

NGUYỄN TIẾN QUANG

ĐẠI SỐ ĐẠI CƯƠNG



NHÀ XUẤT BẢN GIÁO DỤC

NGUYỄN TIẾN QUANG

ĐẠI SỐ ĐẠI CƯƠNG

NHÀ XUẤT BẢN GIÁO DỤC

Bản quyền thuộc HEVOBCO – Nhà xuất bản Giáo dục

113-2008/CXB/60-175/GD

Mã số: 7B706Y8-DAI

Lời nói đầu

Môn học Đại số đại cương hay Đại số hiện đại được giảng dạy cho sinh viên toán vào những học kỳ đầu của khoá học. Với môn học này sinh viên được làm quen với những cấu trúc trừu tượng vượt ra ngoài khuôn khổ quen thuộc của các hệ thống số và phương trình trong Đại số cổ điển. Và cũng từ đó hình thành tư duy trừu tượng ở mức độ sâu sắc với phạm vi rộng rãi hơn. Chính sự trừu tượng ở nội dung và phương pháp tư duy này đã là một trở ngại không nhỏ cho một số người học và đồng thời cũng chính điều này lại lôi cuốn, hấp dẫn cho số đông những người bước đầu tìm hiểu Toán học hiện đại.

Đã có khá nhiều giáo trình trong và ngoài nước viết về Đại số đại cương. Nội dung và phương pháp trình bày khác nhau tùy thuộc vào quan niệm của từng tác giả về tính hệ thống, sự cần thiết của những kiến thức được coi là cơ bản, về khả năng tiếp thu của người đọc và tùy thuộc vào thẩm mỹ riêng của từng tác giả. Hơn thế nữa, sự phong phú của các giáo trình không phải ở chỗ khác biệt về nội dung kiến thức mà có lẽ ở nghệ thuật trình bày, nghệ thuật truyền thụ.

Chúng ta cũng phải nói thêm rằng sự phát triển của khoa học và đời sống đã dẫn tới những thay đổi cơ bản về sự nhận thức của người học cũng như những thay đổi về quan niệm các kiến thức thiết yếu. Ví dụ, sự phát triển và ứng dụng rộng rãi của công nghệ thông tin đòi hỏi chúng ta phải có nhiều cách nhìn mới, trong đó có việc đưa các kỹ thuật gần hơn với các vấn đề ứng dụng.

Cuốn sách này được biên soạn dựa trên những điều mà chúng tôi vừa trình bày. Nội dung của nó bao gồm 6 chương.

Chương I, ngoài một số yếu tố cơ bản của đại số hiện đại như tập hợp, ánh xạ, quan hệ hai ngôi, chúng tôi trình bày về số nguyên, tuy không đòi hỏi sự chặt chẽ nhưng có đủ những kết quả cần thiết để sử dụng trong các chương sau như định lý về phép chia với dư, ước chung lớn nhất. Điều này là rất cần thiết để có thể chứng minh những tính chất cơ bản về cấp trong lý thuyết nhóm.

Chương II trình bày những kiến thức cơ sở về nhóm. Ở đây chúng tôi thấy cần thiết phải đưa ra một số ví dụ cho thấy tính ứng dụng của khái niệm nhóm, cấu trúc đại số trừu tượng đầu tiên mà sinh viên được làm quen. Một số kiến thức đi sâu hơn về nhóm được trình bày

trong chương III. Một vài mục của chương này có thể xem như phần đọc thêm, tùy theo đối tượng.

Lý thuyết về vành và trường được viết theo ba chương. Chương IV trình bày những vấn đề chung. Chương V nói về một lớp vành quen thuộc có vai trò quan trọng trong đại số là vành đa thức, và những lớp vành khái quát của lớp vành này và vành các số nguyên, trong đó có tính nhân tử hoá và thuật toán chia Óclit. Chương VI được xem như một ứng dụng của lý thuyết vành vào các đa thức trên các trường số.

Để giảm bớt tính khó khăn cho người đọc, chúng tôi cố gắng trình bày cụ thể một số ví dụ. Điều này còn giúp cho người đọc hiểu sâu hơn những vấn đề của lý thuyết. Hệ thống bài tập được cho theo từng tiết. Việc giải một số lớn những bài tập này là cần thiết và hết sức bổ ích đối với người đọc.

Cuốn sách được hình thành dựa trên những quan sát chúng tôi có được từ thực tế giảng dạy cho sinh viên khoa Toán-Tin trường Đại học Sư phạm Hà Nội cũng như cho sinh viên tại chức ở nhiều địa phương trong cả nước. Chúng tôi hy vọng đây là một tài liệu có ích về đại số cho sinh viên không chỉ ở hệ Đại học mà cả ở hệ Cao đẳng Sư phạm.

Những thảo luận cùng các đồng nghiệp trong quá trình giảng dạy đã giúp cho chúng tôi nhiều ý kiến quý báu khi biên soạn cuốn sách này.

Cuốn sách không thể tránh khỏi những thiếu sót. Chúng tôi mong nhận được sự góp ý của bạn đọc.

Thư góp ý xin gửi về: Công ty cổ phần sách Đại học - Dạy nghề, 25 Hàn Thuyên, Hà Nội.

Tác giả

Mục lục

<i>Lời nói đầu</i>	3
<i>Bảng ký hiệu</i>	7
<i>Chương I. Cơ sở</i>	9
1. Tập hợp	9
2. Ánh xạ	15
3. Quan hệ hai ngôi	22
4. Số nguyên	29
<i>Chương II. Nhóm-Đồng cấu nhóm</i>	44
1. Đại số hai ngôi	44
2. Nhóm	54
3. Nhóm con	61
4. Nhóm con chuẩn tắc - nhóm thương	67
5. Đồng cấu nhóm	76
<i>Chương III. Cấu trúc nhóm</i>	87
1. Tích trực tiếp	87
2. Nhóm đối xứng	97
3. Nhúng một nửa nhóm vào một nhóm	101
4. Tác động của một nhóm trên một tập	104
<i>Chương IV. Vành và trường</i>	110
1. Định nghĩa và ví dụ	110
2. Idêan, vành thương	120
3. Đồng cấu vành	132
4. Trường các thương	144
4. Vành, trường sắp thứ tự	149
<i>Chương V. Vành đa thức và vành Oclit</i>	155
1. Vành đa thức	155

2.	Thuật toán chia trong miền nguyên	168
3.	Vành chính	172
4.	Vành Ốclit (Euclide)	182
<i>Chương VI. Phân tích đa thức trên các trường số</i>		192
1.	Phân tích đa thức thực và phức	192
2.	Phân tích đa thức nguyên và hữu tỷ	195
3.	Phân tích đa thức trên trường hữu hạn	203
	<i>Bảng thuật ngữ</i>	207
	<i>Tài liệu tham khảo</i>	210

Bảng ký hiệu

Ký hiệu	Ý nghĩa
$\mathbb{N}$	Tập các số tự nhiên
$\mathbb{Z}$	Tập hợp các số nguyên
$\mathbb{Q}$	Tập hợp các số hữu tỷ
$\mathbb{R}$	Tập hợp các số thực
$\mathbb{C}$	Tập hợp các số phức
$a b$	a là ước của b
$A \subset B$ ($A \subseteq B$)	A là tập con của tập hợp B
$B \supset A$ ($B \supseteq A$)	
$A - B, A \setminus B$	Hiệu của hai tập hợp A và B
$A \cup B$	Hợp của hai tập hợp A và B
$A \cap B$	Giao của hai tập hợp A và B
$\emptyset$	Tập hợp rỗng
$C_A B$	Phần bù của tập hợp B trong A
$A \times B$	Tích Đề-các của hai tập hợp A và B
$(a_i)_{i \in I}$	Họ phần tử chỉ số hóa bởi tập I
$(A_i)_{i \in I}$	Họ tập hợp chỉ số hóa bởi tập I
(a, b)	Cặp phần tử a và b
A^2	Bình phương Đề-các của tập hợp A
$\prod_{i \in I} A_i$	Tích Đề-các của họ tập hợp A_i
	Tích trực tiếp của nhóm A_i
A^I	Lũy thừa Đề-các bậc I của tập hợp A
$f: X \rightarrow Y$	Ánh xạ f từ X đến Y
$X \xrightarrow{f} Y$	
$1_X, id_X$	Ánh xạ đồng nhất của tập X
$\text{Hom}(X, Y)$	Tập hợp các ánh xạ từ X đến Y
$S(X)$	Tập hợp các song ánh từ X đến Y
$\langle A \rangle$	Nhóm sinh bởi tập hợp A
$\langle x \rangle$	Nhóm cyclic sinh bởi phần tử x
S_n	Nhóm các phép thế bậc n
$\mathcal{P}(X)$	Tập hợp các bộ phận của tập hợp X
$C(G)$	Tâm của nhóm G
$\langle a \rangle$	Idêan sinh bởi phần tử a

$A \cong B$	Hai nhóm (vành, trường) A và B đẳng cấu với nhau
$A[x]$	Vành đa thức của ẩn x trên vành A
$A(x)$	Trường phân thức của ẩn x trên miền nguyên A
$C(a), \bar{a}$	Lớp các phần tử tương đương với phần tử a
$\text{Im} f$	Ảnh của đồng cấu f
$\text{Ker} f$	Hạt nhân của đồng cấu f
G/H	Nhóm thương của nhóm G trên nhóm con chuẩn tắc H
R/I	Vành thương của vành R trên idêan I
R_S	Vành các thương
$\bar{R}$	Trường các thương của miền nguyên R
C_n	Nhóm các phép quay của một đa giác đều n đỉnh trong mặt phẳng

Chương I

CƠ SỞ

1. Tập hợp
2. Ánh xạ
3. Quan hệ hai ngôi
4. Số nguyên

1. Tập hợp

Trong phần này chúng ta sẽ trình bày một số tính chất của các phép toán cơ bản trên tập hợp.

