

TRƯỜNG ĐẠI HỌC ĐỒNG THÁP
KHOA SƯ PHẠM TOÁN - TIN



TS. LÊ HOÀNG MAI

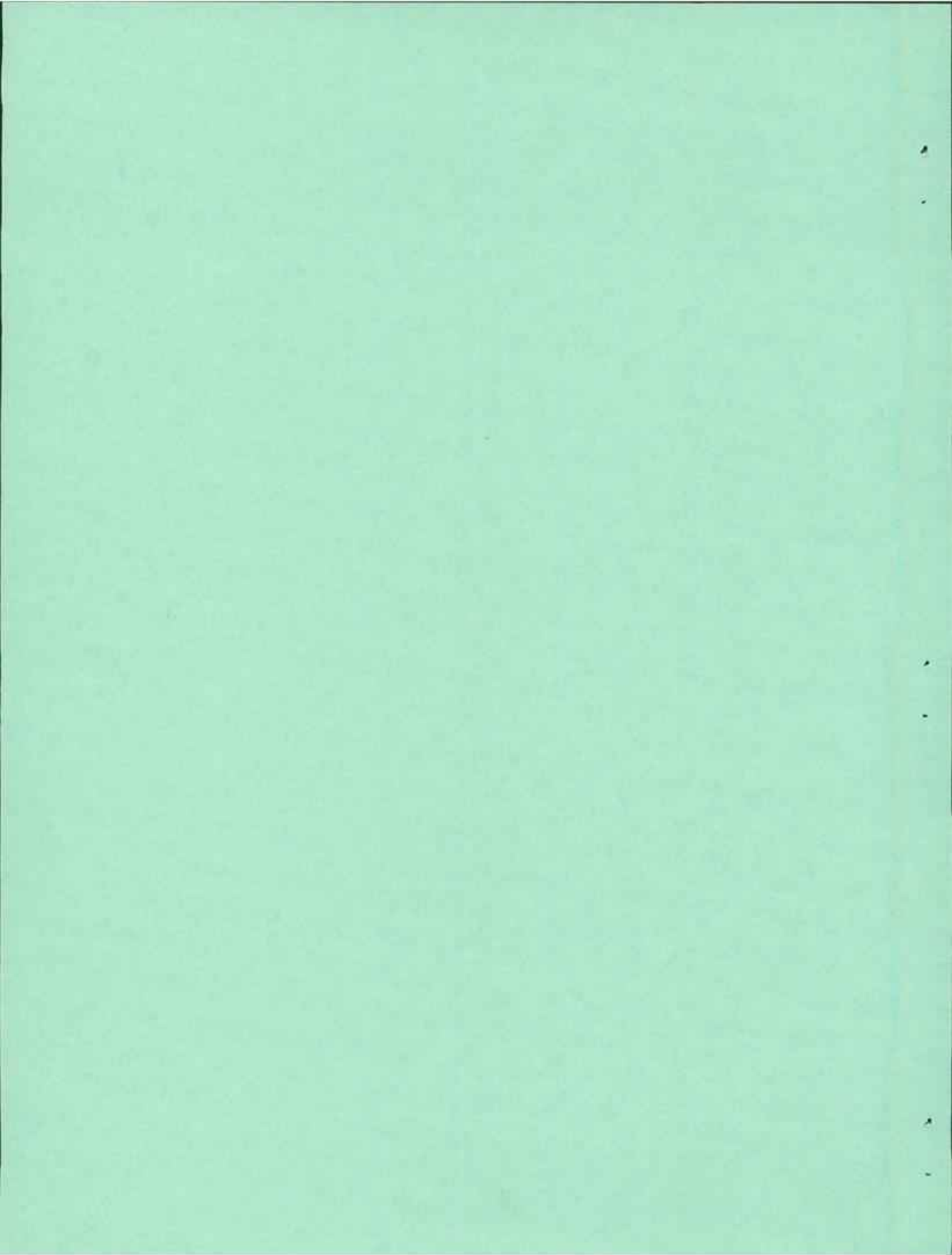
BÀI GIẢNG
ĐẠI SỐ ĐẠI CƯƠNG



DH Đồng Tháp - TV Lê Văn Hùng



KGT.0053213



TRƯỜNG ĐẠI HỌC ĐỒNG THÁP
KHOA SƯ PHẠM TOÁN - TIN



TS. LÊ HOÀNG MAI

BÀI GIẢNG
ĐẠI SỐ ĐẠI CƯƠNG

TRƯỜNG ĐẠI HỌC ĐỒNG THÁP
TRUNG TÂM THÔNG TIN - THƯ VIỆN LÊ VU HÙNG

Số: 65-52213



1947-1948
1949-1950

1947-1948
1949-1950

TRƯỜNG ĐẠI HỌC ĐỒNG THÁP
KHOA SƯ PHẠM TOÁN - TIN

LÊ HOÀNG MAI

Bài giảng
ĐẠI SỐ ĐẠI CƯƠNG
(Tài liệu lưu hành nội bộ)

ĐỒNG THÁP - NĂM 2017

LỜI NÓI ĐẦU

Trong Chương trình đào tạo ngành Đại học Sư phạm (ĐHSP) Toán từ năm 2015 theo hệ thống tín chỉ tại Trường Đại học Đồng Tháp, học phần Đại số đại cương chiếm 3 tín chỉ và giữ một vị trí khá quan trọng. Học phần này được giảng dạy vào học kì 3 của khóa học. Nó hình thành và phát triển tư duy trừu tượng cho sinh viên, khả năng tính toán và giải quyết công việc thực tiễn khi sinh viên tốt nghiệp, cung cấp cho giáo viên tương lai một thể giới toán học bao trùm tất cả các kiến thức đại số ở trường trung học phổ thông.

