

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

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

❷ **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

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

❸ **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

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

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: $\mathbb{Q}^* \leq \mathbb{R}^* \leq \mathbb{C}^*$.

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.

- ❶ Ta có $\det(I_n) = 1$ nên $I_n \in SL_n(\mathbb{R})$. Do đó $SL_n(\mathbb{R}) \neq \emptyset$.
- ❷ 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 $\bar{x} = xH$.

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

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 $f : (\mathbb{R}, +) \longrightarrow (\mathbb{C}^*, \cdot)$ 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 $GL(n, \mathbb{R})/SL(n, \mathbb{R}) \simeq \mathbb{R}^*$.