BỘ GIÁO DỤC VÀ ĐÀO TẠO
ĐẠI HỌC THÁI NGUYÊN

LÊ THỊ THANH NHÀN (chủ biên)
VŨ MẠNH XUÂN

GIÁO TRÌNH
LÝ THUYẾT NHÓM

(DÙNG CHO SINH VIÊN NGÀNH TOÁN HỌC)

NHÀ XUẤT BẢN ĐẠI HỌC QUỐC GIA HÀ NỘI

SÁCH ĐƯỢC XUẤT BẢN BỞI SỰ TÀI TRỢ CỦA DỰ ÁN GIÁO DỤC ĐẠI HỌC 2

MỤC LỤC

Trang

LỜI NÓI ĐẦU

Mục đích của giáo trình là cung cấp những kiến thức cơ bản nhất về nhóm để phục vụ công tác giảng dạy và học tập môn "Lý thuyết nhóm" ở bậc đại học.

Giáo trình gồm 7 chương. Chương 1 và Chương 2 trình bày kiến thức cơ sở về nhóm, nhóm con, lớp ghép và đồng cấu nhóm. Chương 3 quan tâm đến một số kết quả mang tính kĩ thuật về nhóm như tác động của nhóm lên tập hợp và một ứng dụng trong bài toán tổ hợp. Chương 4 trình bày về nhóm hữu hạn, Định lý Sylow và ứng dụng trong bài toán phân loại nhóm. Chương 5 viết về chuỗi hợp thành và nhóm giải được, một loại nhóm liên quan chặt chẽ với tính giải được bằng căn thức của các đa thức. Chương 6 quan tâm đến nhóm tự do, một ứng dụng của nhóm tự do trong bài toán biểu diễn nhóm bằng hệ sinh và các quan hệ và bài toán phân tích nhóm thành tổng trực tiếp. Chương cuối trình bày các vấn đề về nhóm Abel.

Bạn đọc có thể tự học môn "Lý thuyết nhóm" với cuốn giáo trình này, nếu đã được trang bị một số kiến thức sơ lược về tập hợp, quan hệ, ánh xạ, số phức và không gian véc tơ. Nếu ai đã học "Đại số đại cương" ở chương trình đại học thì có thể bỏ qua các chương 1 và 2 để tiếp cận thẳng các chương sau. Để người đọc dễ theo dõi, trong suốt giáo trình, các khái niệm và kết quả đều được diễn giải chi tiết, có ví dụ minh hoạ; cụm từ "hiển nhiên ta có" tránh được dùng trong các chứng minh; phần bài tập được thiết kế ngay sau một vài mục nhỏ của chương.

Trong toàn bộ cuốn giáo trình, các nhóm được kí hiệu bởi $G, H, K, \ldots$;

các đồng cấu nhóm thường được kí hiệu bởi $f, g, h, k...$; tác động của một phần tử x của nhóm G lên phần tử s của tập hợp S thường được kí hiệu là xs hay $x \bullet s$; tập các số tự nhiên, tập các số nguyên, tập các số hữu tỷ, tập các số thực và tập các số phức lần lượt được kí hiệu bởi $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ và $\mathbb{C}$. Tài liệu tham khảo chính sử dụng trong giáo trình này là các cuốn sách "Giới thiệu về lý thuyết nhóm" của Joseph J. Rotman [7] và "Đại số hiện đại" của Nguyễn Tự Cường [1]. Ngoài ra, giáo trình này được viết trên cơ sở tham khảo một số cuốn sách về Đại số của Bùi Huy Hiền - Phan Doãn Thoại [2], Nguyễn Hữu Việt Hưng [3], M. Aschbacher [5], S. Lang [6], Ngô Thúc Lanh [4].

Trong rất nhiều kiến thức về lý thuyết nhóm, để chọn những nội dung cần thiết viết trong khuôn khổ một giáo trình nhỏ phù hợp với chương trình đào tạo bậc đại học là rất khó khăn. Các tác giả mong muốn nhận được những nhận xét, góp ý của các đồng nghiệp, các sinh viên và đọc giả để cuốn sách được hoàn thiện hơn.