Trên cơ sở giảng dạy học phần Đại số đại cương cho sinh viên ngành ĐHSPToán trong những năm qua, chúng tôi biên soạn bài giảng này nhằm mục đích giúp cho sinh viên có một tài liệu học tập tương ứng với Đề cương chi tiết học phần đại số đại cương trong chương trình đào tạo ngành ĐHSPToán tại Trường Đại học Đồng Tháp.

Nội dung cơ bản của bài giảng này gồm 3 chương.

Chương 1. Nửa nhóm và nhóm;

Chương 2. Vành và trường;

Chương 3. Vành đa thức.

Trong chương 1, chúng tôi trình bày các khái niệm cơ bản về nhóm như: nửa nhóm, nhóm, nhóm con, nhóm con chuẩn tắc, nhóm thương, đồng cấu nhóm và đối xứng hóa.

Trong chương 2, chúng tôi giới thiệu các khái niệm cơ bản liên quan đến vành và trường như: vành, miền nguyên, trường, vành con, trường con, idêan, vành thương, đồng cấu vành và trường các thương của một miền nguyên.

Trong chương 3, chúng tôi giới thiệu một lớp vành khá quen thuộc có vai trò quan trọng trong đại số đó là vành đa thức một ẩn và nhiều ẩn.

Ngoài nội dung cơ bản trang bị cho sinh viên, chúng tôi đưa vào phần Hướng dẫn tự học và Bài tập ở cuối mỗi chương nhằm giúp cho sinh viên xác định được những nội dung trọng tâm trong mỗi chương và tăng kỹ năng giải toán thông qua việc giải các bài tập.

Đây là lần đầu chúng tôi biên soạn bài giảng đào tạo theo hệ thống tín chỉ, vì thế mặc dù chúng tôi cố gắng rất nhiều nhưng chắc chắn còn có những sai sót. Chúng tôi rất mong nhận được sự góp ý, phê bình của người đọc.

Đồng Tháp, ngày 15 tháng 05 năm 2017

Tác giả

MỤC LỤC

LỜI NÓI ĐẦU	1
BẢNG KÝ HIỆU	3
Chương 1 NỬA NHÓM VÀ NHÓM	5
1.1 Nửa nhóm	5
1.2 Nhóm	9
1.3 Nhóm con	14
1.4 Nhóm con chuẩn tắc. Nhóm Thương	19
1.5 Đồng cấu nhóm	25
1.6 Đối xứng hóa	31
Chương 2 VÀNH VÀ TRƯỜNG ^{ring} (R) ^{vành thụt (R)}	42
2.1 Vành, miền nguyên và trường	42
2.2 Vành con, trường con, ideal và vành thương	47
2.3 Đồng cấu vành	55
2.4 Trường các thương của một miền nguyên	60
Chương 3 VÀNH ĐA THỨC ^{đ. Toán TT}	68
3.1 Vành đa thức một ẩn	68
3.2 Vành đa thức nhiều ẩn	76
TÀI LIỆU THAM KHẢO	95

BẢNG KÝ HIỆU

Kí hiệu	Ý nghĩa
$\mathbb{N}$	Tập hợp các số tự nhiên
$\mathbb{N}^*$	Tập hợp các số nguyên dương
$\mathbb{Z}$	Tập hợp các số nguyên
$\mathbb{Z}^*$	Tập hợp các số nguyên khác không
$\mathbb{Q}$	Tập hợp các số hữu tỷ
$\mathbb{Q}^*$	Tập hợp các số hữu tỷ khác không
$\mathbb{Q}_+$	Tập hợp các số hữu tỷ dương
$\mathbb{R}$	Tập hợp các số thực
$\mathbb{R}^*$	Tập hợp các số thực khác không
$\mathbb{R}_+$	Tập hợp các số thực dương
$\mathbb{C}$	Tập hợp các số phức
$\mathbb{C}^*$	Tập hợp các số phức khác không
$\mathbb{Z}_n$	Tập hợp các số nguyên modulo n
$k \mid n$	Số nguyên k là ước của số nguyên n
$k \nmid n$	Số nguyên k không là ước của số nguyên n
$\overline{a, b}$	Tập các số nguyên $\{a, a+1, \dots, b\}$ với $a, b \in \mathbb{Z}$ và $a < b$
$A \subseteq B$	A là tập con của B
$A \subset B$	A là tập con thực sự của B
$H \leq G$	H là nhóm con của nhóm G
$H < G$	H là nhóm con thực sự của nhóm G
$H \trianglelefteq G$	H là nhóm con chuẩn tắc của nhóm G
$H \triangleleft G$	H là nhóm con chuẩn tắc thực sự của nhóm G
$ G $	Cấp của nhóm G
$ a $	Cấp của phần tử a
$[G : H]$	Chỉ số của nhóm con chuẩn tắc H trong nhóm G
e (hoặc 1)	Phần tử đơn vị (trung hòa) của nhóm, phần tử đơn vị của vành
S_n	Nhóm đối xứng bậc n
G/H	Nhóm thương của nhóm G theo nhóm con chuẩn tắc H

$R[x]$	Vành đa thức ẩn x với hệ tử trên vành giao hoán R
$R[x_1, \dots, x_n]$	Vành đa thức n ẩn $x_1, \dots, x_n$ với hệ tử trên vành giao hoán R
$\text{End}(M)$	Vành các tự đồng cấu của nhóm giao hoán $(M, +)$
$\text{Ker}(f)$	Nhân của đồng cấu f
$\text{Im}(f)$	Ảnh của đồng cấu f
$\prod_{i \in I} R_i$	Tích trực tiếp của một họ các vành $(R_i)_{i \in I}$
$\langle S \rangle$	Idêan sinh bởi tập S
$\langle a \rangle$	Nhóm con xyclic sinh bởi phần tử a
$\cong$	Đồng cấu nhóm, đẳng cấu vành
$\deg(f(x))$	Bậc của đa thức $f(x)$
R^*	Nhóm nhân các phần tử khả nghịch của vành R
$\square$	Kết thúc chứng minh

