CHƯƠNG 1. NHÓM

§1. Phép toán hai ngôi

1.1. 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 $*, \circ, +, ., \ldots$ ta có các ký hiệu $x * y$, $x \circ y$, $x + y$, $x.y$, ... Khi ký hiệu phép toán là . ta gọi đây là phép toán nhân và thường viết xy thay cho $x.y$ mà ta gọi là tích của x và y. Còn khi ký hiệu phép toán là $+$ ta gọi đây là phép toán cộng và $x + y$ là tổng của x và y.

CHƯƠNG 1. NHÓM

1.2. Ví dụ

1) 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 $\mathbb{N}$.

2) Phép cộng và phép nhân ma trận là các phép toán trên $M(n, \mathbb{R})$ gồm các ma trận vuông cấp n với hệ số thực.

CHƯƠNG 1. NHÓM

1.3. Định nghĩa

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

(i) *giao hoán*, nếu với mọi $x, y \in X, x * y = y * x$;

(ii) *kết hợp*, nếu với mọi $x, y, z \in X, (x * y) * z = x * (y * z)$;

(iii) 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 $*$.

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

CHƯƠNG 1. NHÓM

1.6. 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.

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

CHƯƠNG 1. NHÓM

1.8. Thuật ngữ và ký hiệu

1) Trường hợp phép toán cộng: Phần tử trung hòa được gọi là *phần tử không* và được ký hiệu là 0, tính chất khả đối xứng được gọi là *khả đối*, phần tử đối xứng của x được gọi là *phần tử đối* của x và ký hiệu là $-x$.

2) Trường hợp phép toán nhân: Phần tử trung hòa được gọi là *phần tử đơn vị* và được ký hiệu là e hay 1, tính chất khả đối xứng được gọi là *khả nghịch*, phần tử đối xứng của x được gọi là *phần tử nghịch đảo* của x và ký hiệu là x^{-1}.

Từ đây trở về sau, nếu không có gì gây nhầm lẫn, ta dùng phép toán nhân để chỉ một phép toán tùy ý trên tập hợp đang khảo sát.

CHƯƠNG 1. NHÓM

§2. Nửa nhóm

2.1. Định nghĩa

Cho tập hợp X với phép toán nhân. Ta nói $(X, .)$ (gọi tắt là X) là:

(i) một *nửa nhóm* nếu phép toán nhân kết hợp trên X;

(ii) một *vị nhóm* nếu phép toán nhân kết hợp trên X và có phần tử trung hòa trên X.

Một nửa nhóm được gọi là *giao hoán* hay *Abel* nếu phép toán tương ứng giao hoán.

CHƯƠNG 1. NHÓM

2.2. Ví dụ

1) Với phép cộng thông thường, các tập hợp $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ trở thành các vị nhóm giao hoán.

2) Với phép cộng thông thường, tập hợp $\mathbb{N}^*$ gồm các số nguyên dương trở thành một nửa nhóm giao hoán nhưng không là vị nhóm.

3) Cho S là khoảng đóng [0, 1]$\subset$ R. Ta định nghĩa phép toán trên S như sau:

$$a * b = \frac{a + b}{1 + ab}, \forall a, b \in S.$$

Trong đó các phép toán trong vế phải là các phép cộng, nhân chia số thực. Khi đó S là một vị nhóm giao hoán.

Thật vậy, nếu.

$$a, b \in [-1, 0] \Rightarrow (1 - a)(1 - b) \geq 0 \Rightarrow 1 + ab \geq a + b$$

$$\Rightarrow 1 \geq \frac{a + b}{1 + ab} = a * b \geq 0 \Rightarrow a * b \in [0, 1] = S$$

Vậy (*) là một phép toán hai ngôi trên S. Hơn nữa,

$$(a * b) * c = \left(\frac{a + b}{1 + ab}\right) * c = \frac{\left(\frac{a + b}{1 + ab}\right) + c}{1 + \frac{a + b}{1 + ab}c} = \frac{a + b + c + abc}{1 + ab + bc + ac}$$

$$= \frac{a + \left(\frac{b + c}{1 + bc} \right)}{1 + a \left(\frac{b + c}{1 + bc} \right)} = a * \left(\frac{b + c}{1 + bc} \right) = a * b * c$$

$$a * b = \frac{a + b}{1 + ab} = \frac{b + a}{1 + ba} = b * a ; \; a * 0 = \frac{a + 0}{1 + a.0} = a$$

Do đó (S;*) là một vị nhóm giao hoán trong đó phần tử đơn vị là số thực 0.

