng cấu vành.

Định lý. Cho đồng cấu vành $f: R \rightarrow R'$ và A là một vành con của R , A' là một vành con của R' . Khi đó

❶ $f(A)$ là một vành con của R' .

❷ $f^{-1}(A')$ là một vành con của R . Hơn nữa, nếu A' là một ideal của R' thì $f^{-1}(A')$ cũng là ideal của R .

Đặc biệt, $\text{Im} f = f(R)$ là vành con của R' và $\text{Ker} f = f^{-1}(0_{R'})$ là ideal của R . Ta gọi $\text{Im} f$ là **ảnh** của f và $\text{Ker} f$ là **nhân** của f .

Chứng minh. (i) Vì $(A, +) \leq (R, +)$ nên $(f(A), +) \leq (R', +)$.

Hơn nữa, với mọi $x', y' \in f(A)$, tồn tại $x, y \in A$ sao cho $f(x) = x', f(y) = y'$ nên

$$x'y' = f(x)f(y) = f(xy) \in f(A).$$

Điều này chứng tỏ $f(A)$ là vành con của R' .

(ii) Vì $(A', +) \leq (R', +)$ nên $(f^{-1}(A'), +) \leq (R, +)$.

Mặt khác, với mọi $x, y \in f^{-1}(A')$, ta có $f(x), f(y) \in A'$ nên

$$f(xy) = f(x)f(y) \in A',$$

nghĩa là $xy \in f^{-1}(A')$. Điều này chứng tỏ $f^{-1}(A')$ là vành con của R .

Giả sử A' là một ideal của R' . Khi đó theo chứng minh trên $f^{-1}(A')$ là vành con của R . Hơn nữa với mọi $r \in R$ và $x \in f^{-1}(A')$ ta có

$$f(rx) = f(r)f(x) \in A' \quad (\text{do } f(x) \in A' \text{ và } A' \text{ là ideal của } R'),$$

nghĩa là $rx \in f^{-1}(A')$; tương tự $xr \in f^{-1}(A')$. Điều này chứng tỏ $f^{-1}(A')$ là ideal của R .

Cuối cùng, nhận xét rằng R là vành con của R và $\{0_{R'}\}$ là ideal của R' nên theo kết quả trên ta có khẳng định sau cùng trong định lý. ■

Định lý. Đồng cấu vành $f : R \longrightarrow R'$ là đơn cấu khi và chỉ khi $\text{Ker } f = \{0_R\}$.

Định lý. [Định lý đẳng cấu 1] Cho đồng cấu vành $f : R \longrightarrow R'$. Khi đó ánh xạ $\overline{f} : R/\text{Ker } f \longrightarrow R'$ định bởi $\overline{f}(x + \text{Ker } f) = f(x)$ là đơn cấu vành. Đặc biệt, $R/\text{Ker } f \simeq \text{Im } f$.

Chứng minh. Ta có $\text{Ker } f$ là ideal của R nên ta lập được vành thương $R/\text{Ker } f$. Theo Định lý đẳng cấu nhóm 1, ta có \overline{f} là đơn cấu nhóm cộng. Ta chỉ cần kiểm chứng \overline{f} bảo toàn phép nhân. Thật vậy, đặt $I = \text{Ker } f$, khi đó với mọi $x, y \in R$, ta có

$$\begin{aligned}\overline{f}((x + I)(y + I)) &= \overline{f}(xy + I) = f(xy) \\ &= f(x)f(y) = \overline{f}(x + I)\overline{f}(y + I)\end{aligned}$$

Điều này chứng tỏ \overline{f} là đơn cấu vành. ■

Ví dụ. Xét đồng cấu vành $f : \mathbb{Z}_6 \longrightarrow \mathbb{Z}_6$ định bởi $f(\overline{x}) = 4\overline{x}$, ta có

- $\text{Im } f = 4\mathbb{Z}_6 = -2\mathbb{Z}_6 = 2\mathbb{Z}_6 = \{2\overline{x} \mid \overline{x} \in \mathbb{Z}_6\};$
- $\begin{aligned}\text{Ker } f &= \{\overline{x} \in \mathbb{Z}_6 \mid 4\overline{x} = \overline{0}\} \\ &= \{\overline{x} \in \mathbb{Z}_6 \mid 4x \equiv 0 \pmod{6}\} \\ &= \{\overline{x} \in \mathbb{Z}_6 \mid x \equiv 0 \pmod{3}\} = 3\mathbb{Z}_6.\end{aligned}$

Theo Định lý trên, ta có

$$\mathbb{Z}_6/3\mathbb{Z}_6 \simeq 2\mathbb{Z}_6.$$

Ví dụ. Xét vành \mathbb{R} là các số thực với phép cộng phép nhân thông thường. Đặt

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}.$$

- a) Chứng minh rằng $\mathbb{Z}[\sqrt{2}]$ là vành con của \mathbb{R} .
- b) $\mathbb{Z}[\sqrt{2}]$ có là ideal của \mathbb{R} hay không? Giải thích.

Ví dụ. Trong vành $M(2, \mathbb{R})$ các ma trận vuông cấp 2 với hệ số thực, cho

$$I = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}.$$

- a) Chứng minh rằng I là vành con của $M(2, \mathbb{R})$.
- b) I có là ideal của $M(2, \mathbb{R})$ hay không? Tại sao.

Ví dụ. Xét vành \mathbb{Z}_{10} các số nguyên đồng dư modulo 10.

- a) Chứng minh rằng ánh xạ $f : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{10}$ định bởi $f(\bar{x}) = 6\bar{x}$ là một đồng cấu vành.
- b) Xác định tất cả các số nguyên a sao cho ánh xạ $g : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{10}$ định bởi $g(\bar{x}) = 2a\bar{x}$ là một đồng cấu vành.

Ví dụ. Trong vành $M_2(\mathbb{R})$ các ma trận vuông cấp 2 với hệ số thực, cho

$$I = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}.$$

- a) Chứng minh rằng I là vành con của $M_2(\mathbb{R})$.
- b) I có là ideal trái của $M_2(\mathbb{R})$ không?
- c) I có là ideal phải của $M_2(\mathbb{R})$ không?
- d) I có là ideal của $M_2(\mathbb{R})$ không?

Ví dụ. Xét ánh xạ $f : \mathbb{Z} \rightarrow \mathbb{Z}_{12}$ định bởi $f(a) = 4\bar{a}$.

- a) Chứng minh rằng f là một đồng cấu vành.
- b) Xác định $\text{Ker } f$.

Ví dụ. Xét vành \mathbb{Z}_{10} và ánh xạ $f : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{10}$ định bởi $f(\bar{x}) = 6\bar{x}$

- a) Chứng minh rằng ánh xạ f là đồng cấu vành.
- b) Chứng minh $\text{Im } f = \langle \bar{2} \rangle$ và $\text{Ker } f = \langle \bar{5} \rangle$.

Ví dụ. Cho R là một vành giao hoán có đơn vị 1 và $a \in R$ thỏa $a^3 = 0$. Chứng minh rằng

- a) $1 + a$ khả nghịch và tìm $(1 + a)^{-1}$.
- b) Nếu $x \in R$ thỏa $x + a$ khả nghịch thì x khả nghịch.

2.4. Miền nguyên và trường

Định nghĩa.

- ❶ Cho R là một vành giao hoán. Phần tử $x \in R \setminus \{0\}$ được gọi là *ước của không* nếu tồn tại $y \in R \setminus \{0\}$ sao cho $xy = 0$.
- ❷ Một vành giao hoán, có đơn vị, có nhiều hơn một phần tử và không có ước của không được gọi là *miền nguyên*.
- ❸ Một vành giao hoán, có đơn vị, có nhiều hơn một phần tử trong đó mọi phần tử khác 0 đều khả nghịch được gọi là một *trường*.

Nhận xét.

- ❶ Trong miền nguyên R , phép nhân có tính giản ước cho các phần tử khác không nghĩa là nếu $xy = xz$ và $x \neq 0$ thì $y = z$.
Thật vậy, từ $xy = xz$ ta suy ra $x(y - z) = xy - xz = 0$. Do đó $y - z = 0$, nghĩa là $y = z$ (do $x \neq 0$ và R không có ước của không).
- ❷ Mọi trường R chỉ có hai ideal là $\{0\}$ và R .

Nhận xét. $(R, +, \cdot)$ là một trường khi và chỉ khi các tính chất sau đây được thỏa:

- i) $(R, +)$ là nhóm Abel;
- ii) $(R \setminus \{0\}, \cdot)$ là nhóm Abel;
- iii) Phép nhân phân phối với phép cộng.

Ví dụ.