CHƯƠNG 1

NỬA NHÓM VÀ NHÓM

Trong chương này, chúng tôi trình bày những khái niệm cơ bản nhất liên quan đến cấu trúc nhóm, đồng cấu nhóm. Yêu cầu đối với sinh viên khi học xong chương này là:

Hiểu được các khái niệm như: Phép toán hai ngôi, tính kết hợp, tính giao hoán của phép toán, phần tử đơn vị, phần tử nghịch đảo, khái niệm nhóm, nhóm con, nhóm con xyclic, nhóm con chuẩn tắc, nhóm thương. Nắm vững các khái niệm ảnh, nhân, đồng cấu, đơn cấu, toàn cấu, đẳng cấu nhóm. Nắm vững mối liên hệ giữa các khái niệm này. Nắm vững các đối tượng liên quan đến một số cấu trúc nhóm thường gặp như: Nhóm cộng các số nguyên, nhóm cộng các ma trận cấp n , nhóm các phép thế bậc n , nhóm nhân các số hữu tỷ khác không,...

Có các kỹ năng kiểm tra một tập hợp cùng với phép toán hai ngôi cho trước có phải là một nhóm hay không? Kỹ năng chứng minh nhóm con, nhóm con chuẩn tắc, nhóm con xyclic. Kỹ năng xây dựng ánh xạ và chứng minh ánh xạ là đồng cấu, đơn cấu, toàn cấu, đẳng cấu nhóm. Kỹ năng trình bày lời giải một bài toán chặt chẽ, ngắn gọn và chính xác.

1.1 Nửa nhóm

1.1.1 Phép toán hai ngôi

Định nghĩa 1.1.1.1. Cho X là một tập hợp khác rỗng. Một ánh xạ

$$f: X \times X \rightarrow X$$

đi từ tập hợp tích Đề-các $X \times X$ đến X được gọi là một *phép toán hai ngôi* (gọi tắt là *phép toán*) trên tập hợp X .

Với mỗi cặp $(x, y) \in X \times X$, ảnh $f(x, y) \in X$; kí hiệu xfy , được gọi là *hợp thành* của hai phần tử x và y . Hợp thành xfy là $x.y$, $x+y$, $x*y$, $x \perp y$, ... nếu f là phép toán $., +, *, \perp, \dots$

Phép toán được kí hiệu theo lối nhân "." được gọi là *phép nhân*, hợp thành xfy chính là $x.y$ hay xy được gọi là *tích* của x và y .

Phép toán được kí hiệu theo lối cộng "+" được gọi là *phép cộng*, hợp thành xfy chính là $x+y$ được gọi là *tổng* của x và y .

thứ hợp ánh xạ

Ví dụ 1.1.1.2. (1) Phép cộng, phép nhân thông thường trên tập hợp $\mathbb{N}$ các số tự nhiên là các phép toán hai ngôi trên $\mathbb{N}$. Phép mũ hóa

phản ví dụ:

$$f: \mathbb{N}^* \times \mathbb{N}^* \rightarrow \mathbb{N}^*$$

$$(m, n) \mapsto m^n \text{ số nguyên}$$

cũng là phép toán hai ngôi trên $\mathbb{N}^*$ các số nguyên dương. Tuy nhiên, phép trừ thông thường trên $\mathbb{N}$ không phải là phép toán hai ngôi trên $\mathbb{N}$ vì hiệu của hai số tự nhiên có thể là số nguyên âm, chẳng hạn $2, 5 \in \mathbb{N}$ nhưng $2 - 5 = -3 \notin \mathbb{N}$. *phải có dấu*

(2) Phép cộng, phép trừ và phép nhân thông thường trên các tập $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ và $\mathbb{C}$ là các phép toán hai ngôi trên chúng. Phép chia thông thường trên $\mathbb{Q}^*, \mathbb{R}^*$ và $\mathbb{C}^*$ là các phép toán hai ngôi trên chúng, nhưng phép chia thông thường trên $\mathbb{Z}^*$ không là phép toán hai ngôi trên $\mathbb{Z}^*$ vì thương của hai số nguyên khác không có thể là số hữu tỷ thực sự, chẳng hạn $-3, 7 \in \mathbb{Z}$ nhưng $\frac{-3}{7} \notin \mathbb{Z}$. *phép chia*

(3) Ký hiệu $V(O)_2$ là tập tất cả các vectơ trong mặt phẳng có chung điểm gốc O . Phép cộng hai vectơ được thực hiện theo quy tắc hình bình hành, tức là với mọi $\vec{OA}, \vec{OB} \in V(O)_2: \vec{OA} + \vec{OB} = \vec{OC}$ sao cho $OACB$ là hình bình hành, là một phép toán hai ngôi trên $V(O)_2$.

(4) Cho A là một tập hợp khác rỗng và ký hiệu

$$A^A = \{f: A \rightarrow A \mid f \text{ là ánh xạ}\}$$

là tập tất cả các ánh xạ từ A vào A . Phép hợp thành các ánh xạ trên tập hợp A^A , tức là mọi $f, g \in A^A$ ánh xạ $fg: A \rightarrow A$ xác định bởi $(fg)(a) := f(g(a))$ với mọi $a \in A$, là một phép toán hai ngôi trên tập hợp A^A .