2.3. Ký hiệu

Trong nửa nhóm $(X, .)$, do phép toán nhân kết hợp nên với mọi x, y, z:

$$(xy)z = x(yz).$$

Giá trị chung của hai vế trong đẳng thức trên được ký hiệu là xyz và gọi là *tích* của các phần tử x, y, z theo thứ tự đó. Bằng quy nạp, ta định nghĩa *tích* của n phần tử $x_1, ..., x_n$ như sau:

$$x_1...x_n = x_1(x_2...x_n).$$

2.4. Định lý. *Cho $x_1, ..., x_n$ là n phần tử tùy ý của nửa nhóm $(X, .)$ với $n \geq 3$. Khi đó:*

$$x_1...x_n = (x_1...x_i)(x_{i+1}...x_j)...(x_{k+1}...x_n),$$

trong đó $1 \leq i < j < ... < k < n$.

2.5. Ký hiệu

Trong nửa nhóm $(X, .)$, tích của n phần tử, mỗi phần tử đều bằng x, được gọi là *lũy thừa* bậc n của x và được ký hiệu là x^n. Do Định lý 2.4 ta có

$$x^m x^n = x^{m+n} \text{ và } (x^m)^n = x^{mn}, \forall m, n \in \mathbb{N}^*.$$

Trường hợp nửa nhóm cộng $(X, +)$, tổng của n phần tử được gọi là *bội* n của x và ký hiệu là nx. Khi đó các tính chất trên trở thành

$$mx + nx = (m + n)x \text{ và } m(nx) = (mn)x.$$

2.6. Định lý. *Trong nửa nhóm giao hoán, tích của n phần tử tùy ý không phụ thuộc vào thứ tự của các phần tử.*

CHƯƠNG 1. NHÓM

3.1. Định nghĩa

Nhóm là một vị nhóm mà mọi phần tử đều khả đối xứng. Nói cách khác, tập hợp G khác rỗng với phép toán nhân được gọi là một nhóm nếu các tính chất sau được thỏa:

(G_1) Với mọi $x, y, z \in G, (xy)z = x(yz)$;

(G_2) Tồn tại $e \in G$ sao cho với mọi $x \in G$, $ex = xe = x$;

(G_3) Với mọi $x \in G$, tồn tại $x^{-1} \in G$ sao cho $xx^{-1} = x^{-1}x = e$.

CHƯƠNG 1. NHÓM

Nếu phép toán trên G là phép cộng thì các tính chất trên trở thành:

(G_1) Với mọi $x, y, z \in G, (x + y) + z = x + (y + z)$;

(G_2) Tồn tại $0 \in G$ sao cho với mọi $x \in G$, $0 + x = x + 0 = x$;

(G_3) Với mọi $x \in G$, tồn tại $-x \in G$ sao cho $x+(-x) = (-x)+x = 0$.

Trường hợp phép toán trên nhóm G giao hoán thì ta nói G là *nhóm giao hoán* hay là *nhóm Abel*.

Nhóm G được gọi là *nhóm hữu hạn* khi tập hợp G hữu hạn. Khi đó số phần tử của G được gọi là *cấp* của nhóm G. Nếu nhóm G không hữu hạn thì ta nói G là *nhóm vô hạn*.

CHƯƠNG 1. NHÓM

3.2. Ví dụ

1) Tập hợp các số nguyên $\mathbb{Z}$ cùng với phép cộng thông thường là một nhóm giao hoán mà ta gọi là nhóm cộng các số nguyên. Tương tự ta có nhóm cộng các số hữu tỷ $\mathbb{Q}$, nhóm cộng các số thực $\mathbb{R}$ và nhóm cộng các số phức $\mathbb{C}$.

2) Tập hợp các số hữu tỷ khác không $\mathbb{Q}^*$ cùng với phép nhân thông thường là một nhóm giao hoán mà ta gọi là nhóm nhân các số hữu tỷ khác không. Tương tự ta có nhóm nhân các số thực khác không $\mathbb{R}^*$ và nhóm nhân các số phức khác không $\mathbb{C}^*$.

3) Với $X = \{1, 2, ..., n\}$, đặt

$$S_n = \{\sigma | \sigma : X \longrightarrow X \text{ là một song ánh}\}.$$

Khi đó S_n với phép hợp nối ánh xạ là một nhóm (có phần tử đơn vị là ánh xạ đồng nhất Id_X và phần tử nghịch đảo của $\sigma \in S_n$ chính là ánh xạ ngược σ^{-1}). Ta gọi $(S_n, \circ)$ là nhóm hoán vị hay nhóm đối xứng bậc n. Đây là một nhóm hữu hạn có cấp $n!$ (xem §4).

