ĐẠI SỐ (CƠ SỞ)

Tài liệu ôn thi cao học năm 2005

Phiên bản đã chỉnh sửa

TS Trần Huyên

Ngày 19 tháng 11 năm 2004

Bài 3. Các Dạng Toán Kiểm Tra Nhóm Cyclic Và Cấp Một Phần Tử Trong Nhóm

Để kiểm tra một nhóm cho trước là cyclic, thông thường ta áp dụng định nghĩa về nhóm cyclic. Ta nhắc lại định nghĩa đó:

Định nghĩa 1 *Nhóm X được gọi là nhóm cyclic nếu tồn tại một phần tử $a \in X$ và $X = \langle a \rangle$, tức X trùng với nhóm con sinh bởi phần tử a, bao gồm tất cả các lũy thừa nguyên của a.*

$$Vậy: X = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$$

Như vậy, để chứng minh nhóm X là cyclic, theo định nghĩa 1, ta bắt buộc phải chỉ ra cho được một phần tử sinh $a \in X$, đồng thời phải chứng minh rằng bất kỳ phần tử $x \in X$ đều viết được dưới dạng một lũy thừa nguyên của a.

Ví dụ 1 *Cho X là nhóm cyclic, $X = \langle a \rangle$. Chứng minh rằng mọi nhóm con $A \leqslant X$ đều là nhóm cyclic.*

Bài giải Trường hợp $A = \{e\}$ thì $A = \langle e \rangle$.

Trường hợp $A \neq \{e\}$, do $A \leqslant X = \{a^n : n \in \mathbb{Z}\}$, ắt tồn tại một lũy thừa $a^k \neq e$ mà $a^k \in A$, và khi đó $a^{-k} \in A$ do A là nhóm con. Tức tồn tại một lũy thừa nguyên dương của a thuộc vào A (hoặc a^k, hoặc a^{-k}).

Đặt $m = \min\{k > 0 : a^k \in A\}$, ta chứng minh $A = \langle a^m \rangle$. Thật vậy, với mọi $x \in A$ thì $x = a^k$ với $k = q.m + r (0 \leq r < m)$, và từ $a^k = a^{q.m+r} = (a^m)^q .a^r$ ta suy ra: $a^r = a^k.(a^m)^{-q} \in A$ do $a^k, a^m \in A$. Bởi điều kiện $0 \leq r < m$ và m là một số nguyên dương bé nhất để $a^m \in A$, buộc $r = 0$. Tức là $k = q.m$ hay $x = a^k = (a^m)^q$. Vậy A là nhóm cyclic.

Nhận xét Để dự đoán được phần tử sinh của A là lũy thừa nguyên dương bé nhất $a^m \in A$, ta căn cứ vào tính chất của phần tử sinh: nếu a^m là phần tử sinh của A thì mọi phần tử $a^k \in A$ tất phải có $a^k = (a^m)^q$, tức $k = m.q$ từ đó có thể thấy m phải là số bé nhất bởi nó là ước của mọi số k mà $a^k \in A$.

Ví dụ 2 *Cho A là tập các căn phức bậc n của đơn vị 1. Chứng minh A với phép nhân thông thường các số phức là một nhón cyclic.*

Phân tích ban đầu: Vì $A \subset (\mathcal{C}^*, \cdot)$ nên ta chứng minh A là nhóm con cyclic của $(\mathcal{C}^*, \cdot)$ bằng cách tìm một phần tử $a \in \mathcal{C}^*$ mà $A = \langle a \rangle$, và từ đó có kết luận A là nhóm cyclic.

Bài giải Ta biểu diễn $A = \left\{ \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} : k \in \mathbb{Z} \right\}$

hay $A = \left\{ \left(\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} \right)^k : k \in \mathbb{Z} \right\}$

Vậy: $A = \langle a \rangle$ với $a = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} \in \mathcal{C}^*$ tức là A là nhóm cyclic

Nhận xét Việc chứng minh A là nhóm cyclic buộc ta phải lựa chọn cách biểu diễn các phần tử của A dưới dạng cụ thể, để từ đó có thể nhận ra được phần tử sinh của A.

Liên quan đến các nhóm cyclic là khái niệm cấp của phần tử trong nhóm.

Định nghĩa 2 *Cho nhóm X và $a \in X$. Cấp của phần tử a là cấp của nhóm con cyclic sinh bởi phần tử a*

(cấp của nhóm con là số phần tử của nhóm đó, khi nhóm là hữu hạn; còn nếu nhóm con có số phần tử là vô hạn thì cấp của nó là ∞!)

Để tính cấp của phần tử $a \in X$, thông thường ta sử dụng một kết quả tiện dụng hơn sau đây:

"*Cấp của phần tử a (trong trường hợp hữu hạn) là số nguyên dương n bé nhất mà $a^n = e$.*"

Khái niệm *bé nhất* trong mệnh đề trên hiểu theo nghĩa so sánh về giá trị lớn bé của các số, tuy nhiên nó còn được chính xác hóa hơn như ví dụ sau:

Ví dụ 3 *Cho X là nhóm và $a \in X$ với cấp $a = n$. Chứng minh rằng $a^k = e$ khi và chỉ khi $k \vdots n$.*

Bài giải

– Hiển nhiên khi $k \vdots n$ thì $k = l.n$, do đó $a^k = a^{l.n} = (a^n)^l = e^l = e$

– Nếu $a^k = e$ và $k = q.n + r$ với $0 \le r < n$ thì từ $a^k = a^{qn+r} = (a^n)^q .a^r = e^q.a^r = a^r$ Suy ra $a^r = e$ với $0 \le r < n$. Vì n là số nguyên dương bé nhất mà $a^n = e$ nên các điều kiện $a^r = e$ và $0 \le r < n$, buộc $r = 0$.