- i) Tập các số nguyên \mathbb{Z} với phép cộng và nhân thông thường là miền nguyên nhưng không là trường.
- ii) Tập hợp các số hữu tỷ \mathbb{Q} với phép cộng và nhân thông thường là trường. Ta gọi đó là *trường các số hữu tỷ \mathbb{Q}* . Tương tự, ta có *trường các số thực \mathbb{R}* và *trường các số phức \mathbb{C}* .
- iii) Vành \mathbb{Z}_n các số nguyên modulo n là trường khi và chỉ khi $n = p$ nguyên tố.

Định lý.

- ➊ Mọi trường đều là miền nguyên.
- ➋ Mọi miền nguyên hữu hạn đều là trường.

Chứng minh. (i) Ta chỉ cần chứng minh rằng mọi trường R đều không có ước của không. Thật vậy, giả sử $xy = 0$ và $x \neq 0$. Khi đó x khả nghịch nên tồn tại $x^{-1} \in R$ sao cho $x^{-1}x = e$. Do đó

$$y = ey = x^{-1}xy = x^{-1}0 = 0.$$

Điều này chứng tỏ R không có ước của không và do đó R là miền nguyên.

(ii) Giả sử R là một miền nguyên hữu hạn. Cho $a \in R \setminus \{0\}$ bất kỳ. Ta chứng minh a khả nghịch. Thật vậy, xét ánh xạ

$$\begin{array}{ccc} f : R \setminus \{0\} & \longrightarrow & R \setminus \{0\} \\ x & \longmapsto & ax \end{array}$$

Vì trong miền nguyên R phép nhân có tính giản ước nên ta thấy ngay f là đơn ánh.

Theo giả thiết $R \setminus \{0\}$ hữu hạn nên f phải là song ánh. Suy ra tồn tại $b \in R \setminus \{0\}$ sao cho $f(b) = e$, nghĩa là $ab = e$. Điều này chứng tỏ a khả nghịch, và do đó R là trường. ■

Nhận xét. Giả thiết hữu hạn trong (ii) của Định lý trên không thể bỏ được. Chẳng hạn \mathbb{Z} là miền nguyên vô hạn nhưng không phải là trường.

Định nghĩa. Cho R là trường và e là phần tử đơn vị của R . Ta xét cấp của e trong nhóm $(R, +)$, khi đó

- ❶ Nếu e có cấp n , ta nói trường R có đặc số n , ký hiệu $\text{char} R = n$.
- ❷ Nếu e có vô hạn ta nói trường R có đặc số 0, ký hiệu $\text{char} R = 0$

Ví dụ.

- ❶ Các trường số \mathbb{Q} , \mathbb{R} , \mathbb{C} đều có đặc số 0;
- ❷ Với p nguyên tố, trường \mathbb{Z}_p các số nguyên modulo p , có đặc số p .

Mệnh đề. Cho R là trường. Khi đó $\text{char} R = 0$ hoặc $\text{char} R$ là số nguyên tố.

Chứng minh. Giả sử $\text{char} R = n > 0$. Khi đó e có cấp trong nhóm $(R, +)$ là n . Giả sử n không là số nguyên tố, khi đó ta có $1 < m, k < n$ sao cho $n = mk$ nên

$$0 = ne = (mk)e = (me)(ke).$$

Suy ra $me = 0$ hoặc $ke = 0$, mâu thuẫn với tính chất của cấp n . Do đó n là số nguyên tố.

Định nghĩa. Cho R là một trường và I là một tập con khác rỗng của R ổn định đối với hai phép toán trong R . Ta nói I là một **trường con** của R nếu I với hai phép toán cảm sinh từ R cũng là một trường.

Ví dụ. Trường các số hữu tỷ \mathbb{Q} là trường con của trường các số thực \mathbb{R} . Tương tự, \mathbb{R} là trường con của \mathbb{C} .

Định lý. [Đặc trưng của trường con] Cho R là một trường và I là tập con của R có chứa ít nhất hai phần tử. Các mệnh đề sau tương đương:

- i) I là một trường con của R ;
- ii) Với mọi $x, y \in I$, $x + y \in I$, $xy \in I$, $-x \in I$ và hơn nữa, nếu $x \neq 0$ thì $x^{-1} \in I$;
- iii) Với mọi $x, y \in I$, $x - y \in I$ và hơn nữa, nếu $x \neq 0$ thì $x^{-1}y \in I$.

Ví dụ. Trong trường số thực \mathbb{R} đặt

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

- a) Chứng minh rằng $\mathbb{Q}(\sqrt{2})$ là một trường con của \mathbb{R}
- b) Tìm tất các tự đồng cấu của $\mathbb{Q}(\sqrt{2})$.

Ví dụ. Chứng minh rằng hai trường sau là đẳng cấu:

$$F = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \mid a, b \in \mathbb{Q} \right\} \text{ và } \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

Định lý. Cho R là một trường. Các mệnh đề sau tương đương:

- (i) $\text{char} R = 0$;
- (ii) Với mọi $x \in R \setminus \{0\}$ và $n \in \mathbb{Z}$, nếu $nx = 0$ thì $n = 0$;
- (iii) R chứa một trường con đẳng cấu (vành) với \mathbb{Q} .

Chứng minh. (i) \Rightarrow (ii) Giả sử $\text{char} R = 0$. Xét $x \in R \setminus \{0\}$ và $n \in \mathbb{Z}$ thỏa $nx = 0$. Khi đó $0 = nx = (ne)x$. Vì $x \neq 0$ nên $ne = 0$. Suy ra $n = 0$ (do $\text{char} R = 0$).

(ii) \Rightarrow (iii) Với giả thiết (ii), ta xét ánh xạ $f : \mathbb{Q} \longrightarrow R$ định bởi

$$f\left(\frac{m}{n}\right) = (me)(ne)^{-1}.$$

Ta thấy f được xác định và là đơn ánh vì

$$\begin{aligned}\frac{m}{n} = \frac{m'}{n'} &\Leftrightarrow mn' - m'n = 0 \\ &\Leftrightarrow (mn' - m'n)e = 0 \text{ (do (ii))} \\ &\Leftrightarrow (me)(n'e) - (m'e)(ne) = 0\end{aligned}$$

$$\Leftrightarrow (me)(ne)^{-1} - (m'e)(n'e)^{-1} = 0 \text{ (vì nhân cho } (ne)^{-1}(n'e)^{-1})$$

$$\Leftrightarrow f\left(\frac{m}{n}\right) = f\left(\frac{m'}{n'}\right).$$

Hơn nữa, f bảo toàn các phép toán vì

$$\begin{aligned} f\left(\frac{m}{n} + \frac{m'}{n'}\right) &= f\left(\frac{mn' + m'n}{nn'}\right) \\ &= [(mn' + m'n)e](nn'e)^{-1} \\ &= [(me)(n'e) + (m'e)(ne)](ne)^{-1}(n'e)^{-1} \\ &= (me)(ne)^{-1} + (m'e)(n'e)^{-1} \\ &= f\left(\frac{m}{n}\right) + f\left(\frac{m'}{n'}\right) \end{aligned}$$

và tương tự

$$f\left(\frac{m}{n} \frac{m'}{n'}\right) = f\left(\frac{m}{n}\right)f\left(\frac{m'}{n'}\right).$$

Vậy f là đơn cấu vành. Suy ra $\text{Im } f$ là trường con của R đẳng cấu với \mathbb{Q} .

(iii) \Rightarrow (i) Vì $\text{char } \mathbb{Q} = 0$ nên trường con của R đẳng cấu với \mathbb{Q} cũng có đặc số không. Do đó R cũng có đặc số không. ■

Định lý. Cho R là một trường và p là một số nguyên tố. Các mệnh đề sau tương đương:

- (i) $\text{char} R = p$;
- (ii) Với mọi $x \in R \setminus \{0\}$ và $n \in \mathbb{Z}$, $nx = 0$ khi và chỉ khi $p \mid n$;
- (iii) R chứa một trường con đẳng cấu (vành) với \mathbb{Z}_p .

Chứng minh. (i) \Rightarrow (ii) Giả sử $\text{char} R = p$. Xét $x \in R \setminus \{0\}$ và $n \in \mathbb{Z}$ thỏa $nx = 0$. Khi đó $0 = nx = (ne)x$ và $x \neq 0$ nên $ne = 0$. Từ đây do $\text{char} R = p = |e|$ nên $p \mid n$. Đảo lại, nếu $p \mid n$ thì $nx = (ne)x = 0x = 0$.

(ii) \Rightarrow (iii) Với giả thiết (ii), xét ánh xạ

$$f : \mathbb{Z} \longrightarrow R$$

định bởi $f(n) = ne$. Dễ thấy f là đồng cấu vành và $\text{Ker} f = p\mathbb{Z}$. Do đó, theo Định lý đẳng cấu 1, ta có

$$\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} \simeq \text{Im} f.$$

Chú ý rằng \mathbb{Z}_p là trường do p nguyên tố, nên R chứa trường con $\text{Im} f$ đẳng cấu với \mathbb{Z}_p .