(5) Phép cộng và phép nhân thông thường hai ma trận trên tập hợp $M_n(\mathbb{R})$ các ma trận thực vuông cấp n ($n \geq 2$) là các phép toán hai ngôi trên $M_n(\mathbb{R})$.

thứ hợp tập nguồn

Định nghĩa 1.1.1.3. Cho $f: X \times X \rightarrow X$ là một phép toán hai ngôi trên X và A là một bộ phận khác rỗng của X . Nếu ánh xạ $g: A \times A \rightarrow A$ xác định bởi $g(a, b) = f(a, b) \in A$ với mọi $(a, b) \in A \times A$ thì g được gọi là phép toán cảm sinh trên A bởi phép toán f của X . Ký hiệu $g = f|_A$.

Ví dụ 1.1.1.4. (1) Phép toán cộng và phép toán nhân thông thường trên $\mathbb{N}$ là các phép toán cảm sinh trên $\mathbb{N}$ bởi các phép toán cộng và phép toán nhân thông thường trên $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ và $\mathbb{C}$.

(2) Phép toán cộng và phép toán nhân thông thường hai ma trận trên $M_n(\mathbb{Q})$ là các phép toán cảm sinh trên $M_n(\mathbb{Q})$ bởi các phép toán cộng và phép toán nhân ma trận trên $M_n(\mathbb{R})$.

1.1.2 Nửa nhóm và vị nhóm

Định nghĩa 1.1.2.1. Cho tập hợp khác rỗng X và một phép toán nhân $"."$ trên X , kí hiệu $(X, .)$.

- (1) Phép toán $"."$ trên X được gọi là kết hợp nếu với mọi $x, y, z \in X$ ta có
- $$(xy)z = x(yz).$$

Trong trường hợp này tích $(xy)z$ hay $x(yz)$ được viết là xyz gọi là tích của ba phần tử x, y, z lấy theo thứ tự đó.

- (2) Phép toán $"."$ trên X được gọi là giao hoán nếu với mọi $x, y \in X$ ta có

- (3) Phần tử e' (e'') $\in X$ được gọi là đơn vị trái (phải) của X đối với phép toán $"."$ nếu với mọi $x \in X$ ta có

Phần tử $e \in X$ được gọi là đơn vị của X đối với phép toán $"."$ nếu e đồng thời là đơn vị trái và phải của X , tức là $ex = xe = x$ với mọi $x \in X$. Phần tử đơn vị của X thường còn được kí hiệu là 1_X hay 1 *theo*.

Lưu ý rằng nếu phép toán trên X được kí hiệu theo lối cộng $"+"$ thì phần tử đơn vị được gọi là phần tử trung lập, kí hiệu 0_X hay 0 .

Mệnh đề 1.1.2.2. Giả sử $(X, .)$ là một tập hợp khác rỗng và $"."$ là một phép toán hai ngôi trên X . Khi đó,

- (1) Nếu X có đơn vị trái e' và đơn vị phải e'' thì $e' = e''$.
 (2) Phần tử đơn vị của $(X, .)$ (nếu có) là duy nhất.

Chứng minh. (1) Vì e' là đơn vị trái của X nên $e'e'' = e''$ và vì e'' là đơn vị phải của X nên $e'e'' = e'$. Suy ra, $e' = e''$.

(2) Giả sử e_1 và e_2 là các phần tử đơn vị của X . Khi đó, e_1 cũng là đơn vị trái và e_2 cũng là đơn vị phải của X . Theo chứng minh (1), ta có $e_1 = e_2$. $\square$

Định nghĩa 1.1.2.3. Cho tập hợp khác rỗng X và $"."$ là một phép toán hai ngôi trên X .

- (1) $(X, .)$ được gọi là nửa nhóm nếu phép toán $"."$ trên X có tính kết hợp.
 (2) Nửa nhóm $(X, .)$ được gọi là vị nhóm nếu X có phần tử đơn vị e đối với phép toán $"."$.
 (3) Nửa nhóm (vị nhóm) $(X, .)$ được gọi là nửa nhóm (vị nhóm) giao hoán nếu phép toán $"."$ có tính giao hoán.

empty $x = \phi$: 0 có phần tử
 $x = \{a\}$: phần tử hàng ϕ^n study

Ví dụ 1.1.2.4. (1) Các tập hợp $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ và $\mathbb{C}$ cùng với phép toán cộng (nhân) thông thường là các vị nhóm giao hoán với phần tử trung lập (đơn vị) là số 0 (số 1).

(2) Tập hợp $M_n(\mathbb{R})$ cùng với phép cộng thông thường hai ma trận là một vị nhóm giao hoán với phần tử trung lập là ma trận không 0_n cấp n . Tuy nhiên, Tập hợp $M_n(\mathbb{R})$ cùng với phép nhân thông thường hai ma trận là một vị nhóm không giao hoán với phần tử đơn vị là ma trận đơn vị I_n cấp n với $n \geq 2$. Chẳng hạn, trên $M_2(\mathbb{R})$ ta có

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}.$$

Định nghĩa 1.1.2.5. Cho $(X, \cdot)$ là một nửa nhóm.

(1) Với mỗi số nguyên dương n , tích của n phần tử $x_1, x_2, \dots, x_n$ thuộc X , kí hiệu là $x_1 x_2 \dots x_n$ hay $\prod_{i=1}^n x_i$, được xác định bởi các công thức quy nạp như sau:

$$\prod_{i=1}^1 x_i = x_1 \text{ và } \prod_{i=1}^n x_i = \left(\prod_{i=1}^{n-1} x_i \right) x_n \text{ với } n > 1.$$

(2) Nếu $x_1 = x_2 = \dots = x_n = x$ thì tích $xx \dots x$ được kí hiệu x^n và được gọi là lũy thừa nguyên dương mũ n của phần tử x .

