

**GIÁO DỤC VÀ ĐÀO TẠO
ĐẠI HỌC ĐÀ NẴNG**

NGÔ THỊ HOÀI PHƯƠNG

TÍNH DUY NHẤT CỦA NHÓM CẤP n

**Chuyên ngành: PHƯƠNG PHÁP TOÁN SƠ CẤP
Mã số: 60.46.40**

TÓM TẮT LUẬN VĂN THẠC SĨ KHOA HỌC

Đà Nẵng - Năm 2011

Công trình được hoàn thành tại
ĐẠI HỌC ĐÀ NẴNG

Người hướng dẫn khoa học: TS. NGUYỄN NGỌC CHÂU

Phản biện 1: TS. LÊ HOÀNG TRÍ

Phản biện 2: PGS.TS NGUYỄN GIA ĐỊNH

Luận văn sẽ được bảo vệ trước Hội đồng chấm Luận văn tốt nghiệp thạc sĩ khoa học họp tại Đại học Đà Nẵng vào ngày ... tháng ... năm 2011.

Có thể tìm hiểu luận văn tại:

- Trung tâm Thông tin – Học liệu, Đại học Đà Nẵng
- Thư viện trường Đại học Sư Phạm, Đại học Đà Nẵng

MỞ ĐẦU

1. Lí do chọn đề tài

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. Năm 1951, Định lý cơ bản về nhóm Abel hữu hạn sinh đã cho lời giải của bài toán này đối với các nhóm Abel hữu hạn. Tuy nhiên bài toán tổng quát của nhóm hữu hạn là một bài toán khó, và đến nay vẫn chưa có lời giải đầy đủ.

Trong các giáo trình Lý Thuyết Nhóm, 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 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 ”.

Nhằm tìm hiểu lời giải cho câu hỏi này, tôi chọn đề tài luận văn Thạc sĩ của mình là : **"TÍNH DUY NHẤT CỦA NHÓM CẤP n "**.

2. Mục tiêu và nhiệm vụ nghiên cứu

1. Nghiên cứu cấu trúc nhóm và các tính chất của một nhóm.
2. Nghiên cứu lý thuyết số.
3. Xác định các số nguyên dương n sao cho có duy nhất một nhóm cấp n .

3. Đối tượng và phạm vi nghiên cứu

1. Các nhóm hữu hạn.
2. Quan hệ đẳng cấu giữa các nhóm.
3. Tính chất số học của tập các số nguyên.

4. Phương pháp nghiên cứu

1. Tập hợp và hệ thống các tài liệu về lý thuyết nhóm có liên quan đến nội dung đề tài. Đặc biệt là các tài liệu về phân loại đẳng cấu các nhóm hữu hạn.

2. Khảo sát các tính chất số học của tập các số nguyên. Tìm hiểu về hàm Euler.

3. Áp dụng các tính chất của tập số nguyên và hàm Euler vào bài toán phân loại đẳng cấu các nhóm, từ đó xác định với số nguyên dương n nào thì có duy nhất một nhóm cấp n , và ngược lại.

5. Cấu trúc của luận văn

Luận văn gồm hai chương:

Chương I: Kiến thức chuẩn bị

Chương này sẽ trình bày sơ lược về lý thuyết nhóm, lý thuyết số và một số kiến thức cần thiết để chuẩn bị cho chương sau.

Chương II: Tính duy nhất của nhóm cấp n

Chương này là nội dung chính của luận văn, xác định các số nguyên dương n sao cho có duy nhất một nhóm cấp n (sai khác một đẳng cấu). Phần cuối chương sẽ xác định một số trường hợp của số nguyên dương n để chỉ có hai nhóm cấp n không đẳng cấu nhau.

Chương 1

KIẾN THỨC CHUẨN BỊ

Chương này sẽ trình bày sơ lược về cấu trúc nhóm, lý thuyết số và một số kiến thức cần thiết để chuẩn bị cho chương sau. Các chi tiết liên quan có thể xem trong [1], [2], [3], [4].

1.1. CẤU TRÚC NHÓM

1.1.1. Nhóm hữu hạn, p -nhóm

1.1.1.1. Định nghĩa 1

Cho một tập không rỗng G và một phép toán hai ngôi trên G được kí hiệu bởi $\bullet$, cặp $(G, \bullet)$ được gọi là một nhóm nếu

(i) Với mọi $x, y, z \in G$,

$$(x \bullet y) \bullet z = x \bullet (y \bullet z),$$

(ii) Tồn tại một phần tử ký hiệu $1 \in G$, gọi là phần tử đơn vị,

sao cho $x \bullet 1 = 1 \bullet x = x$, với mọi $x \in G$,

(iii) Với mỗi $x \in G$ có một phần tử nghịch đảo trong G , nghĩa là có một phần tử $x^{-1} \in G$ sao cho $x \bullet x^{-1} = x^{-1} \bullet x = 1$.

Nếu với mọi $x, y \in G$, $x \bullet y = y \bullet x$ thì $(G, \bullet)$ được gọi là một nhóm abel (hay nhóm giao hoán).

Nếu không sợ nhầm lẫn về phép toán, ta còn nói G là một nhóm thay cho nhóm $(G, \bullet)$.