Khái niệm tập hợp là một trong những khái niệm cơ bản nhất của toán học. Một tập hợp được quan niệm một cách trực quan như là một tụ tập, một nhóm những đối tượng nào đó. Đây không phải là một định nghĩa mà chỉ là sự mô tả bằng những từ đồng nghĩa. Có thể nêu ra một vài ví dụ về tập hợp như: tập hợp các học sinh trong một lớp; tập hợp các số nguyên; tập hợp các nghiệm của phương trình $2x^2 - 3x + 1 = 0$.

Các đối tượng của một tập hợp đã cho nào đó được gọi là các *phần tử* của tập hợp đó. Để ký hiệu phần tử a thuộc tập hợp A ta viết $a \in A$; còn nếu phần tử a không thuộc tập hợp A ta viết $a \notin A$.

Một tập hợp thường được cho bởi một tính chất nào đó, xác định các phần tử của tập hợp đó. Chẳng hạn, nếu $p(x)$ là tính chất đặc trưng cho các phần tử $x \in A$ thì ta viết

$$A = \{x \mid p(x)\}$$

và hiểu A là tập hợp bao gồm tất cả các phần tử x có tính chất $p(x)$.

Trong lý thuyết tập hợp, tiên đề khẳng định rằng, *mỗi tính chất* $p(x)$ *xác định trên một tập hợp* S *nào đó các phần tử có tính chất này,*

thường được gọi là *tiên đề tách*. Tiên đề này nằm trong số những tiên đề cơ bản của logic.

Ta cũng thường cho một tập hợp bằng phương pháp liệt kê các phần tử thuộc tập hợp đó. Chẳng hạn, tập A gồm hữu hạn phần tử $a_1, a_2, \dots, a_n$ sẽ được ký hiệu bởi

$$A = \{a_1, a_2, \dots, a_n\}.$$

Tập hợp không chứa phần tử nào được gọi là *tập rỗng*, và ký hiệu bởi $\emptyset$. Ví dụ, tập hợp các nghiệm thực của phương trình $x^2 + 1 = 0$ là tập hợp rỗng.

Tập hợp B được gọi là *tập con* của tập hợp A nếu mọi phần tử thuộc B đều thuộc A , và ký hiệu bởi $B \subset A$ hay $A \supset B$. Như vậy

$$(B \subset A) \Leftrightarrow (x \in B \Rightarrow x \in A).$$

Khi đó, ta cũng nói rằng B *chứa trong* A hay A *chứa* B hay B *bao hàm trong* A .

Rõ ràng quan hệ bao hàm có những tính chất sau:

- i) $\emptyset \subset A, A \subset A$ với mọi tập A .
- ii) $A \subset B$ và $B \subset C$ kéo theo $A \subset C$.

Hai tập hợp A, B được gọi là *bằng nhau* nếu và chỉ nếu chúng có cùng các phần tử. Rõ ràng

$$A = B \Leftrightarrow A \subset B \text{ và } B \subset A.$$

Nếu $A \subset B$ và $A \neq B$ thì A được gọi là tập con *thực sự* của B .

Các phép toán trên tập hợp

1. Phép giao

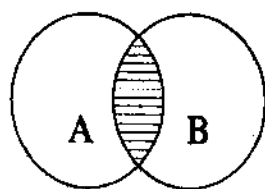
Giao của hai tập hợp A và B , ký hiệu bởi $A \cap B$, là tập hợp gồm tất cả các phần tử thuộc cả A lẫn B ,

$$A \cap B = \{x \mid x \in A \text{ và } x \in B\}.$$

Khi $A \cap B = \emptyset$ ta nói rằng A và B *không giao nhau*, hay *rời nhau*.

Ta thường biểu diễn hai tập hợp A, B bởi hai hình tròn và giao

của chúng bởi phần chung (phần gạch chéo) của hai hình tròn đó như hình vẽ dưới đây (gọi là *biểu đồ Ven*).



$$A \cap B$$

Ví dụ

Với hai số nguyên a, b đã cho, giao của hai tập hợp

$$A = \{ak \mid k \in \mathbb{Z}\}; B = \{bk \mid k \in \mathbb{Z}\}.$$

là tập hợp tất cả các bội của bội chung nhỏ nhất của a và b :

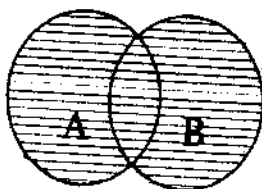
$$A \cap B = \{[a, b]k \mid k \in \mathbb{Z}\}.$$

2. Phép hợp

Hợp của hai tập hợp A và B , ký hiệu $A \cup B$, là tập hợp gồm tất cả các phần tử thuộc ít nhất một trong các tập hợp A, B .

$$A \cup B = \{x \mid x \in A \text{ hoặc } x \in B\}.$$

Nếu ta biểu diễn hai tập hợp A, B bởi hai hình tròn thì hợp của chúng là toàn bộ phần hình gạch chéo như trong hình vẽ sau:



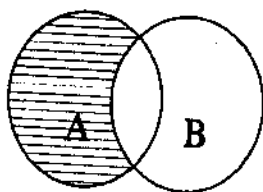
$$A \cup B$$

3. Phép lấy hiệu

Hiệu của hai tập hợp A và B , ký hiệu $A \setminus B$, là tập hợp gồm tất cả các phần tử thuộc A mà không thuộc B ,

$$A \setminus B = \{x \mid x \in A \text{ và } x \notin B\}.$$

Hiệu của hai tập hợp được biểu diễn bởi phần gạch chéo trong hình vẽ sau:



$A \setminus B$

4. Phần bù

Trong trường hợp A là tập con của một tập hợp M thì hiệu $M \setminus A$ được gọi là *phần bù* của A trong M và ký hiệu bởi $C_M A$, hay $\bar{A}$ nếu như ta biết rõ A là tập con của tập hợp nào.

Mệnh đề 1.1. Giả sử A, B là những tập hợp con tùy ý của tập hợp M . Khi đó các điều sau là tương đương:

- | | |
|-------------------|---------------------------------|
| a) $A \subset B$ | d) $\bar{B} \subset \bar{A}$ |
| b) $A \cap B = A$ | e) $A \cap \bar{B} = \emptyset$ |
| c) $A \cup B = B$ | f) $M = \bar{A} \cup B$. |

Chứng minh. Ta chứng minh các phép kéo theo $e) \Rightarrow f)$ và $f) \Rightarrow a)$, các phép kéo theo còn lại dành cho bạn đọc. Ta cũng sẽ thấy rằng các phép chứng minh được suy ra trực tiếp từ định nghĩa của các phép toán tập hợp đã nêu.

$e) \Rightarrow f)$. Giả sử $x \in M$. Nếu $x \in A$ thì do giả thiết ta có $x \notin \bar{B}$, nghĩa là $x \in B$. Nếu $x \notin A$ thì $x \in \bar{A}$. Như vậy $x \in \bar{A} \cup B$. Từ đó, $M \subset (\bar{A} \cup B)$.

Hiển nhiên ta có bao hàm thức ngược lại nên $M = \bar{A} \cup B$.

$f) \Rightarrow a)$. Giả sử $x \in A$, thế thì $x \notin \bar{A}$. Bởi vì $x \in \bar{A} \cup B$ nên $x \in B$. Điều này chứng tỏ $A \subset B$. □

Mệnh đề 1.2. Giả sử A, B, C, M là những tập hợp tùy ý. Khi đó:

- 1) $A \cup B = B \cup A$; $A \cap B = B \cap A$ (luật giao hoán).
- 2) $A \cap (B \cap C) = (A \cap B) \cap C$;
 $A \cup (B \cup C) = (A \cup B) \cup C$ (luật kết hợp).

$$3) A \cap (B \cup C) = (A \cap B) \cup (A \cap C);$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \quad (\text{luật phân phối}).$$

4) Công thức De Morgan

$$M \setminus (A \cup B) = (M \setminus A) \cap (M \setminus B);$$

$M \setminus (A \cap B) = (M \setminus A) \cup (M \setminus B)$. *Chứng minh.* Ta sẽ chứng minh hệ thức đầu tiên của 3), các hệ thức còn lại dành cho bạn đọc như một bài tập. Ta có

$$\begin{aligned} A \cap (B \cup C) &= \{x | x \in A \text{ và } x \in B \cup C\} \\ &= \{x | x \in A \text{ và } (x \in B \text{ hoặc } x \in C)\} \\ &= \{x | (x \in A \text{ và } x \in B) \text{ hoặc } (x \in A \text{ và } x \in C)\} \\ &= \{x | x \in A \cap B \text{ hoặc } x \in A \cap C\} \\ &= (A \cap B) \cup (A \cap C). \end{aligned}$$

□

Số phần tử của một tập hợp

Cho X là một tập hợp bất kỳ. Tập hợp tất cả các tập con của X được ký hiệu bởi $P(X)$, $P(X) = \{A \mid A \subset X\}$.

Mệnh đề 1.3. Nếu X là tập có n phần tử thì $P(X)$ có 2^n phần tử.

