ĐẠI HỌC THÁI NGUYÊN
ĐẠI HỌC KHOA HỌC
================

Nguyễn Tuyết Nga

LUẬN VĂN THẠC SĨ TOÁN HỌC

ỨNG DỤNG CỦA LÍ THUYẾT NHÓM TRONG MỘT SỐ BÀI TOÁN SƠ CẤP

Thái Nguyên, năm 2009

ĐẠI HỌC THÁI NGUYÊN
ĐẠI HỌC KHOA HỌC
================

Nguyễn Tuyết Nga

ỨNG DỤNG CỦA LÍ THUYẾT NHÓM TRONG MỘT SỐ BÀI TOÁN SƠ CẤP

Chuyên ngành: Phương pháp Toán sơ cấp
Mã số: 60.46.40

Hướng dẫn: ***PGS.TS Lê Thị Thanh Nhàn***

Thái Nguyên, năm 2009

Mục lục

LỜI CẢM ƠN

Sau hơn nửa năm nghiên cứu miệt mài, luận văn thạc sĩ của tôi với đề tài nghiên cứu *"Ứng dụng của lý thuyết nhóm trong một số bài toán sơ cấp"* đã được hoàn thành. Những kết qủa ban đầu mà tôi thu được đó là nhờ sự hướng dẫn tận tình và nghiêm khắc của cô giáo PGS. TS Lê Thị Thanh Nhàn. Tôi xin được bày tỏ lòng biết ơn sâu sắc đối với Cô.

Tôi xin chân thành cảm ơn Ban Giám hiệu, phòng Đào tạo và Khoa Toán-Tin của Trường Đại học Khoa học - Đại học Thái Nguyên đã tạo mọi điều kiện thuận lợi cho tôi hoàn thành đề tài này trong thời gian qua. Đội ngũ cán bộ thuộc phòng Đào tạo và Khoa Toán - Tin đã hết lòng ủng hộ, giúp đỡ lớp cao học Khóa I chúng tôi với một thái độ nhiệt tình, thân thiện nhất. Điều này sẽ mãi là ấn tượng rất tốt đẹp trong lòng mỗi chúng tôi đối với nhà Trường.

Tôi cũng rất tự hào rằng trong quá trình học tập đã được Trường Đại học Khoa học - Đại học Thái Nguyên bố trí những nhà toán học hàng đầu Việt nam về lĩnh vực Phương pháp toán sơ cấp giảng dạy cho chúng tôi như GS Hà Huy Khoái, GS Nguyễn Minh Hà, GS Phan Huy Khải...

Và cũng là lời cảm ơn chân thành của tôi tới bạn bè, những người thân đã luôn động viên, cổ vũ tôi trong suốt qúa trình nghiên cứu.

LỜI NÓI ĐẦU

Lí thuyết nhóm là một trong những lĩnh vực nghiên cứu quan trọng của Đại số hiện đại. Lí thuyết này có những ứng dụng sâu sắc trong nhiều hướng khác nhau của toán học, vật lí... Đặc biệt, một số kĩ thuật trong lí thuyết nhóm đã được sử dụng để mang lại những kết quả đẹp của toán sơ cấp. Chẳng hạn, tính giải được của các đa thức đã được giải quyết trọn vẹn bởi E. Galois thông qua việc sử dụng các kiến thức của lí thuyết nhóm phối hợp một cách tài tình với lí thuyết trường và đa thức.

Trong luận văn này, chúng tôi khai thác một số ứng dụng của lí thuyết nhóm vào toán sơ cấp ở 2 lĩnh vực: Số học và Tổ hợp. Công cụ chủ yếu của lí thuyết nhóm được vận dụng ở đây là Định lý Lagrange "*Cấp và chỉ số của một nhóm con của một nhóm hữu hạn là ước của cấp của toàn nhóm*" và Định lý Burnside "*Nếu nhóm hữu hạn G tác động lên tập hữu hạn X thì số quỹ đạo của tác động là* $\dfrac{1}{(G:e)}\sum_{g\in G} f(g)$, *trong đó* $f(g)$ *là số phần tử của* X *cố định qua tác động của* g".

Luận văn được trình bày trong 3 chương. Chương 1 là những kiến thức chuẩn bị về lý thuyết nhóm nhằm phục vụ cho 2 chương sau, bao gồm các khái niệm và tính chất cơ bản về nhóm, đồng cấu nhóm, nhóm đối xứng và tác động của nhóm lên tập hợp. Các kiến thức và thuật ngữ của Chương I được tham khảo chủ yếu trong các cuốn sách về lý thuyết nhóm của J. Rotman [Rot] và J. F. Humphreys [Hum].