Nhóm G được gọi là nhóm hữu hạn nếu G là một tập hữu hạn. Lúc đó số phần tử của tập hợp G được gọi là cấp của nhóm G và được kí hiệu là $|G|$. Nếu nhóm G không phải là nhóm hữu hạn thì ta nói G là nhóm (có cấp) vô hạn.

1.1.1.2. Định nghĩa 2

Một p -nhóm là một nhóm có cấp là một lũy thừa của một số nguyên tố p .

1.1.2. Nhóm con, p -nhóm con Sylow

1.1.2.1. Định nghĩa 3

Một bộ phận ổn định A của một nhóm X là một nhóm con của X nếu A cùng với phép toán cảm sinh là một nhóm, kí hiệu

$$A \leq X.$$

1.1.2.2. Định lý 1

Một bộ phận A của nhóm X là một nhóm con của X nếu và chỉ nếu các điều kiện sau đây thỏa mãn :

i) Với mọi $x, y \in A$, $xy \in A$.

ii) $e \in A$, với e là phần tử trung lập của X .

iii) Với mọi $x \in A$, $x^{-1} \in A$.

1.1.2.3. Hệ quả 1

Giả sử A là một bộ phận khác rỗng của một nhóm X . Các điều kiện sau đây là tương đương :

i) A là một nhóm con của X .

ii) Với mọi $x, y \in A$, $xy \in A$ và $x^{-1} \in A$.

iii) Với mọi $x, y \in A$, $xy^{-1} \in A$.

1.1.2.4. Định nghĩa 4

i) Nhóm H được gọi là p -nhóm con của G nếu H vừa là một nhóm con của G vừa là một p -nhóm.

ii) Nhóm H được gọi là một p -nhóm con Sylow của G nếu H là một p -nhóm con của G và $|H| = p^n$ là lũy thừa cao nhất của p chia hết $|G|$.

1.1.2.5. Định nghĩa 5 (Nhóm con cực đại)

Nhóm con thực sự M của G được gọi là nhóm con cực đại của G nếu không có nhóm con H nào của G để $M < H < G$.

1.1.2.6. Định nghĩa 6

Hai nhóm con S và T của nhóm G được gọi là liên hợp nếu có một phần tử $g \in G$ sao cho $g^{-1}Sg = T$.

Trong đó : $g^{-1}Sg = \{g^{-1}sg / s \in S\}$.

1.1.3. Nhóm cyclic

1.1.3.1. Mệnh đề 1

Giao của một họ bất kỳ các nhóm con của một nhóm G cũng là nhóm con của G .

1.1.3.2. Định nghĩa 7

Cho G là một nhóm và X là một tập con khác rỗng của G . Nhóm con của G sinh bởi tập hợp X là giao của tất cả các nhóm con của G có chứa X , kí hiệu $\langle X \rangle$.

$\langle X \rangle = \{x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n} / x_i \in X, \varepsilon_i = \pm 1, n \text{ là một số nguyên dương}\}$.

1.1.3.3. Nhận xét 1

$\langle X \rangle$ là nhóm con nhỏ nhất của G có chứa X .

Nếu $\langle X \rangle = G$ thì ta nói G là nhóm được sinh bởi X và X là tập sinh của G .

1.1.3.4. Định nghĩa 8

Nhóm hữu hạn sinh là nhóm được sinh bởi một tập sinh hữu hạn.

1.1.3.5. Định nghĩa 9

Một nhóm X gọi là cyclic nếu và chỉ nếu X được sinh ra bởi một phần tử $a \in X$, kí hiệu $\langle a \rangle$. Phần tử a được gọi là một phần tử sinh của X . Nhóm cyclic cấp n được kí hiệu là $C(n)$.

1.1.3.6. Nhận xét 2

Nếu $G = \langle x \rangle$ và G là một nhóm con hữu hạn cấp r , $(r, s) = 1$, thì $\langle x^s \rangle = G$.

1.1.3.7. Định nghĩa 10

Giả sử G là một nhóm với phần tử đơn vị 1 , $a \in G$. Nếu $a^m \neq 1, \forall m \in \mathbb{Z}^*$ thì a gọi là có cấp vô hạn. Nếu m là số nguyên dương nhỏ nhất sao cho $a^m = 1$ thì m được gọi là cấp của a . Cấp của phần tử a được kí hiệu là $ord(a)$.

Từ định nghĩa trên ta có

$$ord(a) = |\langle a \rangle|, \text{ và } ord(a) = 1 \Leftrightarrow a = 1.$$

1.1.3.8. Bổ đề 1

Cho X là một nhóm với phần tử đơn vị e , $a \in X$ có cấp là n . Chứng minh rằng $a^k = e$ khi và chỉ khi $n \mid k$.

1.1.3.9. Mệnh đề 2

Cho X và Y là những nhóm cyclic có cấp là m và n . Chứng minh rằng $X \times Y$ là nhóm cyclic khi và chỉ khi $(m, n) = 1$.