(iii) \Rightarrow (i) Vì $\text{char}\mathbb{Z}_p = p$ nên trường con của R đẳng cấu với \mathbb{Z}_p cũng có đặc trưng p . Do đó $\text{char}R = p$. ■

Nhận xét. Cho R là một trường có đặc số p nguyên tố. Khi đó ánh xạ $\varphi : R \rightarrow R$ định bởi $\varphi(x) = x^p$ là một tự đẳng cấu của R .

Chứng minh. Thật vậy, với mọi $x, y \in R$ ta có

$$\varphi(xy) = (xy)^p = x^p y^p = \varphi(x)\varphi(y).$$

Hơn nữa

$$\begin{aligned}\varphi(x + y) &= (x + y)^p \\ &= x^p + \sum_{k=1}^{p-1} C_p^k x^{p-k} y^k + y^p \\ &= x^p + y^p \\ &= \varphi(x) + \varphi(y)\end{aligned}$$

do $C_p^k = \frac{p!}{k!(p-k)!}$ là bội số của p (p nguyên tố) với mọi

$1 \leq k \leq p-1$. Điều này chứng tỏ φ là đồng cấu. Mặt khác do $\text{Ker}\varphi = \{0\}$ nên φ là đơn cấu. ■

Xét R là một miền nguyên. Khi đó phép nhân trong R có tính giản ước cho các phần tử khác không. Tuy nhiên điều đó chưa đủ để khẳng định mọi phần tử khác không đều khả nghịch trong R . Ta sẽ xây dựng trường \overline{R} nhỏ nhất có chứa R , trong đó mọi phần tử khác không của R đều khả nghịch trong \overline{R} . Ta gọi \overline{R} là **trường các thương của miền nguyên R** .

Định nghĩa. Cho R là một miền nguyên và \overline{R} là một trường. Ta nói \overline{R} là **trường các thương** của miền nguyên R nếu tồn tại một đơn cấu (vành) $f: R \rightarrow \overline{R}$ sao cho mọi phần tử của \overline{R} đều có dạng $f(a)f(b)^{-1}$ với $a, b \in R, b \neq 0$.

Định lý. Cho R là một miền nguyên. Khi đó trường các thương \overline{R} của R luôn luôn tồn tại và duy nhất (sai khác một đẳng cấu).

Chứng minh. Sự tồn tại. Đặt $D = R \setminus \{0\}$. Trên $R \times D$ xét quan hệ

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Khi đó, hiển nhiên \sim có tính chất phản xạ và đối xứng. Ta chứng minh \sim bắc cầu. Giả sử $(a, b) \sim (c, d)$ và $(c, d) \sim (u, v)$. Khi đó $ad = bc$ và $cv = du$ nên

$$d(av) = (bc)v = b(cv) = b(du) = d(bu).$$

Vì $d \neq 0$ nên $av = bu$, nghĩa là $(a, b) \sim (u, v)$. Vậy \sim bắc cầu và do đó \sim là quan hệ tương đương trên $R \times D$.

Đặt $\overline{R} = (R \times D) / \sim$ là tập thương của $R \times D$ trên quan hệ \sim . Các phần tử của \overline{R} là các lớp tương đương $\overline{(a, b)}$ mà ta ký hiệu là $\frac{a}{b}$. Trên \overline{R} ta định nghĩa hai phép toán cộng và nhân như sau:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{và} \quad \frac{a}{b} \frac{c}{d} = \frac{ac}{bd}.$$

Ta chứng minh các phép toán trên được xác định. Thật vậy, giả sử $\frac{a}{b} = \frac{a'}{b'}$ và $\frac{c}{d} = \frac{c'}{d'}$. Khi đó $ab' = a'b$ và $cd' = c'd$ nên

$$(ad + bc)b'd' = ab'dd' + cd'bb' = a'bdd' + c'dbb' = (a'd' + b'c')bd,$$

hay

$$(ad + bc, bd) \sim (a'd' + b'c', b'd'),$$

nghĩa là

$$\frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'}.$$

Mặt khác,

$$(ac)(b'd') = (ab')(cd') = (a'b)(c'd) = (a'c')(bd)$$

nên

$$(ac, bd) \sim (a'c', b'd'),$$

nghĩa là

$$\frac{ac}{bd} = \frac{a'c'}{b'd'}.$$

Vậy các phép toán cộng và nhân trên \overline{R} được xác định. Dễ thấy rằng $(\overline{R}, +)$ là nhóm Abel, trong đó phần tử không là $\frac{0}{e}$ và phần tử đối của $\frac{a}{b}$ là $\frac{-a}{b}$. Hơn nữa, $(\overline{R} \setminus \{0\}, \cdot)$ là nhóm giao hoán với phần tử đơn vị là $\frac{e}{e}$ trong đó mọi phần tử $x = \frac{a}{b} \neq \frac{0}{e}$ đều có $a = ae - b0 \neq 0$ nên x có phần tử nghịch đảo $x^{-1} = \frac{b}{a}$.

Ngoài ra, bằng cách thử trực tiếp ta thấy phép nhân phân phối đối với phép cộng. Do đó \overline{R} là trường.

Xét ánh xạ $f : R \longrightarrow \overline{R}$ định bởi $f(a) = \frac{a}{e}$. Hiển nhiên f là đơn cấu vành.

Với $x = \frac{a}{b} \in \overline{R}$ tùy ý ta có

$$x = \frac{a}{b} = \frac{a e}{e b} = \frac{a}{e} \left(\frac{b}{e} \right)^{-1} = f(a) f(b)^{-1}.$$

Do đó \overline{R} chính là trường các thương của miền nguyên R .

Sự duy nhất. Giả sử ngoài \overline{R} như đã xây dựng ở trên, R còn có trường các thương S với đơn cấu vành $g : R \longrightarrow S$ sao cho mọi phần tử trong S đều được viết dưới dạng $g(a)g(b)^{-1}$ với $a, b \in R, a \neq 0$. Xét ánh xạ $\varphi : \overline{R} \longrightarrow S$ định bởi

$$\varphi(f(a)f(b)^{-1}) = g(a)g(b)^{-1} \quad \text{với mọi } a, b \in R, b \neq 0.$$

Ta thấy φ được xác định và là đơn ánh vì

$$\begin{aligned} f(a)f(b)^{-1} = f(c)f(d)^{-1} &\Leftrightarrow f(a)f(d) = f(b)f(c) \\ &\Leftrightarrow f(ad) = f(bc) \\ &\Leftrightarrow ad = bc \\ &\Leftrightarrow g(ad) = g(bc) \\ &\Leftrightarrow g(a)g(b)^{-1} = g(c)g(d)^{-1}. \end{aligned}$$

Hiển nhiên φ là toàn ánh. Vậy φ là song ánh. Ta còn phải chứng minh φ là đồng cấu, nghĩa là bảo toàn các phép toán. Thật vậy, giả sử $x = f(a)f(b)^{-1}$ và $y = f(c)f(d)^{-1}$, khi đó

$$\begin{aligned}
x + y &= f(a)f(b^{-1}) + f(c)f(d)^{-1} \\
&= [f(a)f(d) + f(b)f(c)]f(b)^{-1}f(d)^{-1} \\
&= f(ad + bc)f(bd)^{-1}; \\
xy &= f(a)f(b)^{-1}f(c)f(d)^{-1} \\
&= f(ac)f(bd)^{-1}
\end{aligned}$$

nên

$$\begin{aligned}
\varphi(x + y) &= g(ad + bc)g(bd)^{-1} \\
&= [g(a)g(d) + g(b)g(c)]g(b)^{-1}g(d)^{-1} \\
&= g(a)g(b)^{-1} + g(c)g(d)^{-1} = \varphi(x) + \varphi(y); \\
\varphi(xy) &= g(ac)g(bd)^{-1} \\
&= g(a)g(c)g(b)^{-1}g(d)^{-1} \\
&= g(a)g(b)^{-1}g(c)g(d)^{-1} = \varphi(x)\varphi(y).
\end{aligned}$$

Vậy φ là đồng cấu vành. Suy ra φ là đẳng cấu vành và $\overline{R} \simeq S$. Điều này chứng tỏ sự duy nhất (sai khác một đẳng cấu) của trường các thương của R .

