BỘ GIÁO DỤC VÀ ĐÀO TẠO
ĐẠI HỌC ĐÀ NẴNG

GIAO THỊ KIM ĐÔNG

ĐỊNH LÝ CƠ BẢN CỦA NHÓM HỮU HẠN

Chuyên nghành: PHƯƠNG PHÁP TOÁN SƠ CẤP
Mã số: 60.46.36

TÓM TẮT LUẬN VĂN THẠC SỸ KHOA HỌC

ĐÀ NẴNG- NĂM 2011

Công trình được hoàn thành tại

ĐẠI HỌC ĐÀ NẴNG

– – – – – – – – – –

Người hướng dẫn khoa học: PGS.TS. NGUYỄN GIA ĐỊNH

Phản biện 1: TS. NGUYỄN NGỌC CHÂU:

Phản biện 2: PGS. TS TRẦN ĐẠO DÕNG:

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 22 tháng 10 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

Với những gì khảo sát được, luận văn sẽ là một tài liệu tham khảo hữu ích cho bản thân khi tiếp tục đi sâu nghiên cứu sau này và hy vọng cũng là nguồn tư liệu tốt cho những ai quan tâm nghiên cứu về lý thuyết nhóm.

MỞ ĐẦU

1. Lý do chọn đề tài.

Việc giải các phương trình đại số là một vấn đề kinh điển của toán học. Người ta đã tìm thấy những bảng đất sét thời Babylon cách đây gần 4000 năm trong đó có ghi những bài toán mẫu giải phương trình bậc hai. Nhưng mãi đến thế kỷ thứ 16, Tartaglia, Cardano và Ferrari mới tìm được công thức tính nghiệm cho các phương trình bậc 3, 4. Các công thức này đều là các biểu thức chỉ chứa các căn thức. Từ đây nảy sinh vấn đề liệu có tồn tại các công thức tính nghiệm tương tự cho các phương trình đại số bậc ≥ 5 hay không. Đến đầu thế kỷ thứ 19, Abel chỉ ra rằng không thể tìm thấy một công thức tổng quát như vậy. Ngay sau đó, Galois đưa ra tiêu chuẩn để một phương trình đại số có nghiệm là các biểu thức chứa căn thức. Phương pháp xét nghiệm tổng quát của ông được gọi là lý thuyết Galois và nó liên quan đến *"nhóm giải được"*. Trong toán học và đại số trừu tượng, một nhóm hữu hạn là một nhóm mà tập nền của nó có hữu hạn phần tử. Trong suốt thế kỷ 20, các nhà toán học nghiên cứu rất sâu một số hướng của lý thuyết nhóm hữu hạn, đặc biệt là phân tích địa phương nhóm hữu hạn và lý thuyết nhóm giải được, nhóm lũy linh. Việc xác định đầy đủ cấu trúc của tất cả các nhóm hữu hạn là quá nhiều để biết được, số các cấu trúc có thể sớm trở nên tràn ngập. Tuy nhiên, việc phân loại đầy đủ các nhóm đơn hữu hạn đã hoàn thành, nghĩa là các "khối xây" mà từ đó tất cả các nhóm hữu hạn có thể được dựng thành bấy giờ đã được biết đến, vì mỗi nhóm hữu hạn có một dãy hợp thành. Xuất phát từ nhu cầu phát triển của lý thuyết nhóm và những ứng dụng của nó, chúng tôi quyết định chọn đề tài với tên gọi: *Các định lý cơ bản của nhóm hữu hạn* để tiến hành nghiên cứu.

2. Mục tiêu và nhiệm vụ.

Luận văn tập trung nghiên cứu những kết quả từ một số công trình nghiên cứu về lý thuyết nhóm của các nhà khoa học thông qua việc tổng hợp, chọn lọc và cô

đọng những nội dung: Các định lý về p-nhóm, các định lý Sylow và ứng dụng cho việc xác định các nhóm có cấp thấp.

Hiểu được các vấn đề quan trọng trong nhóm giải được, dãy hợp thành và nhóm đơn.

Nhiệm vụ của luận văn là việc chứng minh chi tiết những nội dung, từ đó giới thiệu các ví dụ minh họa cụ thể để làm sáng tỏ vấn đề cần nghiên cứu và hệ thống một cách đầy đủ các định lý cơ bản và quan trọng của lý thuyết nhóm hữu hạn.

3. Đối tượng và phạm vi nghiên cứu.

Luận văn tập trung nghiên cứu một số vấn đề sau:

- Tổng quan và hệ thống một cách đầy đủ các định lý cơ bản và quan trọng của lý thuyết p-nhóm.

- Tìm hiểu các khái niệm và kết quả về nhóm con Frattini của một p-nhóm.

- Trình bày một cách đầy đủ và chi tiết Định lý Sylow, một bộ phận cực kỳ quan trọng của lý thuyết nhóm hữu hạn, và các kết quả dẫn xuất. Định lý Sylow suy rộng và nghiên cứu thông qua tác động của một nhóm lên một nhóm bằng nhóm các toán tử.

- Nghiên cứu ứng dụng Định lý Sylow, phân loại đẳng cấu các nhóm có cấp từ 1 đến 15.

- Nghiên cứu nhóm giải được, một vấn đề quan trọng trong lý thuyết nhóm hữu hạn và lý thuyết Galois.

- Nghiên cứu một vấn đề liên quan mật thiết với nhóm giải được là dãy hợp thành và Định lý Jordan Hölder.

- Cuối cùng là khảo sát tính đơn của nhóm thay phiên A_n với $n \geq 5$ từ đó suy ra được nhóm đối xứng S_n là giải được, nhóm dẫn xuất $D(A_n) = A_n$, tâm $Z(A_n)$ là nhóm đơn vị và ba nhóm con chuẩn tắc duy nhất của S_n là $S_n, A_n, \{\iota\}$, với $n \geq 5$.

4. Phương pháp nghiên cứu.

Thu thập các bài báo khoa học của các tác giả nghiên cứu liên quan đến Lý thuyết nhóm hữu hạn.

Tham gia các buổi xêmina hằng tuần để trao đổi các kết quả đang nghiên cứu.

5. Ý nghĩa khoa học và thực tiễn của đề tài.

Tổng quan các kết quả của các tác giả đã nghiên cứu liên quan đến các định lý cơ bản của nhóm hữu hạn nhằm xây dựng một tài liệu tham khảo cho những ai muốn nghiên cứu lý thuyết nhóm hữu hạn.

KẾT LUẬN

Qua một thời gian tìm hiểu, tiếp cận và nghiên cứu về lý thuyết nhóm , luận văn đã hoàn thành và đạt được mục tiêu nghiên cứu đề tài với những kết quả cụ thể sau:

- *Tổng quan và hệ thống một cách đầy đủ các định lý cơ bản và quan trọng của lý thuyết p-nhóm. Các kết quả này dựa vào các định lý cổ điển của lý thuyết nhóm như Định lý Lagrange, Định lý Đối ứng, các định lý đẳng cấu, ... và các vấn đề liên quan đến tác động của một nhóm lên một tập hợp. Từ đó, tìm hiểu các khái niệm và kết quả về nhóm con Frattini của một p-nhóm.*

- *Trình bày một cách đầy đủ và chi tiết Định lý Sylow, một bộ phận cực kỳ quan trọng của lý thuyết nhóm hữu hạn, và các kết quả dẫn xuất. Định lý Sylow suy rộng cũng được tìm hiểu và nghiên cứu thông qua tác động của một nhóm lên một nhóm bằng nhóm các toán tử.*

- *Ứng dụng Định lý Sylow, phân loại đẳng cấu các nhóm có cấp từ 1 đến 15.*

- *Nhóm giải được, một vấn đề quan trọng trong lý thuyết nhóm hữu hạn và lý thuyết Galois, được tìm hiểu thông qua các định lý cơ bản và cốt yếu. Một vấn đề liên quan mật thiết với nhóm giải được là dãy hợp thành và Định lý Jordan Hölder cũng được nghiên cứu do tính quan trọng của chúng trong lý thuyết nhóm.*