Chứng minh. Giả sử $X = \{1, 2, \dots, n\}$ và A là một tập con của X . Thế thì A ứng với dãy các trạng thái $a_1 a_2 \dots a_n$ (*), trong đó a_i chỉ trạng thái phần tử i có thuộc A hay không. Mỗi a_i nhận hai giá trị: có hoặc không, nên số dãy các trạng thái (*) là 2^n và đó chính là số tập con của X .

Ta cũng có thể lập luận như sau: Số tập con gồm r phần tử của tập X có n phần tử là tổ hợp C_n^r . Khi đó số phần tử của $P(X)$ sẽ là

$$k = C_n^0 + C_n^1 + \dots + C_n^n.$$

Để tính tổng này ta xét khai triển nhị thức Niuton

$$(1 + x)^n = C_n^0 + C_n^1 x + \dots + C_n^n x^n.$$

Thay $x = 1$ vào hệ thức trên ta có $k = 2^n$.

□

Bài tập

1.1. Chứng tỏ rằng từ một trong các hệ thức

$$S \subset T, S \cap T = S, S \cup T = T$$

của các tập hợp S và T có thể suy ra được các hệ thức còn lại.

1.2. Ký hiệu $P(X)$ là tập hợp tất cả các tập con của tập hợp X . Hãy biểu diễn các tập hợp:

$$P(P(\{1\})) \text{ và } P(P(P(\{1\}))).$$

1.3. Cho E là một tập hợp, n là một số nguyên dương, và $A_0, A_1, \dots, A_n$ là những tập con khác nhau của E sao cho

$$\emptyset = A_0 \subset A_1 \subset \dots \subset A_n = E.$$

Ta ký hiệu $B_1 = A_1 \setminus A_0, \dots, B_n = A_n \setminus A_{n-1}$. Chứng minh rằng:

a) $E = \bigcup_{i=1}^n B_i$;

b) $B_i \cap B_j = \emptyset$, với $i \neq j$.

1.4. Xét tập hợp $\{A_1, A_2, \dots, A_n\}$ mà các phần tử $A_1, A_2, \dots, A_n$ là những tập hợp. Chứng minh rằng có ít nhất một tập hợp A_i không chứa một tập nào trong các tập còn lại.

1.5. Chứng minh rằng $A \setminus (A \setminus B) = B$ khi và chỉ khi $B \subset A$.

1.6. Giả sử $(A_i)_{i \in I}$ là một họ những tập con của tập hợp X , B là một tập hợp tùy ý. Chứng minh:

a) $\bigcup_{i \in I} A_i \supset A_j$ với mọi $j \in I$;

b) $\bigcap_{i \in I} A_i \subset A_j$ với mọi $j \in I$;

c) $B \cap (\bigcup_{i \in I} A_i) = \bigcup_{i \in I} (B \cap A_i)$;

d) $B \cup (\bigcap_{i \in I} A_i) = \bigcap_{i \in I} (B \cup A_i)$;

e) $C_X(\bigcup_{i \in I} A_i) = \bigcap_{i \in I} C_X(A_i)$;

f) $C_X(\bigcap_{i \in I} A_i) = \bigcup_{i \in I} C_X(A_i)$.

1.7. Hãy chứng minh đầy đủ các mệnh đề 1.1, 1.2.

1.8. Hiệu đối xứng của hai tập hợp A và B được định nghĩa bởi

$$A \triangle B = (A \cup B) \setminus (A \cap B).$$

Hãy chứng minh rằng:

- 1) $A \triangle B = (A \setminus B) \cup (B \setminus A),$
- 2) $A \triangle B = B \triangle A$
- 3) $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C).$

2. Ánh xạ

Định nghĩa. Cho X và Y là những tập hợp. Một ánh xạ (hay một hàm) f từ X tới Y là một quy tắc đặt tương ứng mỗi phần tử $x \in X$ với một phần tử duy nhất xác định $y \in Y$, ký hiệu bởi $y = f(x)$. Một ánh xạ thường được viết

$$\begin{aligned} f : X &\rightarrow Y \\ x &\mapsto y = f(x) \end{aligned}$$

Tập X được gọi là *tập nguồn* hay *miền xác định*, tập Y được gọi là *tập đích* hay *miền giá trị* của ánh xạ f . Phần tử $y = f(x)$ gọi là *ảnh* của x , còn x gọi là *tạo ảnh* của y .

Như vậy, mỗi ánh xạ được xác định bởi tập nguồn, tập đích và quy tắc lấy ảnh.

Hai ánh xạ $f, g : X \rightarrow Y$ được gọi là *bằng nhau* nếu $f(x) = g(x)$ với mọi $x \in X$.

Ví dụ

1. Cho B là một tập hợp con của tập hợp A . Phép đặt tương ứng mỗi phần tử $a \in B$ với chính nó xác định một ánh xạ từ B đến A :

$$\begin{aligned} i : B &\rightarrow A \\ a &\mapsto a \end{aligned}$$

Đặc biệt, nếu $B = A$ ta gọi i là *ánh xạ đồng nhất* của A và ký hiệu bởi id_A .

2. Xét tập hợp các số tự nhiên $\mathbb{N}$ và tập hợp m tất cả các số tự nhiên nhỏ hơn số nguyên dương đã cho m . Với mỗi $n \in \mathbb{N}$ gọi $f(n)$ là số dư trong phép chia n cho m . Thế thì ta được một ánh xạ:

$$\begin{aligned} f : \mathbb{N} &\rightarrow m \\ n &\mapsto f(n) \end{aligned}$$

3. Cho hai tập hợp X, Y và y là một phần tử cố định thuộc Y . Khi đó tương ứng

$$\begin{aligned} f : X &\rightarrow Y \\ x &\mapsto f(x) = y \end{aligned}$$

là một ánh xạ, được gọi là *ánh xạ hằng*.

Ảnh và tạo ảnh toàn phần của một tập

Định nghĩa. Cho ánh xạ $f : X \rightarrow Y$. Khi đó:

1) Với mọi tập con A của X tập hợp

$$f(A) = \{f(a) \mid a \in A\}$$

được gọi là *ảnh* của A qua f . Đặc biệt, ảnh $f(X)$ của X qua f được gọi là *ảnh* của f và ký hiệu bởi $\text{Im} f$, $f(X) = \text{Im} f$.

2) Với mọi tập con B của Y tập hợp

$$f^{-1}(B) = \{x \in X \mid f(x) \in B\}$$

được gọi là *tạo ảnh toàn phần* của B qua f .

Định nghĩa. 1) Ánh xạ $f : X \rightarrow Y$ được gọi là một *đơn ánh* nếu

$$x \neq x' \Rightarrow f(x) \neq f(x')$$

với mọi $x, x' \in X$. Ta còn nói f là ánh xạ 1-1 từ X vào Y .

2) Ánh xạ $f : X \rightarrow Y$ được gọi là một *toàn ánh* nếu với mỗi y thuộc Y đều tồn tại x thuộc X sao cho $f(x) = y$. Ta cũng nói rằng f là một ánh xạ từ X lên Y .

3) Ánh xạ $f : X \rightarrow Y$ được gọi là một *song ánh* nếu nó đồng thời là đơn ánh và toàn ánh. Khi đó ta còn nói f là một ánh xạ 1-1 lên. Hiển nhiên f là song ánh khi và chỉ khi với mỗi $y \in Y$ tồn tại duy nhất $x \in X$ sao cho $f(x) = y$.

Ví dụ

1. Ánh xạ cho dưới đây là một đơn ánh nhưng không là toàn ánh.

$$\begin{aligned} f : \mathbb{Z} &\rightarrow \mathbb{Z} \\ x &\mapsto 2x. \end{aligned}$$

2. Trong ví dụ trên nếu ta thay đổi miền giá trị $\mathbb{Z}$ bởi $2\mathbb{Z}$ thì ta lại được một song ánh

$$\begin{aligned} f : \mathbb{Z} &\rightarrow 2\mathbb{Z} \\ x &\mapsto 2x \end{aligned}$$

(trong đó $2\mathbb{Z}$ ký hiệu cho tập các số nguyên chẵn).

Chú ý. Hai ví dụ trên cho thấy, theo định nghĩa, một ánh xạ không chỉ phụ thuộc vào quy tắc lấy ảnh mà còn phụ thuộc vào tập nguồn và tập đích của nó.

Hợp thành của các ánh xạ

Định nghĩa. Cho các ánh xạ $f : X \rightarrow Y$ và $g : Y \rightarrow Z$. Khi đó ánh xạ $h : X \rightarrow Z$ biến x thành $g(f(x))$ được gọi là *hợp thành* (hay *tích*) của f và g , ký hiệu bởi $g \circ f$ hoặc đơn giản là gf . Như vậy

$$(g \circ f)(x) = g[f(x)], \quad \forall x \in X.$$

Mệnh đề 2.1. Đối với các ánh xạ $f : X \rightarrow Y$, $g : Y \rightarrow Z$ và $h : Z \rightarrow W$ ta có

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Chứng minh. Thật vậy, với mọi phần tử $x \in X$ ta có

$$\begin{aligned} [h \circ (g \circ f)](x) &= h[(g \circ f)(x)] = h[g(f(x))] \\ &= (h \circ g)(f(x)) = [(h \circ g) \circ f](x). \end{aligned} \quad \square$$

Nhận xét. Với mọi ánh xạ $f : X \rightarrow Y$ ta có

$$f \circ id_X = id_Y \circ f = f,$$

trong đó id_A là ánh xạ đồng nhất của tập A lên chính nó.