1.1.4. Nhóm con chuẩn tắc

1.1.4.1. Định nghĩa 11

Cho G là một nhóm và H là một nhóm con của G . Khi đó, các lớp trái của H trong G là các bộ phận có dạng $xH = \{y / y = xh, h \in H\}$ với $x \in G$. Tương tự, các lớp phải của H trong G là các bộ phận có dạng $Hx = \{y / y = hx, h \in H\}$.

1.1.4.2. Định nghĩa 12

Cho G là một nhóm với phép toán nhân, một nhóm con H của G được gọi là một nhóm con chuẩn tắc của G nếu $xH = Hx$, với mọi phần tử $x \in G$, kí hiệu $H \triangleleft G$.

1.1.4.3. Mệnh đề 3

Ắt có và đủ để một nhóm con H của G là nhóm con chuẩn tắc của G là $xhx^{-1} \in H$, với mọi $x \in G$ và với mọi $h \in H$.

1.1.4.4. Định lý 2 (Lagrange)

Cấp của một nhóm con H của một nhóm hữu hạn G chia hết cấp của G .

1.1.4.5. Hệ quả 2

Cấp của một phần tử tùy ý của nhóm hữu hạn G là ước cấp của G .

1.1.4.6. Hệ quả 3

Mọi nhóm hữu hạn có cấp nguyên tố đều là cyclic và được sinh ra bởi phần tử bất kì, khác phần tử trung lập, của nhóm.

1.1.4.7. Định nghĩa 13

Số các lớp trái (phải) của H trong G được gọi là chỉ số của H trong G , kí hiệu $[G:H]$.

1.1.4.8. Nhận xét 2

Nếu G là một nhóm hữu hạn thì $|G| = |H| \cdot [G:H]$.

1.1.5. Nhóm thương

1.1.5.1. Định nghĩa 14

Cho G là một nhóm và $H \triangleleft G$. Tập thương của G trên H là một tập hợp của tất cả các lớp trái của H trong G , kí hiệu G/H .

$$G/H = \{xH/x \in G\}.$$

1.1.5.2. Định lý 3

Nếu $H \triangleleft G$ thì

i) Quy tắc cho tương ứng cặp (xH, yH) với lớp trái xyH là một ánh xạ từ $G/H \times G/H$ đến G/H .

ii) G/H cùng với phép toán hai ngôi $(xH, yH) \mapsto xyH$

là một nhóm, gọi là nhóm thương của G trên H .

1.1.5.3. Mệnh đề 4

Mọi nhóm con và mọi nhóm thương của nhóm cyclic là nhóm cyclic.

1.1.6. Đồng cấu nhóm

1.1.6.1. Định nghĩa 15

Giả sử G và G' là các nhóm (với phép toán nhân). Một ánh xạ $\varphi: G \rightarrow G'$ được gọi là một đồng cấu nhóm nếu:

$$\varphi(xy) = \varphi(x)\varphi(y); \forall x, y \in G.$$

1.1.6.2. Mệnh đề 5

Cho X, Y là hai nhóm tùy ý, ánh xạ

$$f: X \rightarrow Y$$

$$x \mapsto e_Y \quad (e_Y \text{ là phần tử đơn vị của } Y)$$

là một đồng cấu.

Đồng cấu f được xác định như trên gọi là đồng cấu tầm thường.

1.1.6.2. Mệnh đề 6

Giả sử $\varphi: G \rightarrow G'$ là một đồng cấu nhóm. Khi đó:

i) φ chuyển đơn vị của G thành đơn vị của G' , tức là: $\varphi(1_G) = 1_{G'}$.

ii) φ chuyển nghịch đảo của phần tử $x \in G$ thành nghịch đảo của phần tử $\varphi(x) \in G'$, tức là: $\varphi(x^{-1}) = \varphi(x)^{-1}$.

1.1.6.3. Định nghĩa 16

i) Một đồng cấu nhóm đồng thời là một đơn ánh được gọi là một đơn cấu nhóm.

ii) Một đồng cấu nhóm đồng thời là một toàn ánh được gọi là một toàn cấu nhóm.

iii) Một đồng cấu nhóm đồng thời là một song ánh được gọi là một đẳng cấu nhóm.

1.1.6.4. Mệnh đề 7

Đồng cấu nhóm $\varphi: G \rightarrow G'$ là một toàn cấu nếu và chỉ nếu $\text{Im } \varphi = G'$. Nó là một đơn cấu nếu và chỉ nếu $\text{Ker } \varphi = \{1_G\}$, trong đó e là đơn vị của G .

1.1.6.5. Mệnh đề 8

Nếu $\varphi: G \rightarrow G'$ là một đồng cấu nhóm thì $\text{Ker } \varphi$ và $\text{Im } \varphi$ là các nhóm con tương ứng của G và G' . Tâm của G được định nghĩa:

$$Z(G) = \{a \in G : ax = xa, \forall x \in G\}.$$

Rõ ràng $e \in Z(G)$, hơn nữa G là một nhóm abel nếu và chỉ nếu $G = Z(G)$.

1.1.6.6. Mệnh đề 9

Giả sử G là một nhóm. Gọi $\text{Aut}(G)$ là tập hợp tất cả các đẳng cấu nhóm từ G vào chính nó. Khi đó, $\text{Aut}(G)$ là một nhóm đối với phép hợp thành các ánh xạ.