Nhận xét. Vì ánh xạ $f : R \longrightarrow \overline{R}$ định bởi $f(a) = \frac{a}{e}$ là đơn cấu vành nên ta có thể đồng nhất $a \in R$ với $\frac{a}{e} \in \overline{R}$. Do đó có thể xem \overline{R} như là một trường chứa miền nguyên R và mọi phần tử thuộc \overline{R} đều có dạng

$$\frac{a}{b} = \frac{a}{e} \left(\frac{b}{e} \right)^{-1} = ab^{-1} \text{ với } a, b \in R \text{ và } b \neq 0.$$

Rõ ràng mọi trường chứa miền nguyên R đều phải chứa các phần tử có dạng ab^{-1} như thế nên \overline{R} là trường nhỏ nhất chứa R .

Ví dụ. Trường các số hữu tỷ \mathbb{Q} chính là trường các thương của miền nguyên \mathbb{Z} vì $\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z} \right\} = \{ ab^{-1} \mid a, b \in \mathbb{Z} \}.$

Chương 3

VÀNH ĐA THỨC

Đại học Khoa Học Tự Nhiên Tp. Hồ Chí Minh

Chương 3. Vành đa thức

- Vành đa thức một ẩn
- Nghiệm của đa thức
- Đa thức trên trường số thực và số phức
- Đa thức trên trường số hữu tỷ

3.1. Vành đa thức một ẩn

Định nghĩa. Giả sử R là một vành giao hoán và có đơn vị 1. Gọi A là tập hợp tất cả các dãy

$$(a_0, a_1, \dots, a_n, \dots),$$

trong đó các $a_i \in R, \forall i \in \mathbb{N}$ và bằng 0 tất cả trừ một số hữu hạn.

Ta định nghĩa phép cộng và nhân trong A như sau:

Với $f = (a_0, a_1, \dots, a_n, \dots), g = (b_0, b_1, \dots, b_n, \dots) \in A$. Khi đó

$$f + g = (a_0 + b_0, a_1 + b_1, \dots, a_n + b_n, \dots),$$

$$f \cdot g = (c_0, c_1, \dots, c_n, \dots),$$

trong đó

$$c_k = \sum_{i+j=k} a_i b_j, \quad k = 0, 1, 2, \dots$$

Khi đó $(A, +, \cdot)$ là một vành giao hoán, có

- phần tử đơn vị là $(1, 0, 0, \dots)$, ký hiệu **1**.
- phần tử không là $(0, 0, 0, \dots)$, ký hiệu là **0**.

Đặt $x = (0, 1, 0, 0, \dots)$. Dễ thấy rằng

$$\begin{aligned}x^2 &= (0, 0, 1, 0, \dots); \\x^3 &= (0, 0, 0, 1, 0, \dots); \\x^n &= (\underbrace{0, 0, \dots, 0}_n, 1, 0, \dots).\end{aligned}$$

Ta quy ước $x^0 = (1, 0, 0, \dots)$ và mỗi phần tử $a \in R$ có thể đồng nhất với dãy $(a, 0, 0, \dots)$ nhờ đơn cấu vành

$$\begin{aligned}R &\longrightarrow A \\a &\longmapsto (a, 0, 0, \dots).\end{aligned}$$

Như vậy

$$ax^n = (\underbrace{0, 0, \dots, 0}_n, a, 0, \dots), \forall a \in R.$$

Do đó

$$f = (a_0, a_1, \dots, a_n, 0, 0, \dots) = a_0 + a_1x + \dots + a_nx^n,$$

và thường được viết là

$$f(x) = a_nx^n + \dots + a_1x + a_0.$$

Cách biểu thị như vậy là duy nhất đối với mỗi phần tử $f \in A$. Nói cách khác,

$$a_nx^n + \dots + a_1x + a_0 = b_nx^n + \dots + b_1x + b_0$$

khi và chỉ khi

$$a_n = b_n, \dots, a_1 = b_1, a_0 = b_0.$$

Vành A nói trên được gọi là **vành đa thức** của ẩn x (hoặc biến x) với các hệ số trong R , và được ký hiệu là $R[x]$.

Mỗi phần tử của $R[x]$ được gọi là một **đa thức của ẩn x** trên R . Đa thức dạng ax^n ($a \in R$) được gọi là một **đơn thức**.

Định nghĩa. Cho

$$f(x) = a_n x^n + \dots + a_1 x + a_0$$

với $a_n \neq 0$. Khi đó

- Đa thức $f(x)$ có **bậc** là n và ký hiệu $\deg f = n$ hay $\deg f(x) = n$.
- Phần tử a_i được gọi là **hệ số thứ i** của $f(x)$
- phần tử a_n được gọi là **hệ số cao nhất**
- phần tử a_0 được gọi là **hệ số tự do**.
- Bậc của đa thức 0 được quy ước là $-\infty$.

Với $f(x)$ và $g(x)$ là hai đa thức bất kỳ trên R , ta có

- ① $\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}$
- ② $\deg(f(x)g(x)) \leq \deg f(x) + \deg g(x)$

Định lý. Nếu D là một miền nguyên thì $D[x]$ cũng là một miền nguyên.

Chứng minh. Giả sử $f(x), g(x) \in D[x]$ là các đa thức khác 0 có bậc tương ứng là m và n

$$\begin{aligned}f(x) &= a_mx^m + \dots + a_1x + a_0, \quad a_m \neq 0; \\g(x) &= b_nx^n + \dots + b_1x + b_0, \quad b_n \neq 0.\end{aligned}$$

Theo định nghĩa phép toán trên đa thức ta có

$$f(x)g(x) = a_mb_nx^{m+n} + \dots + (a_0b_1 + a_1b_0)x + a_0b_0.$$

Vì D là miền nguyên và $a_m, b_n \neq 0$ nên $a_mb_n \neq 0$, do đó $f(x)g(x) \neq 0$.

Ta cũng suy ra được

$$\deg(f(x)g(x)) = \deg f(x) + \deg g(x).$$

Tuy nhiên đẳng thức trên không còn đúng nữa khi R không phải là miền nguyên. Chẳng hạn, $\bar{2}x + \bar{1}$ và $\bar{3}x + \bar{1}$ là các đa thức bậc nhất trong $\mathbb{Z}_6[x]$ nhưng tích của chúng lại là một đa thức bậc nhất.

Định lý. [Phép chia Euclide] Giả sử K là một trường và $f(x), g(x) \in K[x], g(x) \neq 0$. Khi đó tồn tại duy nhất các đa thức $q(x), r(x) \in K[x]$ sao cho

$$f(x) = g(x)q(x) + r(x),$$

với $\deg r(x) < \deg g(x)$.

Các đa thức $q(x)$ và $r(x)$ được gọi tương ứng là **thương** và **dư** trong phép chia $f(x)$ cho $g(x)$.

Chứng minh.

i) Sự duy nhất. Giả sử

$$f(x) = g(x)q(x) + r(x) = g(x)q'(x) + r'(x)$$

với $\deg r(x) < \deg g(x)$ và $\deg r'(x) < \deg g(x)$. Khi đó ta có

$$g(x)[q(x) - q'(x)] = r'(x) - r(x).$$

Nếu $q(x) \neq q'(x)$ thì

$$\deg[r'(x) - r(x)] = \deg g(x) + \deg[q(x) - q'(x)] \geq \deg g(x).$$

Điều này mâu thuẫn với giả thiết $\deg r(x) < \deg g(x)$ và $\deg r'(x) < \deg g(x)$. Do đó $q(x) = q'(x)$. Vì vậy $r(x) = r'(x)$.

ii) Sự tồn tại. Ta chứng minh sự tồn tại của $q(x)$ và $r(x)$ bằng phương pháp quy nạp theo bậc của $f(x)$. Giả sử

$$\begin{aligned} f(x) &= a_n x^n + \dots + a_1 x + a_0, \quad a_n \neq 0; \\ g(x) &= b_m x^m + \dots + b_1 x + b_0, \quad b_m \neq 0. \end{aligned}$$

• Với $n = 0$.

- $m = 0$ thì đặt $r(x) = 0, q(x) = a_0 b_0^{-1}$,
- $m > 0$ thì đặt $q(x) = 0, r(x) = f(x)$.

• Với $n > 0$. Giả sử định lý được chứng minh cho mọi đa thức f có bậc nhỏ hơn n .

- Nếu $m > n$ thì ta chọn $q(x) = 0, r(x) = f(x)$.
- Nếu $m \leq n$ thì đặt

$$\bar{f}(x) = f(x) - (a_n b_m^{-1}) x^{n-m} g(x).$$

Khi đó $\bar{f}(x)$ là đa thức có bậc $< n$. Theo giả thiết quy nạp, tồn tại các đa thức $\bar{q}(x)$ và $r(x)$ sao cho

$$\bar{f}(x) = \bar{q}(x)g(x) + r(x), \deg r(x) < m.$$

Do đó

$$f(x) = (a_n b_m^{-1} x^{n-m} + \bar{q}(x))g(x) + r(x).$$

Đặt $q(x) = a_n b_m^{-1} x^{n-m} + \bar{q}(x)$, ta có các đa thức thương và dư cần tìm trong phép chia $f(x)$ cho $g(x)$. ■

Ví dụ. Trong $\mathbb{Z}_{11}[x]$, hãy tìm thương và dư trong phép chia đa thức $f(x) = -\bar{1}x^3 - \bar{7}x^2 + \bar{3}x - \bar{5}$ cho $g(x) = -\bar{2}x^2 + \bar{2}x - \bar{1}$.

