

Groups

Tóm tắt lý thuyết

Tập hợp G và toán tử 2 ngôi \star trên G tạo thành một nhóm nếu:

- Tồn tại phần tử $e \in G$ sao cho với mọi $g \in G$, $e \star g = g \star e = g$. Khi đó e là phần tử đơn vị của G .
- Với mọi phần tử $g \in G$, tồn tại $g' \in G$ sao cho $g \star g' = g' \star g = e$. Khi đó g' gọi là phần tử nghịch đảo của g trong G .
- Với mọi $a, b, c \in G$ thì $a \star (b \star c) = (a \star b) \star c$ (tính kết hợp)

Nếu có thêm tính chất $a \star b = b \star a$ với mọi $a, b \in G$ thì G gọi là nhóm giao hoán (nhóm Abel).

Bài tập

7. Đặt $S = \mathbb{R} \setminus \{-1\}$ và định nghĩa toán tử 2 ngôi trên S là $a \star b = a + b + ab$. Chứng minh rằng (S, \star) là nhóm Abel

Chứng minh. • Giả sử tồn tại phần tử đơn vị e , khi đó $e \star s = s \star e = s$ với mọi $s \in S$. Nghĩa là $e + s + es = s + e + se = s$. Vậy $e + se = 0$ mà $s \neq -1$ nên $e = 0$

- Với $e = 0$, giả sử với mọi $s \in S$ có nghịch đảo s' . Do $s \star s' = s' \star s = e$ nên $s + s' + ss' = s' + s + s's = e = 0$, tức là $s'(1 + s) = -s$. Vậy $s' = \frac{-s}{1+s}$
- Với mọi $a, b, c \in S$, $a \star (b \star c) = a \star (b + c + bc) = a + (b + c + bc) + a(b + c + bc) = a + b + c + ab + bc + ca + abc$ và $(a \star b) \star c = (a + b + ab) \star c = a + b + ab + c + c(a + b + bc) = a + b + c + ab + bc + ca + abc$. Như vậy $a \star (b \star c) = (a \star b) \star c$, tính kết hợp

□

39. Gọi G là tập các ma trận 2×2 với dạng

$$\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$$

với $\theta \in \mathbb{R}$. Chứng minh rằng G là subgroup của $SL_2(\mathbb{R})$

Chứng minh. Với $\theta_1, \theta_2 \in \mathbb{R}$, ta có

$$\begin{aligned} & \det \left(\begin{pmatrix} \cos \theta_1 & -\sin \theta_1 \\ \sin \theta_1 & \cos \theta_1 \end{pmatrix} \begin{pmatrix} \cos \theta_2 & -\sin \theta_2 \\ \sin \theta_2 & \cos \theta_2 \end{pmatrix} \right) \\ &= \det \left(\begin{pmatrix} \cos \theta_1 \cos \theta_2 - \sin \theta_1 \sin \theta_2 & -\cos \theta_1 \sin \theta_2 - \sin \theta_1 \cos \theta_2 \\ \sin \theta_1 \cos \theta_2 + \cos \theta_1 \sin \theta_2 & -\sin \theta_1 \sin \theta_2 + \cos \theta_1 \cos \theta_2 \end{pmatrix} \right) \\ &= \det \left(\begin{pmatrix} \cos(\theta_1 + \theta_2) & -\sin(\theta_1 + \theta_2) \\ \sin(\theta_1 + \theta_2) & \cos(\theta_1 + \theta_2) \end{pmatrix} \right) \\ &= 1 \cdot 1 = 1 \end{aligned}$$

Như vậy phép nhân 2 ma trận có dạng trên đóng trên $SL_2(\mathbb{R})$.

Phần tử đơn vị là $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ tương ứng với $\theta = 0$

Phần tử nghịch đảo là $\begin{pmatrix} \cos(-\theta) & -\sin(-\theta) \\ \sin(-\theta) & \cos(-\theta) \end{pmatrix}$ suy ra từ công thức định thức ban này

Cuối cùng, phép nhân ma trận có tính kết hợp. Như vậy G là subgroup của $SL_2(\mathbb{R})$

□

47. Đặt G là nhóm và $g \in G$. Chứng minh rằng

$$Z(G) = \{x \in G : gx = xg \forall g \in G\}$$

là subgroup của G . Subgroup này gọi là **center** của G

Chứng minh. Giả sử trong G có 2 phần tử là x_1 và x_2 thuộc $Z(G)$. Khi đó

$$x_1g = gx_1 \text{ và } x_2g = gx_2 \text{ với mọi } g \in G.$$

Xét phần tử x_1x_2 , ta có

$$(x_1x_2)g = x_1(x_2g) = x_1(gx_2) = (gx_1)x_2 = g(x_1x_2)$$

với mọi $g \in G$. Do đó $x_1x_2 \in Z(G)$ nên $Z(G)$ là subgroup.