4) Tập hợp $GL(n, \mathbb{R})$ gồm các ma trận vuông cấp n, khả nghịch với hệ số thực cùng với phép nhân ma trận là một nhóm không giao hoán với mọi $n > 1$ (với phần tử đơn vị là ma trận đơn vị I_n và phần tử nghịch đảo của $A \in GL(n, \mathbb{R})$ chính là ma trận nghịch đảo A^{-1}). Ta gọi $GL(n, \mathbb{R})$ là *nhóm tuyến tính đầy đủ* bậc n (hay *nhóm tuyến tính tổng quát* bậc n) trên $\mathbb{R}$.

3.3. Định lý. *Cho nhóm* $(G, .)$ *và* $x, y, x_1, ..., x_n \in G$. *Khi đó:*

(i) Phần tử đơn vị e *là duy nhất.*

(ii) Phần tử nghịch đảo x^{-1} *của* x *là duy nhất và* $(x^{-1})^{-1} = x$.

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

(iv) $(x_1...x_n)^{-1} = {x_n}^{-1}...{x_1}^{-1}$. *Đặc biệt* $(x^n)^{-1} = (x^{-1})^n$ *với mọi* n *nguyên dương.*

(v) Phép toán nhân có tính giản ước, nghĩa là với mọi $x, y, z \in G$, *từ đẳng thức* $xy = xz$ *hay* $yx = zx$ *đều dẫn đến* $y = z$.

3.4. Ký hiệu

Trong nhóm nhân $(G, .)$ ta dùng ký hiệu x^{-n} để chỉ phần tử $(x^{-1})^n$ với mọi n nguyên dương và đặt $x^0 = e$. Như vậy ta đã định nghĩa lũy thừa bậc n của một phần tử bất kỳ trong một nhóm nhân với n nguyên. Chú ý rằng, do tính chất (iv) trong Định lý 3.3, các công thức $x^m.x^n = x^{m+n}$ và $(x^m)^n = x^{mn}$ (hay $mx + nx = (m + n)x$ và $m(nx) = (mn)x$ đối với nhóm cộng) vẫn còn đúng với mọi m, n nguyên.

CHƯƠNG 1. NHÓM

3.5. 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 $xx'' = e'$.

§4. Nhóm hoán vị

4.1. Định nghĩa

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

Nhóm hoán vị S_n là nhóm hữu hạn có cấp $n!$, có phần tử trung hòa là ánh xạ đồng nhất Id_X và phần tử nghịch đảo của $\sigma \in S_n$ là ánh xạ ngược σ^{-1}. Nhóm này không giao hoán nếu $n > 2$.

4.2. Một số thuật ngữ và ký hiệu

1) 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 loại $2 \times n$:

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

trong đó ở dòng thứ nhất, các phần tử của tập X được sắp xếp theo một thứ tự nào đó (thường là $1, 2, \cdots, n$), dòng thứ hai gồm ảnh của các phần tử tương ứng ở dòng thứ nhất qua song ánh σ.

2) Phép hoán vị $\sigma \in S_n$ được gọi là một *r-chu trình* hay một *chu trình có chiều dài* r nếu tồn tại các phần tử phân biệt $i_1, i_2, ..., i_r \in X$ sao cho $\sigma(i_1) = i_2, \cdots, \sigma(i_{r-1}) = i_r, \sigma(i_r) = i_1$ và $\sigma(i) = i, \forall i \in X \setminus \{i_1, i_2, \cdots, i_r\}$. Khi đó ta viết $\sigma = (i_1 i_2 \cdots i_r)$.

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

3) Mỗi 2-chu trình trong S_n được gọi là một chuyển vị. Như vậy mỗi chuyển vị có dạng $(i\ j)$ với $1 \leq i \neq j \leq n$.

Ví dụ: a) Trong nhóm hoán vị S_6, phép hoán vị σ xác định bởi $\sigma(1) = 2, \sigma(2) = 5, \sigma(3) = 4, \sigma(4) = 1, \sigma(5) = 3, \sigma(6) = 6$ được mô tả như sau:

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

b) Trong nhóm hoán vị S_7, chu trình $\sigma = (1\,3\,4\,7)$ có chiều dài 4 và là phép hoán vị:

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

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

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

d) Trong nhóm hoán vị S_5, cho

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

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

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

4.3. Nhận xét

Hai chu trình σ và τ rời nhau thì chúng giao hoán lẫn nhau, nghĩa là $\sigma\tau = \tau\sigma$.