Chương 2 là một số ứng dụng vào số học. Một số kết quả ở các Tiết 2.1 và 2.2 là sự tổng hợp lại theo một chủ đề những ứng dụng đã biết của lí thuyết nhóm trong số học (xem 2.1.3, 2.1.4, 2.1.5, 2.2.1, 2.2.2), nhưng cũng có những tính chất mà tác giả luận văn tự tìm tòi bằng hiểu biết của mình (xem 2.1.1, 2.1.2). Tiết 2.3, được trình bày theo bài báo công bố năm 2005 của T. Evans và B. Holt [EH], chứng minh lại những công thức số học cổ điển bằng phương pháp sử dụng công thức các lớp và Định lý Burnside trong lí thuyết nhóm.

Chương cuối của luận văn là những ứng dụng của lý thuyết nhóm vào một số bài toán tổ hợp. Thực chất, khi có lí thuyết nhóm soi vào, các bài toán tổ hợp này đã bớt phức tạp hơn, cách giải quyết nó cũng không còn là những mẹo mực hay bí ẩn dễ nhầm lẫn của Toán tổ hợp nữa, mà nó trở thành rõ ràng, hệ thống và dễ hiểu.

Chương 1

Kiến thức chuẩn bị về lí thuyết nhóm

Mục đích của chương này là nhắc lại một số kiến thức về nhóm, định lí Lagrange, tác động của nhóm lên tập hợp, công thức các lớp và Định lí Burnside. Kiến thức này là cần thiết cho những ứng dụng giải một số bài toán sơ cấp được trình bày trong Chương II và Chương III. Các kiến thức và thuật ngữ ở đây được tham khảo trong các cuốn sách về lí thuyết nhóm [Ash], [Rot] và [Hum].

1.1 Nhóm, nhóm xylic và nhóm con

1.1.1. Định nghĩa. *Nhóm* là một tập G cùng với một phép toán thoả mãn các điều kiện

(i) Phép toán có tính kết hợp: $a(bc) = (ab)c$, $\forall a, b, c \in G$.

(ii) G có đơn vị: $\exists e \in G$ sao cho $ex = xe = x$, $\forall x \in G$.

(iii) Mọi phần tử của G đều khả nghịch: Với mỗi $x \in G$, tồn tại $x^{-1} \in G$ sao cho $xx^{-1} = x^{-1}x = e$.

Một nhóm G được gọi là *nhóm giao hoán* (hay *nhóm Abel*) nếu phép toán là giao hoán. Nếu G có hữu hạn phần tử thì số phần tử của G được gọi là *cấp của* G. Nếu G có vô hạn phần tử thì ta nói G *có cấp vô hạn*.

• Một số ví dụ về nhóm.

- Tập $\mathbb{Z}$ các số nguyên, tập $\mathbb{Q}$ các số hữu tỷ, tập $\mathbb{R}$ các số thực, tập $\mathbb{C}$ các số phức với phép cộng thông thường đều là nhóm giao hoán cấp vô hạn.

- Tập $S(X)$ các song ánh từ một tập X đến chính nó với phép hợp thành các ánh xạ là một nhóm, gọi là *nhóm đối xứng* của X. Nếu X có n phần tử thì $S(X)$ có cấp $n!$ và nhóm này không giao hoán khi $n \geq 3$.

- Với mỗi số tự nhiên $m \geq 1$, tập $\mathbb{Z}_m$ các lớp thặng dư theo môđun m với phép cộng các lớp thặng dư là một nhóm giao hoán cấp m. Tập $\mathbb{Z}_m^*$ các lớp thặng dư theo môđun m nguyên tố cùng nhau với m với phép nhân các lớp thặng dư là một nhóm giao hoán cấp $\varphi(m)$, trong đó φ là hàm Euler.

• Một số tính chất cơ sở: Cho G là một nhóm với đơn vị e. Khi đó

- Phần tử đơn vị của G là duy nhất.
- Phần tử nghịch đảo của mỗi phần tử của G là duy nhất.
- Mọi phần tử của G đều chính quy, tức là thỏa mãn luật giản ước.

1.1.2. Định nghĩa. Tập con H của một nhóm G được gọi là *nhóm con* của G nếu $e \in H$ và $a^{-1} \in H, ab \in H$ với mọi $a, b \in H$.

1.1.3. Định nghĩa. Một nhóm G được gọi là *xyclic* nếu tồn tại $a \in G$ sao cho mỗi phần tử của G đều là một luỹ thừa của a. Trong trường hợp này G được gọi là nhóm xyclic *sinh bởi* a và viết $G =< a >$.

