# TÍNH DUY NHẤT CỦA NHÓM CẤP *N*

*Nguyễn Ngọc Châu, Ngô Thị Hoài Phương**

**TÓM TẮT**

Cho *n* là một số nguyên dương. ***"Khi nào có duy nhất một nhóm cấp n?".*** Câu trả lời đã có từ lâu, tuy nhiên không được biết rộng rãi, ngay cả trong những giáo trình về lý thuyết nhóm. Bài viết này sẽ giới thiệu lời giải của câu hỏi nói trên.

Từ khóa **: nhóm cyclic, hàm euler**

## Mở đầu

Cho *n* là một số nguyên dương. Bài toán tổng quát của nhóm hữu hạn là xác định tất cả các nhóm không đẳng cấu nhau có cấp *n*, đã được A. Cayley đặt ra vào năm 1878, và đến nay vẫn chưa có lời giải đầy đủ. Chúng ta đã biết khi $n = 1$ hoặc *n* là một số nguyên tố thì có duy nhất một nhóm cấp *n* (tất nhiên là nhóm cyclic). Ngoài ra, bằng cách áp dụng các định lý Sylow vào nhóm có cấp $pq$, $p < q$, $p, q$ là các số nguyên tố, chúng ta cũng chứng minh được rằng một nhóm như vậy là duy nhất khi và chỉ khi *p* không chia hết $q - 1$. Từ đó, một câu hỏi được đặt ra một cách tự nhiên là ***" Với các số nguyên dương n nào, thì có duy nhất một nhóm cấp n ?"***. Câu trả lời đã có từ lâu, tuy nhiên không được biết rộng rãi, ngay cả trong những giáo trình về lý thuyết nhóm. Bài viết này sẽ giới thiệu lời giải của câu hỏi nói trên, cụ thể ta có:

**Định lý.** *Cho n là một số nguyên dương. Khi đó nhóm cyclic cấp n là nhóm duy nhất có cấp n, nếu và chỉ nếu* $(n, \phi(n)) = 1$, *trong đó* $\phi$ *là hàm Euler.*

Định lý trên là một trường hợp riêng của một kết quả được cho bởi Dickson [1]. Định lý này và phép chứng minh của nó trình bày trong bài viết này đã được Dieter Jungnickel giới thiệu trong [2].

## 1. Các kết quả dùng để chứng minh Định lý

***1.1. Định nghĩa: Cho m là một số nguyên dương, hàm Euler*** $\phi(m)$ ***biểu thị số các số tự nhiên không vượt quá (m -1) và nguyên tố cùng nhau với m.***

***1.2. Mệnh đề:[3] Với hai số nguyên dương*** $m_1$ ***và*** $m_2$ ***nguyên tố cùng nhau, ta có***

$$\phi(m_1.m_2) = \phi(m_1)\phi(m_2).$$

***1.3. Công thức tính*** $\phi(m)$***. [3]***

*i)* Nếu $m = 1$, thì $\phi(m) = 1$.

*ii)* Nếu $m = p^{\alpha}$, trong đó *p* là một số nguyên tố và $\alpha$ là một số nguyên dương, thì $\phi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1} = p^{\alpha}(1 - \frac{1}{p})$.

*iii)* Nếu $m > 1$ và $m = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, trong đó $p_i$, $i = 1,2,...,k$ là các số nguyên tố khác nhau đôi một; $\alpha_i$, $i = 1,2,...,k$ là các số nguyên dương, *ta có*

$$\phi(m) = m\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$$

***1.4. Định nghĩa: Một số nguyên n được gọi là không có nhân tử chính phương nếu n không có nhân tử là bình phương của một số nguyên khác 1.***

***1.5. Mệnh đề: Giả sử n là một số nguyên dương có nhân tử chính phương, tức là n = $mp^a$, trong đó p là số nguyên tố không chia hết m, và a là số nguyên, a ≥ 2. Khi đó:***

*i)* Có ít nhất hai nhóm có cấp *n* không đẳng cấu nhau là nhóm cyclic *C(n)* cấp *n* và nhóm $C(m)\times C(p)^a$.

*ii)* $(n, \phi(n)) \geq p$.

***Chứng minh:***

*i)* Vì $a \geq 2$ nên phần *i)* của Mệnh đề hiển nhiên đúng

*ii)* Với $n = mp^a$, trong đó *p* là số nguyên tố không chia hết m, a là số tự nhiên, a ≥ 2, thì (m, $p^a$) = 1. Suy ra $\phi(n) = \phi(p^\alpha)\phi(m) = p^{\alpha-1}(p-1)\phi(m)$. Do đó, cả $n$ và $\phi(n)$ đều chia hết cho $p$. Vậy $(n, \phi(n)) \geq p$.

Mệnh đề trên cho phép để chứng minh Định lý, chỉ cần xét $n$ là số nguyên dương không có nhân tử chính phương. Trong các Bổ đề dưới đây, ta giả sử $n$ là số nguyên dương không có nhân tử chính phương nhỏ nhất sao cho $(n, \phi(n)) = 1$ và $G$ là một nhóm không cyclic cấp $n$.