Lưu ý rằng nếu phép toán trong nửa nhóm X kí hiệu theo lối cộng "+" thì tổng của n phần tử $x_1, x_2, \dots, x_n \in X$ được kí hiệu $x_1 + x_2 + \dots + x_n$ hay $\sum_{i=1}^n x_i$. Nếu $x_1 = x_2 = \dots = x_n = x$ thì tổng $x + x + \dots + x$ được kí hiệu nx và được gọi là bội nguyên dương n của phần tử x .

Định lý 1.1.2.6. (về tính kết hợp) Giả sử $(X, \cdot)$ là một nửa nhóm và $x_1, x_2, \dots, x_n$ là n ($n \geq 3$) phần tử của X . Khi đó,

$$x_1 x_2 \dots x_n = (x_1 \dots x_i)(x_{i+1} \dots x_k) \dots (x_{m+1} \dots x_n).$$

Chứng minh. Quy nạp theo n . Với $n = 3$ thì định lý đúng vì $(X, \cdot)$ là một nửa nhóm. Giả sử định lý đúng với k nhân tử $3 \leq k \leq n - 1$. Theo định nghĩa tích

Số lượng phần tử

của nhiều phần tử và theo giả thiết quy nạp, ta có

$$\begin{aligned}
 (x_1 \dots x_i)(x_{i+1} \dots x_k) \dots (x_{m+1} \dots x_n) &= [(x_1 \dots x_i) \dots (x_{j+1} \dots x_m)](x_{m+1} \dots x_n) \\
 &= (x_1 \dots x_m)(x_{m+1} \dots x_n) \\
 &= (x_1 \dots x_m)[(x_{m+1} \dots x_{n-1})x_n] \\
 &= [(x_1 \dots x_m)(x_{m+1} \dots x_{n-1})]x_n \\
 &= (x_1 \dots x_{n-1})x_n \\
 &= x_1 \dots x_n.
 \end{aligned}$$

Vậy định lý đúng với mọi số nguyên dương $n \geq 3$. □

Từ Định lý 1.1.2.6 ta tức thì có được hệ quả sau đây.

Hệ quả 1.1.2.7. Nếu x là một phần tử của nửa nhóm $(X, \cdot)$ và m, n là hai số nguyên dương thì

$$x^{m+n} = x^m \cdot x^n \text{ và } x^{mn} = (x^m)^n.$$

Lưu ý rằng nếu x là một phần tử của nửa nhóm $(X, +)$ và m, n là hai số nguyên dương thì

$$(m+n)x = mx + nx \text{ và } (mn)x = n(mx).$$

Sử dụng Định lý 1.1.2.6 và tính giao hoán của phép toán, ta chứng minh được hệ quả sau bằng quy nạp theo $n \geq 2$.

Hệ quả 1.1.2.8. Cho $x_1, x_2, \dots, x_n$ là n ($n \geq 2$) phần tử của nửa nhóm giao hoán $(X, \cdot)$ và $(i_1, i_2, \dots, i_n)$ là một hoán vị của tập $\{1, 2, \dots, n\}$. Khi đó,

$$x_1 x_2 \dots x_n = x_{i_1} x_{i_2} \dots x_{i_n}.$$

1.2 Nhóm

1.2.1 Định nghĩa và ví dụ

Định nghĩa 1.2.1.1. Cho $(G, \cdot)$ là một vị nhóm "nhân" với phần tử đơn vị e . Phần tử $x \in G$ được gọi là *khả nghịch* nếu tồn tại phần tử $x' \in G$ sao cho

$$x'x = xx' = e.$$

Phần tử x' được gọi là *phần tử nghịch đảo* của phần tử x .

Lưu ý rằng nếu $(G, +)$ là một vị nhóm "cộng" với phần tử trung lập 0 thì phần tử $x \in G$ được gọi là *khả đối* khi tồn tại phần tử $x' \in G$ sao cho

$$x' + x = x + x' = 0.$$

Phần tử x' được gọi là *phần tử đối xứng* của phần tử x .

Định lý 1.2.1.2. (tính duy nhất của phần tử nghịch đảo) *Giả sử $(G, \cdot)$ là một vị nhóm với phần tử đơn vị e . Khi đó, phần tử nghịch đảo của phần tử $x \in G$ (nếu có) là duy nhất.*

Chứng minh. Giả sử $x \in G$ có hai phần tử nghịch đảo là $x', x'' \in G$. Khi đó, $xx' = x'x = e$ và $xx'' = x''x = e$. Ta cần chứng minh $x' = x''$. Thật vậy,

$$x' = x'e = x'(xx'') = (x'x)x'' = ex'' = x''.$$

Vậy phần tử nghịch đảo (nếu có) là duy nhất. □

Phần tử nghịch đảo của phần tử $x \in G$ được kí hiệu x^{-1} . Dễ dàng thấy rằng, nếu phần tử x có phần tử nghịch đảo là x^{-1} thì $(x^{-1})^{-1} = x$.

Định nghĩa 1.2.1.3. Cho G là một tập hợp khác rỗng và $\cdot$ là phép toán trên G . Ta gọi $(G, \cdot)$ là một *nhóm (group)* nếu thỏa mãn 3 điều kiện sau:

- (1) Phép toán $\cdot$ trên G có tính kết hợp;
- (2) $(G, \cdot)$ có phần tử đơn vị;
- (3) Mọi phần tử $x \in G$ có phần tử nghịch đảo trong G .

Nhóm $(G, \cdot)$ gọi là *nhóm giao hoán* nếu phép toán có tính giao hoán.