1.1.6.7. Định nghĩa 17

Nhóm $\text{Aut}(G)$ được xác định như trên gọi là nhóm các tự đẳng cấu của G .

1.1.7. Các định lý Sylow

1.1.7.1. Định lý 4

(i) Giả sử G là một nhóm hữu hạn và p là một số nguyên tố chia hết $|G|$. Khi đó, tồn tại một p -nhóm con Sylow của G .

(ii) Mọi p -nhóm con của G đều được chứa trong một p -nhóm con Sylow của G .

(iii) Bất kỳ hai p -nhóm con Sylow nào của một nhóm hữu hạn G đều liên hợp. Số các p -nhóm con Sylow phân biệt của G chia

hết cấp của G và bằng $1 + kp$, với k là một số nguyên không âm nào đó.

1.1.7.2. Bổ đề 2

Nếu nhóm G có duy nhất một p -nhóm con Sylow P , với $|P| = p^r$ thì $P \triangleleft G$.

1.1.8. Nhóm tâm hóa, nhóm chuẩn hóa

1.1.8.1. Mệnh đề 10

Cho A là một tập con của nhóm G . Khi đó

$$C_G(A) = \{c \in G : ca = ac, \forall a \in A\} \text{ là một nhóm con của } G.$$

1.1.8.2. Định nghĩa 18

Ta gọi $C_G(A)$ là nhóm con tâm hóa của A trong G .

1.1.8.3. Mệnh đề 11

Cho A là một tập con của nhóm G . Khi đó

$$N_G(A) = \{n \in G : nA = An\} \text{ là một nhóm con của } G.$$

1.1.8.4. Định nghĩa 18

Ta gọi $N_G(A)$ là nhóm con chuẩn hóa của A trong G .

1.1.8.5. Mệnh đề 12

Số liên hợp của nhóm con S của nhóm G bằng chỉ số của nhóm chuẩn hóa của S trong G .

1.1.8.6. Mệnh đề 13

$$C_G(A) \text{ là nhóm con chuẩn tắc của } N_G(A).$$

1.2. TÍCH TRỰC TIẾP, TÍCH NỬA TRỰC TIẾP

1.2.1. Tích trực tiếp

1.2.1.1. Mệnh đề 1

Cho H và K là các nhóm, khi đó tập tích Đề các

$$H \times K = \{(h, k) : h \in H, k \in K\}$$

cùng với phép toán •

$$(h_1, k_1) \bullet (h_2, k_2) = (h_1 h_2, k_1 k_2), \quad (h_1, k_1), (h_2, k_2) \in H \times K$$

là một nhóm.

1.2.1.2. Định nghĩa 1

Nhóm $H \times K$ được gọi là tích trực tiếp của hai nhóm H và K .

1.2.1.3. Mệnh đề 2

Nếu H và K là các nhóm hữu hạn thì $|H \times K| = |H||K|$.

H và K là các nhóm con chuẩn tắc của $H \times K$.

1.2.1.4. Mệnh đề 3

Cho G là nhóm, H và K là các nhóm con chuẩn tắc của G .

Khi đó: Nếu $H \cap K = \{1\}$ và $HK = G$ thì $G \cong H \times K$, với

$$HK = \{hk / h \in H, k \in K\}.$$

1.2.2. Tích nửa trực tiếp

1.2.2.1. Mệnh đề 4

Cho H và K là hai nhóm và φ là một đồng cấu từ K vào $\text{Aut}(H)$. Khi đó tập tích Đề các $H \times K = \{(h, k) / h \in H, k \in K\}$ cùng với phép toán

$$(h_1, k_1) \bullet (h_2, k_2) = (h_1 \varphi(k_1)(h_2), k_1 k_2), \quad (h_1, k_1), (h_2, k_2) \in H \times K$$

là một nhóm.

1.2.2.2. Định nghĩa 2

Nhóm $H \times K$ được xác định như trên gọi là tích nửa trực tiếp của H và K theo đồng cấu φ . Kí hiệu $H \rtimes_{\varphi} K$.

1.2.2.3. Mệnh đề 5

$H \rtimes_{\varphi} K = H \times K$ khi và chỉ khi φ là đồng cấu tầm thường.

1.2.2.4. Mệnh đề 6

Cho φ và φ' là liên hợp, tức là tồn tại $\alpha \in \text{Aut}(H)$ sao cho

$$\varphi'(k) = \alpha \circ \varphi(k) \circ \alpha^{-1}, \quad \forall k \in K.$$

Khi đó $H \rtimes_{\varphi} K \cong H \rtimes_{\varphi'} K$.

1.2.2.5. Mệnh đề 7

Nếu $\varphi = \varphi' \circ \alpha$ với $\alpha \in \text{Aut}(K)$ thì $H \rtimes_{\varphi} K \cong H \rtimes_{\varphi'} K$.