***1.6. Bổ đề: Ta có (m, ϕ(m)) = 1, với mọi số nguyên dương m là ước của n.***

***Chứng minh:***

Giả sử ngược lại $(m, \phi(m)) \neq 1$. Gọi $(m, \phi(m)) = h$, với $h$ là số nguyên lớn hơn 1. Do $m$ là ước của $n$ nên tồn tại một số nguyên $q$ sao cho $n = mq$. Từ đó ta có

$$\phi(n) = \phi(mq) = \phi(m)\phi(q) \text{ và } (n, \phi(n)) = (mq, \phi(m)\phi(q)) \geq h > 1$$

trái với giả thiết $(n, \phi(n)) = 1$.

Vậy $(m, \phi(m)) = 1$, với mọi số nguyên dương $m$ là ước của $n$.

***1.7. Bổ đề:***

*i)* Mọi nhóm con thực sự và mọi nhóm thương theo một nhóm con chuẩn tắc

không tầm thường của *G* đều là nhóm cyclic.

*ii) Tâm* $Z(G) = \{1\}$.

***Chứng minh:***

*i)* Theo Bổ đề 2.6, thì $(m, \phi(m)) = 1$, với mọi *m* là ước của *n*. Do đó, mọi nhóm con thực sự và mọi nhóm thương theo một nhóm con chuẩn tắc không tầm thường của *G* đều là cyclic (vì có cấp nhỏ hơn *n*).

*ii)* Giả sử $Z(G) \neq \{1\}$. Theo *i)* nhóm thương *G/Z(G)* là nhóm cyclic. Do đó *G* là nhóm abel và là nhóm cyclic (vô lý). Vậy $Z(G) = \{1\}$.

***1.8. Bổ đề:***

*Cho* $x \neq 1$ *là một phần tử của một nhóm con cực đại U của G. Khi đó U là nhóm tâm hóa* $C_G(x)$ *của x trong G. Hơn nữa, bất kỳ hai nhóm con cực đại phân biệt U, V của G đều có giao tầm thường.*

***Chứng minh:***

Vì $U$ là nhóm con thực sự của $G$ nên $U$ là nhóm cyclic, suy ra $U \subset C_G(x)$.

Theo Bổ đề 2.7, $Z(G) = \{1\}$, nên $C_G(x)$ là nhóm con thực sự của *G*. Do tính cực đại của *U*, ta có $U = C_G(x)$.

Giả sử $U, V$ là hai nhóm con cực đại phân biệt của *G* sao cho $U \cap V \neq \{1\}$. Khi đó tồn tại $1 \neq x \in U \cap V$, và ta có $U = C_G(x) = V$ (mâu thuẫn). Vậy $U \cap V = \{1\}$.

Bổ đề đã được chứng minh.

***1.9. Bổ đề:***

Bất kỳ nhóm con cực đại $U$ nào của *G* đều bằng nhóm chuẩn hóa $N_G(U)$ của $U$ trong *G*. Ngoài ra, nếu $U$ là một nhóm con cực đại cấp $u$ của $G$, thì các lớp liên hợp của $U$ chứa đúng $n - n/u$ phần tử khác 1.

***Chứng minh:***

Vì $U$ là nhóm con thực sự của *G* nên $U \subset N_G(U)$, và *U* là nhóm cyclic.

$\forall x \in N_G(U) \Rightarrow x^{-1}ax \in U, \forall a \in U$. Do đó ánh xạ $\alpha : U \to U$, $a$ a $x^{-1}ax$, là một tự đẳng cấu của $U$. Nếu $U$ có cấp *m*,thì nhóm *Aut(U)* có cấp $\phi(m)$. Vì $m \mid n$ nên $\phi(m)$ chia hết $\phi(n)$.

Do $ord(x) \mid n$, nên $\alpha^n(a) = x^{-n}ax^n = a$, suy ra $\alpha^n = 1_U$ và $ord(\alpha) \mid n$.

Đồng thời $ord(\alpha) \mid \phi(n)$, và $(n, \phi(n)) = 1$, suy ra $ord(\alpha) = 1$. Do đó $\alpha$ là tự

đẳng cấu đồng nhất của $U$, và $x \in C_G(U)$.

Nếu $x \notin U \Rightarrow \langle U, x \rangle = G \Rightarrow x \in Z(G)$ (trái với Bổ đề 2.7). Vậy $x \in U$, và do đó $N_G(U) \subset U$, hay $N_G(U) = U$.

Ta biết, số các liên hợp của $U$ bằng $[G : N_G(U)]$. Nhưng $N_G(U) = U$ nên $[G : N_G(U)] = n/u$. Do $U$ là nhóm con cực đại của $G$, nên các liên hợp của $U$ cũng là nhóm con cực đại của $G$.

Từ Bổ đề 2.8, ta có bất kỳ hai nhóm liên hợp phân biệt nào của $U$ đều có giao tầm thường nên các lớp liên hợp của $U$ chứa $(u - 1)n/u$ phần tử khác 1.

Bổ đề đã được chứng minh.