□

49. Cho ví dụ về nhóm vô hạn mà mọi nhóm con không tầm thường của nó đều vô hạn

Ví dụ tập \mathbb{Z} và phép cộng số nguyên. Khi đó mọi nhóm con của \mathbb{Z} có dạng $n\mathbb{Z}$ với $n \in \mathbb{Z}$. Ví dụ

$$2\mathbb{Z} = \{\dots, -4, -2, 0, 2, 4, \dots\} \text{ với phần tử sinh là } 2$$

$$n\mathbb{Z} = \{\dots, -2n, -n, 0, n, 2n, \dots\} \text{ với phần tử sinh là } n$$

54. Cho H là subgroup của G và

$$C(H) = \{g \in G : gh = hg \forall h \in H\}$$

Chứng minh rằng $C(H)$ là subgroup của G . Subgroup này được gọi là **centralizer** của H trong G

Chứng minh. Gọi g_1 và g_2 thuộc $C(H)$. Khi đó

$$g_1h = hg_1 \text{ và } g_2h = hg_2 \text{ với mọi } h \in H$$

Xét phần tử g_1g_2 , với mọi $h \in H$ ta có

$$(g_1g_2)h = g_1(g_2h) = g_1(hg_2) = (g_1h)g_2 = (hg_1)g_2 = h(g_1g_2)$$

Như vậy $g_1g_2 \in C(H)$, từ đó $C(H)$ là subgroup của G

□

Kết luận

Bài tập số 47 và 54 là 2 khái niệm quan trọng cho bổ đề Burnside và định lý Polya.

Permutation Groups

Tóm tắt lý thuyết

Đặt S_n là nhóm hoán vị trên tập n phần tử. Như vậy S_n có $n!$ phần tử.

Mỗi phần tử trong S_n có thể biểu diễn dưới dạng các chu trình (cycle) độc lập (disjoint).

Bài tập

13. Đặt $\sigma = \sigma_1 \cdots \sigma_m \in S_n$ là tích của các cycle độc lập. Chứng minh rằng order của σ là LCM của độ dài các cycle $\sigma_1, \dots, \sigma_m$.

Chứng minh. Đặt l_i là độ dài cycle σ_i ($i = 1, \dots, m$). Khi đó $\sigma_i^{k_i l_i}$ sẽ ở dạng các cycle độ dài 1 ($k_i \in \mathbb{Z}$).

Từ đó, $\sigma^l = \sigma_1^l \cdots \sigma_m^l = (1) \cdots (n)$ nếu $l = k_1 l_1 = \cdots k_m l_m$. Số l nhỏ nhất thỏa mãn điều kiện này là $\text{lcm}(l_1, \dots, l_m)$ (đpcm) □

23. Nếu σ là chu trình với độ dài lẻ, chứng minh rằng σ^2 cũng là chu trình

Chứng minh. Giả sử $\sigma = (g_1, g_2, \dots, g_{n-1}, g_n)$ với n lẻ. Khi đó $\sigma^2 = (g_1, g_3, \dots, g_n, g_2, g_4, \dots, g_{n-1})$ cũng là chu trình. □

30. Cho $\tau = (a_1, a_2, \dots, a_k)$ là chu trình độ dài k .

(a) Chứng minh rằng với mọi hoán vị σ thì

$$\sigma \tau \sigma^{-1} = (\sigma(a_1), \sigma(a_2), \dots, \sigma(a_k))$$

là chu trình độ dài k .