- *Cuối cùng là khảo sát tính đơn của nhóm thay phiên A_n với $n \geq 5$ từ đó suy ra được nhóm đối xứng S_n là giải được, nhóm dẫn xuất $D(A_n) = A_n$, tâm $Z(A_n)$ là nhóm đơn vị và ba nhóm con chuẩn tắc duy nhất của S_n là $S_n, A_n, \{\iota\}$, với $n \geq 5$*

$$i \mapsto i, i \in \{1, 2, ..., n\} \{a_1, a_2, ..., a_m\}.$$

Ta gọi một hoán vị như thế là một chu trình độ dài m hay một m-chu trình. Tập hợp $(a_1, a_2, ..., a_m)$ được gọi là tập nền của nó. Ta quy ước chu trình độ dài 1 là phần tử đơn vị. Một chu trình độ dài 2 được gọi là một chuyển vị. Nghịch đảo của chu trình $\alpha = (a_1, ..., a_{m-1}, a_m)$ là chu trình $\beta = (a_m, a_{m-1}, ..., a_1)$. Rõ ràng rằng không phải mọi hoán vị đều là chu trình và tích của hai chu trình không nhất thiết là một chu trình; chẳng hạn, trong $S_4, (1,2)(3,4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ không là một chu trình.

Mệnh đề 3.5. *Mọi phần tử của S_n có thể được viết thành tích của các chu trình rời nhau.*

Mệnh đề 3.6. *Mỗi chu trình là tích của những chuyển vị.*

Bổ đề 3.2. *Cho $\theta \in S_n$ và $(a_1, ..., a_m)$ là một chu trình. Khi đó*

$$\theta^{-1}(a_1, ..., a_m)\theta = (a_1\theta, ..., a_m\theta).$$

Mệnh đề 3.7. *Mọi chuyển vị đều là hoán vị lẻ. Nếu θ là một hoán vị chẵn (tương ứng lẻ) và được viết thành tích của những chuyển vị thì số chuyển vị là chẵn (tương ứng lẻ).*

Bổ đề 3.3. *Mỗi phần tử của A_n là tích của những 3-chu trình, với $n \geq 5$.*

Bổ đề 3.4. *Cho $H \lhd A_n$. Nếu H chứa một 3-chu trình thì $H = A_n$.*

Bổ đề 3.5. *Cho $H \lhd A_n$. Nếu H chứa tích hai chuyển vị rời nhau thì $H = A_n$.*

Định lí 3.7. *A_n là nhóm đơn với $n \geq 5$.*

Hệ quả 3.2. *Nhóm đối xứng S_n là không giải được với ≥ 5.*

Hệ quả 3.3. *Nếu $G = A_n$ thì nhóm dẫn xuất G' của G là G và tâm $Z(G)$ là nhóm đơn vị $\{\iota\}$.*

Bổ đề 3.6. *Nhóm đối xứng S_n có tâm $Z(S_n) = \{\iota\}$ với $n \geq 3$.*

Mệnh đề 3.8. *Nhóm đối xứng S_n chỉ có ba nhóm con chuẩn tắc là A_n, S_n và $\{\iota\}$ với $n \geq 5$.*

Chứng minh chi tiết và làm rõ một số mệnh đề, cũng như đưa ra một số ví dụ minh hoạ đặc sắc nhằm làm cho người đọc dễ dàng tiếp cận vấn đề được đề cập.

6. Cấu trúc của luận văn.

Ngoài phần mở đầu, kết luận và tài liệu tham khảo, luận văn được chia thành ba chương.

Chương 1: Trình bày khái niệm và kết quả về tác động của nhóm lên một tập hợp. Tiếp đến, giới thiệu phần quan trọng của chương này là các định lý về p-nhóm. Ngoài ra, nhóm con Frattini của một p-nhóm cũng được đề cập đến.

Chương 2: Trình bày các định lý Sylow cùng các hệ quả của chúng. Đồng thời, các định lý Sylow suy rộng cũng được giới thiệu thông qua tác động của một nhóm lên một nhóm bằng nhóm các toán tử. Vào cuối chương là sự phân loại các nhóm cấp thấp ≤ 15 qua phép đẳng cấu.

Chương 3: Trình bày các kết quả về nhóm giải được, một khái niệm rất quan trọng trong lý thuyết nhóm hữu hạn và lý thuyết Galois. Một khái niệm liên quan cùng với định lý nổi tiếng Jordan-Hölder được đề cập đến. Cuối cùng là tính đơn của nhóm thay phiên A_n với $n \geq 5$ là các hệ quả quan trọng của nó được trình bày.

Chương 1

ĐỊNH LÝ VỀ p-NHÓM

Các khái niệm và kết quả trong chương này có thể tìm thấy trong các tài liệu [1], [5], [6], [9].

1.1 NHÓM HOÁN VỊ VÀ G-TẬP HỢP.

Định nghĩa 1.1. *Cho X là một tập hợp. Một song ánh từ X lên X được gọi là một hoán vị trên X. Ký hiệu $\sum(X)$ là tập hợp tất cả các hoán vị trên X.*

Mệnh đề 1.1. *Cho θ là một song ánh từ tập X lên tập Y. Với một hoán vị p trên X, ta định nghĩa ánh xạ $\theta(p)$ trên Y bởi công thức:*

$$\theta(p)(y) = \theta(p(\theta^{-1}(y))), y \in Y.$$

Khi đó, $\theta(p)$ là một hoán vị trên Y. Ngoài ra, ánh xạ $\theta : p \mapsto \theta(p)$ là một đẳng cấu từ nhóm đối xứng $\sum(X)$ lên nhóm đối xứng $\sum(Y)$.

Định nghĩa 1.2. *Cho X là một tập hợp và $\sum(X)$ là nhóm đối xứng trên X. Một nhóm con bất kỳ của $\sum(X)$ được gọi là nhóm hoán vị trên X.*

Mệnh đề 1.2. *(Định lý Cayley). Cho G là một nhóm. Khi đó tồn tại một tập X sao cho G đẳng cấu với một nhóm hoán vị trên X.*

Hệ quả 1.1. *Với số tự nhiên bất kỳ n, số các lớp đẳng cấu của các nhóm có cấp n là hữu hạn.*

Định nghĩa 1.3. *Cho G là một nhóm. Một G-tập hợp là một cặp (X,ρ) gồm một tập X và một đồng cấu ρ từ G vào nhóm đối xứng $\sum(X)$ trên X.*

Định lí 3.5. *Một nhóm G là giải được khi và chỉ khi dãy dẫn xuất đạt đến $\{1\}$ sau một số hữu hạn bước; tức là , $G^{(n)} = \{1\}$ với một số nguyên n nào đó.*

Bổ đề 3.1. *Nếu H là một nhóm con của nhóm G thì với số nguyên dương k tùy ý ta có $H^{(k)} \subset G^{(k)}$.*

3.2 DÃY HỢP THÀNH VÀ ĐỊNH LÝ JORDAN-HÖLDER.

Định nghĩa 3.3. *Cho G là một nhóm. Nếu một dãy hữu hạn các nhóm con của G*

$$(\mathcal{G}) : G_0 = G \supset G_1 \supset G_2 \supset \cdots \supset G_r = \{1\} \tag{3.3}$$

thỏa mãn tính chất với mỗi $i = 1, 2, ..., r$, G_i là nhóm con chuẩn tắc cực đại của G_{i-1}, ta nói $(\mathcal{G})$ là một dãy hợp thành độ dài r của G. Tập các nhóm thương

$$\{G_0/G_1, G_1/G_2, ..., G_{r-1}/G_r\}$$

được gọi là tập các nhân tử hợp thành và mỗi nhân tử hợp thành là một nhóm đơn.