Chúng ta cũng có thể định nghĩa nhóm từ nửa nhóm và vị nhóm như sau:

- (1) Một nửa nhóm $(G, \cdot)$ được gọi là nhóm khi G có phần tử đơn vị và mọi phần tử $x \in G$ luôn có phần tử nghịch đảo trong G .
- (2) Một vị nhóm $(G, \cdot)$ được gọi là nhóm khi mọi phần tử $x \in G$ luôn có phần tử nghịch đảo trong G .

Ví dụ 1.2.1.4. (1) Các tập hợp $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ và $\mathbb{C}$ cùng với phép cộng thông thường là các nhóm giao hoán. Tuy nhiên, tập hợp $\mathbb{N}$ cùng với phép cộng thông thường chỉ là vị nhóm giao hoán nhưng không là nhóm vì các số tự nhiên khác không thì không khả đối trong $\mathbb{N}$.

(2) Các tập hợp $\mathbb{Q}^*, \mathbb{R}^*$ và $\mathbb{C}^*$ cùng với phép nhân thông thường là các nhóm giao hoán. Tuy nhiên, tập hợp $\mathbb{Z}^*$ cùng với phép nhân thông thường chỉ là vị

nhóm giao hoán mà không là nhóm vì chỉ có các số nguyên 1 và -1 là khả nghịch trong $\mathbb{Z}^*$.

(3) Tập hợp $M_n(\mathbb{R})$ cùng với phép cộng ma trận là một nhóm giao hoán. Tuy nhiên, tập hợp $M_n(\mathbb{R})$ cùng với phép nhân ma trận chỉ là một vị nhóm không giao hoán ($n \geq 2$) nhưng không là nhóm vì các ma trận có định thức khác không mới khả nghịch trong $M_n(\mathbb{R})$.

(4) Tập hợp $GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det(A) \neq 0\}$ cùng với phép nhân ma trận là một nhóm không giao hoán ($n \geq 2$). Nhóm này được gọi là *nhóm tuyến tính tổng quát bậc n trên $\mathbb{R}$* .

(5) Đặt $X = \{1, 2, \dots, n\}$ với $n \geq 1$ và

$$S_n = \{f : X \rightarrow X \mid f \text{ là song ánh}\}$$

là tập hợp tất cả các song ánh từ X vào chính nó. Khi đó, S_n là một nhóm với phép nhân ánh xạ với phần tử đơn vị là ánh xạ đồng nhất id_X và phần tử nghịch đảo của phần tử $f \in S_n$ là song ánh ngược f^{-1} . Nhóm S_n được gọi là *nhóm đối xứng bậc n* . Mỗi song ánh $f \in S_n$ được gọi là một *phép thế* bậc n , kí hiệu là

$$f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}.$$

1.2.2 Một số tính chất

Định lý 1.2.2.1. (luật giản ước) Cho $(G, \cdot)$ là một nhóm. Nếu $xy = xz$ ($yx = zx$) với $x, y, z \in G$ thì $y = z$.

Chứng minh. Vì $(G, \cdot)$ là nhóm nên tồn tại phần tử nghịch đảo x^{-1} của phần tử $x \in G$. Nhân bên trái hai vế của đẳng thức $xy = xz$ với x^{-1} và áp dụng tính chất kết hợp, ta được

$$\begin{aligned} x^{-1}(xy) &= x^{-1}(xz) \\ \Rightarrow (x^{-1}x)y &= (x^{-1}x)z \\ \Rightarrow ey &= ez \\ \Rightarrow y &= z. \end{aligned}$$

Chứng minh tương tự đối với trường hợp còn lại. □

Định lý 1.2.2.2. Cho $(G, \cdot)$ là một nhóm. Khi đó, phương trình $ax = b$ ($xa = b$) với $a, b \in G$ luôn tồn tại duy nhất nghiệm $x = a^{-1}b$ ($x = ba^{-1}$).

Chứng minh. • Tồn tại: Vì $a(a^{-1}b) = (aa^{-1})b = eb = b$ nên $x_0 = a^{-1}b$ là nghiệm của phương trình $ax = b$.

• Duy nhất: Giả sử $c \in G$ cũng là nghiệm của phương trình $ax = b$. Ta cần chứng minh $c = x_0$. Thật vậy, vì x_0 và c đều là nghiệm của phương trình $ax = b$ nên $ac = ax_0 = b$. Từ luật giản ước của Định lý 1.2.2.1 suy ra $x_0 = c$.

Chứng minh tương tự cho phương trình $xa = b$. $\square$

Định lý 1.2.2.3. Cho $(G, \cdot)$ là một nhóm và với mọi phần tử $x, y \in G$. Khi đó, phần tử nghịch đảo của phần tử xy là tích phần tử nghịch đảo của y với phần tử nghịch đảo của x theo thứ tự đó, tức là

$$(xy)^{-1} = y^{-1}x^{-1}.$$

Chứng minh. Vì $(G, \cdot)$ là một nhóm và $x, y \in G$ nên tồn tại các phần tử nghịch đảo $x^{-1}, y^{-1} \in G$. Ta có

$$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xex^{-1} = xx^{-1} = e$$

$$(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}ey = y^{-1}y = e$$

tức là $(xy)^{-1} = y^{-1}x^{-1}$. $\square$

Định lý 1.2.2.3 có thể mở rộng cho n phần tử tùy ý của nhóm G với $n \geq 2$. Tức là, với bất kì $x_1, x_2, \dots, x_n \in G$ ta luôn có

$$(x_1x_2 \dots x_n)^{-1} = x_n^{-1}x_{n-1}^{-1} \dots x_1^{-1}.$$

Đặc biệt, khi $x_1 = x_2 = \dots = x_n = x$ thì $(x^n)^{-1} = (x^{-1})^n$ với mọi số tự nhiên n khác 0. Phần tử nghịch đảo của phần tử x^n với $n \in \mathbb{N}^*$ được quy ước là x^{-n} , tức là $x^{-n} = (x^{-1})^n$ và đặt $x^0 = e$.