Ánh xạ ngược

Định nghĩa. Cho các ánh xạ $f : X \rightarrow Y$ và $g : Y \rightarrow X$. Khi đó nếu $g \circ f = id_X$ thì g được gọi là ánh xạ *ngược trái* của f , còn f là ánh xạ *ngược phải* của g . Ngoài ra, nếu còn có $f \circ g = id_Y$ thì ta nói g là *ngược đối* với f , và một cách đối xứng, f là *ngược đối* với g .

Mệnh đề 2.2. (i) Một ánh xạ có *ngược trái* khi và chỉ khi nó là đơn ánh.

(ii) Một ánh xạ có *ngược phải* khi và chỉ khi nó là toàn ánh.

Chứng minh. (i) Trước hết ta chứng minh mọi ánh xạ có *ngược trái* đều là đơn ánh. Giả sử $f : X \rightarrow Y$ có ánh xạ *ngược trái* là $g : Y \rightarrow X$, thế thì $g \circ f = id_X$. Từ đó với mọi $x \in X$, ta có

$$(g \circ f)(x) = x.$$

Giả sử $f(x) = f(x')$. Khi đó

$$x' = (g \circ f)(x') = g[f(x')] = g[f(x)] = x.$$

Điều này chứng tỏ f là đơn ánh.

Ngược lại, giả sử f là đơn ánh. Ta chứng tỏ f có ánh xạ *ngược trái*. Để làm điều này chọn một phần tử tùy ý $x_0 \in X$ và xác định ánh xạ $g : Y \rightarrow X$ như sau:

$$g(y) = \begin{cases} x & \text{nếu } y = f(x) \\ x_0 & \text{nếu } y \notin \text{Im} f \end{cases}$$

Khi đó

$$(g \circ f)(x) = g(f(x)) = x \Rightarrow g \circ f = id_X.$$

(ii) Phần thứ hai của mệnh đề được chứng minh tương tự. Giả sử f có ánh xạ *ngược phải*. Thế thì với mọi $y \in Y$, do $f \circ g = id_Y$ ta có

$$y = (f \circ g)(y) = f(g(y)).$$

Đặt $x = g(y)$ ta có $y = f(x)$, nghĩa là f toàn ánh.

Ngược lại, nếu $f : X \rightarrow Y$ toàn ánh thì với mỗi $y \in Y$ có ít nhất một phần tử $x \in X$ sao cho $y = f(x)$. Bởi vậy với mỗi $y \in Y$ ta có thể chọn cố định một tạo ảnh x và đặt $x = g(y)$. Khi đó ta nhận được ánh xạ $g : Y \rightarrow X$ sao cho $f(g(y)) = y$ với mọi $y \in Y$. Nghĩa là $f \circ g = id_Y$. $\square$

Từ Mệnh đề 2.2 ta có ngay kết quả sau.

Hệ quả 2.3. Một ánh xạ là song ánh khi và chỉ khi nó có đồng thời một ánh xạ ngược trái và một ánh xạ ngược phải.

Kết luận này được làm sâu sắc hơn bởi định lý sau.

Định lý 2.4. Nếu ánh xạ $f : X \rightarrow Y$ có ánh xạ ngược trái g và ánh xạ ngược phải h thì $g = h$. Ánh xạ ngược duy nhất này của f , ký hiệu bởi f^{-1} , là song ánh và

$$(f^{-1})^{-1} = f.$$

Chứng minh. Từ giả thiết ta có

$$g = g \circ id_Y = g \circ (f \circ h) = (g \circ f) \circ h = id_X \circ h = h.$$

Điều này nói lên rằng tất cả các ánh xạ ngược trái và ánh xạ ngược phải của f đều trùng nhau. Do $h = g$ nên

$$g \circ f = id_Y, f \circ g = id_X.$$

Điều này chứng tỏ f là ngược của $g = f^{-1}$. Bởi vậy f^{-1} là song ánh và

$$f = g^{-1} = (f^{-1})^{-1}. \quad \square$$

Bài tập

- 2.1. Xét các ánh xạ $f(n) = 3n$; $g(n) = 3n + 1$ và $h(n) = 3n + 2$ từ $\mathbb{Z}$ vào $\mathbb{Z}$. Hãy tìm ánh xạ là ngược trái đồng thời của f, g và h .
- 2.2. Cho các ánh xạ $g : X \rightarrow Y$, $f : Y \rightarrow Z$.
 - a) Chứng minh rằng nếu $f \circ g$ được xác định và cả hai hàm f, g đều có ngược trái thì $f \circ g$ cũng có ngược trái.
 - b) Chứng tỏ bằng ví dụ mệnh đề đảo nói chung không đúng: $f \circ g$ có ngược trái cả khi f không có ngược trái.

- 2.3. a) Có bao nhiêu toàn ánh từ một tập có 3 phần tử lên một tập có 2 phần tử.
b) Có bao nhiêu đơn ánh từ một tập có 4 phần tử đến một tập có 3 phần tử.

2.4. Xét ánh xạ $x \mapsto x^2$ của mỗi tập hợp sau lên chính nó:

$$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{C}.$$

Xác định ảnh của mỗi ánh xạ này và chỉ rõ những ánh xạ nào trong đó là đơn ánh.

2.5. Giả sử X là một tập hợp hữu hạn. Chứng tỏ rằng ánh xạ $f : X \rightarrow X$ là đơn ánh khi và chỉ khi nó là toàn ánh.

2.6. Cho ánh xạ $f : X \rightarrow Y$, A và B là hai tập con tùy ý của X . Chứng minh rằng:

1) $f(A) \setminus f(B) \subset f(A \setminus B)$.

Hơn nữa, cho ví dụ chứng tỏ $f(A) \setminus f(B) \neq f(A \setminus B)$.

2) Nếu f là đơn ánh thì

$$f(A) \setminus f(B) = f(A \setminus B).$$

2.7. Chứng minh rằng ánh xạ

$$\begin{aligned} f : \mathbb{R} &\rightarrow \mathbb{R} \\ x &\mapsto 2(1 - 3x) \end{aligned}$$

là một song ánh và hãy tìm ánh xạ ngược của nó.

2.8. Giả sử $f : X \rightarrow Y$ là một ánh xạ, A và B là hai bộ phận của X , C và D là hai bộ phận của Y . Chứng minh:

a) $f(A \cup B) = f(A) \cup f(B)$;

b) $f(A \cap B) \subset f(A) \cap f(B)$;

c) $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$;

d) $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$;

e) $f(X \setminus A) \supset f(X) \setminus f(A)$;

f) $f^{-1}(Y \setminus C) = X \setminus f^{-1}(C) (= f^{-1}(Y) \setminus f^{-1}(C))$.

2.9. Cho ba ánh xạ $f : X \rightarrow Y$; $g, g' : Y \rightarrow X$. Chứng minh hai điều sau là tương đương:

a) f là đơn ánh.

b) Với mọi g, g' và với mọi V từ $fg = fg'$ suy ra $g = g'$.

- 2.10.** Cho ba ánh xạ $f : X \rightarrow Y$; $h, h' : Y \rightarrow Z$. Chứng minh hai điều sau là tương đương:
- f là một toàn ánh.
 - Với mọi h, h' và với mọi Z từ $hf = h'f$ suy ra $h = h'$.
- 2.11.** Giả sử n là một số tự nhiên cho trước, $f : \mathbb{N} \rightarrow \mathbb{N}$ là một ánh xạ được xác định bởi

$$f(k) = \begin{cases} n - k & \text{nếu } k < n \\ n + k & \text{nếu } k \geq n \end{cases}$$

f có phải là một đơn ánh, toàn ánh, song ánh không?

- 2.12.** Giả sử $f : X \rightarrow Y$ và $g : Y \rightarrow X$ là hai ánh xạ và $h = gf$ là ánh xạ tích của chúng. Chứng minh:
- Nếu h là đơn ánh thì f là đơn ánh, nếu thêm f là toàn ánh thì g là đơn ánh.
 - Nếu h là toàn ánh thì g là toàn ánh, nếu thêm g là đơn ánh thì f là toàn ánh.
- 2.13.** Giả sử $f : X \rightarrow Y$ là một ánh xạ. $(A_i)_{i \in I}$ là một họ những bộ phận của X , $(B_j)_{j \in J}$ là một họ những bộ phận của Y . Chứng minh:
- $f(\bigcup_{i \in I} A_i) = \bigcup_{i \in I} f(A_i)$;
 - $f(\bigcap_{i \in I} A_i) \subset \bigcap_{i \in I} f(A_i)$;
 - $f^{-1}(\bigcup_{j \in J} B_j) = \bigcup_{j \in J} f^{-1}(B_j)$;
 - $f^{-1}(\bigcap_{j \in J} B_j) = \bigcap_{j \in J} f^{-1}(B_j)$;

3. Quan hệ hai ngôi

Tích Đề-các (Descartes)

Tích Đề-các của hai tập hợp A, B đã cho, ký hiệu bởi $A \times B$, là tập hợp tất cả các cặp (a, b) với $a \in A, b \in B$.

$$A \times B = \{(a, b) | a \in A, b \in B\}.$$

Định nghĩa. Một quan hệ hai ngôi $\mathfrak{R}$ giữa các tập hợp X và Y là một tập hợp tùy ý các cặp sắp thứ tự (x, y) , với $x \in X, y \in Y$.