Giải. Ta viết

$$\begin{array}{r|l}
 -\bar{1}x^3 - \bar{7}x^2 + \bar{3}x - \bar{5} & -\bar{2}x^2 + \bar{2}x - \bar{1} \\
 -\bar{1}x^3 + \bar{1}x^2 - \bar{6}x & \hline
 \hline
 & -\bar{8}x^2 + \bar{9}x - \bar{5} \\
 & -\bar{8}x^2 + \bar{8}x - \bar{4} \\
 \hline
 & \bar{1}x - \bar{1}
 \end{array}$$

Vậy

$$-\bar{1}x^3 - \bar{7}x^2 + \bar{3}x - \bar{5} = (-\bar{2}x^2 + \bar{2}x - \bar{1})(\bar{6}x + \bar{4}) + \bar{1}x - \bar{1}.$$

Ví dụ.(tự làm) Trong $\mathbb{Z}_5[x]$, hãy tìm thương và dư trong phép chia đa thức $f(x) = \bar{2}x^3 - \bar{4}x^2 + \bar{1}x - \bar{3}$ cho $g(x) = \bar{3}x - \bar{4}$.

Ước chung lớn nhất

Định nghĩa. Cho K là trường và $f(x), g(x) \in K[x], g(x) \neq 0$. Khi đó

- Nếu tồn tại $q(x) \in K[x]$ sao cho $f(x) = q(x)g(x)$ thì ta nói $f(x)$ **chia hết cho** $g(x)$ (hay $g(x)$ là **ước** của $f(x)$) trong $K[x]$.
- Một đa thức $d(x) \in K[x]$ là ước của hai đa thức $f(x)$ và $g(x)$ được gọi là **ước chung** của $f(x)$ và $g(x)$.
- Nếu $d(x)$ là ước chung của $f(x)$ và $g(x)$, đồng thời $d(x)$ chia hết cho mọi ước chung khác của $f(x)$ và $g(x)$ thì $d(x)$ được gọi là **ước chung lớn nhất** của $f(x)$ và $g(x)$, viết tắt là UCLN, ký hiệu là

$$d(x) = (f(x), g(x)).$$

Thuật chia Euclide

Để tìm UCLN của hai đa thức $f(x), g(x) \in K[x]$ ta dùng thuật chia Euclide bằng cách thực hiện một số hữu hạn phép chia liên tiếp như sau:

$$f(x) = g(x)q(x) + r(x), \quad \deg r(x) < \deg g(x)$$

$$g(x) = r(x)q_1(x) + r_1(x), \quad \deg r_1(x) < \deg r(x)$$

.....

$$r_{k-2}(x) = r_{k-1}(x)q_k(x) + r_k(x), \quad \deg r_k(x) < \deg r_{k-1}(x)$$

$$r_{k-1}(x) = r_k(x)q_{k+1}(x).$$

Đa thức dư cuối cùng khác 0 trong dãy phép chia nói trên chính là $r_k(x)$ và

$$\text{UCLN} = \frac{r_k(x)}{\text{hệ số cao nhất của } r_k(x)}.$$

Từ thuật toán Euclide ta thấy rằng nếu $d(x) = (f(x), g(x))$ thì ta có thể tìm được hai đa thức $u(x), v(x) \in K[x]$ sao cho

$$f(x)u(x) + g(x)v(x) = d(x).$$

Ví dụ. Trong $\mathbb{R}[x]$ cho các đa thức $f(x) = 4x^4 - 2x^3 - 16x^2 + 5x + 9$ và $g(x) = 2x^3 - x^2 - 5x + 4$. Hãy tìm $d(x) = (f(x), g(x))$ và tìm các đa thức $u(x), v(x) \in \mathbb{R}[x]$ sao cho

$$f(x)u(x) + g(x)v(x) = d(x).$$

Giải. Để tìm UCLN của $f(x)$ và $g(x)$, ta thực hiện dãy các phép chia liên tiếp

$$\begin{array}{r|l} 4x^4 - 2x^3 - 16x^2 + 5x + 9 & 2x^3 - x^2 - 5x + 4 \\ 4x^4 - 2x^3 - 10x^2 + 8x & 2x \\ \hline & -6x^2 - 3x + 9 \end{array}$$

Ta có $f(x) = g(x)q(x) + r(x)$ với $r(x) = -6x^2 - 3x + 9$, $q(x) = 2x$.

Nhân $g(x)$ với 3 rồi chia cho $r(x)$.

$$\begin{array}{r|l}
 6x^3 - 3x^2 - 15x + 12 & -6x^2 - 3x + 9 \\
 6x^3 + 3x^2 - 9x & \hline
 -6x^2 - 6x + 12 & \\
 -6x^2 - 3x + 9 & \\
 \hline
 -3x + 3 &
 \end{array}$$

Ta có $3g(x) = r(x)q_1(x) + r_1(x)$ với $q_1(x) = -x + 1, r_1(x) = -3x + 3$.

Lấy $r(x)$ chia cho $r_1(x)$ ta có

$$\begin{array}{r|l}
 -6x^2 - 3x + 9 & -3x + 3 \\
 -6x^2 + 6x & \hline
 -9x + 9 & \\
 -9x + 9 & \\
 \hline
 0 &
 \end{array}$$

$$r(x) = (2x + 3)r_1(x).$$

Do đó ta có $r_1(x) = -3x + 3$ là dư cuối cùng khác 0.

Theo quy ước, ta sẽ lấy

$$d(x) = (f(x), g(x)) = x - 1.$$

Theo quá trình trên ta có

$$\begin{aligned}r_1 l(x) &= 3g(x) - r(x)q_1(x) \\&= 3g(x) - q_1(x)[f(x) - g(x)q(x)] \\&= [3 + q(x)q_1(x)]g(x) - q_1(x)f(x).\end{aligned}$$

Suy ra

$$d(x) = \frac{-x+1}{3}f(x) + \frac{2x^2-2x-3}{3}g(x).$$

Ví dụ.(tự làm) Trong \mathbb{Z}_7 cho các đa thức cho các đa thức $f(x) = \overline{2}x^4 - \overline{4}x^3 + x^2 - \overline{3}x + \overline{2}$ và $g(x) = x^3 - x^2 + x - \overline{6}$. Hãy tìm $d(x) = (f(x), g(x))$ và tìm các đa thức $u(x), v(x) \in \mathbb{Z}_7[x]$ sao cho

$$f(x)u(x) + g(x)v(x) = d(x).$$

Đáp án. $d(x) = x + \overline{5}$ $u(x) = \overline{6}x + 2$ $g(x) = \overline{2}x^2 + x + \overline{1}$

Đa thức bất khả quy trên miền nguyên

Định nghĩa. Cho D là miền nguyên. Đa thức $0 \neq f(x) \in D[x]$ không khả nghịch được gọi là **bất khả quy** trong $D[x]$ (hay còn gọi là bất khả quy trên D) nếu nó không có ước thực sự trong $D[x]$, tức là nếu

$$f(x) = g(x)h(x) \quad (g(x), h(x) \in D[x])$$

thì $g(x)$ hay $h(x)$ phải là phần tử khả nghịch của D .

Ví dụ.

- $x^2 - 2$ bất khả quy trên $\mathbb{Q}[x]$, nhưng khả quy trên $\mathbb{R}[x]$.
- $x^2 + 1$ bất khả quy trên $\mathbb{R}[x]$, nhưng khả quy trên $\mathbb{C}[x]$.

Nhận xét. Cho K là một trường. Khi đó đa thức $0 \neq f(x) \in K[x]$ không khả nghịch là bất khả quy trên K khi và chỉ khi nếu

$$f(x) = g(x)h(x), \quad (g(x), h(x) \in K[x])$$

thì $g(x)$ hay $h(x)$ là phần tử khác không của K .

Định lý. Có vô số đa thức với hệ số cao nhất là 1 bất khả quy trên trường K .


Chứng minh. Nếu K là trường vô hạn thì các đa thức dạng $x - a, a \in K$ là các đa thức với hệ số cao nhất là 1 bất khả quy trên K . Có vô số đa thức như vậy.