4.4. Định lý. *Mọi phép hoán vị bậc n khác ánh xạ đồng nhất đều được phân tích thành tích các chu trình rời nhau có chiều dài lớn hơn hay bằng 2. Cách phân tích là duy nhất sai khác một sự đổi chỗ các chu trình.*

Ví dụ: Trong nhóm hoán vị S_{10} ta có

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

CHƯƠNG 1. NHÓM

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

4.6 Định lý. *Mọi phép hoán vị trong S_n đều được phân tích thành tích của các chuyển vị.*

Ví dụ: Với σ như trong ví dụ trên, ta có

$$\sigma = (15)(18)(17)(13)(46)(49).$$

Nhận xét rằng sự phân tích thành tích các chuyển vị của một chu trình là không duy nhất. Do đó sự phân tích trong Định lý 4.6 là không duy nhất.

4.7. Định nghĩa

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

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

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

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

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

4.8. Nhận xét

(i) $\mathrm{sgn}(Id_X) = 1$.

(ii) $\mathrm{sgn}(\sigma) = \mathrm{sgn}(\sigma^{-1})$.

(iii) Nếu σ là một chuyển vị thì $\mathrm{sgn}(\sigma) = -1$.

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

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

4.10. Định lý. *Với mọi hoán vị $\sigma \in S_n$, ta có*

$$\operatorname{sgn}(\sigma) = (-1)^l$$

với l là số chuyển vị trong phân tích σ thành tích các chuyển vị. Đặc biệt, tính chẵn lẻ của số các chuyển vị trong Định lý 4.6 là duy nhất.

Ví dụ: Xét tính chẵn lẻ của phép hoán vị $\sigma \in S_{10}$ sau:

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

4.11. Hệ quả. *Nếu σ là một r-chu trình thì*

(i) $\operatorname{sgn}(\sigma) = (-1)^{r-1}$;

(ii) σ chẵn $\Leftrightarrow$ r lẻ; và σ lẻ $\Leftrightarrow$ r chẵn.

CHƯƠNG 1. NHÓM

§5. Nhóm con

5.1. Định nghĩa

Một tập con H của nhóm $(G, .)$ được gọi là tập con *ổn định* của nhóm G nếu với mọi $x, y \in H, xy \in H$. Khi đó phép toán nhân thu hẹp trên H xác định một phép toán trên H mà ta gọi là phép toán cảm sinh trên H (từ phép toán trên G).

5.2. Định nghĩa

Nhóm con H của nhóm G là một tập con ổn định của nhóm G sao cho cùng với phép toán cảm sinh H là một nhóm. Ký hiệu $H \leq G$ để chỉ H là một nhóm con của G.

5.3. Định lý. *Cho H là một tập con khác rỗng của nhóm $(G, .)$. 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 $x, y \in H, x^{-1}y \in H$.

5.4. Ví dụ

1) Các tập hợp $\{e\}$ và G đều là các nhóm con của G. Ta gọi đây là các *nhóm con tầm thường* của G.

2) Từ Ví dụ 3.2 ta thấy $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ và $\mathbb{Q}^* \leq \mathbb{R}^* \leq \mathbb{C}^*$.

3) Gọi A_n là tập hợp gồm tất cả những hoán vị chẵn trong nhóm hoán vị S_n. Khi đó từ Nhận xét 4.8 và các Định lý 4.9, 5.3 ta thấy $A_n \leq S_n$. Ta gọi A_n là *nhóm thay phiên* bậc n.

4) Tập hợp $SL(n, \mathbb{R})$ gồm các ma trận vuông cấp n với hệ số thực có định thức bằng 1 là một nhóm con của nhóm tuyến tính đầy đủ $GL(n, \mathbb{R})$. Ta gọi $SL(n, \mathbb{R})$ là *nhóm tuyến tính đặc biệt* bậc n trên $\mathbb{R}$.