Nếu $(x, y) \in \mathfrak{R}$ ta nói rằng x nằm trong quan hệ $\mathfrak{R}$ với y và viết $x\mathfrak{R}y$. Nếu (x, y) không thuộc tập hợp đó ta nói rằng x không có quan hệ với y và viết $x\not\mathfrak{R}y$.

Nói cách khác, một quan hệ hai ngôi giữa các tập X, Y là một tập con của tích Đề-các $X \times Y$. Nếu $\mathfrak{R}$ là một quan hệ giữa X và Y thì với $x \in X, y \in Y$ ta luôn có hoặc $x\mathfrak{R}y$ hoặc $x\not\mathfrak{R}y$.

Trong trường hợp $X = Y$ ta nói quan hệ hai ngôi giữa X và Y là quan hệ trên X .

Trong nhiều trường hợp quan hệ hai ngôi $\mathfrak{R}$ được cho bởi một tính chất nào đó.

Ví dụ

1. Trên tập hợp các số nguyên $\mathbb{Z}$ ta xác định một quan hệ hai ngôi $\mathfrak{R}$ như sau

$$a\mathfrak{R}b \Leftrightarrow a : b.$$

Thế thì $(6, 2) \in \mathfrak{R}$ và $(6, 5) \notin \mathfrak{R}$.

2. Giả sử $X = Y = \mathbb{R}$ là tập hợp các số thực. Quan hệ hai ngôi $\mathfrak{R}$ trên $\mathbb{R}$ được cho bởi:

$$x\mathfrak{R}y \Leftrightarrow x^2 + y^2 = 25.$$

Như vậy $(x, y) \in \mathfrak{R}$ khi chỉ khi trong mặt phẳng tọa độ điểm (x, y) nằm trên đường tròn tâm O , bán kính $r = 5$. Ta nói rằng đường tròn này là đồ thị của quan hệ $\mathfrak{R}$.

Nhận xét. Khái niệm quan hệ hai ngôi giữa các tập hợp X và Y là sự mở rộng của khái niệm ánh xạ $f : X \rightarrow Y$. Thật vậy, mỗi ánh xạ $f : X \rightarrow Y$ xác định một quan hệ hai ngôi $\mathfrak{R}$ cho bởi

$$x\mathfrak{R}y \Leftrightarrow y = f(x).$$

Ngược lại, giả sử đã cho quan hệ hai ngôi $\mathfrak{R}$ giữa các tập X và Y . Với mỗi $x \in X$ xét tập hợp tất cả các phần tử $y \in Y$ có tính chất $x\mathfrak{R}y$. Tương ứng này xác định một ánh xạ khi và chỉ khi có đúng một phần tử $y \in Y$ sao cho $x\mathfrak{R}y$ với mỗi $x \in X$.

Như vậy, khái niệm ánh xạ là một trường hợp riêng của khái niệm quan hệ hai ngôi.

Bây giờ chúng ta đề cập tới hai kiểu quan hệ hai ngôi thường gặp, đóng vai trò cơ bản trong Đại số hiện đại.

Quan hệ tương đương

Định nghĩa. Quan hệ hai ngôi $\mathfrak{R}$ trên tập S được gọi là một *quan hệ tương đương* nếu nó thoả mãn các tính chất sau:

- (i) $a\mathfrak{R}a$ (tính phản xạ)
- (ii) Nếu $a\mathfrak{R}b$ thì $b\mathfrak{R}a$ (tính đối xứng)
- (iii) Nếu $a\mathfrak{R}b$ và $b\mathfrak{R}c$ thì $a\mathfrak{R}c$ (tính bắc cầu)

đối với $a, b, c \in S$.

Nếu E là một quan hệ tương đương trên tập hợp S và $a \in S$ thì tập hợp tất cả các phần tử của S có quan hệ tương đương với phần tử a được gọi là *lớp tương đương* của a , ký hiệu bởi $\bar{a}$ hoặc C_a .

$$\bar{a} = \{x \in S \mid a\mathfrak{R}x\}.$$

Rõ ràng, do quan hệ $\mathfrak{R}$ có tính chất phản xạ nên $a \in \bar{a}$.

Bổ đề 3.1. (i) Với hai phần tử bất kỳ $a, b \in S$ ta có hoặc $\bar{a} = \bar{b}$ hoặc $\bar{a} \cap \bar{b} = \emptyset$.

(ii) S là hợp rời rạc của tất cả các lớp tương đương phân biệt.

Chứng minh. (i) Giả sử $\bar{a} \cap \bar{b} \neq \emptyset$, ta sẽ chứng minh $\bar{a} = \bar{b}$. Giả sử z là một phần tử thuộc giao, thế thì điều đó có nghĩa là

$$a\mathfrak{R}z \text{ và } b\mathfrak{R}z.$$

Theo tính chất đối xứng của $\mathfrak{R}$ thì $z\mathfrak{R}a$ và khi đó theo tính chất bắc cầu của $\mathfrak{R}$ ta suy ra $a\mathfrak{R}b$.

Bây giờ nếu $x \in \bar{b}$ thì $b\mathfrak{R}x$ và theo tính bắc cầu ta có $a\mathfrak{R}x$, nghĩa là $x \in \bar{a}$. Như vậy ta đã chứng minh được $\bar{b} \subset \bar{a}$. Thay đổi vai trò của a và b , bằng lập luận tương tự ta có $\bar{a} \subset \bar{b}$. Do đó $\bar{a} = \bar{b}$.

(ii) Phần (i) chỉ ra rằng hai lớp tương đương trùng nhau hoặc phân biệt. Tính phản xạ của $\mathfrak{R}$ chỉ ra rằng mỗi phần tử $a \in S$ thuộc lớp $\bar{a}$. Do đó, S là hợp rời rạc của tất cả các lớp tương đương phân biệt. $\square$

Định nghĩa. Một *phân hoạch* của tập hợp S là một tập hợp các tập con S_k , $k \in I$ của S có hai tính chất sau:

- (i) $S_i \cap S_j = \emptyset$ với $i \neq j$,
- (ii) $\bigcup_i S_k = S$.

Như vậy, trong một phân hoạch của tập hợp S mỗi phần tử $x \in S$ thuộc vào một và chỉ một tập con S_k .

Bổ đề 3.2. Mỗi quan hệ tương đương $\mathfrak{R}$ trên tập S xác định một phân hoạch trên tập S và ngược lại.

Chứng minh. Nếu $\mathfrak{R}$ là một quan hệ tương đương trên S thì tập các lớp tương đương $\bar{a}$, $a \in S$ cho một phân hoạch trên S do bổ đề trên.

Ngược lại, nếu trên S đã cho một phân hoạch $\{S_i | i \in I\}$ ta xác định trên S một quan hệ hai ngôi $\mathfrak{R}$ như sau: $x\mathfrak{R}y$ nếu x và y cùng thuộc một tập con S_i nào đó của phân hoạch.

Rõ ràng đây là một quan hệ tương đương trên tập hợp S . $\square$

Định nghĩa. Một phân hoạch trên tập S còn được gọi là một *sự chia lớp* của S . Tập hợp các tập con S_k trong sự chia lớp của S được gọi là *tập thương* của S theo quan hệ tương đương $\mathfrak{R}$ và ký hiệu bởi $S/\mathfrak{R}$.

Ảnh xạ

$$\begin{aligned} p : S &\rightarrow S/\mathfrak{R} \\ a &\mapsto \bar{a} \end{aligned}$$

biến mỗi phần tử của S thành lớp tương đương chứa nó được gọi là *phép chiếu tự nhiên* của S lên tập thương $S/\mathfrak{R}$.

Ví dụ. Cho n là một số nguyên dương; a và b là hai số nguyên bất kỳ. Ta nói a đồng dư với b theo môđun n nếu n chia hết $a - b$ và ký hiệu là:

$$a \equiv b \pmod{n}.$$

Ta sẽ chứng minh quan hệ đồng dư môđun n là quan hệ tương đương trên $\mathbb{Z}$. Tập các lớp tương đương được gọi là tập các số nguyên môđun n và ký hiệu là $\mathbb{Z}_n$. Để chỉ n chia hết m , ta viết $n \mid m$, điều đó có nghĩa là tồn tại một số k sao cho $m = nk$. Do đó $a \equiv b \pmod{n}$ nếu và chỉ nếu $n \mid (a - b)$.

(i) Với mọi $a \in \mathbb{Z}$, $n \mid (a - a)$ vì vậy $a \equiv a \pmod{n}$ nên quan hệ này là phản xạ.

(ii) Nếu $a \equiv b \pmod{n}$ thì $n \mid (a - b)$. Từ đó $n \mid (b - a)$, vì vậy $b \equiv a \pmod{n}$.

(iii) Nếu $a \equiv b \pmod{n}$ và $b \equiv c \pmod{n}$ thì $n \mid (a - b)$ và $n \mid (b - c)$. Vì vậy n là ước của $(a - b) + (b - c) = a - c$, nghĩa là $a \equiv c \pmod{n}$. Do đó, đồng dư mod n là một quan hệ tương đương trên $\mathbb{Z}$.

Với quan hệ đồng dư môđun 3, ta có các lớp tương đương sau:

$$\begin{aligned}\bar{0} &= \{..., -3, 0, 3, 6, 9, ...\} \\ \bar{1} &= \{..., -2, 1, 4, 7, 10, ...\} \\ \bar{2} &= \{..., -1, 2, 5, 8, 11, ...\}\end{aligned}$$

Một lớp tương đương bất kỳ phải là một trong các lớp $\bar{0}, \bar{1}, \bar{2}$, vì vậy $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$.