Mệnh đề 3.3. *Mọi nhóm hữu hạn đều có dãy hợp thành.*

Định lí 3.6. *(Jordan-Hölder). Cho G là một nhóm có dãy hợp thành*

$$(\mathcal{G}) : G_0 = G \supset G_1 \supset G_2 \supset \cdots \supset G_r = \{1\}.$$

Cho $(\mathcal{H}) : H_0 = G \supset H_1 \supset H_2 \supset \cdots \supset H_s = \{1\}$ là một dãy hợp thành bất kỳ của G. Khi đó độ dài của $(\mathcal{H})$ bằng độ dài của $(\mathcal{G})$; nghĩa là, $r = s$. Hơn nữa, có một tương ứng một-một giữa các nhân tử hợp thành của $(\mathcal{G})$ và các nhân tử hợp thành của $(\mathcal{H})$ sao cho các nhóm tương ứng là đẳng cấu với nhau.

Mệnh đề 3.4. *Cho G là một nhóm với dãy hợp thành $(\mathcal{G})$ độ dài r và cho H_1 là một nhóm con chuẩn tắc cực đại bất kỳ của G. Khi đó G có một dãy hợp thành mà thành phần đầu tiên của nó là H_1 và một dãy hợp thành bất kỳ $(\mathcal{H})$ của G với thành phần đầu tiên H_1 là tương đương với $(\mathcal{G})$.*

3.3 TÍNH ĐƠN CỦA NHÓM THAY PHIÊN A_n, $n \geq 5$.

Định nghĩa 3.4. *Nếu $a_1, ..., a_m$ là các số nguyên phân biệt trong tập $\{1, 2, ..., n\}$, ký hiệu $(a_1, a_2, ..., a_m)$ là hoán vị (phép thế) trong nhóm đối xứng S_n xác định bởi*

$$a_1 \mapsto a_2, a_2 \mapsto a_3, ..., a_{m-1} \mapsto a_m, a_m \mapsto a_1,$$

Hệ quả 3.1. *Nếu G là nhóm Aben hữu hạn thì G giải được.*

Định lí 3.3. *G là nhóm giải được khi và chỉ khi G là hữu hạn và có một dãy chuẩn tắc con*

$$\{1\} = K_0 \subset K_1 \cdot \cdot \subset K_n = G \tag{3.2}$$

trong đó K_{i+1}/K_i là Aben $(i = 0, 1, 2, ..., n-1)$

Định lí 3.4. *Cho G là một nhóm giải được. Khi đó,*

(i) Một nhóm con bất kỳ của G là giải được và

(ii) $N \lhd G$ thì G/N là giải được.

Mệnh đề 3.1. *Mọi nhóm G có cấp p^2, pq hoặc p^2q, trong đó p và q là hai số nguyên tố khác nhau, là giải được.*

Định nghĩa 3.2. *Cho x và y là hai phần tử của nhóm G. Phần tử dạng $x^{-1}y^{-1}xy$ được gọi là giao hoán của x và y, ta viết $[x, y] = x^{-1}y^{-1}xy$. Nhóm con của G sinh bởi mọi giao hoán tử xác định trong G được gọi là nhóm dẫn xuất hay nhóm giao hoán tử, ký hiệu là G',$G^{(1)}$ hoặc $D(G)$. Nhóm con giao hoán tử của nhóm con giao hoán tử, nghĩa là $D(G')$, được gọi là nhóm dẫn xuất thứ hai và được ký hiệu G'',$G^{(2)}$ hoặc $D^2(G)$.*

Tổng quát, nhóm con giao hoán tử của $G^{(i)}$ được viết là $G^{(i+1)}$ và dãy các nhóm con

$$G = G^{(0)}, G^{(1)}, G^{(2)}, ..., G^{(i)}, ...$$

được gọi là dãy dẫn xuất. Ta viết $G^{\infty} = \sum_{i=0}^{\infty} G^{(i)}$, nếu G hữu hạn, ta có $G^{(\infty)} = G^{(n)}$ với số nguyên n nào đó.

Các tính chất sau đây của giao hoán tử là dễ dàng thấy được:

1) $[x, y] = 1 \Leftrightarrow x$ và y là giao hoán.

2) $[x, y] = x^{-1}y^y = (y^{-1})^x y$.

3) $f([x, y]) = [f(x), f(y)$, với f là một đồng cấu.

4) $f(D(G)) = D(f(G))$, với f là một đồng cấu từ G vào H.

5) Cho N là một nhóm con chuẩn tắc của nhóm G và $\overline{G} = G/N$. Gọi H là nhóm con của của G tương ứng với nhóm dẫn xuất $D(\overline{G})$, tức là $H/N = D(\overline{G})$. Khi đó ta có

$$H = ND(\overline{G}).$$

Mệnh đề 3.2. *Cho D là nhóm dẫn xuất của nhóm G. Khi đó, nhóm thương G/D là Aben. Nếu nhóm thương G/H bởi nhóm chuẩn tắc H là aben thì H chứa D. Vì vậy, D là nhóm con chuẩn tắc nhỏ nhất có tính chất nhóm thương là aben.*

Định nghĩa 1.4. *Cho X là một G-tập. Tập hợp*

$$\{(x)^g | g \in G\}$$

được gọi là một quỹ đạo chứa $x \in X$, ta viết là O_x (hay $O(x)$). Số phần tử trong O_x,$|O_x|$ được gọi là độ dài của quỹ đạo O_x. Một tập con Y của X được gọi là G-bất biến nếu với mọi $g \in G$

$$y \in Y \Rightarrow y^g \in Y.$$

Mệnh đề 1.3. *Cho X là một G-tập và O_x là quỹ đạo chứa phần tử x của X.*

(i) Nếu $y \in O_x$, ta có $O_y = O_x$.

(ii) Nếu O là một quỹ đạo khác O_x thì $O \cap O_x = \emptyset$.

(iii) Một tập con khác rỗng của X là một quỹ đạo khi và chỉ khi nó là một tập con G-bất biến cực tiểu.

(iv) Một tập con G-bất biến bất kỳ của X là hợp rời rạc của các quỹ đạo.

Mệnh đề 1.4. *Cho X là một G-tập, $O = O_x$ là một quỹ đạo chứa phần tử x của X và H là tập con của G xác định bởi: $H = \{g \in G | x^g = x\}$.*

(i) H là một nhóm con của G.

(ii) Tồn tại một song ánh φ từ tập O lên tập các lớp kề phải của H thỏa mãn:

$$\varphi(y^g) = \varphi(y)g, \forall y \in X, \forall g \in G$$

(iii) Nếu O là một tập hữu hạn, ta có $|O| = [G : H]$. Nếu G là một nhóm hữu hạn thì độ dài của một quỹ đạo là ước cấp $|G|$ của G.

Định nghĩa 1.5. *Nhóm con H xác định trong Mệnh đề 1.4 được gọi là nhóm con ổn định của x, ký hiệu $H = S_G(x)$.*

Với $x \in X, g, h \in G, (x^g)^h = x^g \Leftrightarrow x^{ghg^{-1}} = x \Leftrightarrow ghg^{-1} \in S_G(x) \Leftrightarrow h \in S_G(x)^g$. Do đó $S_G(x^g) = S_G(x)^g$.

Mệnh đề 1.5. *Cho X là một G-tập hữu hạn. Khi đó X là hợp rời của các quỹ đạo $O_1, O_2, ..., O_m$:*

$$X = O_1 \cup O_2 \cup ... \cup O_m, (O_i \cap O_j = \emptyset, (i \neq j)).$$

Nếu x_i là phần tử của O_i với $i = 1, 2, ..., m$, ta có

$$|X| = \sum_{i=1}^{m} [G : S_G(x_i)].$$

1.2 CÁC ĐỊNH LÝ VỀ p-NHÓM.

Từ đây về sau, ký hiệu p để chỉ số nguyên tố cố định.

Định nghĩa 1.6. *Một nhóm hữu hạn được gọi là một p-nhóm nếu cấp của nó là một lũy thừa của p.*

Mệnh đề 1.6. *Cho G là một p-nhóm và X là một G-tập hữu hạn khác rỗng. Nếu* $|X| \not\equiv 0 (mod\ p)$ *thì X chứa một điểm G- bất biến; nghĩa là, có một điểm cố định tác động của G lên X.*

Hệ quả 1.2. *Giả sử một p-nhóm Q tác động lên một p-nhóm G khác. Nếu* $G \neq \{1\}$ *thì tồn tại một phần tử Q-bất biến của G khác đơn vị.*

Định lí 1.1. *Cho G là một p-nhóm và H là một nhóm con chuẩn tắc của G. Nếu* $H \neq 1$ *thì* $H \cap Z(G) \neq 1$. *Đặc biệt,* $G \neq 1$ *thì* $Z(G) \neq 1$.