5.5. Định lý. *Giao của một họ không rỗng các nhóm con của một nhóm G cũng là nhóm con của G.*

CHƯƠNG 1. NHÓM

5.6. Định nghĩa

Cho S là một tập con của nhóm G. *Nhóm con sinh bởi* S là nhóm con nhỏ nhất của G chứa S và được ký hiệu là $\langle S \rangle$. Tập hợp S được gọi là *tập sinh* của nhóm $\langle S \rangle$. Nếu S hữu hạn: $S = \{x_1, ..., x_n\}$ thì ta nói $\langle S \rangle$ là *nhóm hữu hạn sinh* với các phần tử sinh $x_1, ..., x_n$ mà ta thường ký hiệu nhóm này là $\langle x_1, ..., x_n \rangle$.

5.7. Định lý. *Cho S là một tập con của nhóm G. Khi đó:*

(i) Nếu $S = \emptyset$ thì $\langle S \rangle = \{e\}$.

(ii) Nếu $S \neq \emptyset$ thì

$$\langle S \rangle = \{x_1^{\varepsilon_1} ... x_n^{\varepsilon_n} | n \in \mathbb{N}^*, x_i \in S, \varepsilon_i = \pm 1\}.$$

5.8. Ví dụ

1) Ta có $\mathbb{Z} = \langle 1 \rangle$ và $\mathbb{Q} = \langle \frac{1}{n} | n \in \mathbb{N}^* \rangle$.

2) Ta có $\mathbb{Q}^* = \langle P \rangle$, trong đó

$$P = \{-1\} \cup \{p |\ p \text{ nguyên tố dương}\}.$$

3) Xét nhóm hoán vị S_n. Vì mỗi phép hoán vị đều được phân tích thành tích các chuyển vị nên S_n là nhóm sinh bởi các chuyển vị.

5.9. Chú ý

Nếu H và K là hai nhóm con của nhóm G thì $H \cup K$ không nhất thiết là một nhóm con của G (Xem bài tập 1.20). Ta ký hiệu $H \vee K$ để chỉ nhóm con sinh bởi $H \cup K$.

CHƯƠNG 1. NHÓM

§6. Nhóm con cyclic và nhóm cyclic

6.1. Định nghĩa

Cho G là một nhóm. Nhóm con $\langle a \rangle$ của G sinh bởi phần tử $a \in G$ được gọi là *nhóm con cyclic sinh bởi* a. Nếu tồn tại phần tử $a \in G$ sao cho $\langle a \rangle = G$ thì ta nói G là một *nhóm cyclic* và a là *phần tử sinh* của G.

6.2. Mệnh đề. *Nhóm con cyclic sinh bởi a là tập hợp gồm tất cả các lũy thừa a^n với $n \in \mathbb{Z}$, nghĩa là* $\langle a \rangle = \{a^n | \ n \in \mathbb{Z}\}$.

. . nếu tất cả các lũy thừa của a đều khác nhau thì $\langle a \rangle$ là nhóm vô hạn, còn nếu tồn tại những lũy thừa của a bằng nhau thì $\langle a \rangle$ là nhóm hữu hạn cấp n: $\langle a \rangle = \{e, a, ..., a^{n-1}\}$, trong đó n là số nguyên dương nhỏ nhất sao cho $a^n = e$. Từ đây ta có định nghĩa sau:

6.3. Định nghĩa

Cấp của một phần tử a trong nhóm G là cấp của nhóm con cyclic $\langle a \rangle$. Ta thường ký hiệu $o(a)$ hay $|a|$ để chỉ cấp của phần tử a.

6.4. Hệ quả. *Cho $(G, .)$ là một nhóm và $a \in G$. Ta có:*

(i) a có cấp vô hạn khi và chỉ khi với mọi $k \in \mathbb{Z}$, nếu $a^k = e$ thì $k = 0$.

(ii) a có cấp hữu hạn khi và chỉ khi tồn tại $k \in \mathbb{Z}^*$ sao cho $a^k = e$.

(iii) Nếu a có cấp hữu hạn thì cấp của a là số nguyên dương n nhỏ nhất sao cho $a^n = e$. Hơn nữa, khi đó với mọi $k \in \mathbb{Z}$, $a^k = e$ khi và chỉ khi k là bội số của n.

6.5. Ví dụ

1) Nhóm cộng các số nguyên $\mathbb{Z}$ là nhóm cyclic sinh bởi 1.