Tổng quát, tập thương của $\mathbb{Z}$ theo quan hệ đồng dư môđun n có tất cả n phần tử,

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \bar{n-1}\},$$

vì một số nguyên bất kỳ đều đồng dư môđun n với số dư của nó khi chia cho n .

Quan hệ thứ tự

Định nghĩa. 1) Quan hệ hai ngôi $\mathfrak{R}$ trên tập hợp được gọi là *thứ tự bộ phận* hay gọi ngắn gọn là *thứ tự* của tập hợp này nếu nó thoả mãn các điều kiện sau đối với mọi $a, b, c \in S$:

- (i) $a\mathfrak{R}a$ (phản xạ)
- (ii) $a\mathfrak{R}b$ và $b\mathfrak{R}a$ kéo theo $a = b$ (phản xứng)
- (iii) $a\mathfrak{R}b$ và $b\mathfrak{R}c$ kéo theo $a\mathfrak{R}c$ (bắc cầu).

Quan hệ thứ tự bộ phận như thế thường được ký hiệu bởi $\leq$.

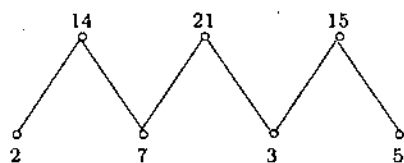
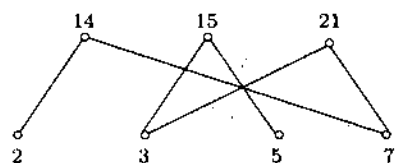
2) Một tập hợp được sắp thứ tự là một cặp $(S, \leq)$, trong đó $\leq$ là một thứ tự trên S .

Ví dụ

1. Trên tập $P = 2, 3, 5, 7, 14, 15, 21$ quan hệ

$$a \leq b \Leftrightarrow a \text{ chia hết } b$$

có thể được biểu diễn bởi một trong các biểu đồ sau:



2. Quan hệ $\leq$ thông thường trên tập hợp tất cả các số nguyên dương là quan hệ thứ tự bộ phận.

3. Quan hệ $m \mid n$ (m chia hết n) là một quan hệ thứ tự bộ phận khác trên tập hợp tất cả các số nguyên dương.

4. Đối với tập hợp bất kỳ X , quan hệ bao hàm $A \subset B$ là một quan hệ thứ tự bộ phận trên tập hợp $P(X)$ tất cả các tập con của X .

Định nghĩa. 1) Một tập hợp cùng với một quan hệ thứ tự bộ phận cho trên nó được gọi là *tập sắp thứ tự tuyến tính*, hay *sắp thứ tự toàn phần*, hay thường được gọi là *một dây chuyền* nếu đối với hai phần tử bất kỳ $a, b \in S$ hoặc $a \leq b$ hoặc $b \leq a$. Khi đó ta cũng nói rằng hai phần tử bất kỳ của S là so sánh được.

2) Tập sắp thứ tự được gọi là *tập sắp thứ tự tốt* nếu mọi tập con khác rỗng của nó đều có phần tử *bé nhất*, nghĩa là tồn tại phần tử $a \in S$ sao cho $a \leq x$ với mọi $x \in S$.

Bổ đề 3.3. Trong một tập hợp sắp thứ tự bộ phận tùy ý $(S, \leq)$ tồn tại không quá một phần tử bé nhất.

Chứng minh. Thật vậy, nếu a, a' là hai phần tử bé nhất của $(S, \leq)$ thì $a \leq a'$ (do a là phần tử bé nhất) và $a' \leq a$ (do a' là phần tử bé nhất). Từ đó suy ra $a = a'$. $\square$

Tồn tại những tập hợp sắp thứ tự bộ phận không có phần tử bé nhất, chẳng hạn tập hợp $\mathbb{R}$ các số thực với quan hệ thứ tự $\leq$ thông thường. Tuy nhiên $(\mathbb{R}, \leq)$ là một dây chuyền.

Định nghĩa. Phần tử u của tập sắp thứ tự bộ phận $(S, \leq)$ được gọi là *tối tiểu* nếu không tồn tại phần tử $x \in S$ sao cho $x < u$. Phần tử v được gọi là *tối đại* nếu không tồn tại phần tử $x \in S$ sao cho $x > v$. (Ta nói rằng $x < u$ có nghĩa là $x \leq u$ nhưng $x \neq u$ và tương tự cho $x > v$).

Định nghĩa. Giả sử S là tập con của tập hợp sắp thứ tự bộ phận P . Ta gọi

1) $a \in P$ là *cận dưới* (tương ứng, *cận trên*) của tập hợp S nếu $a \leq x$ (tương ứng, nếu $x \leq a$) với mọi $x \in S$.

2) $b \in P$ là *cận dưới đúng* (tương ứng, *cận trên đúng*) của tập hợp S nếu:

(i) b là cận dưới (tương ứng, cận trên) của S ,

(ii) $a \leq b$ (tương ứng $b \leq a$) với mọi cận dưới (tương ứng, cận trên) a của S .

Cận dưới đúng và cận trên đúng của S được ký hiệu lần lượt bởi $\inf S, \sup S$

Bổ đề 3.4. Một tập con bất kỳ của tập hợp sắp thứ tự bộ phận có không quá một cận trên đúng và một cận dưới đúng.

Chứng minh. Trực tiếp suy ra từ các định nghĩa. □

Chúng ta kết thúc mục này bằng một tính chất, sau này thường sử dụng trong các chứng minh có liên quan tới tập hợp sắp thứ tự, gọi là *Bổ đề Zorn*. Nó được công nhận như một tiên đề của lý thuyết tập hợp.

Bổ đề 3.5 (Bổ đề Zorn). Cho S là một tập hợp sắp thứ tự bộ phận. Nếu mỗi dãy chuyền của S có cận trên trong S thì S có phần tử tối đại.

Bài tập

3.1. Cho E là một quan hệ tương đương trên tập X và cho $f : X \rightarrow S$ là một ánh xạ được xác định bởi $f(x) = f(y) \Leftrightarrow xEy$. Chứng minh rằng khi đó tồn tại duy nhất ánh xạ $g : X/E \rightarrow S$ sao cho $f = g \circ p$, trong đó $p : X \rightarrow X/E$ là phép chiếu tự nhiên. Hơn nữa, nếu f là toàn ánh thì g là song ánh.

- 3.2. Cho quan hệ tương đương E trên S . Chứng minh rằng tập con A của S là một lớp tương đương của E nếu và chỉ nếu với $y \in A, z \in A \Rightarrow yEz$.
- 3.3. Hãy xác định các tính chất phản xạ, đối xứng, phản đối xứng, bắc cầu của những quan hệ $\mathfrak{R}$ sau trên tập $\mathbb{N}^*$. Với $m, n \in \mathbb{N}^*$ thì $m\mathfrak{R}n$ khi và chỉ khi:
- $m + n$ chẵn;
 - $m + n \leq 100$;
 - m/n là lũy thừa của 2;
 - m/n chẵn;
 - mn lẻ.
- 3.4. Trong những quan hệ trên $\mathbb{Z}$ sau đây quan hệ nào là đối xứng:
- $m\mathfrak{P}n$ khi và chỉ khi $m + n$ chia hết cho 3;
 - $m\mathfrak{D}n$ khi và chỉ khi $m - n$ chia hết cho 3?
- Quan hệ nào trong chúng là bắc cầu?
- 3.5. Giả sử $f : S \rightarrow \mathbb{N}$ là một đơn ánh từ tập hợp S đến tập các số tự nhiên $\mathbb{N}$. Quan hệ hai ngôi $\mathfrak{R}$ trong S xác định bởi

$$x \mathfrak{R} x' \text{ khi và chỉ khi } f(x) \leq f(x').$$

Chứng minh $\mathfrak{R}$ là một quan hệ thứ tự toàn phần.

- 3.6. Trên tập tích Đề-các $\mathbb{Z} \times \mathbb{N}^*$ của tập hợp các số nguyên $\mathbb{Z}$ và tập hợp $\mathbb{N}^*$ các số tự nhiên khác 0 cho quan hệ tương đương $\mathfrak{R}$ xác định bởi

$$(a, b)\mathfrak{R}(c, d) \text{ khi và chỉ khi } ad = bc.$$

- Chứng minh rằng $\mathfrak{R}$ là một quan hệ tương đương;
 - Chỉ ra một song ánh từ tập thương $\mathbb{Z} \times \mathbb{N}^*/\mathfrak{R}$ đến tập các số hữu tỷ $\mathbb{Q}$.
- 3.7. Giả sử S là một tập hợp, T là một quan hệ hai ngôi có tính chất phản xạ, đối xứng trong S . Ta xác định quan hệ hai ngôi $\mathfrak{R}$ trong S như sau: $x\mathfrak{R}y$ khi và chỉ khi có $x_1 = x, x_2, \dots, x_n = y$ sao cho

$$x_1Tx_2, x_2Tx_3, \dots, x_{n-1}Tx_n.$$

Chứng minh:

- $\mathfrak{R}$ là một quan hệ tương đương và $T \subset \mathfrak{R}$;
- Với mọi quan hệ tương đương H sao cho $T \subset H$ thì $\mathfrak{R} \subset H$.