Định lí 1.2. *(Matsuyama) Cho H là một nhóm con của một p-nhóm G. Khi đó hoặc* $H \lhd G$ *hoặc một nhóm con liên hợp* H^x *khác H chứa trong* $N_G(H)$.

Định lí 1.3. *Nếu H là một nhóm con thực sự của một p-nhóm G thì ta có* $N_G(H) \neq H$. *Vì vậy nhóm con chuẩn hóa của một nhóm con thực sự H là lớn hẳn hơn H.*

Hệ quả 1.3. *Một nhóm con cực đại bất kỳ M của một p-nhóm G là chuẩn tắc và nhóm thương G/M là nhóm cyclic cấp p. Đặc biệt,* $[G : M] = p$.

Định nghĩa 1.7. *Với bất kỳ nhóm G, ta định nghĩa các nhóm con* $Z_i(G)$ *với* $i = 0, 1, 2, ...$ *như sau (ta viết tắt* $Z_i(G) = Z_i$*). Định nghĩa* $Z_0 = 1$ *và với* $i > 0$, Z_i *là nhóm con của G tương ứng với* $Z(G/Z_{i-1})$ *bởi định lý đối xứng:*

$$Z_i/Z_{i-1} = Z(G/Z_{i-1}).$$

Dãy các nhóm con

$$Z_0 \subset Z_1 \subset Z_2 \subset ...$$

được gọi là dãy tâm tăng của G; số hạng thứ i là Z_i *của nó được gọi là tâm thứ i của G. Một nhóm G được gọi là lũy linh nếu* $Z_m(G) = G$ *với một số nguyên m nào đó; trong trường hợp này, số nguyên c nhỏ nhất sao cho* $Z_c(G) = G$ *được gọi là lớp của G.*

Định lí 1.4. *Mọi p-nhóm đều là nhóm lũy linh.*

Chương 3

NHÓM GIẢI ĐƯỢC, DÃY HỢP THÀNH VÀ NHÓM ĐƠN

Các khái niệm và kết quả ttrong chương này có thể tìm thấy trong [4],[5],[6],[8],[9].

3.1 NHÓM GIẢI ĐƯỢC.

Định nghĩa 3.1. *Cho G là một nhóm và giả sử nó có một dãy các nhóm con*

$$\{1\} \subset G_0 \subset G_1 \subset \cdots \subset G_r = G \tag{3.1}$$

Nếu mỗi $G_i \lhd G_{i+1}$ *với* $i = 1, ..., r-1$ *thì (3.1) được gọi là một dãy chuẩn tắc con của G.*

Nếu (3.1) là một dãy chuẩn tắc con của G và $[G_{i+1} : G_i]$ là một số nguyên tố nào đó với $i = 1, ..., r-1$ thì G được gọi là nhóm giải được và (3.1) được gọi là một dãy giải được của G. Khi đó, G là một nhóm hữu hạn.

Nếu (3.1) là một dãy chuẩn tắc con của G và nhóm thương G_{i+1}/G_i là đơn nghĩa là G_{i+1}/G_i không có nhóm con chuẩn tắc nào khác G_{i+1}/G_i và nhóm đơn vị thì (3.1) được gọi là một dãy hợp thành của G. Ta gọi nhóm thương G_{i+1}/G_i của dãy chuẩn tắc con (3.1) là các nhân tử (3.1).

Định lí 3.1. *Mọi p-nhóm đều là nhóm giải được.*

Định lí 3.2. *Nếu G là một nhóm và* $N \lhd G$ *sao cho N và G/N là giải được thì G cũng giải được.*

Cho G là nhóm có cấp 15. Vì 15=3.5, theo Định lý Sylow, có ít nhất một S_3-nhóm con H cấp 3 và một S_5-nhóm con K cấp 5 của G. Ngoài ra, số S_3-nhóm con là $s_3 = 1 + 3k$ với k là một số tự nhiên nào đó và s_3 chia hết $|G|$. Do đó $1 + 3k = 1$ hoặc $1 + 3k = 3$ hoặc $1 + 3k = 5$ hoặc $1 + 3k = 15$. Chỉ có một trường hợp thỏa mãn là $1 + 3k = 1$. Khi đó $H \lhd G$. Tương tự, số S_5-nhóm con của G là $s_5 = 1$ hay $K \lhd G$. Hơn nữa $|H||K| = |G|$ và $H \cap K = \{1\}$. Vì vậy $G \cong H \times K \cong C_3 \times C_5$ hay $G \cong C_{15}$.

Cấp của nhóm	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Số nhóm	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1

1.3 NHÓM CON FRATTINI.

Định nghĩa 1.8. *Gọi $\mathcal{M}$ là tập hợp các nhóm con cực đại của một nhóm G. Giao của tất cả nhóm con của $\mathcal{M}$ được gọi là nhóm con Frattini hay Φ-nhóm con của G, ký hiệu là $\Phi(G)$.*

Mệnh đề 1.7. *Cho $\Phi = \Phi(G)$ là Φ-nhóm con của một p-nhóm G. Khi đó ta có:*

(i) Φ là nhóm con đặc trưng của G; nghĩa là, $\sigma(\Phi) = \Phi$.

(ii) Nhóm thương G/Φ là một nhóm aben, trong đó mọi phần tử đều thỏa mãn $x^p = 1$.

(iii) Với một tập con X của G, $< X, \Phi >= G \Rightarrow < X >= G$.

Định lí 1.5. *Cho Φ là nhóm con Frattini của một p-nhóm G và xét $V = G/\Phi$ là không gian vectơ trên F_p. Đặt $|G/\Phi| = p^d$. Cho $x_1, ..., x_n$ là các phần tử của G và $v_i = \Phi x_i$ với $i = 1, 2, ..., n$.*

(i) Số chiều của V trên F_p là d.

(ii) Ta có $G =< x_1, ..., x_n >$ khi và chỉ khi V trùng với không gian con sinh bởi $v_1, v_2, ..., v_n$. Đặc biệt, nếu $G =< x_1, ..., x_n >$ thì ta có $n \geq d$.

(iii) Nhóm G có thể được sinh bởi đúng d phần tử. Tập con $x_1, x_2, ..., x_d$ sinh ra G khi và chỉ khi $v_1, v_2, ..., v_d$ là một cơ sở của không gian vectơ V trên F_p.

Định lí 1.6. *Cho Φ là nhóm con Frattini của một p-nhóm G sao cho $[G : \Phi] = p^d$và $|G| = p^n$. Gọi P là tập hợp các tự đẳng cấu của G mà làm cho mọi phần tử của G/Φ bất biến.*

(i) Tập P là nhóm con chuẩn tắc của $Aut(G)$ và nhóm thương $Aut(G)/P$ đẳng cấu với một nhóm con của $GL(d, p)$.

(ii) Nhóm con P là một p-nhóm có cấp là một ước của $p^{(n-d)d}$. Vì vậy $|Aut(G)|$ chia hết

$$p^m \prod_{i=1}^{d} (p^i - 1)$$

trong đó $m = nd - d(d + 1)/2 \leqslant n(n - 1)/2$.

Hệ quả 1.4. *Cho ρ là một tự đẳng cấu của một p-nhóm G. Nếu cấp của ρ là một nguyên tố với p và nếu ρ làm cho mọi phần tử của G/Φ bất biến thì $\rho = 1$.*

Hệ quả 1.5. *Cho A là một nhóm con chuẩn tắc aben có cấp cực đại của một p-nhóm G. Nếu $|G| = p^n$ thì ta có $2n \leqslant a(a + 1)$.*

Chương 2

CÁC ĐỊNH LÝ SYLOW

Các khái niệm và kết quả trong chương này có thể tìm thấy trong các tài liệu [1], [2], [5], [6], [9].