**2. Chứng minh Định lý**

***2.1. Định lý.[2] Cho n là một số nguyên dương. Khi đó nhóm cyclic cấp n là nhóm duy nhất có cấp n, nếu và chỉ nếu $(n, \phi(n)) = 1$, trong đó $\phi$ là hàm Euler.***

**Chứng minh:** Nếu $n = 1$, hoặc $n$ là một số nguyên tố thì Định lý hiển nhiên đúng.

**Điều kiện cần:** Để có duy nhất một nhóm cấp $n$, theo Mệnh đề 2.5 thì $n$ là số nguyên không có nhân tử chính phương, nghĩa là $n = p_1 p_2 \text{L}\ p_k$ là tích của k số nguyên tố phân biệt từng đôi một. Theo 2.3. thì $\phi(n) = (p_1 - 1)(p_2 - 1)...(p_k - 1)$.

Giả sử $(n, \phi(n)) \neq 1$. Khi đó, tồn tại các số nguyên tố $p, q$ sao cho $n = pqm$, với $p$ chia hết $q - 1$ và $m$ không chia hết cho $p$ và $q$.

Ta có Aut(C(q)) là nhóm cyclic cấp $q-1$. Do $p$ chia hết $q-1$, nên nhóm Aut(C(q)) có một phần tử f cấp p, và ta có đồng cấu sau đây

$$\theta: \text{C(p)} = < \text{a} > \longrightarrow \text{Aut(C(q))}$$

$$a^t \quad \text{a} \quad f^t = f \text{ o } f \text{ o...o } f \text{ (t lần)}$$

trong đó $0 \leq \text{t} < \text{p}$.

Khi đó tích nửa trực tiếp $C(q) \rtimes_\theta C(p)$ là một nhóm không giao hoán cấp $pq$, và do đó $[\text{C(q)} \rtimes_\theta \text{C(p)}] \times \text{C(m)}$ là nhóm không giao hoán cấp $n = pqm$. Điều này trái với giả thiết có duy nhất một nhóm cấp $n$ là nhóm cyclic $C(n)$. Vậy $(n, \phi(n)) = 1$.

**Điều kiện đủ:** Ta sẽ chứng minh điều kiện đủ của định lý bằng phản chứng.

Giả sử tồn tại số nguyên dương $m$, với $(m, \phi(m)) = 1$ mà có nhiều hơn một nhóm cấp $m$. Gọi $n$ là số nguyên dương nhỏ nhất sao cho $(n, \phi(n)) = 1$ và $G$ là một nhóm không cyclic cấp $n$.

Gọi $U$ là nhóm con cực đại cấp $u$ của $G$, khi đó $u > 1$ (vì $G$ không cyclic). Theo Bổ đề 2.9, tồn tại phần tử $x \in G$ không chứa trong bất kỳ liên hợp nào của $U$. Gọi $V$ là nhóm con cực đại của $G$ chứa $x$ và không liên hợp với $U$. Khi đó, các liên hợp của $U$, và các liên hợp của V đều là nhóm con cực đại của G. Theo Bổ đề 2.8, thì bất kỳ liên hợp của $U$ và bất kỳ liên hợp của $V$ đều có giao tầm thường.

Áp dụng Bổ đề 2.9 đối với $V$, ta có các liên hợp của $V$ chứa $n - n/v$ phần tử khác 1. Nhưng $G$ chỉ có $n - 1$ phần tử khác 1, từ đó cho ta bất đẳng thức

$$n - n/u + n - n/v < n \Leftrightarrow uv < u + v$$

điều này mâu thuẫn vì $u > 1$.

Vậy định lý đã được chứng minh.

## TÀI LIỆU THAM KHẢO

[1] L. E. Dickson, Definitions of a group and a field by independent postulates, Trans. Amer. Math. Soc. 6 (1905), 198-204.

[2] Dieter Jungnickel, On the uniqueness of the cyclic group of order $n$, Trans. Amer. Math. Soc. 93 (1992), 545-547.

[3] Ngô Thị Hoài Phương, Tính duy nhất của nhóm cấp $n$, Luận văn thạc sỹ khoa học, Đại học Đà Nẵng (2011).

## THE UNIQUENESS OF THE GROUP OF ORDER $N$

***Nguyen Ngoc Chau[1], Ngo Thi Hoai Phuong[2]***

*[1] The University of Da Nang - University of Science and Education*
*[2] Thanh Khe Secondary School, Lien Chieu Danang*

**ABSTRACT**

Let $n$ be a positive integer. ***"When is there a unique group of order n ?"***. The answer was given to this question but has not been widely known, even in textbooks on group theory. In this paper, we would like to introduce an answer to the above question.

**Key words**: The Cyclic Group, The Euler Function

*Nguyễn Ngọc Châu, E-mail: chaunn@dce.udn.vn, Khoa Toán, Trường Đại học Sư phạm, Đại học Đà Nẵng

Ngô Thị Hoài Phương, Trường Phổ thông Trung học Thanh Khê, Quận Liên Chiểu, Thành phố Đà Nẵng