Từ kết quả này và Định nghĩa 1.1.2.5, chúng ta đã hoàn thành việc xác định x^α với $x \in G$ và mọi $\alpha \in \mathbb{Z}$.

Kết quả tiếp theo là mở rộng của Hệ quả 1.1.2.7 ra tập số nguyên $\mathbb{Z}$. Việc chứng minh kết quả này xem như một bài tập cho người đọc.

Hệ quả 1.2.2.4. Nếu x là một phần tử của nhóm $(G, \cdot)$ và α, β là hai số nguyên thì

$$x^{\alpha+\beta} = x^\alpha x^\beta \text{ và } x^{\alpha\beta} = (x^\alpha)^\beta.$$

Lưu ý rằng nếu x là một phần tử của nhóm $(G, +)$ và α, β là hai số nguyên thì

$$(\alpha + \beta)x = \alpha x + \beta x \text{ và } (\alpha\beta)x = \alpha(\beta x).$$

Hai định lý sau đây cho ta các điều kiện tương đương với định nghĩa nhóm.

Định lý 1.2.2.5. Một nửa nhóm $(G, \cdot)$ là một nhóm nếu và chỉ nếu hai điều kiện sau đây được thỏa mãn:

(1) Tồn tại một đơn vị trái e , tức là tồn tại $e \in G$ sao cho $ex = x$ với mọi $x \in G$;

(2) Tồn tại nghịch đảo trái, tức là với mọi $x \in G$ có một $x' \in G$ sao cho $x'x = e$.

Chứng minh. $(\Rightarrow)$ Giả sử $(G, \cdot)$ là một nhóm. Từ Định nghĩa 1.2.1.3 suy ra (1) và (2).

$(\Leftarrow)$ Giả sử nửa nhóm $(G, \cdot)$ thỏa mãn (1) và (2). Lấy một phần tử tùy ý $x \in G$, theo (2) có một phần tử $x' \in G$ sao cho $x'x = e$. Vì $x' \in G$ nên tiếp tục sử dụng (2), có một phần tử $x'' \in G$ sao cho $x''x' = e$. Ta có

$$xx' = e(xx') = (x''x')(xx') = x''(x'x)x' = x''ex' = x''x' = e.$$

Mặt khác, ta lại có

$$xe = x(x'x) = (xx')x = ex = x.$$

Vậy $ex = xe = x$ và $x'x = xx' = e$ nên e là đơn vị của G và x' là nghịch đảo của x . Suy ra $(G, \cdot)$ là một nhóm. $\square$

Định lý 1.2.2.6. Một nửa nhóm $(G, \cdot)$ là một nhóm nếu và chỉ nếu các phương trình $ax = b$ và $ya = b$ có nghiệm trong G với mọi $a, b \in G$.

Chứng minh. $(\Rightarrow)$ Giả sử $(G, \cdot)$ là một nhóm. Từ Định lý 1.2.2.2, các phương trình $ax = b$ và $ya = b$ có nghiệm duy nhất trong G lần lượt là $a^{-1}b$ và ba^{-1} .

$(\Leftarrow)$ Giả sử nửa nhóm $(G, \cdot)$ thỏa mãn các phương trình $ax = b$ và $ya = b$ có nghiệm trong G với mọi $a, b \in G$. Vì G khác rỗng nên có phần tử $a \in G$. Gọi $e \in G$ là một nghiệm của phương trình $ya = a$, tức là $ea = a$. Ta chứng minh e chính là đơn vị trái của G . Giả sử b là phần tử tùy ý của G , ta cần chứng minh $eb = b$. Gọi $c \in G$ là một nghiệm của phương trình $ax = b$, tức là $ac = b$. Ta có

$$eb = e(ac) = (ea)c = ac = b.$$

Vậy e là đơn vị trái của G . Bây giờ ta chứng minh b có nghịch đảo trái trong G . Vì phương trình $yb = e$ có nghiệm trong G nên tồn tại $b' \in G$ sao cho $b'b = e$ hay b' là nghịch đảo trái của b . Theo Định lý 1.2.2.5, suy ra $(G, \cdot)$ là một nhóm. $\square$

1.3 Nhóm con

1.3.1 Định nghĩa và ví dụ

Định nghĩa 1.3.1.1. Cho $(G, \cdot)$ là một nhóm.

(1) Một tập con khác rỗng H của G được gọi là *ổn định* đối với phép toán " $\cdot$ " nếu $ab \in H$ với mọi $a, b \in H$.

(2) Một tập con ổn định H của G được gọi là *nhóm con* của G , kí hiệu $H \leq G$, nếu H cùng với phép toán cảm sinh trên H là một nhóm.

Ví dụ 1.3.1.2. (1) Tập con $\mathbb{Z}$ của $\mathbb{Q}$ ($\mathbb{R}, \mathbb{C}$) ổn định đối với phép toán cộng thông thường và $(\mathbb{Z}, +)$ cũng là một nhóm nên $(\mathbb{Z}, +)$ là nhóm con của $(\mathbb{Q}, +)$ ($(\mathbb{R}, +)$, $(\mathbb{C}, +)$). Tương tự, $(\mathbb{Q}, +)$ là nhóm con của $(\mathbb{R}, +)$ và $(\mathbb{C}, +)$; $(\mathbb{R}, +)$ là nhóm con của $(\mathbb{C}, +)$.