2.1 CÁC ĐỊNH LÝ SYLOW.

Định nghĩa 2.1. *Cho G là một nhóm hữu hạn. Ta viết*

$$|G| = p^n m, (p, m) = 1.$$

Một nhóm con của G được gọi là một p-nhóm con Sylow nếu cấp của nó đúng bằng p^n. Một p-nhóm con Sylow còn được viết tắt là một S_p-nhóm con.

Như vậy một nhóm con U của G là một S_p-nhóm con của G khi và chỉ khi

(i) U là một p-nhóm và

(ii) Chỉ số [G: U] nguyên tố với p.

Định lí 2.1. *Cho G là một nhóm hữu hạn.*

(i) Nhóm G là một S_p-nhóm con.

(ii) Hai S_p-nhóm con bất kỳ là liên hợp trong G.

(iii) Một p-nhóm con bất kỳ của G chứa trong một S_p-nhóm con của G.

(iv) Số S_p-nhóm con của G là một ước số của $|G|$ và đồng dư 1 môđulô p.

Bổ đề 2.1. *Cho L là một nhóm hữu hạn và H là một S_p-nhóm con của L. Với bất kỳ nhóm con K của L, tồn tại một phần tử x của L sao cho $K \cap H^x$ là một S_p-nhóm con của K.*

Bổ đề 2.2. *Cho S là S_p-nhóm con của một nhóm hữu hạn G. Một p-nhóm con bất kỳ U của $N_G(S)$ được chứa trong S.*

Bảng 2.5

.	1	a	a^2	a^3	c	c^2	ac	a^2c	a^3c	ac^2	a^2c^2	a^3c^2
1	1	a	a^2	a^3	c	c^2	ac	a^2c	a^3c	ac^2	a^2c^2	a^3c^2
a	a	a^2	a^3	1	ac	ac^2	a^2c	a^3c	c	a^2c^2	a^3c^2	c^2
a^2	a^2	a^3	1	a	a^2c	a^2c^2	a^3c	c	ac	a^3c^2	c^2	ac^2
a^3	a^3	1	a	a^2	a^3c	a^3c^2	c	ac	a^2c	c^2	ac^2	a^2c^2
c	c	ac^2	a^2c	a^3c^2	c^2	1	a	a^2c^2	a^3	ac	a^2	a^3c
c^2	c^2	ac	a^2c^2	a^3c	1	c	ac^2	a^2	a^3c^2	a	a^2c	a^3
ac	ac	a^2c^2	a^3c	c^2	ac^2	a	a^2	a^3c^2	1	a^2c	a^3	c
a^2c	a^2c	a^3c^2	c	ac^2	a^2c^2	a^2	a^3	c^2	a	a^3c	1	ac
a^3c	a^3c	c^2	ac	a^2c^2	a^3c^2	a^3	1	ac^2	a^2	c	a	a^2c
ac^2	ac^2	a^2c	a^3c^2	c	a	ac	a^2c^2	a^3	c^2	a^2	a^3c	1
a^2c^2	a^2c^2	a^3c	c^2	ac	a^2	a^2c	a^3c^2	1	ac^2	a^3	c	a
a^3c^2	a^3c^2	c	ac^2	a^2c	a^3	a^3c	c^2	a	a^2c^2	1	ac	a^2

(b) $F = \{1, x, y, z\}$ và $T = \{1, c, c^2\}$. Vì $T \lhd G$, ta có $f^{-1}cf \in T$ với mọi $f \in F$. Theo giả thiết, có ít nhất $f \in F, f^{-1}cf \neq c$. Vì thế không mất tính chất tổng quát, ta có thể xem $x^{-1}cx = c^2$. Cũng như trên, đặt $x = a, y = b, z = ba$. Khi đó $ca = ac^2$. Lưu ý rằng $c^2a = c(ca) = c(ac^2) = (ca)c^2 = ac^2c^2 = ac$.

Kiểm tra dễ dàng $S = 1, c, c^2, a, ca, c^2a$ là một nhóm con không aben của G. Do đó S đẳng cấu với nhóm Dihedral D_3 vì có duy nhất một nhóm không aben cấp 6 (sai khác đẳng cấu). Do $[G : S] = 2$, ta có $S \lhd G$. Do đó $b^{-1}cb \in S$. Vì $b^{-1}cb$ là một phần tử cấp 3, nên nó bằng c hoặc c^2. Nếu $b^{-1}cb = c$, đặt $h = b$.

Nếu $b^{-1}cb = c^2$, đặt $h = ab$. Khi đó $(ab)^{-1}c(ab) = b^{-1}(a^{-1}ca)b = b^{-1}c^2b = b^{-1}cb.b^{-1}cb = c^2.c^2 = c$. Do đó tồn tại phần tử $h \in F, h \notin S$ sao cho $h^{-1}ch = c$. Xét $H =< h >$. Rõ ràng $S \cap H = \{1\}$, S và H giao hoán từng phần tử và $|S||H| = |G|$ và vì vậy $G \cong S \times H$. Do $S \cong D_3$ và $H \cong C_2$. Vì thế ta kết luận một nhóm G bất kỳ với $s_2 = 3, s_3 = 1$ và S_2-nhóm con đẳng cấu với K_4 là đẳng cấu với $D_3 \times C_2$. Nhóm Dihedral D_6 là nhóm thuộc loại này.

(iv) $s_2 = 3$ và $s_3 = 4$. Vì các nhóm cyclic phân biệt cấp 3 có giao là phần tử đơn vị, nên bốn S_3-nhóm con có 9 phần tử phân biệt. Một S_2-nhóm con có cấp là 4 và một nhóm cấp 3 chỉ có thể là phần tử đơn vị, nên số các phần tử phân biệt trong bốn S_3-nhóm con và một S_2-nhóm con duy nhất là 12. Nhưng $|G| = 12$, nên không thể có một S_2-nhóm con phân biệt khác. Vậy không có nhóm nào thuộc loại (iv).

nên $c^2a = cac^2 = ac^4 = ac$. *Các phương trình mà xác định một bảng nhân đối với nhóm này là:*

$$ca = ac^2, c^2a = ac, c^3 = 1, a^4 = 1.$$

Khi đó các phần tử phân biệt của G *là*

$$1, a, a^2, a^3, c, c^2, ac, a^2c, a^3c, ac^2, a^2c^2, a^3c^2$$

và ta có Bảng 2.5 bên dưới.

Bằng một lập luận tương tự như trong trường hợp nhóm không aben cấp 8, nhóm bất kỳ có cấp 12 với $s_2 = 3, s_3 = 1$ *và trong đó* S_2*-nhóm con là cyclic cấp 4 là đẳng cấu với nhóm* G *xác định theo bảng này.*

Xét ma trận $A = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ *và* $B = \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon \end{pmatrix}$*, trong đó* $i = \sqrt{-1}$ *và* ϵ *là căn bậc ba phức của 1 (tức là* $\epsilon \in \mathbb{C}, \epsilon^3 = 1, \epsilon \neq 1$ *). Ta có:*

$$A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, A^3 = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, A^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1,$$

$$B^2 = \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon \end{pmatrix}, B^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I, AB = \begin{pmatrix} 0 & i\epsilon^2 \\ i\epsilon & 0 \end{pmatrix},$$

$$A^2B = \begin{pmatrix} -\epsilon & 0 \\ 0 & -\epsilon^2 \end{pmatrix}, A^3B = \begin{pmatrix} 0 & -i\epsilon^2 \\ -i\epsilon & 0 \end{pmatrix} = I, AB^2 = \begin{pmatrix} 0 & i\epsilon \\ i\epsilon & 0 \end{pmatrix},$$

$$A^2B^2 = \begin{pmatrix} -\epsilon^2 & 0 \\ 0 & -i\epsilon \end{pmatrix} A^3B^2 = \begin{pmatrix} 0 & -i\epsilon \\ -i\epsilon^2 & 0 \end{pmatrix}$$

Gọi $H = \left\{I, A, A^2, A^3, B, B^2, AB, A^2B, A^3B, AB^2, A^2B^2, A^3B^2\right\}$.