2) Với mỗi n nguyên dương, quan hệ đồng dư modulo n trên $\mathbb{Z}$ định bởi

$$x \equiv y (\text{mod } n) \Leftrightarrow x - y \text{ chia hết cho } n.$$

Đây là một quan hệ tương đương trên $\mathbb{Z}$ với các lớp tương đương là

$$\overline{x} = \{x + kn | k \in \mathbb{Z}\}.$$

Tập thương của $\mathbb{Z}$ theo quan hệ đồng dư modulo n định bởi

$$\mathbb{Z}_n = \{\overline{x} | x \in \mathbb{Z}\} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}.$$

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

$$\overline{x} + \overline{y} = \overline{x + y}.$$

Kiểm chứng dễ dàng rằng định nghĩa trên được hoàn toàn xác định và $\mathbb{Z}_n$ trở thành một nhóm giao hoán. Hơn nữa, $\mathbb{Z}_n$ là nhóm cyclic hữu hạn cấp n sinh bởi $\overline{1}$. Ta gọi $\mathbb{Z}_n$ là *nhóm cộng các số nguyên modulo* n.

3) Trong nhóm hoán vị S_n, một r-chu trình $\sigma = (i_1\ i_2\ \ldots\ i_r)$ luôn luôn có cấp r vì $\sigma^r = Id$ và $\sigma^l \neq Id$ với mọi $0 < l < r$.

6.6. 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* $a^n \in H$.

6.7. Hệ quả. *H là một nhóm con của nhóm cộng các số nguyên $\mathbb{Z}$ khi và chỉ khi H có dạng $n\mathbb{Z}$ với $n \in \mathbb{N}$, trong đó*

$$n\mathbb{Z} = \{nk | k \in \mathbb{Z}\}.$$

CHƯƠNG 1. NHÓM

7.1. Định lý. *Cho $(G, .)$ là một nhóm và H là một nhóm con của G. Xét quan hệ $\sim$ trên G như sau:*

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

Khi đó

(i) $\sim$ là một quan hệ tương đương trên G.

(ii) Lớp tương đương chứa x là $\overline{x} = xH$, trong đó G.

$$xH = \{xh | h \in H\}.$$

Ta gọi xH là *lớp ghép trái* của H (bởi phần tử x). Tập hợp thương của G theo quan hệ $\sim$, ký hiệu là G/H, được gọi là *tập thương* của G trên H và $|G/H|$ là *chỉ số* của nhóm con H trong G, ký hiệu là $[G : H]$.

7.2. Chú ý

Hoàn toàn tương tự, ta định nghĩa được quan hệ $\sim'$ trên G như sau:

$$x \sim' y \Leftrightarrow xy^{-1} \in H.$$

Khi đó $\sim'$ cũng là một quan hệ tương đương trên G và lớp tương đương chứa x là $\overline{x} = Hx$, trong đó $Hx = \{hx | h \in H\}$. Ta gọi Hx là *lớp ghép phải* của H (bởi phần tử x).

7.3. Định lý Lagrange. *Cho G là một nhóm hữu hạn và H là một nhóm con của G. Khi đó*

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

7.4. Hệ quả. *Cho G là một nhóm hữu hạn. Khi đó:*

(i) Cấp của mỗi nhóm con của G là một ước số của cấp của G.

(ii) Cấp của mỗi phần tử thuộc G là một ước số của cấp của G.

(iii) Nếu G có cấp nguyên tố thì G là nhóm cyclic và G được sinh bởi một phần tử bất kỳ khác e.

Chú ý rằng nếu H là một nhóm con tùy ý của G thì tập thương G/H như đã xây dựng trong Định lý 7.1 không nhất thiết là một nhóm.

7.5. Định nghĩa

Một nhóm con H của nhóm $(G, .)$ được gọi là *chuẩn tắc* nếu với mọi $x \in G$ và $h \in H$, $x^{-1}hx \in H$. Ký hiệu $H \lhd G$ để chỉ H là một nhóm con chuẩn tắc của G.

7.6. Mệnh đề. *Cho H là một nhóm con của nhóm $(G, .)$. Các mệnh đề sau tương đương:*

(i) $H \lhd G$;

(ii) $\forall x \in G, x^{-1}Hx \subset H$;

(iii) $\forall x \in G, x^{-1}Hx = H$;

(iv) $\forall x \in G, xH = Hx$;

trong đó $x^{-1}Hx = \{x^{-1}hx | h \in H\}$.

7.7. Nhận xét

1) Nếu G giao hoán thì mọi nhóm con của G đều chuẩn tắc.

2) Các nhóm con tầm thường $\{e\}$ và G đều chuẩn tắc trong G.