(b) Gọi μ là chu trình độ dài k . Chứng minh rằng tồn tại hoán vị σ sao cho $\sigma \tau \sigma^{-1} = \mu$

Chứng minh. (a) Ta thấy rằng bất kì phần tử nào khác a_1, a_2, \dots, a_k thì khi qua τ không đổi, do đó khi đi qua $\sigma \tau \sigma^{-1}$ thì chỉ đi qua $\sigma \sigma^{-1}$ và cũng không đổi. Nói cách khác các phần tử a_1, a_2, \dots, a_k vẫn nằm trong chu trình nên ta có đpcm.

(b) Từ câu (a), với $\mu = (b_1, b_2, \dots, b_k)$ thì ta chọn σ sao cho $b_i = \sigma(a_i)$. □

Kết luận

Bổ đề Burnside và định lý Polya dùng để đếm số cấu hình khác nhau dựa trên nhóm hoán vị.

Cosets

Tóm tắt lý thuyết

Định nghĩa 1 (Left coset). Cho nhóm G và subgroup của nó là H . Khi đó, với phần tử $g \in G$, **left coset** của g được định nghĩa là tập $gH = \{gh : h \in H\}$

Định nghĩa 2 (Right coset). Tương tự, **right coset** là tập $Hg = \{hg : h \in H\}$

Định lý 1 (Định lý Lagrange). Gọi G là nhóm hữu hạn n phần tử. Khi đó mọi subgroup H của G có số phần tử chia hết cho n .

Định nghĩa 3. Cho nhóm G và subgroup H của nó. Số lượng left coset của H trong G được gọi là **index** và được ký hiệu là $[G : H]$

Định lý 2. Với H là subgroup của G . Khi đó số lượng right coset bằng số lượng left coset

Bài tập

11. Gọi H là subgroup của nhóm G và giả sử $g_1, g_2 \in G$. Chứng minh các mệnh đề sau là tương đương:

- (a) $g_1H = g_2H$
- (b) $Hg_1^{-1} = Hg_2^{-1}$
- (c) $g_1H \subseteq g_2H$
- (d) $g_2 \in g_1H$
- (e) $g_1^{-1}g_2 \in H$

Chứng minh. Từ (a) ra (b): Ta đã biết các coset là rời nhau hoặc trùng nhau, do đó với mọi $g_1h \in g_1H$, tồn tại $g_2h' \in g_2H$ mà $g_1h = g_2h'$. Suy ra $(g_1h)^{-1} = (g_2h')^{-1}$ hay $h^{-1}g_1^{-1} = h'^{-1}g_2^{-1}$ (đpcm)

Từ (a) ra (c): Hiển nhiên

Từ (a) ra (d): Với mọi $g_1h \in g_1H$, tồn tại $g_2h' \in g_2H$ sao cho $g_1h = g_2h'$, hay $g_2 = g_1hh'^{-1}$, đặt $h'' = hh'^{-1}$ thì $h'' \in H$ (H là nhóm con) nên $g_1h'' \in g_1H$. Suy ra $g_2 \in g_1H$

Từ (a) ra (e): Tương tự, ta có $g_1h = g_2h'$, suy ra $hh'^{-1} = g_1^{-1}g_2 \in H$

□

16. Nếu $ghg^{-1} \in H$ với mọi $g \in G$ và $h \in H$, chứng minh rằng right coset trùng với left coset

Chứng minh. Do $ghg^{-1} \in H$ nên tồn tại $h' \in H$ sao cho $ghg^{-1} = h'$. Tương đương $gh = h'g$ với mọi $h \in H$ nên $gH = Hg$. Điều này đúng với mọi $g \in G$ nên các right coset trùng left coset. □

17. Giả sử $[G : H] = 2$. Chứng minh rằng nếu a, b không thuộc H thì $ab \in H$.

Chứng minh. Ta biết rằng 2 coset ứng với 2 phần tử g_1, g_2 bất kì là trùng nhau hoặc rời nhau.

Do đó với $eH = H$, ta suy ra 2 coset của G là H và $G \setminus H$.

Vì $a, b \notin H$ nên coset của chúng trùng nhau. Và nghịch đảo của a cũng nằm trong $G \setminus H$ vì nếu nghịch đảo của a nằm trong H thì a cũng phải nằm trong H .