Khi đó H *là một nhóm với phép nhân ma trận vì nó là một nhóm con của nhóm* $GL(2, \mathbb{C})$ *(nhóm các ma trận vuông cấp 2 phức khả nghịch). Các phần tử của* H *thỏa mãn các phương trình:*

$$BA = AB^2, B^2A = AB, B^3 = I, A^4 = I$$

và thỏa mãn Bảng 2.5 với tương ứng $A \leftrightarrow a, B \leftrightarrow c$.

Mệnh đề 2.1. *Cho* U *là một* p*-nhóm con của một nhóm hữu hạn* G*. Số* S_p*-nhóm con của* G *chứa* U *là đồng dư 1 môđulô* p*. (Nếu* $U = \{1\}$*, Mệnh đề 2.1 quy về (iv).)*

Hệ quả 2.1. *(Định lý Cauchy) Nếu số nguyên tố* p *chia hết cấp của một nhóm hữu hạn* G *thì* G *chứa một phần tử cấp* p*.*

Mệnh đề 2.2. *Cho* P *là một* p*-nhóm con của một nhóm hữu hạn* G*. Nếu* P *là một* S_p*-nhóm con của* $N_G(P)$ *thì* P *là một* S_p*-nhóm con của* G*.*

Định lí 2.2. *Cho* H *là một nhóm con chuẩn tắc của một nhóm hữu hạn* G *và* S *là một* S_p*-nhóm con của* G*. Giao* $S \cap H$ *là một* S_p*-nhóm con của* H *và* SH/H *là một* S_p*-nhóm con của* G/H*.*

Định lí 2.3. *Cho* H *là một nhóm con chuẩn tắc hữu hạn của một nhóm* G*. Nếu* S *là một* S_p*-nhóm con của* H *thì ta có* $G = N_G(S)H$*.*

Mệnh đề 2.3. *Cho* S *là một* S_p*-nhóm con của nhóm hữu hạn* G*. Nếu một nhóm con* H *của* G *chứa* $N_G(S)$ *thì ta có* $H = N_G(H)$*.*

2.2 ĐỊNH LÝ SYLOW SUY RỘNG.

Định nghĩa 2.2. *Cho* Q *và* G *là hai nhóm. Nếu một đồng cấu* φ *từ* Q *vào* $Aut(G)$ *được cho thì ta nói* Q *tác động lên* G *qua* φ *và* Q *là một nhóm toán tử trên* G *đồng cấu* φ *được gọi là một tác động của* Q*.*

Định nghĩa 2.3. *Cho* φ *là một tác động của một nhóm* Q *lên một nhóm* G *khác. Gọi* L *là tập tích trực tiếp; nghĩa là* $L = \{(x, g)|x \in Q, g \in G\}$*. Định nghĩa tích của hai phần tử của* L *bởi công thức*

$$(x, g)(x', g') = (xx', \varphi(x')(g)g').$$

Mệnh đề 2.4. *Cho* L *là một nửa tích trực tiếp trong của hai nhóm* G *và* Q *sao cho* $G \lhd L = GQ$ *và* $G \cap Q = \{1\}$*. Gọi* $\theta(x)$ *là tự đẳng cấu của* G *cảm sinh bởi phép liên hợp của* $x \in Q$*. Khi đó* θ *là một tác động của* Q *lên* G *và tích nửa trực tiếp của* Q *và* G *đối với* θ *đẳng cấu với* L*.*

Định nghĩa 2.4. *Cho* φ *là một tác động của một nhóm* Q *lên một nhóm* G *khác. Một nhóm con* U *của* G *được gọi là* Q*-bất biến nếu* $\varphi(x)U = U$ *với mọi* $x \in Q$*.*

Mệnh đề 2.5. *Cho Q là một nhóm toán tử trên G với tác động φ. Gọi L là tích nửa trực tiếp của Q và G đối với φ. Ta xét Q và G là những nhóm con của L.*

(i) Một nhóm con U của G là Q-bất biến khi và chỉ khi

$$Q \subset N_L(U).$$

Trong trường hợp này, UQ đẳng cấu với nửa tích trực tiếp của U và Q đối với hạn chế của φ lên U.

(ii) Nếu U là nhóm con chuẩn tắc Q-bất biến của G thì $U \lhd L$ và L/U đẳng cấu với tích nửa trực tiếp của G/U và Q đối với tác động cảm sinh.

Định lí 2.4. *Cho q là một số nguyên tố. Giả sử nhóm toán tử Q là một q-nhóm và q không chia hết cấp của nhóm hữu hạn G. Khi đó ta có mở rộng sau đây của Định lý Sylow.*

(i) Tồn tại một S_p-nhóm con Q-bất biến.

(ii) Hai S_p-nhóm con Q-bất biến là liên hợp bởi một phần tử của $C_G(Q)$.

(iii) p-nhóm con Q-bất biến bất kỳ chứa trong một S_p-nhóm con Q-bất biến của G.

Hệ quả 2.2. *Giả sử ngoài các giả thiết của Định lý 2.4 ra, tác động của Q là không có điểm cố định; nghĩa là, giả sử $C_G(Q) = \{1\}$. Khi đó tồn tại duy nhất S_p-nhóm con Q-bất biến của G.*

2.3 ỨNG DỤNG CHO VIỆC XÁC ĐỊNH CÁC NHÓM CÓ CẤP THẤP.

2.3.1 Các nhóm có cấp p và 2p.

Ta sẽ dùng ký hiệu C_n để ký hiệu nhóm cyclic cấp n và K_4 là nhóm bốn (nhóm Klein), cụ thể $K_4 = C_2 \times C_2$ và với việc đặt $1 = (1,1), x = (1,g), y = (g,1), z = (g,g)$, ta có bảng nhân của K_4

Bảng 2.1

.	1	x	y	z
1	1	x	y	z
x	x	1	z	y
y	y	z	1	x
z	z	y	x	1

Bảng 2.4

.	1	c	c^2	a	b	ab	ca	cb	cab	c^2a	c^2b	c^2ab
1	1	c	c^2	a	b	ab	ca	cb	cab	c^2a	c^2b	c^2ab
c	c	c^2	1	ca	cb	cab	c^2a	c^2b	c^2ab	a	b	ab
c^2	c^2	1	c	c^2a	c^2b	c^2ab	a	b	ab	ca	cb	cab
a	a	cb	c^2ab	1	ab	b	cab	c	ca	c^2b	c^2a	c^2b
b	b	cab	c^2a	ab	1	a	cb	ca	c	c^2	c^2ab	c^2b
ab	ab	ca	c^2b	b	a	1	c	cab	cb	c^2ab	c^2	c^2a
ca	ca	c^2b	ab	c	cab	cb	c^2ab	c^2	c^2a	b	a	1
cb	cb	c^2ab	a	cab	c	ca	c^2b	c^2a	c^2	1	ab	b
cbb	cab	c^2a	b	cb	ca	c	c^2	c^2ab	c^2b	ab	1	a
c^2a	c^2a	b	cab	c^2	c^2ab	c^2b	ab	1	a	cb	ca	c
c^2b	c^2b	ab	ca	c^2ab	c^2	c^2a	b	a	1	c	cab	cb
c^2ab	c^2ab	a	cb	c^2b	c^2a	c^2	1	ab	b	cab	c	ca

Nhóm thay phiên A_4 là nhóm các phép thế chẵn của tập $\{1,2,3,4\}$ gồm các phần tử:

$$\iota = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\ \sigma_1 = \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\ \sigma_2 = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},$$
$$\sigma_3 = \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix},\ \tau_1 = \begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix},\ \tau_2 = \begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix},$$
$$\tau_3 = \begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix},\ \tau_4 = \begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix},\ \tau_5 = \begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix},$$
$$\tau_6 = \begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix},\ \tau_7 = \begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix},\ \tau_8 = \begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}.$$

Các phần tử này thỏa mãn Bảng 2.4 với tương ứng

$$\iota \leftrightarrow 1, \sigma_1 \leftrightarrow a, \sigma_2 \leftrightarrow b, \sigma_3 \leftrightarrow ab, \tau_1 \leftrightarrow c, \tau_2 \leftrightarrow c^2, \tau_3 \leftrightarrow ca$$

$$\tau_4 \leftrightarrow cb, \tau_5 \leftrightarrow cab, \tau_6 \leftrightarrow c^2a, \tau_7 \leftrightarrow c^2b, \tau_8 \leftrightarrow c^2ab.$$

(iii) $s_2 = 3$ và $s_3 = 1$. Gọi F là một S_2-nhóm con và $T = \{1, c, c^2\}$ ($c^3 = 1$) là S_3-nhóm con. Một lần nữa ta có hai khả năng:

(a) $F = \{1, a, a^2, a^3\} \cong C_4$ và (b) $F = \{1, x, y, z\} \cong K_4$.