1.3. TÍNH CHẤT SỐ HỌC TRÊN TẬP CÁC SỐ NGUYÊN

1.3.1. Quan hệ chia hết trên tập các số nguyên

1.3.1.1. Định nghĩa 1

Cho $a, b \in \mathbb{Z}, b \neq 0$.

a được gọi là chia hết cho b , kí hiệu $a : b$, nếu $\exists q \in \mathbb{Z}$: $a = b.q$. Khi đó, ta còn nói a là bội của b hay b là ước của a hay b chia hết a và còn kí hiệu $b | a$.

Nếu a không chia hết cho b thì ta kí hiệu $a \nmid b$ hoặc $b \nmid a$.

1.3.1.2. Tính chất 1

1) $\forall a, b \in \mathbb{Z}, b \neq 0$. Nếu $b | a$ thì $\pm b | \pm a$.

2) $\forall a \in \mathbb{Z}^*, a | a$.

3) $\forall a \in \mathbb{Z}, \pm 1 | a$.

4) $\forall a \in \mathbb{Z}^*, a | 0$.

5) $\forall a, b \in \mathbb{Z}^*$. Nếu $b | a$ thì $|b| \leq |a|$.

6) $\forall a, b \in \mathbb{Z}^*$. Nếu $b | a$ và $a | b$ thì $a = b$ hoặc $a = -b$.

7) $\forall b \in \mathbb{Z}^*$. Nếu $b | 1$ thì $b = 1$ hoặc $b = -1$.

8) $\forall a, b \in \mathbb{Z}^*, c \in \mathbb{Z}$. Nếu $a | b$ và $b | c$ thì $a | c$.

9) $\forall a_1, a_2, \dots, a_n \in \mathbb{Z}, a_i : b \quad \forall i = \overline{1, n}$ thì

$$\forall x_1, x_2, \dots, x_n \in \mathbb{Z}, \sum_{i=1}^n a_i x_i : b.$$

Trong đó $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$.

1.3.1.3. Hệ quả 1

- i) $\forall a_1, a_2 \in \mathbf{Z}, b \in \mathbf{Z}^*$. Nếu $b \mid a_1$ và $b \mid (a_1 + a_2)$ thì $b \mid a_2$.
- ii) $\forall a_i \in \mathbf{Z}, i = \overline{1, n}; \forall b_i \in \mathbf{Z}^*, i = \overline{1, n}$ nếu $b_i \mid a_i, \forall i = \overline{1, n}$ thì $b_1 b_2 \dots b_n \mid a_1 a_2 \dots a_n$.
- iii) $\forall a, b, c \in \mathbf{Z}, b, c \neq 0$. Nếu $bc \mid ac$ thì $b \mid a$.

1.3.1.4. Định lý 1

$\forall a, b \in \mathbf{Z}, b \neq 0, \exists! (q, r) \in \mathbf{Z} \times \mathbf{Z}: a = bq + r$, với $0 \leq r < |b|$.

1.3.1.5. Định nghĩa 2 (Phép chia có dư)

Cho $a, b \in \mathbf{Z}, b \neq 0$, theo định lý trên, $\exists! (q, r) \in \mathbf{Z} \times \mathbf{Z}: a = bq + r$, với $0 \leq r < |b|$. Khi đó, q được gọi là số thương, r được gọi là số dư của phép chia a cho b .

1.3.2. Ước chung lớn nhất**1.3.2.1. Định nghĩa 3**

i) Cho $u \in \mathbf{Z}^*$ và $a_1, a_2, \dots, a_n \in \mathbf{Z}$. u được gọi là một ước chung của $a_1, a_2, \dots, a_n$ nếu $u \mid a_i, \forall i = \overline{1, n}$.

ii) Cho n số nguyên $a_1, a_2, \dots, a_n$. Ước chung lớn nhất của n số nguyên này, kí hiệu $(a_1, a_2, \dots, a_n)$ là số nguyên dương d thỏa hai điều kiện sau:

$$a) d \mid a_i, \forall i = \overline{1, n}$$

$$b) \text{ Nếu có số nguyên dương } d' \text{ mà } d' \mid a_i, \forall i = \overline{1, n}$$

thì $d' \mid d$.

Nói cách khác, $(a_1, a_2, \dots, a_n)$ là số nguyên dương d lớn nhất mà

$$d \mid a_i, \forall i = \overline{1, n}.$$

1.3.2.2. Định lý 2 (về sự tồn tại ước chung lớn nhất)

Giả sử $a_1, a_2, \dots, a_n$ là n số nguyên. Khi đó ước chung lớn nhất của n số nguyên đó tồn tại.

1.3.2.3. Định nghĩa 4

Ta nói hai số nguyên a, b là hai số nguyên tố cùng nhau nếu $(a, b) = 1$

1.3.2.4. Tính chất 2

1) Nếu $d = (a_1, a_2, \dots, a_n)$ thì $\exists x_1, x_2, \dots, x_n \in \mathbf{Z}$:

$$d = a_1 x_1 + a_2 x_2 + \dots + a_n x_n.$$

2) $(a_1, a_2, \dots, a_n) = 1 \Leftrightarrow \exists x_1, x_2, \dots, x_n \in \mathbf{Z}$:

$$a_1 x_1 + a_2 x_2 + \dots + a_n x_n = 1.$$

3) $\forall m \in \mathbf{Z}^+, (ma_1, ma_2, \dots, ma_n) = m(a_1, a_2, \dots, a_n)$.