(2) Tập con $\mathbb{Q}^*$ của $\mathbb{R}^*$ ($\mathbb{C}^*$) ổn định đối với phép toán nhân thông thường và $(\mathbb{Q}^*, \cdot)$ cũng là một nhóm nên $(\mathbb{Q}^*, \cdot)$ là nhóm con của $(\mathbb{R}^*, \cdot)$ và $(\mathbb{C}^*, \cdot)$. Tương tự, $(\mathbb{R}^*, \cdot)$ là nhóm con của $(\mathbb{C}^*, \cdot)$. Lưu ý rằng, tập con $\mathbb{Z}^*$ của $\mathbb{Q}^*$ ổn định đối với phép toán nhân thông thường nhưng $(\mathbb{Z}^*, \cdot)$ không là nhóm con của $(\mathbb{Q}^*, \cdot)$ vì $(\mathbb{Z}^*, \cdot)$ không là một nhóm.

1.3.2 Các tính chất

Định lý 1.3.2.1. Cho $(G, \cdot)$ là một nhóm và H là một tập con khác rỗng của G . Khi đó, H là nhóm con của G nếu và chỉ nếu các điều kiện sau đây thỏa mãn:

- (1) Với mọi $x, y \in H$, $xy \in H$;
- (2) Phần tử $e \in H$ với e là phần tử đơn vị của G ;
- (3) Với mọi $x \in H$, $x^{-1} \in H$.

Chứng minh. ($\Rightarrow$) Giả sử H là nhóm con của nhóm G .

Theo Định nghĩa 1.3.1.1 ta có ngay (1).

Giả sử e' là phần tử đơn vị của nhóm con H , ta cần chứng minh $e' = e$. Với mọi $x \in H$, $e'x = x$ vì e' là phần tử đơn vị của H . Mặt khác, $ex = x$ vì e là phần tử đơn vị của G . Suy ra $e'x = ex$ hay $e' = e$ vì luật giản ước thực hiện được với mọi phần tử của nhóm G . Vậy ta có (2).

Gọi x' là phần tử nghịch đảo của phần tử $x \in H$, ta chứng minh $x' = x^{-1}$ với x^{-1} là phần tử nghịch đảo của x trong G . Ta có $x'x = e$ vì x' là phần tử nghịch đảo của phần tử $x \in H$ và $x^{-1}x = e$ vì x^{-1} là phần tử nghịch đảo của phần tử $x \in G$. Suy ra $x'x = x^{-1}x$ hay $x' = x^{-1}$ vì luật giản ước thực hiện được với mọi phần tử của nhóm G . Vậy ta có (3).

($\Leftarrow$) Giả sử H là một tập con khác rỗng của nhóm G thỏa mãn (1), (2) và (3). Ta cần chứng minh H là nhóm con của G .

Từ (1) suy ra H là tập con ổn định của nhóm G . Hiển nhiên phép toán "." cảm sinh trên H có tính kết hợp vì phép toán trên G có tính kết hợp.

Từ (2) suy ra H có phần tử đơn vị e (cũng là phần tử đơn vị của nhóm G).

Từ (3) suy ra mọi phần tử của H luôn có nghịch đảo trong H .

Vậy $(H, .)$ là một nhóm. Theo Định nghĩa 1.3.1.1, H là nhóm con của G . $\square$

Hệ quả 1.3.2.2. Cho $(G, .)$ là một nhóm và H là một tập con khác rỗng của G . Khi đó, các điều kiện sau là tương đương:

- (1) H là một nhóm con của G .
- (2) Với mọi $x, y \in H$, $xy \in H$ và $x^{-1} \in H$.
- (3) Với mọi $x, y \in H$, $xy^{-1} \in H$.

Chứng minh. (1) $\Rightarrow$ (2): Được suy ra ngay lập tức từ Định lý 1.3.2.1.

(2) $\Rightarrow$ (3): Với mọi $x, y \in H$, từ (2) suy ra $y^{-1} \in H$, tiếp tục từ (2) suy ra $xy^{-1} \in H$.

(3) $\Rightarrow$ (1): Vì $H \neq \emptyset$ nên tồn tại $x \in H$, từ (3) suy ra $e = xx^{-1} \in H$.

Với mọi $x \in H$, vì $e \in H$ nên từ (3) suy ra $ex^{-1} \in H$ hay $x^{-1} \in H$.

Cuối cùng, với mọi $x, y \in H$ suy ra $x, y^{-1} \in H$, tiếp tục từ (3) suy ra $x(y^{-1})^{-1} \in H$ hay $xy \in H$.

Theo Định lý 1.3.2.1, H là một nhóm con của G . $\square$

Ví dụ 1.3.2.3. (1) Cho $(G, .)$ là một nhóm với đơn vị e . Tập con $\{e\}$ và G là hai nhóm con của G . Ta gọi $\{e\}$ và G là các nhóm con tầm thường của G .

(2) Với $m \in \mathbb{Z}$, tập con

$$m\mathbb{Z} = \{mk \mid k \in \mathbb{Z}\}$$

gồm các số nguyên là bội của số nguyên m cho trước là một nhóm con của $(\mathbb{Z}, +)$. Thật vậy, $0 = m0 \in m\mathbb{Z}$ nên $m\mathbb{Z} \neq \emptyset$ và với mọi $mx, my \in m\mathbb{Z}$,

$$mx - my = m(x - y) \in m\mathbb{Z}$$

vì $x - y \in \mathbb{Z}$. Theo Hệ quả 1.3.2.2 từ (3) suy ra (1), ta có $m\mathbb{Z}$ là nhóm con của nhóm cộng $\mathbb{Z}$.

(3) Cho $(G, .)$ là một nhóm và phần tử $a \in G$ bất kì. Tập con

$$H = \{a^\lambda \mid \lambda \in \mathbb{Z}\}$$