- 3.8. Giả sử $\mathfrak{R}$ là một quan hệ tương đương trên tập hợp S . Chứng minh rằng nếu $\mathfrak{R} \neq \{(x, x) | x \in S\}$ thì $\mathfrak{R}$ không phải là một quan hệ thứ tự trong S .
- 3.9. Đối với hai tập con $A \subset B$ của tập hợp S , ta gọi ánh xạ $g : B \rightarrow Y$ là *kéo dài* của ánh xạ $f : A \rightarrow Y$ nếu $g(x) = f(x)$ với mọi $x \in A$. Gọi $\Phi(S, Y)$ là tập hợp các ánh xạ từ các tập con của S đến Y . Xét quan hệ $\mathfrak{R}$ trong $\Phi(S, Y)$ được xác định như sau:
- $f \mathfrak{R} g$ khi và chỉ khi g là kéo dài của f .
- a) Chứng minh $\mathfrak{R}$ là một quan hệ thứ tự.
 b) Tìm các phần tử tối tiểu, tối đại, bé nhất, lớn nhất của $\Phi(S, Y)$ đối với $\mathfrak{R}$.
- 3.10. Chứng minh rằng nếu a là phần tử bé nhất (lớn nhất) của một tập hợp S đối với một quan hệ thứ tự thì a là phần tử tối tiểu (tối đại) duy nhất của S .
- 3.11. Chứng minh rằng nếu tập S sắp thứ tự tốt thì S sắp thứ tự toàn phần.

4. Số nguyên

Dại số hiện đại nghiên cứu việc xây dựng các hệ thống số cũng như các hệ thống đại số trừu tượng. Để làm cơ sở cho việc trình bày chúng ta sẽ bắt đầu từ việc nghiên cứu một số tính chất cơ bản, thường dùng của tập hợp tất cả các số nguyên

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$$

Tập hợp các số nguyên $\mathbb{Z}$ cùng với phép toán cộng, phép toán nhân và quan hệ thứ tự là những đối tượng toán học hết sức quen thuộc. Tuy nhiên những định nghĩa chính xác về những khái niệm này còn chưa được trình bày. Điều này sẽ được thực hiện trong một giáo trình nói về việc xây dựng các hệ thống số: số tự nhiên $\mathbb{N}$, số nguyên $\mathbb{Z}$, số hữu tỷ $\mathbb{Q}$, số thực $\mathbb{R}$, số phức $\mathbb{C}$.

Bây giờ chúng ta thừa nhận một số tính chất khá hiển nhiên làm tiên đề rồi từ đó suy ra nhiều tính chất khác như những hệ quả logic.

Trong tập các số nguyên $\mathbb{Z}$ ta gọi tập hợp

$$\mathbb{N} = \{0, 1, 2, \dots, n, \dots\}$$

là tập hợp các số tự nhiên, còn tập hợp

$$\mathbb{N}^* = \{1, 2, \dots, n, \dots\}$$

được gọi là tập hợp các số nguyên dương. Tập hợp các số nguyên $\mathbb{Z}$ thoả mãn một số tính chất cơ bản của phép cộng, phép nhân, và quan hệ thứ tự mà ta sẽ nêu dưới đây. Đối với mọi $a, b, c \in \mathbb{Z}$ ta có:

$$a + (b + c) = (a + b) + c, \quad a(bc) = (ab)c;$$

$$a + b = b + a, \quad ab = ba;$$

$$a + 0 = a, \quad a1 = a;$$

$$a(b + c) = ab + ac;$$

với mỗi $a \in \mathbb{Z}$ tồn tại $-a \in \mathbb{Z}$ sao cho $a + (-a) = 0$;

$$ab = 0 \Leftrightarrow a = 0 \text{ hoặc } b = 0;$$

$$a \leq b \Leftrightarrow \exists c \in \mathbb{N}, a + c = b;$$

$$a < b \Rightarrow a + c < b + c \text{ với mọi } c \in \mathbb{Z};$$

$$a < b \Rightarrow ac < bc \text{ với mọi } c \in \mathbb{N}^*.$$

Đặc biệt, đối với tập hợp các số tự nhiên $\mathbb{N}$, hai tính chất sau được phát biểu dưới dạng tiên đề.

Tiên đề về tính sắp thứ tự tốt. Mỗi tập con khác rỗng S của $\mathbb{N}$ đều có phần tử nhỏ nhất, nghĩa là tồn tại $m \in S$ sao cho $m \leq c$ với mọi $c \in S$.

Tiên đề quy nạp. Nếu tập con khác rỗng A của $\mathbb{N}$ thoả mãn hai điều kiện:

$$(i) \quad 0 \in A,$$

$$(ii) \quad m \in A \text{ với mọi } 0 \leq m < n \Rightarrow n \in A,$$

thì $A = \mathbb{N}$.

Hai tiên đề nêu trên là tương đương với nhau, nghĩa là ta có thể chứng minh một trong hai tiên đề trên từ tiên đề còn lại.

Tính chia hết

Định nghĩa. Số nguyên a được gọi là *chia hết cho* số nguyên b nếu $a = bq$ với một số nguyên q nào đó. Khi đó ta nói a là *bội* của b và ký hiệu $a : b$.

Ta cũng nói b *chia hết* a hay b là *ước* của a và ký hiệu $b \mid a$.

Quan hệ chia hết có một số tính chất đơn giản sau. Đối với mọi số nguyên a, b, c ta luôn có:

- 1) $a \mid 0$;
- 2) $a \mid a$ (tính phản xạ);
- 3) Nếu $0 \mid a$ thì $a = 0$;
- 4) $a \mid b$ và $b \mid c$ kéo theo $a \mid c$ (tính bắc cầu);
- 5) Nếu a chia hết các số nguyên c_i ($i = 1, \dots, n$) thì a cũng chia hết tổng

$$\sum_{i=1}^n x_i c_i = x_1 c_1 + \dots + x_n c_n, \quad x_i \in \mathbb{Z}.$$

(Ta gọi $\sum_{i=1}^n x_i c_i$ là một *tổ hợp tuyến tính nguyên* của các c_i).

Những tính chất này có thể suy ra trực tiếp từ định nghĩa. Chẳng hạn, đối với tính chất 4) ta có:

$$b = ad_1 \text{ và } c = bd_2 \Rightarrow c = a(d_1 d_2).$$

Định nghĩa. Giá trị tuyệt đối của $a \in \mathbb{Z}$, ký hiệu $|a|$, được xác định là a nếu $a \geq 0$, và là $-a$ nếu $a < 0$.

Từ định nghĩa có thể dễ dàng suy ra một số tính chất thường được sử dụng sau đây:

- (i) $|a| = |-a|$;
- (ii) $|a| = 0 \Leftrightarrow a = 0$;
- (iii) $|ab| = |a| \cdot |b|$;
- (iv) $|a + b| \leq |a| + |b|$.

Mệnh đề 4.1. Các ước của 1 (còn gọi là ước của đơn vị) trong $\mathbb{Z}$ gồm có ± 1 .

Chứng minh. Mệnh đề khẳng định rằng

$$ab = 1 \Rightarrow a = b = 1 \text{ hoặc } a = b = -1.$$

Thật vậy, từ giả thiết $ab = 1$ suy ra $|ab| = |a| \cdot |b| = 1$. Do $a \neq 0$ nên $|a| \geq 1$. Cũng như vậy $|b| \geq 1$. Từ đó $|a| = |b| = 1$, bởi vậy $a = b = 1$ hoặc $a = b = -1$. $\square$

Hệ quả 4.2. Nếu hai số nguyên a và b chia hết lẫn nhau thì $a = \pm b$.

Chứng minh. Do $a|b$ và $b|a$ nên tồn tại các số nguyên u, v sao cho $a = bu, b = av$. Từ đó $a = a(uv)$. Do $a \neq 0$ nên

$$uv = 1 \Rightarrow u = \pm 1 \Rightarrow a = \pm b. \quad \square$$

Phép chia với dư

Định lý 4.3. Cho hai số nguyên a và $b, b \neq 0$. Khi đó tồn tại duy nhất cặp số nguyên q, r , sao cho

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

Chứng minh. a) Sự tồn tại. Gọi M là tập hợp tất cả các bội của b không vượt quá a ,

$$M = \{bx \mid bx \leq a, x \in \mathbb{Z}\}.$$

Tập $M \neq \emptyset$ vì

$$-|b||a| \leq -|a| \leq a \Rightarrow -|b||a| \in M.$$

Tập M bị chặn trên nên nó có số lớn nhất, chẳng hạn số đó là bq . Do số nguyên $bq + |b|$ cũng là bội của b nên từ tính lớn nhất của bq trong M ta có

$$bq \leq a < bq + |b|.$$

Từ đó

$$0 \leq a - bq < |b|.$$

Đặt $r = a - bq$ ta có

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

là điều phải chứng minh.

b) *Tính duy nhất.* Giả sử có

$$a = bq + r = bp + s, \quad 0 \leq r, s < |b|.$$

Từ đó ta có

$$b(q - p) = s - r.$$

Nếu $q - p \neq 0$ thì

$$|b(q - p)| = |b||q - p| \geq |b|. \quad (1)$$

Mặt khác,

$$|s - r| < |b| \quad (2)$$

Mâu thuẫn giữa (1) và (2) chứng tỏ $q = p$. Khi đó $r = s$. $\square$

Ước chung lớn nhất

Định nghĩa. 1) Số nguyên d được gọi là *ước chung* của các số nguyên $a_1, a_2, \dots, a_n$ nếu nó là ước của mỗi số đó.