4) Nếu $c \in \mathbf{Z}^+$ và $c \mid a_i, \forall i = \overline{1, n}$ thì

$$\frac{(a_1, a_2, \dots, a_n)}{c} = \left(\frac{a_1}{c}, \frac{a_2}{c}, \dots, \frac{a_n}{c} \right).$$

5) Giả sử d là ước chung của $a_1, a_2, \dots, a_n$. Khi đó

$$d = (a_1, a_2, \dots, a_n) \Leftrightarrow \left(\frac{a_1}{d}, \frac{a_2}{d}, \dots, \frac{a_n}{d} \right) = 1.$$

6) Cho $a, b, c \in \mathbf{Z}, b \neq 0$. Nếu $b \mid ac$ và $(a, b) = 1$ thì

$$b \mid c.$$

7) Cho $a, b, c \in \mathbf{Z}$. Nếu $(a, b) = 1$ thì $(ac, b) = (c, b)$.

8) $(a, b_1, b_2, \dots, b_n) = 1 \Leftrightarrow (a, b_i) = 1, \forall i = \overline{1, n}$.

9) $(a_1 a_2 \dots a_m, b_1 b_2 \dots b_n) = 1 \Leftrightarrow (a_i, b_j) = 1, \forall i = \overline{1, m}, \forall j = \overline{1, n}$.

10) Cho $b_1, b_2, \dots, b_n$ là n số nguyên nguyên tố cùng nhau từng đôi một, nếu $b_i \mid a, \forall i = \overline{1, n}$ thì $(b_1 b_2 \dots b_n) \mid a$.

11) $\forall a, b \in \mathbf{Z}, b \neq 0$. Nếu $a = bq + r$ thì $(a, b) = (b, r)$.

1.3.2.5. Thuật toán Euclide

Cho $a, b \in \mathbf{Z}, b \neq 0$. Kí hiệu q là thương, r là số dư của phép chia a cho b , khi đó, ta có: $a = bq + r$, với $0 \leq r < |b|$.

Nếu $r = 0$, ta dừng lại.

Nếu $r > 0$, ta chia b cho r và nhận được đẳng thức $b = rq_1 + r_1$, $0 \leq r_1 < r$.

Tiếp tục quá trình trên ta nhận được

$$a = bq + r, \quad 0 \leq r < b$$

$$b = rq_1 + r_1, \quad 0 \leq r_1 < r$$

$$r = r_1q_2 + r_2, \quad 0 \leq r_2 < r_1$$

.....

$$r_{k-2} = r_{k-1}q_k + r_k, \quad 0 \leq r_k < r_{k-1}$$

$$r_{k-1} = r_kq_{k+1}$$

Khi đó $r_k = (a, b)$.

1.3.3. Số nguyên tố

1.3.3.1. Định nghĩa 5

Một số nguyên lớn hơn 1, không có ước nguyên dương nào khác 1 và bản thân nó được gọi là một số nguyên tố.

Một số nguyên lớn hơn 1, không phải là số nguyên tố được gọi là hợp số.

1.3.3.2. Định lý 3

Ước nhỏ nhất lớn hơn 1 của một số tự nhiên lớn hơn 1 là một số nguyên tố.

1.3.3.3. Định lý 4 (định lý cơ bản của số học)

Cho n là số tự nhiên lớn hơn 1. Khi đó, n luôn có thể biểu diễn một cách duy nhất dưới dạng $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, trong đó $k, \alpha_i, i = \overline{1, k}$ là các số nguyên dương; $p_i, i = \overline{1, k}$ là các số nguyên tố thoả mãn $1 < p_1 < p_2 < \dots < p_k$.

Dạng phân tích ở trên được gọi là dạng khai triển chính tắc của số n .

1.3.4. Đồng dư

1.3.4.1. Định nghĩa 6

Cho $a, b \in \mathbf{Z}$ và m là một số nguyên dương. Ta nói a đồng dư b theo môđulo m , kí hiệu $a \equiv b \pmod{m}$, khi và chỉ khi $(a - b) : m$.

1.3.4.2. Tính chất 3 (tính chất cơ bản)

i) Nếu $a \equiv b \pmod{m}$ và $c \equiv d \pmod{m}$ thì:

$$a + c \equiv b + d \pmod{m} \text{ và } ac \equiv bd \pmod{m}.$$

ii) Nếu p là số nguyên tố và $ab \equiv 0 \pmod{p}$ thì

$$a \equiv 0 \pmod{p} \text{ hoặc } b \equiv 0 \pmod{p}.$$

1.3.5. Hệ thặng dư đầy đủ, hệ thặng dư thu gọn

1.3.5.1. Định nghĩa 7

Cho m là một số nguyên dương. Tập hợp H gồm những số nguyên lấy ra ở mỗi lớp thặng dư của $\mathbf{Z}_m$ một và chỉ một số được gọi là một hệ thặng dư đầy đủ môđun m . Viết tắt là hệ TĐĐ mod m .

1.3.5.2. Định nghĩa 8

Cho m là một số nguyên dương. Tập hợp K gồm những số nguyên lấy ra ở mỗi lớp khả nghịch của $\mathbf{Z}_m$ một và chỉ một số được

gọi là một hệ thặng dư thu gọn môđun m . Viết tắt là hệ TDTG mod m .