Các tác giả xin chân thành cảm ơn Ban Đào tạo Đại học Thái Nguyên và Dự án TRIG Đại học Thái Nguyên thuộc Dự án Giáo dục Đại học 2 đã hỗ trợ về kinh phí cũng như các thủ tục thuận lợi để cuốn giáo trình được xuất bản.

Các tác giả

Chương 1

Nhóm và nhóm con

1.1 Định nghĩa nhóm và ví dụ

Để tiện theo dõi, trước khi định nghĩa nhóm, chúng ta nhắc lại một số khái niệm liên quan đến phép toán trên một tập hợp.

1.1.1. Định nghĩa. Cho X là tập hợp. Một *phép toán* (hai ngôi) trên X là một ánh xạ từ $X \times X$ đến X.

Nếu T là một phép toán trên X thì ảnh của phần tử $(a, b) \in X \times X$ qua T được kí hiệu là aTb. Ta kí hiệu ảnh của (a, b) là ab nếu phép toán được kí hiệu theo lối nhân và là $a + b$ nếu phép toán được kí hiệu theo lối cộng.

Rõ ràng phép cộng thông thường là phép toán trên $\mathbb{N}$ và cũng là phép toán trên $\mathbb{Z}$. Phép trừ thông thường là phép toán trên $\mathbb{Z}$ nhưng không là phép toán trên $\mathbb{N}$.

1.1.2. Định nghĩa. Cho X là tập hợp có trang bị một phép toán T. Tập con A của X được gọi là *ổn định* (với phép toán trên X) nếu

$aTb \in A$ với mọi $a, b \in A$. Khi đó ta cũng nói phép toán trên X cảm sinh phép toán trên A.

Dễ thấy tập $S = \{1, -1\}$ là bộ phận ổn định của $\mathbb{Z}$ với phép nhân thông thường, tập $\mathbb{N}$ là bộ phận ổn định của $\mathbb{Z}$ với phép cộng, nhưng không ổn định với phép trừ.

1.1.3. Định nghĩa. Cho X là tập hợp và T là phép toán trên X. Ta nói rằng T có tính chất *kết hợp* nếu $aT(bTc) = (aTb)Tc$ với mọi $a, b, c \in X$. Phép toán T là *giao hoán* nếu $aTb = bTa$ với mọi $a, b \in X$. Phép toán T *phân phối* với phép toán $*$ trên X nếu $aT(b*c) = (aTb)*(aTc)$ và $(b * c)Ta = (bTa) * (cTa)$ với mọi $a, b, c \in X$.

Trên các tập số $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, phép cộng và phép nhân thông thường có tính chất kết hợp, giao hoán, phép nhân phân phối với phép cộng. Tuy nhiên phép trừ và phép chia không có tính chất giao hoán, cũng không có tính chất kết hợp.

1.1.4. Định nghĩa. Cho X là tập hợp với một phép toán T. Phần tử $e \in X$ được gọi là *trung hoà trái* nếu $eTa = a$ với mọi $a \in X$. Tương tự ta có khái niệm *trung hoà phải*. Nếu e là trung hoà cả hai phía thì e được gọi là phần tử *trung hoà*. Giả sử X có phần tử trung hoà e. Với $a, b \in X$, ta nói rằng b là *phần tử ngược trái* của a nếu $bTa = e$. Tương tự ta có khái niệm *phần tử ngược phải*. Nếu b là phần tử ngược cả hai phía thì ta nói b là *phần tử ngược* của a. Phần tử $a \in X$ được gọi là *chính quy phải* nếu $xTa = yTa$ kéo theo $x = y$ với mọi $x, y \in X$. Tương tự ta có khái niệm *phần tử chính quy trái*. Nếu a chính quy hai phía thì ta nói a là *chính quy*. Khi a là chính quy thì ta cũng nói *luật giản ước thực hiện được đối với a*. Ta gọi phần tử trung hoà là *phần* *tử đơn vị* nếu phép toán kí hiệu theo lối nhân, và gọi là *phần tử không* nếu phép toán kí hiệu theo lối cộng. Nếu phép toán kí hiệu theo lối nhân, phần tử ngược của a được gọi là *nghịch đảo* của a, và được kí hiệu là a^{-1}. Khi a có nghịch đảo, ta nói a là *khả nghịch*. Nếu phép toán kí hiệu theo lối cộng, phần tử ngược của a được gọi là *đối xứng* của a, và được kí hiệu là $-a$.