Trong trường hợp K là trường hữu hạn, giả sử chỉ có n đa thức bất khả quy $p_1(x), p_2(x), \dots, p_n(x)$ với hệ số cao nhất là 1. Đa thức

$$f(x) = p_1(x)p_2(x) \dots p_n(x) + 1$$

có ít nhất một ước bất khả quy (với hệ số cao nhất là 1) vì $\deg f(x) \geq n$. Ước đó phải khác $p_1(x), p_2(x), \dots, p_n(x)$ vì nếu không nó sẽ là ước của

$$f(x) - p_1(x)p_2(x) \dots p_n(x) = 1,$$

điều này vô lý. Vậy $K[x]$ phải có vô hạn đa thức bất khả quy với hệ số cao nhất là 1. 

3.2. Nghiệm của đa thức

Định nghĩa. Giả sử $c \in R$ và

$$f(x) = a_n x^n + \dots + a_1 x + a_0 \in R[x].$$

Phần tử $f(c) = a_n c^n + \dots + a_1 c + a_0$ được gọi là **giá trị** của $f(x)$ tại c . Nếu $f(c) = 0$ thì c được gọi là **nghiệm** của $f(x)$.

Tìm nghiệm của $f(x)$ trong R là giải phương trình đại số $a_n x^n + \dots + a_1 x + a_0 = 0$ trong R .

Định lý. [Định lý Bezout.] Phần tử c của trường K là nghiệm của đa thức $f(x) \in K[x]$ khi và chỉ khi $f(x)$ chia hết cho $x - c$.

Chứng minh. Chia $f(x)$ cho $x - c$ ta được

$$f(x) = q(x)(x - c) + r(x)$$


với $\deg r(x) < \deg(x - c) = 1$. Vậy $r(x)$ là một phần tử của K .

Thay $x = c$ ta được

$$f(c) = q(c).0 + r(c) = r(c).$$

Vậy ta có

$$f(x) = q(x)(x - c) + f(c).$$

Do đó dư của phép chia $f(x)$ cho $x - c$ là $f(c)$. Nói riêng, $f(x)$ chia hết cho $x - c$ khi và chỉ khi $f(c) = 0$. 

Cho

$$f(x) = a_n x^n + \dots + a_1 x + a_0 \in K[x] \text{ và } c \in K.$$

Ta dùng **sơ đồ Horner** dưới đây để tìm

$$q(x) = b_{n-1}x^{n-1} + \dots + b_1x + b_0 \text{ và } r = f(c)$$

trong thuật chia Euclide $f(x) = (x - c)q(x) + r$.

	a_n	a_{n-1}	\dots	a_1	a_0
c	$b_{n-1} = a_n$	$b_{n-2} =$ $a_{n-1} + cb_{n-1}$	\dots	$b_0 =$ $a_1 + cb_1$	$r =$ $a_0 + cb_0$

Ví dụ. Trong $\mathbb{Q}[x]$ cho

$$f(x) = 3x^5 + 4x^4 - 2x^3 + 5x^2 - x + 6$$

và $c = 4 \in \mathbb{Q}$. Ta có sơ đồ Horner như sau

	3	4	-2	5	-1	6
4	3	16	62	253	1011	4050

Vậy

$$f(x) = (x - 4)q(x) + r$$

với

$$q(x) = 3x^4 + 16x^3 + 62x^2 + 253x + 1011 \text{ và } r = f(4) = 4050.$$

Ví dụ. Trong $\mathbb{Z}_7[x]$ cho $f(x) = \bar{2}x^5 - x^3 + \bar{3}x^2 - \bar{2}$ và $c = -\bar{3} \in \mathbb{Z}_7$. Ta có sơ đồ Horner như sau

	$\bar{2}$	$\bar{0}$	$-\bar{1}$	$\bar{3}$	$\bar{0}$	$-\bar{2}$
$-\bar{3}$	$\bar{2}$	$\bar{1}$	$\bar{3}$	$\bar{1}$	$-\bar{3}$	$\bar{0}$

Vậy $f(x) = (x + \bar{3})q(x)$ với

$$q(x) = \bar{2}x^4 + x^3 + \bar{3}x^2 + x - \bar{3}, r = 0.$$

Đa thức $f(x)$ chia hết cho $x + \bar{3}$ nên $c = -\bar{3}$ là một nghiệm của $f(x)$.

Định lý. Cho K là trường và $0 \neq f(x) \in K[x]$, $\deg f(x) = n \geq 0$. Khi đó $f(x)$ có nhiều nhất n nghiệm trên K .

Chứng minh. Ta chứng minh bằng phương pháp quy nạp theo n .

- Nếu $n = 0$ thì $f(x)$ là đa thức hằng khác không nên $f(x)$ vô nghiệm trên K .

- Nếu $n \geq 1$. Giả sử định lý đúng cho các đa thức $g(x) \in K[x]$ với $0 \leq \deg g(x) < n$.

Nếu $f(x)$ vô nghiệm trên K thì định lý đúng cho $f(x)$. Nếu $f(x)$ có nghiệm $c \in K$ thì tồn tại $g(x) \in K[x]$, $\deg g(x) = n - 1$ sao cho $f(x) = (x - c)g(x)$.

Theo giả thiết quy nạp, $g(x)$ có không quá $n - 1$ nghiệm trên K , do đó $f(x)$ không có quá n nghiệm trên K .

Hệ quả. Nếu hai đa thức trên trường K có cùng bậc n và lấy những giá trị bằng nhau tại $n + 1$ phần tử khác nhau của K thì chúng bằng nhau.

Chứng minh. Giả sử $f(x), g(x) \in K[x]$ có cùng bậc n và bằng nhau tại $n + 1$ phần tử khác nhau của K . Khi đó đa thức $h(x) = f(x) - g(x)$ có bậc không vượt quá n và có ít nhất $n + 1$ nghiệm. Như vậy $h(x)$ là đa thức không, và do đó $f(x) = g(x)$. ■

Đạo hàm

Định nghĩa. Cho đa thức $f(x)$ trên trường K .

- ❶ Nếu $f(x) = a_0 \in K$, đặt $f'(x) = 0$. Nếu $f(x) = \sum_{k=0}^n a_k x^k$ với $n \geq 1$, đặt

$$f'(x) = \sum_{k=1}^n k a_k x^{k-1}.$$

Ta gọi $f'(x)$ là **đạo hàm** của $f(x)$.

- ❷ Đặt $f^{(0)}(x) = f(x)$, $f^{(1)}(x) = f'(x)$, $f^{(2)}(x) = (f^{(1)}(x))'$, ..., $f^{(k)}(x) = (f^{(k-1)}(x))'$, $\forall k \in \mathbb{N}^*$. Ta nói $f^{(m)}(x)$ là **đạo hàm cấp m** của $f(x)$, $\forall m \in \mathbb{N}$.

Khai triển Taylor

Định lý. Cho đa thức $f(x)$ trên trường K và $\deg f(x) = n$. Khi đó với mỗi $c \in K$ đa thức $f(x)$ có thể khai triển duy nhất dưới dạng

$$f(x) = \sum_{k=0}^n c_k (x - c)^k.$$

Chứng minh. Ta thực hiện phép chia $f(x)$ cho $x - c$ ta có

$$f(x) = (x - c)g(x) + c_0,$$

trong đó $c_0 \in K$ và $g(x) \in K[x]$ ($\deg g(x) = n - 1$). Lại tiếp tục thực hiện phép chia $g(x)$ cho $x - c$ ta có duy nhất $c_1 \in K$ và $g_1(x) \in K[x]$ sao cho

$$g(x) = (x - c)g_1(x) + c_1, \quad \deg g_1(x) = n - 2.$$

Khi đó ta có

$$f(x) = (x - c)^2 g_1(x) + c_1(x - c) + c_0.$$

Lặp lại quá trình trên, cuối cùng ta được

$$f(x) = c_n(x - c)^n + c_{n-1}(x - c)^{n-1} + \cdots + c_1(x - c) + c_0.$$

Nhờ sơ đồ Horner ta dễ dàng thu được các hệ số c_0, \dots, c_n như bảng sau:

	a_n	a_{n-1}	\dots	a_1	a_0
c	a_n	*	\dots	*	c_0
c	a_n	*	\dots	c_1	
\vdots	\vdots	\vdots	\vdots		
c	a_n	c_{n-1}			
c	$c_n = a_n$				

Ví dụ. Trong vành $\mathbb{Q}[x]$, hãy khai triển đa thức $f(x) = x^4 - x^3 + 1$ theo lũy thừa của $x - 3$.

Lập sơ đồ Horner

	1	-1	0	0	1
3	1	2	6	18	55
3	1	5	21	81	
3	1	8	45		
3	1	11			
3	1				

Do đó $f(x) = (x - 3)^4 + 11(x - 3)^3 + 45(x - 3)^2 + 81(x - 3) + 55$.