(a) T là một S_3-nhóm con duy nhất nên chuẩn tắc trong G và vì vậy $a^{-1}ca \in T$. Ta có thể giả sử $a^{-1}ca \neq c$, vì ngược lại thì G aben. Do đó $a^{-1}ca = c^2$ và $ca = ac^2$,

Bảng 2.2 cũng chứng tỏ rằng một nhóm cấp 8 thuộc loại này thực sự tồn tại vì bảng xác định một nhóm. Nhóm này được gọi là nhóm Quaternion và có tính chất thú vị là mọi nhóm con của nó đều chuẩn tắc và chính nó không aben.

(iv) $b^2 = 1$. *Gọi* $K =< b >$ *thì* $H \cap K = \{1\}$ *và* $G = HK$. *Ta có* $b^{-1}ab \in H$ *vì* $H \lhd G$ *và* $b^{-1}ab = a$ *hoặc* a^3 *vì* a *có cấp 4. Như trong (ii),* $b^{-1}ab = a$ *kéo theo* G *aben. Do đó* $b^{-1}ab = a^3$ *và dẫn đến*

$$ba = a^3b.$$

Các phần tử $1, a, a^2, a^3, b, ab, a^2b, a^3b$ *là các phần tử phân biệt của* G. *Các phương trình* $ba = a^3b, b^2 = 1, a^4 = 1$ *cho phép ta xây dựng bảng nhân sau.*

Bảng 2.3

.	*1*	a	a^2	a^3	b	ab	a^2b	a^3b
1	*1*	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	*1*	ab	a^2b	a^3b	b
a^2	a^2	a^3	*1*	a	a^2b	a^3b	b	ab
a^3	a^3	*1*	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	*1*	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	*1*	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	*1*	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	*1*

2.3.3 Các nhóm có cấp 12 và 15.

Để hoàn thành bảng liệt kê tất cả các nhóm đến cấp 15, ta phải tìm tất cả các nhóm có thể có với cấp 12 và 15. Vì $12 = 3.2^2$, *theo Định lý Sylow, có ít nhất một* S_2*-nhóm con cấp* 2^2 *và ít nhất một* S_3*-nhóm con cấp 3. Ngoài ra, số các* S_2*-nhóm con là* $s_2 = 1 + 2k$ *với* k *là một số tự nhiên nào đó và* s_2 *chia hết* $|G|$. *Khi* $k = 0, s_2 = 1$ *và khi* $k = 1, s_3 = 3$. *Nếu* $k > 1$ *rõ ràng rằng* $1 + 2k$ *không chia hết 12. Vì thế ta có hai khả năng:* G *có đúng một* S_2*-nhóm con hoặc* G *có đúng* S_3*-nhóm con hoặc có đúng bốn* S_3*-nhóm con. Vì thế ta có bốn khả năng:*

(i) $s_2 = 1$ *và* $s_3 = 1$,

(ii) $s_2 = 1$ *và* $s_3 = 4$,

(iii) $s_2 = 3$ *và* $s_3 = 1$,

(iv) $s_2 = 3$ *và* $s_3 = 4$,

Từ đó ta có bảng nhân của G :

Do p là số nguyên tố, nhóm bất kỳ có cấp p là cyclic. Vì vậy có duy nhất (sai khác đẳng cấu) một nhóm cấp p. Đặc biệt, các nhóm duy nhất có cấp 2, 3, 5, 7, 11 và 13 là cyclic.

Có đúng hai nhóm không đẳng cấu cấp 4 là C_4 *và* K_4. *Thật ra, có đúng hai nhóm không đẳng cấu cấp* p^2 *là* C_{p^2} *và* $C_p \times C_p$ *(Bài toán 5.36 của [5]).*

Kế đến, ta sẽ thấy rằng có đúng hai nhóm trong mỗi trường hợp cấp 6, 10 hoặc 14. Lưu ý rằng $6 = 2.3, 14 = 2.7$, *nên các nhóm này có cấp* $2p$ *với* p *là nguyên tố khác 2. Cho* G *là một nhóm có cấp* $2p$, *với* p *là số nguyên tố lẻ. Theo Định lý Sylow,* G *có* $1 + kp$ S_p*-nhóm con cấp* p, *với* $k \geq 0$ *và* $1 + kp$ *chia hết* $2p$. *Khi đó* $1 + kp = p$ *hoặc* $1 + kp = 2$ *hoặc* $1 + kp = 2p$ *hoặc* $1 + kp = 1$. *Vì* p *không chia hết* $1 + kp$ *nên* $1 + kp = 2$ *hoặc* $1 + kp = 1$. *Vì* $p > 2, 1 + kp \neq 2$, *nên* $1 + kp = 1$. *Do đó* G *có duy nhất một nhóm con* K *cấp* p. *Cũng theo Định lý Sylow,* G *có* $1 + 2k$ S_2 *nhóm con cấp 2, Với* $k \neq 0$. *Tương tự trên,* $1 + kp = 1, 2, p$ *hoặc* $2p$. *Vì 2 không chia hết* $1 + 2k$, *ta có* $1 + 2k = 1$ *hoặc* $1 + 2k = p$. *Do đó có một trong hai trường hợp sau đây xảy ra:*

(i) có đúng một nhóm con H *cấp 2.*

(ii) có đúng p *nhóm con cấp 2.*

(i) Trong trường hợp này, nhóm G *là cyclic cấp* $2p$. *Để thấy điều này, lưu ý rằng* H *là* S_2*-nhóm con duy nhất và* K *là* S_p*-nhóm con duy nhất, nên* $H \lhd G$ *và* $K \lhd G$. *Hơn nữa,* $H \cap K = \{1\}$ *vì* $(2, p) = 1$. *Rõ ràng* $|H||K| = 2p = |G|$. *Do đó* $G \cong H \times K$. *Nhưng* H *và* K *tương ứng là các nhóm cyclic cấp 2 và* p, *nên* G *là nhóm cyclic cấp* $2p$.

(ii) Giả sử $K =< a >$, *trong đó* $a^p = 1$. *Vì* K *là nhóm con duy nhất cấp* $p, b \notin K$ *kéo theo* $b^2 = 1$. *Rõ ràng* $G = K \cup bK$. *Do đó* G *chứa các phần tử phân biệt*

$$1, a, a^2, ..., a^{p-1}, b, ba, ba^2, ..., ba^{p-1}.$$

Với $i = 0, 1, ..., p-1, ba^i \notin K$ *và mỗi phần tử của* G *nằm ngoài* K *có cấp 2,* $(ba^i)^2 = 1$ *và* $ba^i = (ba^i)^{-1} = (a^i)^{-1}b^{-1} = a^{p-1}b$.