Dễ thấy rằng phần tử trung hoà của X đối với phép toán T (nếu có) là duy nhất, bởi vì nếu e, e' là hai phần tử trung hoà thì $e = eTe' = e'$. Chú ý rằng nếu T có tính chất kết hợp thì phần tử ngược của a (nếu có) là duy nhất, bởi vì nếu b, b' là hai phần tử ngược của a thì

$$b = bTe = bT(aTb') = (bTa)Tb' = eTb' = b'.$$

1.1.5. Định nghĩa. *Phỏng nhóm* là một tập hợp trên đó có trang bị một phép toán. *Nửa nhóm* là một phỏng nhóm sao cho phép toán có tính chất kết hợp. *Vị nhóm* là một nửa nhóm có phần tử trung hoà.

Cho $X \neq \emptyset$ là tập hợp. Kí hiệu Γ là tập các ánh xạ từ X đến X. Với phép hợp thành các ánh xạ, ánh xạ đồng nhất 1_X đóng vai trò là phần tử đơn vị của Γ, và phần tử $f \in \Gamma$ là khả nghịch khi và chỉ khi f là song ánh. Vì phép hợp thành các ánh xạ có tính chất kết hợp nên Γ là một vị nhóm.

Từ nay về sau, nếu không nói rõ thêm, ta quy ước phép toán được kí hiệu theo lối nhân.

1.1.6. Định nghĩa. *Nhóm* là một vị nhóm mà mọi phần tử đều khả nghịch. Như vậy, một tập G cùng với một phép toán làm thành nhóm nếu nó 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.*

Trong phần còn lại của mục này, chúng ta đưa ra một số ví dụ về nhóm.

1.1.7. Ví dụ. Các tập hợp $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ với phép cộng thông thường là các nhóm giao hoán cấp vô hạn. Tập hợp $\mathbb{Q}^*$ các số hữu tỷ khác 0 (tập $\mathbb{R}^*$ các số thực khác 0, tập $\mathbb{C}^*$ các số phức khác 0) với phép nhân thông thường là nhóm giao hoán cấp vô hạn.

1.1.8. Ví dụ. Cho X là một tập hợp khác rỗng. Một *phép thế của X* hay một *hoán vị* của tập X là một song ánh từ X đến X. Kí hiệu $S(X)$ là tập các phép thế của X. Khi đó $S(X)$ cùng với phép hợp thành các ánh xạ là một nhóm với đơn vị là ánh xạ đồng nhất 1_X và nghịch đảo của phần tử $f \in S(X)$ là ánh xạ ngược f^{-1} của f. Nhóm $S(X)$ được gọi là *nhóm đối xứng của X* hay *nhóm các phép thế của X*. Khi X có n phần tử thì $S(X)$ được kí hiệu là S_n. Các phần tử của S_n có thể đồng nhất với các song ánh từ tập $\{1, 2, \ldots, n\}$ đến chính nó. Chú ý rằng S_n có cấp là $n!$ và là nhóm không giao hoán khi $n \geq 3$. Nếu n không lớn, người ta thường viết mỗi phần tử $s \in S_n$ bằng cách liệt kê các phần tử $x \in \{1, 2, \ldots, n\}$ và các giá trị tương