Nhận xét. Trong trường hợp K là trường có đặc số 0 thì các hệ số c_k trong khai triển Taylor có thể tính theo các đạo hàm của đa thức $f(x)$ như sau

$$c_k = \frac{f^{(k)}(c)}{k!},$$

nghĩa là

$$f(x) = \sum_{k=0}^n \frac{f^{(k)}(c)}{k!} (x - c)^k.$$

Định nghĩa. Giả sử k là một số tự nhiên khác không, R là miền nguyên. Phần tử $c \in R$ được gọi là **nghiệm bội k** của đa thức $f(x) \in R[x]$ nếu $f(x)$ chia hết cho $(x - c)^k$ nhưng không chia hết cho $(x - c)^{k+1}$, nghĩa là $f(x)$ có thể phân tích thành

$$f(x) = (x - c)^k g(x)$$

với $g(x) \in R[x]$ và $g(c) \neq 0$.

Nhận xét.

- ❶ Nếu $f(x) = \sum_{k=0}^n c_k(x - c)^k$ là khai triển Taylor của đa thức $f(x)$ thì c là nghiệm bội m khi và chỉ khi $c_m \neq 0$ và $c_i = 0, \forall i < m$.
- ❷ Nói riêng, nếu $f(x) \in K[x]$ với $\text{char} K = 0$ thì $c \in K$ là nghiệm bội m của $f(x)$ khi và chỉ khi $f^{(m)}(c) \neq 0$ và $f^{(i)}(c) = 0, \forall i < m$.

Ví dụ. Trong $\mathbb{Z}_7[x]$, cho $f(x) = \bar{2}x^4 - \bar{3}x^3 + \bar{2}x - \bar{3}$ và $c = -\bar{2}$. Hỏi c có là nghiệm của $f(x)$ hay không, nếu có thì là nghiệm bội bao nhiêu.

3.3. Đa thức trên trường số thực và số phức

Định lý. [Định lý cơ bản của Đại số.] Mọi đa thức $f(x)$ bậc $n \geq 1$ trên trường số phức đều có n nghiệm phức (kể cả số bội)

Hệ quả. Các đa thức bất khả quy của $\mathbb{C}[x]$ là các đa thức bậc nhất.

Chứng minh. Hiển nhiên các đa thức bậc nhất là các đa thức bất khả quy. Giả sử $f(x)$ là một đa thức của $\mathbb{C}[x]$ có bậc lớn hơn 1. Theo Định lý trên, $f(x)$ có nghiệm phức $c \in \mathbb{C}$. Vậy $f(x)$ chia hết cho $x - c$, do đó $f(x)$ không bất khả quy. ■

Mệnh đề. Nếu số phức α là nghiệm của đa thức $f(x)$ với hệ số thực thì số phức liên hợp $\bar{\alpha}$ cũng là một nghiệm của $f(x)$.

Chứng minh. Giả sử

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

là một đa thức với hệ số thực và α là một nghiệm phức của $f(x)$.

Khi đó

$$a_n \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_1 \alpha + a_0 = 0.$$

Lấy liên hợp hai vế của đẳng thức trên ta được

$$a_n \bar{\alpha}^n + a_{n-1} \bar{\alpha}^{n-1} + \dots + a_1 \bar{\alpha} + a_0 = 0.$$

Điều này chứng tỏ số phức liên hợp $\bar{\alpha}$ cũng là nghiệm của $f(x)$. ■

Định lý. [Các đa thức bất khả quy trong $\mathbb{R}[x]$.] Các đa thức bất khả quy trong $\mathbb{R}[x]$ là các đa thức bậc nhất và các đa thức bậc hai $ax^2 + bx + c$ với biệt số $\Delta = b^2 - 4ac < 0$.

Chứng minh. Dễ dàng thấy rằng các đa thức bậc nhất và đa thức bậc hai với biệt số $\Delta < 0$ là các đa thức bất khả quy trên \mathbb{R} . Ta chứng minh chiều ngược lại.

Giả sử $f(x)$ là đa thức bất khả quy trên \mathbb{R} và α là một nghiệm phức.


- Nếu $\alpha \in \mathbb{R}$ thì $f(x)$ chia hết cho $x - \alpha$, do $f(x)$ bất khả quy nên

$$f(x) = k(x - \alpha), \quad k \in \mathbb{R}^*,$$

vậy $f(x)$ là đa thức bậc nhất.

- Nếu $\alpha \in \mathbb{C} \setminus \mathbb{R}$ thì $\bar{\alpha}$ cũng là nghiệm của $f(x)$, do đó $f(x)$ chia hết cho

$$p(x) = (x - \alpha)(x - \bar{\alpha}) = x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha}.$$

$p(x)$ là một tam thức bậc hai với hệ số thực và có biệt số $\Delta < 0$. Do $f(x)$ bất khả quy nên $f(x) = kp(x)$, $k \in \mathbb{R}^*$. Vậy $f(x)$ là tam thức bậc hai với biệt số $\Delta < 0$. 

3.4. Đa thức trên trường số hữu tỷ

Cho $f(x) \in \mathbb{Q}[x]$. Gọi b là mẫu số chung của các hệ số của $f(x)$. Khi đó

$$f(x) = \frac{1}{b}g(x) \text{ với } g(x) \in \mathbb{Z}[x].$$

Hơn nữa tập nghiệm của $f(x)$ bằng tập nghiệm $g(x)$. Giả sử

$$g(x) = b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0 \in \mathbb{Z}[x].$$

Nếu α là nghiệm của đa thức $g(x)$ thì

$$b_n \alpha^n + b_{n-1} \alpha^{n-1} + \dots + b_1 \alpha + b_0 = 0.$$

Nhân hai vế với b_n^{n-1} ta có

$$(b_n \alpha)^n + b_{n-1} (b_n \alpha)^{n-1} + \dots + b_1 b_n^{n-2} (b_n \alpha) + b_0 b_n^{n-1} = 0.$$

Do đó $\beta = b_n \alpha$ là nghiệm của đa thức.

$$h(x) = x^n + b_{n-1} x^{n-1} + \dots + b_1 b_n^{n-2} x + b_0 b_n^{n-1}$$

với hệ số nguyên và hệ số cao nhất bằng 1. Như vậy để tìm các nghiệm của $g(x)$ ta chỉ việc tìm các nghiệm của $h(x)$.

Mệnh đề. Cho

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \quad (n \geq 1) \in \mathbb{Z}[x]$$

và $\alpha = \frac{p}{q}$, $(p, q) = 1$ là nghiệm hữu tỷ của $f(x)$. Khi đó p là ước của a_0 còn q là ước của a_n .

Chứng minh. Vì $\alpha = \frac{p}{q}$, $(p, q) = 1$ là nghiệm của $f(x)$ nên

$$f(x) = a_n \left(\frac{p}{q}\right)^n + a_{n-1} \left(\frac{p}{q}\right)^{n-1} + \dots + a_1 \left(\frac{p}{q}\right) + a_0 = 0.$$

Nhân hai vế cho q^n ta có

$$a_n p^n + a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1} + a_0 q^n = 0$$

$$\Leftrightarrow p(a_n p^{n-1} + a_{n-1} p^{n-2} q + \dots + a_1 q^{n-1}) = -a_0 q^n.$$

Suy ra p là ước của $a_0 q^n$.

Hơn nữa

$$\begin{aligned} a_n p^n + a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1} + a_0 q^n &= 0 \\ \Leftrightarrow -a_n p^n &= q(a_{n-1} p^{n-1} + \dots + a_1 p q^{n-2} + a_0 q^{n-1}) \end{aligned}$$

Suy ra q là ước của $a_n p^n$. Do $(p, q) = 1$ nên suy ra p là ước của a_0 còn q là ước của a_n .

Mệnh đề. Mọi nghiệm hữu tỷ của đa thức với hệ số nguyên

$$g(x) = x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, \quad n \geq 1$$

đều là số nguyên và là ước của a_0 . Nếu α là nghiệm nguyên của $g(x)$ thì $1 - \alpha$ là ước của $g(1)$, còn $1 + \alpha$ là ước của $g(-1)$.

Chứng minh. Nếu $\alpha = \frac{p}{q}$, $(p, q) = 1$ là nghiệm hữu tỷ của $g(x)$ thì theo mệnh đề trên p là ước của a_0 còn q là ước của 1. Do đó α nguyên và là ước của a_0 .

Nếu α là một nghiệm nguyên của $g(x)$ thì $g(x) = (x - \alpha)q(x)$, với $q(x) \in \mathbb{Z}[x]$. Do đó

$$g(1) = (1 - \alpha)q(1) \quad \text{và} \quad g(-1) = -(1 + \alpha)q(-1).$$

Như thế $1 - \alpha$ là ước của $g(1)$, còn $1 + \alpha$ là ước của $g(-1)$.