7.8. Ví dụ

1) Nhóm thay phiên bậc n (Xem Ví dụ 5.4) là nhóm con chuẩn tắc của nhóm hoán vị S_n vì với mọi hoán vị chẵn τ ta có $\sigma^{-1}\tau\sigma$ cũng là hoán vị chẵn với mọi hoán vị $\sigma \in S_n$.

2) Nhóm tuyến tính đặc biệt $SL(n,\mathbb{R})$ (Xem Ví dụ 5.4) là nhóm con chuẩn tắc của nhóm tuyến tính đầy đủ $GL(n,\mathbb{R})$ vì 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 $X^{-1}AX \in SL(n,\mathbb{R})$.

7.9. 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 .

7.10. Nhận xét

1) Nếu G là một nhóm giao hoán thì nhóm thương G/H cũng giao hoán. Chiều đảo không đúng.

2) Với $H \leq G$, nếu tập thương G/H là một nhóm với phép toán được định nghĩa như trên ($(xH)(yH) = xyH$) thì $H \lhd G$. Thật vậy, với mọi $x \in G$ và $h \in H$ ta có $x^{-1}hxH = (x^{-1}H)(hH)(xH) = (x^{-1}H)H(xH) = (x^{-1}H)(xH) = x^{-1}xH = H$ nên $x^{-1}hx \in H$.

7.11. Ví dụ

1) Vì nhóm cộng các số nguyên $\mathbb{Z}$ giao hoán nên với mỗi n nguyên dương nhóm con $n\mathbb{Z}$ chuẩn tắc trong $\mathbb{Z}$. Ứng với nhóm con $H = n\mathbb{Z}$, quan hệ $\sim$ trong Định lý 7.1 định bởi

$$\begin{aligned} x \sim y &\Leftrightarrow x - y \in n\mathbb{Z} \\ &\Leftrightarrow x - y \text{ chia hết cho } n. \end{aligned}$$

Như vậy, $\sim$ chính là quan hệ đồng dư modulo n trên $\mathbb{Z}$ và nhóm thương $\mathbb{Z}/n\mathbb{Z}$ chính là nhóm cộng $\mathbb{Z}_n$ các số nguyên modulo n trong Ví dụ 6.5.

2) Theo Ví dụ 7.8, $A_n \lhd S_n$. Nếu σ và τ là hai hoán vị lẻ thì $\sigma^{-1}\tau$ là hoán vị chẵn nên $\sigma^{-1}\tau \in A_n$, từ đó $\sigma A_n = \tau A_n$. Điều này chứng tỏ nhóm thương S_n/A_n có đúng hai phần tử:

$$S_n/A_n = \{A_n, \overline{A_n}\}, \quad \text{trong đó } \overline{A_n} = S_n \setminus A_n.$$

CHƯƠNG 1. NHÓM

8.1. Định nghĩa

Một ánh xạ f từ nhóm G vào nhóm G' được gọi là một *đồng cấu (nhóm)* nếu f bảo toàn phép toán, nghĩa là với mọi $x, y \in G$,

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

Một đồng cấu từ nhóm 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 $G \simeq G'$.

8.2. Ví dụ

1) Ánh xạ đồng nhất id_G của nhóm G là một tự đẳng cấu, gọi là *tự đẳng cấu đồng nhất* của G.

2) Giả sử H là một nhóm con của nhóm G. Khi đó ánh xạ bao hàm $i_H : H \longrightarrow G$ $(i_H(x) = x)$ là một đơn cấu, gọi là *đơn cấu* chính tắc.

3) Giả sử H là một nhóm con chuẩn tắc của nhóm G. Khi đó ánh xạ $\pi : G \longrightarrow G/H$ định bởi $\pi(x) = xH$ là một toàn cấu, gọi là *toàn cấu chính tắc*.

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

5) Ánh xạ $x \mapsto \cos 2\pi x + i \sin 2\pi x$ là một đồng cấu từ nhóm cộng các số thực $\mathbb{R}$ vào nhóm nhân các số phức khác không $\mathbb{C}^*$.

6) 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.

7) Ánh xạ $x \mapsto \ln x$ là một đẳng cấu từ nhóm nhân $\mathbb{R}^+$ các số thực dương lên nhóm cộng các số thực $\mathbb{R}$.

8) Ánh xạ $\text{sgn} : S_n \longrightarrow (\{-1; 1\}, .)$ là một đồng cấu.

9) Ánh xạ $\det : GL(n, \mathbb{R}) \longrightarrow \mathbb{R}^*$ là một toàn cấu.