Suy ra $a^{-1}H = bH$. Nghĩa là tồn tại 2 phần tử $h_1, h_2 \in H$ sao cho $a^{-1}h_1 = bh_2$, tương đương $h_1h_2^{-1} = ab \in H$ (đpcm). □

21. Gọi G là cyclic group với order n . Chứng minh rằng có đúng $\phi(n)$ phần tử sinh của G

Chứng minh. Gọi g là một phần tử sinh của G . Khi đó g sinh ra tất cả phần tử trong G , hay nói cách khác các phần tử trong G có dạng g^i với $0 \leq i < n$.

Như vậy một phần tử $h = g^i$ cũng là phần tử sinh của G khi và chỉ khi $\gcd(i, n) = 1$ và có $\phi(n)$ số i như vậy (đpcm). □

Kết luận

Isomorphism

Tóm tắt lý thuyết

Cho 2 nhóm (G, \star) và $(H, *)$. Ánh xạ $\varphi : G \rightarrow H$ được gọi là isomorphism từ G tới H nếu:

- với mọi $g_1, g_2 \in G$ thì $\varphi(g_1 \star g_2) = \varphi(g_1) * \varphi(g_2)$
- φ là song ánh (one-to-one và onto)

Bài tập

18. Chứng minh rằng subgroup của \mathbb{Q}^* gồm các phần tử có dạng $2^m 3^n$ với $m, n \in \mathbb{Z}$ là internal direct product tới $\mathbb{Z} \times \mathbb{Z}$

Chứng minh. Xét ánh xạ $\varphi : \mathbb{Q}^* \rightarrow \mathbb{Z} \times \mathbb{Z}$, $\varphi(2^m 3^n) = (m, n)$

Hàm này là well-defined vì với m cố định thì mỗi phần tử $2^m 3^n$ chỉ cho ra một phần tử (m, n) . Tương tự với cố định n .

Hàm này là đơn ánh (one-to-one) vì với $m_1 = m_2$ và $n_1 = n_2$ thì $2^{m_1} 3^{n_1} = 2^{m_2} 3^{n_2}$.

Hàm này cũng là toàn ánh vì với mỗi cặp (m, n) ta đều tính được $2^m 3^n$.

Vậy hàm φ là song ánh.

Thêm nữa,

$$\begin{aligned}\varphi(2^{m_1} 3^{n_1} \cdot 2^{m_2} 3^{n_2}) &= \varphi(2^{m_1+m_2} 3^{n_1+n_2}) \\ &= (m_1 + m_2, n_1 + n_2) = (m_1, n_1) + (m_2, n_2) \\ &= \varphi(2^{m_1} 3^{n_1}) \varphi(2^{m_2} 3^{n_2})\end{aligned}$$

Vậy φ là homomorphism, và là song ánh nên là isomorphism. □

20. Chứng minh hoặc bác bỏ: mọi nhóm Abel có order chia hết bởi 3 chứa một subgroup có order là 3

Chứng minh. Gọi order của nhóm Abel là $n = 3k$, và g là phần tử sinh của nhóm Abel đó. Như vậy $g^n = g^{3k} = e$.

Nếu ta chọn $h = g^k$ thì $h^3 = e$, khi đó subgroup được sinh bởi h có order 3 (đpcm). □

21. Chứng minh hoặc bác bỏ: mọi nhóm không phải Abel có order chia hết bởi 6 chứa một subgroup có order 6

Chứng minh. Với S_3 có order là 6 nhưng không có nhóm con nào order 6 (nhóm con chỉ có order 1, 2 hoặc 3) (bác bỏ). □

22. Gọi G là group với order 20. Nếu G có các subgroup H và K với order 4 và 5 mà $hk = kh$ với mọi $h \in H$ và $k \in K$, chứng minh rằng G là internal direct product của H và K

Chứng minh. Ta chứng minh $H \cap K = \{e\}$. Giả sử tồn tại phần tử $m \in H \cap K$, khi đó do $m \in H$ nên $mk = km$ với mọi $k \in K$. Tuy nhiên $m \in K$ do đó điều này xảy ra khi và chỉ khi $m = e$.

Như vậy $H \cap K = \{e\}$. □

Kết luận

Isomorphism cho phép chúng ta chuyển từ việc tính toán trên một nhóm này thành tính toán trên nhóm khác dễ hơn (về mặt số học, toán tử).

Định lý 3 (Định lý Cayley). Mọi nhóm hữu hạn n phần tử isomorphism với nhóm con nào đó của nhóm hoán vị S_n