1.3.6. Hàm Euler

1.3.6.1. Định nghĩa 9

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 .

1.3.6.2. Định lý 5

Với hai số tự nhiên khác không m_1 và m_2 nguyên tố cùng nhau, ta có $\Phi(m_1 m_2) = \Phi(m_1) \Phi(m_2)$.

1.3.6.3. Định lý Euler.

Nếu a, m là số nguyên dương và $(a, m) = 1$ thì

$$a^{\Phi(m)} \equiv 1 \pmod{m}.$$

1.3.6.4. Công thức tính $\Phi(m)$.

i) Nếu $m = 1$ thì $\Phi(m) = 1$.

ii) Nếu $m = p^\alpha$, trong đó p là một số nguyên tố và α là một số tự nhiên khác 0 thì $\Phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right)$.

iii) Nếu $m > 1$ và $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ là dạng khai triển chính tắc. Khi đó

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

1.3.7. Số nguyên không có nhân tử chính phương (square-free)

1.3.7.1. Định nghĩa 10

Một số nguyên dương n được gọi là số nguyên không có nhân tử chính phương nếu trong tất cả các thừa số nguyên tố của n không có thừa số nào xuất hiện quá một lần. Nghĩa là n có khai triển chính tắc $n = p_1 p_2 \dots p_k$, với $p_i \neq p_j$.

1.3.7.2. Hệ quả 2

i) Tất cả các số nguyên tố đều là số nguyên không có nhân tử chính phương.

ii) Nếu m là số nguyên không có nhân tử chính phương, tức là $m = p_1 p_2 \dots p_k$ thì $\Phi(m) = (p_1 - 1)(p_2 - 1) \dots (p_k - 1)$.

Chương 2

TÍNH DUY NHẤT CỦA NHÓM CẤP n

Chương này là nội dung chính của luận văn, sẽ xác định các số nguyên dương n để có duy nhất một nhóm cấp n (sai khác một đẳng cấu).

Phần cuối chương sẽ xác định một số trường hợp của số nguyên dương n để chỉ có hai nhóm cấp n không đẳng cấu nhau.

2.1. TÍNH DUY NHẤT CỦA NHÓM CẤP n

2.1.1. Mệnh đề 1

Giả sử H là một nhóm con riêng của nhóm G , và S là một tập con hữu hạn của G sao cho $G = \langle H, S \rangle$.

Khi đó tồn tại một nhóm con cực đại của G mà chứa H . Đặc biệt, mọi nhóm hữu hạn sinh đều có nhóm con cực đại.

2.1.2. Bổ đề 1

Cho G là một nhóm, $H \leq G$, $|H| < \infty$.

i) Khi đó, các liên hợp của H đều là nhóm con của G và H đẳng cấu với liên hợp của nó.

ii) Nếu H là nhóm con cực đại của G thì liên hợp của nó cũng là nhóm con cực đại của G .

2.1.3. Mệnh đề 2

i) Nhóm các tự đẳng cấu của một nhóm cyclic cấp n có cấp bằng $\Phi(n)$, với Φ là hàm Euler.

ii) Nhóm các tự đẳng cấu của nhóm cyclic cấp p , với p là một số nguyên tố, là một nhóm cyclic có cấp $p - 1$.

2.1.4. Bổ đề 2

Mọi nhóm G cấp pq (trong đó $p < q$ là các số nguyên tố) hoặc là nhóm cyclic, hoặc là nhóm không abel với một q -nhóm con Sylow chuẩn tắc. Trường hợp sau xảy ra khi và chỉ khi $q - 1$ chia hết cho p .

2.1.5. Bổ đề 3

Cho G là một nhóm và H là một nhóm con chuẩn tắc của G sao cho $H \subset Z(G)$. Khi đó, nếu G/H là nhóm cyclic thì G là nhóm abel.

2.1.6. Định lý 1

Mọi nhóm cyclic có cấp vô hạn đều đẳng cấu với nhóm cộng các số nguyên $\mathbb{Z}$. Mọi nhóm cyclic hữu hạn cấp s đều đẳng cấu với nhóm cộng $\mathbb{Z}_s$ các lớp thặng dư theo mô đun s .

2.1.7. Hệ quả 1

Với mọi số nguyên dương n đều tồn tại duy nhất nhóm cyclic $C(n)$ cấp n .

2.1.8. Mệnh đề 3

Giả sử n là số nguyên dương có nhân tử chính phương, tức là $n = mp^a$, trong đó p là số nguyên tố không chia hết m , a là số tự nhiên, $a \geq 2$.

Khi đó:

i) $(n, \Phi(n)) \geq p$

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

2.1.9. Mệnh đề 4

Nếu G là một nhóm abel hữu hạn và p là một số nguyên tố chia hết cấp của G thì G có một phần tử cấp p .

2.1.10. Định lý 2

Giả sử n là một số nguyên dương sao cho có duy nhất một nhóm cấp n . Khi đó $(n, \Phi(n)) = 1$, với Φ là hàm Euler.