10) Cho $(G, .)$ là một nhóm và $a \in G$. Ánh xạ $\varphi_a : G \longrightarrow G$ định bởi $\varphi_a(x) = axa^{-1}$ là một tự đẳng cấu của G. Thật vậy, φ_a là một đồng cấu vì

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

Mặt khác, φ_a là một song ánh vì với mỗi $y \in G$, tồn tại duy nhất $x = a^{-1}ya \in G$ sao cho $y = \varphi_a(x)$. Ta gọi φ_a là một *tự đẳng cấu trong* của nhóm G.

8.3. Mệnh đề. *Nếu* $f : G \longrightarrow G'$ *là một đồng cấu nhóm thì*

$$f(e) = e' \text{ và } f(x^{-1}) = (f(x))^{-1} \text{ với mọi } x \in G$$

(e *và* e' *lần lượt là các phần tử đơn vị của các nhóm* G *và* G'*).*

8.4. 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).*

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

8.6. Chú ý

Do các Mệnh đề 8.4 và 8.5 ta thấy quan hệ đẳng cấu $\simeq$ giữa các nhóm là một quan hệ tương đương, nghĩa là có ba tính chất phản xạ, đối xứng và bắc cầu.

8.7. Định lý. *Cho đồng cấu nhóm $f : G \longrightarrow G'$ và H là một nhóm con của G, H' là một 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, $Imf = f(G)$ là nhóm con của G' và $\mathrm{Ker}f = f^{-1}(e')$ là nhóm con chuẩn tắc của G.

Ta gọi Imf là *ảnh* của f và $\mathrm{Ker}f$ là *hạt nhân* của f.

8.8. Định lý. *Đồng cấu nhóm* $f : G \longrightarrow G'$ *là đơn cấu khi và chỉ khi* $\mathrm{Ker}f = \{e\}$.

8.9. Định lý đẳng cấu 1. *Cho đồng cấu nhóm* $f : G \longrightarrow G'$. *Khi đó ánh xạ* $\overline{f} : G/\mathrm{Ker}f \longrightarrow G'$ *định bởi* $\overline{f}(x\mathrm{Ker}f) = f(x)$ *là một đơn cấu. Đặc biệt,* $G/\mathrm{Ker}f \simeq Imf$.

8.10. Định lý đẳng cấu 2. *Cho* G *là một nhóm và* H, K *là hai nhóm con của* G, *hơn nữa* H *chuẩn tắc trong* G. *Khi đó* $HK \leq G, H \lhd HK, H\cap K \lhd K$ *và* $K/H\cap K \simeq HK/H$ *qua đẳng cấu* $k(H\cap K) \mapsto kH$, *trong đó* $HK = \{hk | h \in H, k \in K\}$.

8.11. Định lý đẳng cấu 3. *Cho G là một nhóm và H là một nhóm con chuẩn tắc của G. Ta có*

(i) $\mathcal{K}$ là một nhóm con của G/H khi và chỉ khi $\mathcal{K}$ có dạng $\mathcal{K} = K/H$ với $K \leq G$ và $H \leq K$.

(ii) $\mathcal{K}$ là một nhóm con chuẩn tắc của G/H khi và chỉ khi $\mathcal{K}$ có dạng $\mathcal{K} = K/H$ với $K \lhd G$ và $H \leq K$. Hơn nữa, khi đó

$$(G/H)/(K/H) \simeq G/K$$

qua đẳng cấu $xH(K/H) \mapsto xK$.

8.12. Hệ quả. *Mọi nhóm cyclic vô hạn đều đẳng cấu với nhóm cộng các số nguyên $\mathbb{Z}$. Mọi nhóm cyclic hữu hạn cấp n đều đẳng cấu với nhóm cộng $\mathbb{Z}_n$ các số nguyên mod n.*

8.13. Ví dụ

Từ Ví dụ 8.2 ta thấy

1) Đồng cấu $f : \mathbb{R} \longrightarrow \mathbb{C}^*$ định bởi $f(x) = \cos 2\pi x + i \sin 2\pi x$ có $\mathrm{Ker} f = \mathbb{Z}$ và $\mathrm{Im} f = U$ trong đó $U = \{z \in \mathbb{C}^* | \ |z| = 1\}$. Do đó theo Định lý 8.9 $\mathbb{R}/\mathbb{Z} \simeq U$.

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

3) Toàn cấu $f : GL(n, \mathbb{R}) \longrightarrow \mathbb{R}^*$ định bởi $f(A) = detA$ có

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

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