Chú ý rằng nhóm con của nhóm xyclic là xyclic. Cho G là một nhóm và $a \in G$. Đặt

$$< a >= \{a^n \mid n \in \mathbb{Z}\}.$$

Khi đó $< a >$ là nhóm con của G, được gọi là *nhóm con xyclic sinh bởi* a. Cấp của nhóm con $< a >$ được gọi là *cấp của phần tử* a. Dễ thấy rằng a có cấp vô hạn nếu và chỉ nếu $a^n = 0$ kéo theo $n = 0$ với mọi

$n \in \mathbb{Z}$. Hơn nữa, a có cấp n nếu và chỉ nếu n là số nguyên dương bé nhất sao cho $a^n = e$.

1.1.4. Định nghĩa. Cho A là tập con của một nhóm G. Khi đó tồn tại những nhóm con của G chứa A, chẳng hạn G. Giao của tất cả các nhóm con của G chứa A là nhóm con nhỏ nhất của G chứa A. Nhóm con này được gọi là *nhóm con sinh bởi tập* A và kí hiệu là $< A >$.

Rõ ràng nhóm con sinh bởi tập rỗng là $\{e\}$. Nếu $A \neq \emptyset$ thì

$$< A >= \{a_1 a_2 \ldots a_n \ \mid \ n \in \mathbb{N},\ a_1, \ldots, a_n \in A \cup A^{-1}\},$$

trong đó $A^{-1} = \{x^{-1} \ \mid \ x \in A\}$.

1.2 Định lí Lagrange, đồng cấu nhóm

1.2.1. Định nghĩa. Cho H là một nhóm con của một nhóm G. Ta định nghĩa quan hệ $\sim$ trên G như sau: $a \sim b$ nếu và chỉ nếu $ab^{-1} \in H$ với mọi $a, b \in G$. Dễ kiểm tra được $\sim$ là một quan hệ tương đương tren G. Với mỗi $a \in G$, gọi $\overline{a}$ là lớp tương đương của a. Ta có

$$\overline{a} = \{ha \ \mid \ h \in H\} = Ha.$$

Mỗi lớp tương đương Ha được gọi là *một lớp ghép trái của* H trong G. Tập thương của G theo quan hệ tương đương $\sim$ được kí hiệu bởi G/H. Khi H chỉ có hữu hạn lớp ghép trái thì ta gọi *chỉ số của* H *trong* G, kí hiệu là $(G : H)$, là số các lớp ghép trái của H.

1.2.2. Định lý. (**Định lí Lagrange**). *Trong một nhóm hữu hạn, cấp và chỉ số của một nhóm con là ước của cấp của toàn nhóm.*

- Sau đây là một số hệ quả trực tiếp của Định lí Lagrange.

- Cho G là nhóm cấp n và $a \in G$. Khi đó cấp của a là ước của n. Hơn nữa, $a^n = e$.

- Mỗi nhóm cấp nguyên tố đều là nhóm xylic sinh bởi một phần tử tùy ý khác đơn vị.

- Mọi nhóm cấp $\leqslant 5$ đều giao hoán.

1.2.3. Định nghĩa. Cho G là một nhóm. Một nhóm con H của G được gọi là *nhóm con chuẩn tắc* nếu $Ha = aH$ với mọi $a \in G$.

Cho H là nhóm con chuẩn tắc của một nhóm G. Kí hiệu G/H là tập các lớp ghép trái của H trong G. Khi đó quy tắc nhân

$$HaHb = Hab \text{ với mọi } Ha, Hb \in G/H$$

là một phép toán trên G/H, và cùng với phép toán này, G/H làm thành một nhóm. Nhóm G/H xác định như trên được gọi là *nhóm thương của G theo nhóm con chuẩn tắc H*.

1.2.4. Định nghĩa. Cho G và H là các nhóm. Ánh xạ $f : G \longrightarrow H$ được gọi là *đồng cấu nhóm* nếu $f(xy) = f(x)f(y)$ với mọi $x, y \in G$. Một đồng cấu nhóm được gọi là *đơn cấu* (*toàn cấu, đẳng cấu*) nếu nó là đơn ánh (toàn ánh, song ánh). Hai nhóm G và H được gọi là *đẳng cấu với nhau*, viết là $G \cong H$, nếu có một đẳng cấu giữa G và H.

• Một số tính chất:

- Hợp thành của hai đồng cấu nhóm là một đồng cấu nhóm.

- Nếu $f : G \longrightarrow H$ là đồng cấu nhóm thì $f(x^{-1}) = (f(x))^{-1}$ và $f(e) = e$ với mọi $x \in G$.

- Nếu $f : G \longrightarrow H$ là đồng cấu nhóm, A là nhóm con của G và B là nhóm con của H thì $f(A)$ là nhóm con của H và $f^{-1}(B)$ là nhóm con của G. Hơn nữa, nếu B là nhóm con chuẩn tắc thì $f^{-1}(B)$ là nhóm con chuẩn tắc.