Vậy: $k = q.n$ hay $k \vdots n$.

Nhận xét Ví dụ này cho thấy khái niệm *bé nhất* của cấp a còn có thể được hiểu theo quan hệ thứ tự chia hết: "*Cấp a là số tự nhiên n thỏa $a^n = e$ và là ước số của mọi số nguyên k mà $a^k = e$*".

Thật ra mệnh đề này thường được dùng để tính cấp của một phần tử. Chẳng hạn xem ví dụ sau:

Ví dụ 4 *Cho X là nhóm cyclic cấp n sinh bởi a và $b = a^k$. Chứng minh cấp $b = \frac{n}{d}$ với $d = (k, n)$.*

Bài giải Trước hết ta có: $b^{\frac{n}{d}} = \left(a^k\right)^{\frac{n}{d}} = (a^n)^{\frac{k}{d}} = e$. (Chú ý vì $d = (k, n)$ nên $\dfrac{k}{d} \in \mathbb{Z}$!)

Để kết thúc chứng minh ta còn phải chứng minh nếu $b^m = e$ thì $m \vdots \dfrac{n}{d}$. Ta có:

$$e = b^m = \left(a^k\right)^m = a^{km} \Longrightarrow km \vdots n \Longrightarrow \frac{k}{d} m \vdots \frac{n}{d} \Longrightarrow m \vdots \frac{n}{d} \quad (\text{do } \left(\frac{k}{d}, \frac{n}{d}\right) = 1).$$

Vậy: cấp $b = \dfrac{n}{d}$.

Nhận xét Bài toán sẽ khó hơn chút ít nếu yêu cầu tìm cấp b (thay cho chứng minh cấp $b = \dfrac{n}{d}$)

Nếu vậy bạn có thể xử lý được không?

Đến đây ta quay lại vấn đề nhóm cyclic. Để chứng minh nhóm cyclic, như ta đã lưu ý ở trên là thông thường dùng định nghĩa, tuy nhiên trong trường hợp nhóm cho trước X là hữu hạn, tức cấp $X = n$ thì có thể chứng minh X là cyclic bằng cách chỉ ra trong X có tồn tại một phần tử $a \in X$ mà cấp $a = n =$ cấp X.

Ví dụ 5 *Cho X và Y là các nhóm cyclic và cấp $X = m$, cấp $Y = n$. Chứng minh rằng nếu $(m, n) = 1$ thì nhóm tích $X \times Y$ là cyclic. (Ta nhắc rằng $X \times Y = \{(x, y), x \in X, y \in Y\}$ và phép nhân được xác định như sau:*

$(x_1, y_1)(x_2, y_2) = (x_1x_2, y_1y_2)$ *biến $X \times Y$ trở thành nhóm)*

Bài giải Ta chỉ cần chỉ ra nếu $X = \langle a \rangle_m$ và $Y = \langle b \rangle_n$ thì phần tử $(a, b) \in X \times Y$ có cấp là $m.n =$ cấp $X \times Y$

- Hiển nhiên là $(a, b)^{mn} = (a^{mn}, b^{mn}) = (e, e)$ - là đơn vị của $X \times Y$
- Và nếu $(a, b)^k = (e, e)$ thì $\left(a^k, b^k\right) = (e, e)$

  Do vậy: $\left\{ \begin{array}{ll} a^k & = e \\ b^k & = e \end{array} \right. \Longrightarrow \left\{ \begin{array}{l} k \vdots m \\ k \vdots n \end{array} \right. \Longrightarrow k \vdots mn \quad (\text{ do } (m, n) = 1)$

Vậy: cấp $(a, b) = m.n =$ cấp $X \times Y$
Suy ra: $X \times Y = \langle (a, b) \rangle_{mn}$.

Bài tập

1. Cho $A \trianglelefteq (\mathbb{Z}; +)$. Chứng minh rằng tồn tại số m sao cho $A = m.\mathbb{Z}$
2. Chứng minh rằng nhóm thương của nhóm cyclic là nhóm cyclic.
3. Cho X là nhóm và các phần tử $a, b \in X$. Chứng minh rằng cấp $(ab) =$ cấp (ba).
4. Cho nhóm X và 2 phần tử $a, b \in X$ thỏa $ab = ba$. Chứng tỏ rằng cấp $a.b = [m, n]$, trong đó $m =$ cấp a, $n =$ cấp b và $[m, n]$ là BCNN của m, n.
5. Cho X là nhóm cyclic cấp n và k là một ước số của n. Chứng minh rằng trong X tồn tại đúng một nhóm con A cấp k.
6. Cho X là nhóm cyclic. Tìm số tất cả các phần tử sinh của X nếu: a) Cấp $X = n$ b) Cấp $X = \infty$.
7. Cho X là nhóm con đơn, tức X chỉ có duy nhất hai nhóm con là $\{e\}$ và X. Chứng minh X là nhóm cyclic hữu hạn và cấp $X = p$ là số nguyên tố.