2.1.11. Bổ đề 4

Ta có $(m, \Phi(m)) = 1$, với mọi số nguyên dương m là ước của n .

2.1.12. Bổ đề 5

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 $Z(G)$ của nhóm G là tầm thường.

2.1.13. Bổ đề 6

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.

2.1.14. Bổ đề 7

Bất kỳ nhóm con cực đại U nào của G đều bằng chính 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.

Định lý sau là kết quả chính của luận văn:

2.1.15. Định lý 3

Cho n là một số nguyên dương. Điều kiện cần và đủ để có duy nhất một nhóm cấp n là $(n, \Phi(n)) = 1$.

2.1.16. Hệ quả 2

Các số nguyên dương $n \leq 100$, sao cho có duy nhất một nhóm cấp n là :

1, 2, 3, 5, 7, 11, 13, 15, 17, 19, 23, 29, 31, 33, 35, 37, 41, 43, 47, 51, 53, 55, 57, 59, 61, 65, 67, 69, 71, 73, 77, 79, 83, 85, 87, 89, 91, 93, 95, 97.

2.2. MỘT SỐ TRƯỜNG HỢP CỦA n ĐỂ CÓ ĐÚNG HAI NHÓM CẤP n

Trong phần này, chúng tôi sẽ khảo sát một số trường hợp của số nguyên dương n , để chỉ có đúng hai nhóm cấp n không đẳng cấu nhau.

2.2.1. Hệ quả 1

Nếu N là một nhóm con chuẩn tắc của G và L là một nhóm con của G/N thì G có một nhóm con H chứa N và $L = H/N$. Nếu L là một nhóm con chuẩn tắc của G/N thì H là nhóm con chuẩn tắc của G . Ngoài ra, nếu $H_1/N = H/N$, với H_1 và H đều là các nhóm con chứa N của G thì $H_1 = H$.

2.2.2. Định lý 1

Nếu $G \neq \{1_G\}$ và G là p -nhóm hữu hạn thì $Z(G)$ có cấp khác 1.

2.2.3. Hệ quả 2

Cho G là một nhóm có cấp p^r ($r \geq 1$). Khi đó G chứa 1 nhóm con chuẩn tắc có cấp p^{r-1} .

2.2.4. Mệnh đề 1

Cho p là số nguyên tố. Khi đó, mọi nhóm có cấp p^2 đều là nhóm abel.

2.2.5. Mệnh đề 2

Cho p là số nguyên tố lớn hơn 1. Khi đó nhóm cyclic $C(p^2)$ có cấp p^2 không đẳng cấu với nhóm $C(p) \times C(p)$.

2.2.6. Mệnh đề 3

Có hai nhóm không đẳng cấu nhau có cấp p^2 .

2.2.7. Định nghĩa

Xét đa giác đều n cạnh P_n với $n > 2$. Gọi a là phép quay mặt phẳng xung quanh tâm của P_n một góc có hướng bằng $\frac{2\pi}{n}$, còn b là phép đối xứng qua một đường thẳng đi qua tâm của P_n và một đỉnh của nó. Khi đó, tất cả các phép đối xứng của P_n được liệt kê như sau: $e, a, a^2, \dots, a^{n-1}, b, ab, \dots, a^{n-1}b$.

Chúng ta lập thành một nhóm, kí hiệu D_n được gọi là nhóm dihedral cấp $2n$. Như thế D_n có thể biểu thị như sau

$$D_n = \langle a, b \mid a^n = e, b^2 = e, (ab)^2 = e \rangle.$$

2.2.8. Bổ đề 1

Giả sử G là nhóm cấp $2p$, với p là số nguyên tố lẻ. Khi đó G có đúng một nhóm con K cấp p và hoặc G

- i) có đúng một nhóm con H cấp 2, hoặc
- ii) G có đúng p nhóm con cấp 2.

2.2.9. Bổ đề 2

Cho G là một nhóm cấp $2p$, với p là số nguyên tố lẻ. Nếu G có duy nhất một nhóm con cấp 2 thì G là nhóm cyclic cấp $2p$.

2.2.10. Bổ đề 3

Giả sử G là một nhóm cấp $2p$, với p là một số nguyên tố lẻ. Nếu G có đúng p nhóm con cấp 2 thì G đẳng cấu với nhóm D_p .

2.2.11. Định lý 2

Với mỗi số nguyên tố lẻ p có đúng hai nhóm có cấp $2p$ không đẳng cấu nhau một nhóm cyclic $C(2p)$ và một nhóm D_p .

KẾT LUẬN

Với mục tiêu đã được đặt ra, luận văn "**TÍNH DUY NHẤT CỦA NHÓM CẤP n** " đã thực hiện được các vấn đề sau:

- Thông qua hàm Euler và các tính chất của nó, luận văn đã xác định được các số nguyên dương n sao cho có duy nhất một nhóm cấp n (sai khác một đẳng cấu).
- Xác định một số trường hợp của số nguyên dương n để chỉ có hai nhóm cấp n không đẳng cấu nhau.

Hy vọng nội dung của luận văn sẽ tiếp tục được phát triển, hoàn thiện và mở rộng nhiều hơn nữa.