Bây giờ nếu $\overline{G}$ *là một nhóm có cấp* $2p$ *thì nó thuộc loại (i) hoặc loại (ii). Nếu* $\overline{G}$ *thuộc loại (i) thì nó là một nhóm cyclic cấp* $2p$, *mà mọi nhóm cyclic cùng cấp thì đẳng cấu. Do đó mọi nhóm có cấp* $2p$ *có tính chất (i) là đẳng cấu.*

Giả sử $\overline{G}$ *thuộc loại (ii). Lập luận như trên,* $\overline{G}$ *có một nhóm con* $\overline{K} =< \overline{a} >$ *cấp* p *và một phần tử* $\overline{b}$ *cấp 2 sao cho*

$$\overline{G} = \left\{1, \overline{a}, ..., \overline{a}^{p-1}, \overline{b}, \overline{b}\overline{a}, ..., \overline{b}\overline{a}^{p-1}\right\},$$

$$(\overline{b}\overline{a}^i)^2 = 1, \overline{b}\overline{a}^i = \overline{a}^{p-1}\overline{b}, 0 \leq i \leq p-1.$$

Khi đó ánh xạ $\alpha : G \to \overline{G}$ *xác định bởi* $\alpha(a^i) = \overline{a}^i, \alpha(b) = \overline{b}, \alpha(ba^i) = \overline{b}\overline{a}^i$ *là một đẳng cấu. Vì thế hai nhóm bất kỳ thuộc loại (ii) là đẳng cấu.*

Xét đa giác đều n cạnh P_n *với* $n > 2$. *Gọi a là phép quay mặt phẳng xung quanh tâm của* P_n. *Khi đó* $a^n = 1, b^2 = 1$ *và tất cả các phép đối xứng của* P_n *(tức là các phép biến đổi đẳng cự của mặt phẳng biến* P_n *thành chính nó) là*

$$1, a, a^2, ..., a^{n-1}, b, ba, ba^2, ..., ba^{n-1}$$

thỏa mãn $(ba^i)^2 = 1, ba^i = a^{n-i}b, 0 \leq i \leq n-1$. *Các phép đối xứng này lập thành một nhóm với phép toán hợp thành, ký hiệu* D_n *và được gọi là nhóm Dihedral (hay nhóm nhị diện). Như vậy nhóm Dihedral* D_p *thuộc loại (ii). Vì thế có đúng hai nhóm (sai khác đẳng cấu) có cấp* $2p$ *là nhóm cyclic* C_{2p} *và nhóm Dihedral* D_p. *Đặc biệt, có đúng hai nhóm không đẳng cấu có cấp* i, $i = 6, 10, 14$.

2.3.2 Các nhóm có cấp 8 và 9.

Cho G là một nhóm cấp 8. Có ít nhất ba nhóm aben không đẳng cấu cấp 8: C_8, $C_2 \times C_4$ *và* $C_2 \times K_4$. *Ta sẽ thấy rằng nếu G là aben thì nó đẳng cấu với một trong ba nhóm này.*

Nếu G là phần tử cấp 8, G là cyclic. Nếu G không có phần tử nào cấp 8 mà có một phần tử a cấp 4, đặt $H =< a >$. *Cho* $b \in G \setminus H$. *Nếu b cấp 4 thì* b^2 *là phần tử cấp 2 và nằm trong H (vì phân tích lớp kề của G) là* $H \cup bH$. *Do đó* $(ab)^2 = a^2b^2 = a^2a^2 = 1$. *Ta có* $ab \in G \setminus H$ *có cấp 2. Đặt* $X =< ab >$. $G = XH$, $X \cap H = \{1\}$. *Vì thế* $G \cong X \times H$. *Do* $X \cong C_2$ *và* $H \cong C_4$, *ta có* $G \cong C_2 \times C_4$.

Nếu G không có phần tử nào cấp 4 hoặc cấp 8, mọi phần tử khác đơn vị của nó đều có cấp 2. Gọi a và b là hai phần tử khác nhau có cấp 2 trong G. Đặt $A =< a >$, $B =< b >$. *Khi đó AB là một nhóm. Do* $A \cap B = \{1\}$, *ta có* $AB \cong A \times B \cong C_2 \times C_2$. *Với* $c \in G \setminus AB$ *và* $C =< c >$, $C \cap AB = \{1\}$. *Vì vậy* $G \cong (C_2 \times C_2) \times C_2 = K_4 \times C_2$.

Do đó có đúng (sai khác đẳng cấu) ba nhóm aben cấp 8.

Giả sử G là nhóm không aben cấp 8. G có một phần tử cấp 4 và không có phần tử nào cấp 8; vì nếu $g \in G$ *có cấp 8,* $G \cong C_8$. *Mặt khác, nếu mọi phần tử của G đều có cấp 2 thì* $(ab)^2 = 1$ *với bất kỳ* $a, b \in G$ *và suy ra*

$$ba = a^2bab^2 = a(abab)b = ab$$

mâu thuẫn với giả thiết G không aben. Cho $a \in G$ *là phần tử có cấp 4 và đặt* $H =< a >$. *Khi đó* $G = H \cup Hb$ *với* $b \in G$ *nào đó và* $H \lhd G$ *vì nó có chỉ số 2 trong G.* $b^2 \in H$; *vì nếu không các lớp kề H, Hb,* Hb^2 *là phân biệt và điều này mâu thuẫn với* $[G : H] = 2$. *Ta có 4 khả năng đối với* b^2*:*
(i) $b^2 = a$, *(ii)* $b^2 = a^2$, *(iii)* $b^2 = a^3$, *(iv)* $b^2 = 1$.

Nếu (i) và (iii) xảy ra, rõ ràng $G =< b >$, *mâu thuẫn với giả thiết. Vì vậy chỉ còn hai khả năng (ii) và (iv).*

(ii) $b^2 = a^2$. *Vì* $H \cong G$, $b^{-1}ab = a$ *hay* $b^{-1}ab = a^3$. *Nếu* $b^{-1}ab = a$ *thì* $ab = ba$. *Nhưng mọi phần tử của G có thể được viết dưới dạng* a^ib *hay* a^i *vì* $G = H \cup Hb$. *Do đó* $ab = ba$ *kéo theo G aben, mâu thuẫn với giả thiết. Vì vậy* $b^{-1}ab = a^3$ *hoặc* $ab = ba^3$. *Vì* $G = H \cup Hb$, *các phần tử của G là* $1, a, a^2, a^3, b, ab, a^2b, a^3b$. *Nếu một nhóm thuộc kiểu này thật sự tồn tại thì* $ab = ba^3$, $b^2 = a^2$, $a^4 = 1$ *cung cấp cho ta đủ thông tin để xây dựng bảng nhân của nó.*

Bảng 2.2

.	1	a	a^2	a^3	b	ab	a^2b	a^3b
1	1	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	1	ab	a^2b	a^3b	b
a^2	a^2	a^3	1	a	a^2b	a^3b	b	ab
a^3	a^3	1	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	a^2	a	1	a^3
ab	ab	b	a^3b	a^2b	a^3	a^2	a	1
a^2b	a^2b	ab	b	a^3b	1	a^3	a^2	a
a^3b	a^3b	a^b	ab	b	a	1	a^3	a^2

Để tính các tích trong bảng, ta sử dụng $ba = ba^3$ *và* $b^2 = a^2$ *và kéo theo* $ba = a^3b$ *vì* $a^3b = a^2(ba^3) = b^3a^3 = b(a^2a^3) = ba$.

Nếu $\overline{G}$ *là một nhóm con không aben khác có cấp 8 với một phần tử* $\overline{a}$ *có cấp 4 và một phần tử* $\overline{b} \notin < a >$ *sao cho* $\overline{b}^2 = \overline{a}^2$ *thì như lập luận trên,*

$$\overline{G} = \left\{\overline{1}, \overline{a}, \overline{a}^2, \overline{a}^3, \overline{b}, \overline{a}\overline{b}, \overline{a}^2\overline{b}, \overline{a}^3\overline{b}\right\},$$

với các phần tử thỏa mãn các phương trình

$$\overline{a}^4 = \overline{1}, \overline{a}^2 = \overline{b}^2, \overline{a}\overline{b} = \overline{b}\overline{a}^3,$$

mà từ đó ta có được bảng nhân của $\overline{G}$, *được đồng nhất với Bảng 2.2, trong đó* $\overline{a}$ *thay thế a và* $\overline{b}$ *thay thế b. Ánh xạ* $\alpha : G \to \overline{G}$ *xác định bởi* $\alpha(a) = \overline{a}$ *và* $\alpha(a^ib) = \overline{a}^i\overline{b}, i = 0, 1, 2, 3$ *rõ ràng là một đẳng cấu.*