Ví dụ. Tìm nghiệm hữu tỷ của đa thức

$$f(x) = x^5 - 8x^4 + 20x^3 - 20x^2 + 19x - 12.$$

Giải. Vì tổng các hệ số của $f(x)$ bằng 0 nên 1 là một nghiệm của $f(x)$. Chia $f(x)$ cho $x - 1$ ta được đa thức thương là

$$g(x) = x^4 - 7x^3 + 13x^2 - 7x + 12.$$

Dễ thấy rằng $g(\alpha) > 0, \forall \alpha < 0$, do đó $g(x)$ không có nghiệm âm.

Các nghiệm hữu tỷ của $g(x)$ đều nguyên và là các ước dương của 12.

Ta lần lượt xét các ước dương của 12 là 2, 3, 4, 6, 12 ta có $g(1) = 12$, $g(-1) = 40$,

$$\frac{g(-1)}{1+2} = \frac{40}{3}, \quad \frac{g(-1)}{1+6} = \frac{40}{7}, \quad \frac{g(-1)}{1+12} = \frac{40}{13}$$

không phải là các số nguyên nên các số 2, 6, 12 không phải là nghiệm của $g(x)$.

Với $\alpha = 3$ và $\alpha = 4$ thì

$$\frac{g(1)}{1-\alpha}, \frac{g(-1)}{1+\alpha}$$

nguyên nên chúng có thể là nghiệm của $g(x)$. Ta lại sử dụng sơ đồ Horner để kiểm tra xem 3 và 4 có phải là nghiệm của $g(x)$ hay không.

	1	-7	13	-7	12
3	1	-4	1	-4	0
4	1	0	1	0	

Vậy ta có các nghiệm nguyên của $g(x)$ là 3 và 4. Do đó các nghiệm hữu tỷ của $f(x)$ là 1, 3 và 4.

Đa thức bất khả quy của vành $\mathbb{Q}[x]$

Định nghĩa. Một đa thức với hệ số nguyên được gọi là **đa thức nguyên bản** nếu ước chung lớn nhất của các hệ số là 1.

Nhận xét.

- ❶ Nếu $f(x) \in \mathbb{Z}[x]$, ký hiệu a là ước chung lớn nhất của các hệ số thì $f(x) = af^*(x)$, với $f^*(x)$ là một đa thức nguyên bản.
- ❷ Nếu $f(x) \in \mathbb{Q}[x]$ thì $f(x)$ được viết dưới dạng

$$f(x) = \frac{a}{b} f^*(x),$$

trong đó $(a, b) = 1$ và $f^*(x)$ là một đa thức nguyên bản.

Bổ đề. Tích của hai đa thức nguyên bản lại là một đa thức nguyên bản.

Chứng minh. Cho hai đa thức nguyên bản

$$\begin{aligned}f(x) &= a_mx^m + a_{m-1}x^{m-1} + \dots + a_1x + a_0, \\g(x) &= b_nx^n + b_{n-1}x^{n-1} + \dots + b_1x + b_0.\end{aligned}$$

Gọi p là số nguyên tố tùy ý, ta chứng minh rằng p không thể là ước của tất cả các hệ số của $f(x)g(x)$.

Vì $f(x)$ và $g(x)$ là các đa thức nguyên bản nên tồn tại ít nhất một hệ số của $f(x)$ và $g(x)$ không chia hết cho p .

Giả sử $a_0, \dots, a_{r-1}, b_0, \dots, b_{s-1}$ chia hết cho p nhưng a_r và b_s không chia hết cho p . Ta xét hệ số c_{r+s} của đa thức $f(x)g(x)$:

$$c_{r+s} = \sum_{i+j=r+s} a_ib_j,$$

ta thấy rằng tất cả các số hạng của c_{r+s} , trừ a_rb_s đều chia hết cho p . Do đó c_{r+s} không chia hết cho p . Vậy $f(x)g(x)$ là đa thức nguyên bản.

Bổ đề. Nếu $f(x)$ là đa thức với hệ số nguyên có bậc lớn hơn 0 và $f(x)$ không bất khả quy trong $\mathbb{Q}[x]$ thì $f(x)$ phân tích được thành tích những đa thức bậc lớn hơn 0 với hệ số nguyên.

Chứng minh. Giả sử $f(x)$ là đa thức trong $\mathbb{Z}[x]$ không bất khả quy trên \mathbb{Q} . Khi đó $f(x)$ có thể phân tích thành

$$f(x) = \varphi(x)\psi(x),$$

trong đó $0 < \deg \varphi(x), \deg \psi(x) < \deg f(x)$, $\varphi(x), \psi(x) \in \mathbb{Q}[x]$. Theo nhận xét trước, $\varphi(x)$ và $\psi(x)$ có thể viết thành

$$\varphi(x) = \frac{a}{b}g(x), \quad \psi(x) = \frac{c}{d}h(x),$$

trong đó $g(x), h(x)$ là các đa thức nguyên bản, còn $(a, b) = (c, d) = 1$. Khi đó

$$f(x) = \frac{ac}{bd}g(x)h(x).$$

Gọi p, q là các số nguyên mà $\frac{p}{q} = \frac{ac}{bd}$ sao cho $(p, q) = 1$. Đặt các hệ số của đa thức tích $g(x)h(x)$ là c_i . Khi đó các hệ số của $f(x)$ là $\frac{pc_i}{q}$ và là các số nguyên.

Do $(p, q) = 1$ nên c_i chia hết cho q . Mà các hệ số của đa thức nguyên bản $g(x)h(x)$ nguyên tố cùng nhau nên $q = \pm 1$, vì vậy

$$f(x) = \pm pg(x)h(x).$$

Vì $0 < \deg \varphi(x), \deg \psi(x) < n$, suy ra $g(x)$ và $h(x)$ là những đa thức có bậc lớn hơn 0.

Tiêu chuẩn Eisenstein

Định lý. *Giả sử*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \quad (n > 1)$$

là đa thức với hệ số nguyên và giả sử tồn tại số nguyên tố p sao cho:

- ❶ *hệ số cao nhất a_n không chia hết cho p , tất cả các hệ số còn lại đều chia hết cho p ;*
- ❷ *hệ số tự do a_0 không chia hết cho p^2 .*

Khi đó $f(x)$ là một đa thức bất khả quy trong $\mathbb{Q}[x]$.

Chứng minh. Giả sử $f(x)$ không bất khả quy, khi đó theo Bổ đề trên, $f(x)$ có thể phân tích được thành tích của hai đa thức với hệ số nguyên và có bậc lớn hơn 0:


$$f(x) = (b_r x^r + b_{r-1} x^{r-1} + \dots + b_1 x + b_0)(c_s x^s + c_{s-1} x^{s-1} + \dots + c_1 x + c_0),$$

trong đó $0 < r, s < n$.

Theo giả thiết, $a_0 = b_0 c_0$ chia hết cho p mà p nguyên tố nên b_0 hay c_0 chia hết cho p .

Giả sử b_0 chia hết cho p . Thế thì c_0 không chia hết cho p vì a_0 không chia hết cho p^2 . Vì $a_n = b_r c_s$ không chia hết cho p nên b_r không chia hết cho p . Giả sử b_0, \dots, b_{k-1} chia hết cho p và b_k không chia hết cho p , $1 \leq k \leq r$. Ta có

$$a_k = b_k c_0 + b_{k-1} c_1 + \dots,$$

mà a_k, b_{k-1}, \dots đều chia hết cho p , suy ra $b_k c_0$ phải chia hết cho p . Vì p nguyên tố và c_0 không chia hết cho p nên b_k phải chia hết cho p , mâu thuẫn với giả thiết về b_k . 

Ví dụ. Dùng tiêu chuẩn Eisenstein để chứng minh các đa thức sau đây bất khả quy trong $\mathbb{Q}[x]$.

❶ $x^4 - 8x^3 + 12x^2 - 6x + 2;$

❷ $x^4 - x^3 + 2x + 1.$

Giải.

a) $x^4 - 8x^3 + 12x^2 - 6x + 2$

Xét tiêu chuẩn Eisenstein với $p = 2$, ta thấy rằng hệ số cao nhất không chia hết cho 2, tất cả các hệ số còn lại chia hết cho 2, hệ số tự do không chia hết cho 2^2 . Vậy đa thức đã cho bất khả quy trong $\mathbb{Q}[x]$.

b) $x^4 - x^3 + 2x + 1$

Để đa thức đã cho như vậy ta không áp dụng được tiêu chuẩn Eisenstein nên ta phân tích đa thức theo lũy thừa của $x - 1$, ta có

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

Đa thức $y^4 + 3y^3 + 3y^2 + 3y + 3$ là bất khả quy vì thỏa mãn tiêu chuẩn Eisenstein với $p = 3$. Do đó đa thức đã cho bất khả quy trong $\mathbb{Q}[x]$.