2) Ước chung d của các số nguyên $a_1, a_2, \dots, a_n$ được gọi là *ước chung lớn nhất* (viết tắt là UCLN) nếu d là bội của mọi ước chung của $a_1, a_2, \dots, a_n$.

Nhận xét. 1) Theo định nghĩa, hai ước chung lớn nhất của các số $a_1, a_2, \dots, a_n$ phải chia hết lẫn nhau, do đó chúng chỉ khác nhau bởi dấu. Trong hai số $\pm d$ cùng là ước chung của các số $a_1, a_2, \dots, a_n$ số dương thường được ký hiệu là

$$\text{UCLN}(a_1, a_2, \dots, a_n) \text{ hoặc } (a_1, a_2, \dots, a_n).$$

2) Tập hợp các ước chung của $a_1, a_2, \dots, a_n$ trùng với tập hợp các ước của UCLN của n số đó.

Định lý 4.4 (Về sự tồn tại của ước chung lớn nhất). *Ước chung lớn nhất d của n số nguyên ($n > 1$) không cùng bằng 0 luôn tồn tại. Hơn nữa, d là một tổ hợp tuyến tính nguyên của các số nguyên này.*

Chứng minh. Giả sử $a_1, a_2, \dots, a_n$ là những số nguyên không cùng bằng 0. Xét tập hợp

$$I = \{x_1 a_1 + x_2 a_2 + \dots + x_n a_n \mid x_i \in \mathbb{Z}\}.$$

Do các a_i không cùng bằng 0 nên $I \neq \{0\}$. Hơn nữa ta nhận thấy nếu $c \in I$ thì $-c \in I$, do đó trong I luôn có số nguyên dương. Gọi d là số nguyên dương bé nhất trong I . Ta sẽ chứng minh $d = (a_1, a_2, \dots, a_n)$. Trước hết ta chứng tỏ $d \mid a_i$ ($i = 1, 2, \dots, n$). Theo phép chia với dư

$$a_i = dq_i + r_i, \quad 0 \leq r_i < d.$$

Do a_i và d cùng là những tổ hợp tuyến tính nguyên của $a_1, a_2, \dots, a_n$ nên $r_i = a_i - dq_i$ cũng là một tổ hợp tuyến tính nguyên như vậy, nghĩa là $r_i \in I$. Do tính bé nhất của d ta suy ra $r = 0$, tức là $a_i = dq_i$.

Bây giờ nếu $c \mid a_i$ ($i = 1, 2, \dots, n$) thì c là ước của mọi phân tử dạng

$$x_1 a_1 + x_2 a_2 + \dots + x_n a_n, \quad x_i \in \mathbb{Z}.$$

Nói riêng c là ước của d . Vậy $d = (a_1, a_2, \dots, a_n)$. □

Hệ quả 4.5. Nếu d là một ƯCLN của các số nguyên $a_1, a_2, \dots, a_n$ thì tồn tại các số nguyên $x_1, x_2, \dots, x_n$ sao cho

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

Định nghĩa. Các số $a_1, a_2, \dots, a_n$ được gọi là nguyên tố cùng nhau nếu ước chung lớn nhất của chúng bằng 1.

Mệnh đề 4.6. Các số nguyên $a_1, a_2, \dots, a_n$ nguyên tố cùng nhau khi và chỉ khi tồn tại các số nguyên $x_1, x_2, \dots, x_n$ sao cho

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

Chứng minh. Điều kiện cần là hệ quả trực tiếp của hệ quả vừa nêu trên.

Bây giờ ta chứng minh điều kiện đủ. Hiển nhiên 1 là một ước chung của các số nguyên $a_1, a_2, \dots, a_n$. Hơn nữa do

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

nên mọi ước chung của các số nguyên $a_1, a_2, \dots, a_n$ cũng là ước của 1. Bởi vậy $1 = (a_1, a_2, \dots, a_n)$. □

Từ định nghĩa ước chung lớn nhất dễ dàng chứng minh được tính chất sau.

Mệnh đề 4.7. Nếu k là một số nguyên dương thì

$$(a_1k, a_2k, \dots, a_nk) = (a_1, a_2, \dots, a_n)k.$$

Hệ quả 4.8. $(a, b) = d \Leftrightarrow \left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Chứng minh. Thật vậy, theo Mệnh đề 4.7 ta có

$$(a, b) = d \Leftrightarrow \left(\frac{a}{d}, \frac{b}{d}\right)d = d \Leftrightarrow \left(\frac{a}{d}, \frac{b}{d}\right) = 1. \quad \square$$

Bây giờ ta nêu một trong những tính chất thường gặp có liên quan tới cặp số nguyên tố cùng nhau.

Mệnh đề 4.9. Nếu a và b là hai số nguyên tố cùng nhau và b là ước của ac thì b là ước của a .

Chứng minh. Do $(a, b) = 1$, tồn tại $u, v \in \mathbb{Z}$ sao cho

$$1 = au + bv.$$

Từ đó

$$c = acu + bcv.$$

Nếu b là ước của ac thì b là ước của biểu thức ở vế phải, do đó b là ước của c . $\square$

Mệnh đề 4.10. Nếu hai số a và b nguyên tố cùng nhau thì

$$(ac, b) = (c, b),$$

với mọi $c \in \mathbb{Z}$.

Chứng minh. Nếu d là một ước chung của ac và b thì nó cũng là ước chung của ac và bc , do đó là ước của

$$(ac, bc) = (a, b)c = c.$$

Điều này có nghĩa là nếu d là ước chung của b và c thì d cũng là ước chung của b và ac . Như vậy tập các ước chung của ac và b trùng với tập các ước chung của c và b . Bởi vậy $(ac, b) = (c, b)$. $\square$

Thuật toán Ôclit để tìm ƯCLN

Để tìm ƯCLN của hai số tự nhiên a và b ta thường sử dụng tính chất sau:

$$a = bq + c \Rightarrow (a, b) = (b, c)$$

(Lưu ý rằng ở đây không đòi hỏi $0 < c < b$).

Bây giờ ta trình bày thuật toán Ôclit để tìm ƯCLN của hai số tự nhiên. Thuật toán đó được tiến hành như sau:

- Nếu $a = bq$ thì $(a, b) = b$.
- Nếu a không chia hết cho b thực hiện liên tiếp các phép chia với dư ta được

$$\begin{aligned}a &= bq_0 + r_1, & 0 < r_1 < b \\b &= r_1q_1 + r_2, & 0 < r_2 < r_1 \\&\dots & \dots \\r_{n-2} &= r_{n-1}q_{n-1} + r_n, & 0 < r_n < r_{n-1} \\r_{n-1} &= r_nq_n.\end{aligned}$$

Dãy phép chia này phải là hữu hạn, với phép chia cuối cùng là một phép chia hết. Theo nhận xét ban đầu ta được

$$(a, b) = (b, r_1) = \dots = (r_{n-1}, r_n) = r_n,$$

nghĩa là ƯCLN của a, b bằng số dư cuối cùng r_n trong thuật toán nói trên.

Bây giờ việc tìm ƯCLN của n số ($n > 2$) sẽ được tính theo công thức truy hồi:

$$(a_1, a_2, \dots, a_n) = ((a_1, a_2, \dots, a_{n-1}), a_n).$$

Việc chứng minh công thức này không khó khăn gì và được dành cho bạn đọc như một bài tập.

Ví dụ. Tìm ƯCLN của 713 và 253 trong $\mathbb{Z}$ và tìm 2 số nguyên s và t sao cho

$$713s + 253t = \text{ƯCLN}(713, 253).$$

Lời giải. Theo thuật toán chia, chúng ta có

$$\begin{aligned}\text{(i)} \quad 713 &= 2 \cdot 253 + 207 & a &= 713, b = 253, r_1 = 207 \\ \text{(ii)} \quad 253 &= 1 \cdot 207 + 46 & r_2 &= 46 \\ \text{(iii)} \quad 207 &= 4 \cdot 46 + 23 & r_3 &= 23 \\ \text{(iv)} \quad 46 &= 2 \cdot 23 + 0 & r_4 &= 0\end{aligned}$$

Số dư khác 0 cuối cùng là 23. Do đó $\text{UCLN}(713, 253) = 23$.

Chúng ta có thể tìm được các số nguyên s và t bằng cách sử dụng các đẳng thức (i)-(iv).

$$\begin{aligned} 23 &= 207 - 4 \cdot 46 && \text{từ đẳng thức (iii)} \\ &= 207 - 4(253 - 207) && \text{từ đẳng thức (ii)} \\ &= 5 \cdot 207 - 4 \cdot 253 \\ &= 5 \cdot (713 - 2 \cdot 253) - 4 \cdot 253 && \text{từ đẳng thức (i)} \\ &= 5 \cdot 713 - 14 \cdot 253. \end{aligned}$$

Do đó, $s = 5$ và $t = -14$.

Bội chung nhỏ nhất

Định nghĩa. 1) Số nguyên m được gọi là *bội chung* của các số nguyên khác không $a_1, a_2, \dots, a_n$ ($n \geq 2$) nếu nó chia hết cho mỗi số nguyên đó.

2) Bội chung m của các số nguyên $a_1, a_2, \dots, a_n$ được gọi là *bội chung nhỏ nhất* của các số này (viết tắt là BCNN) nếu nó là ước của mọi bội chung của $a_1, a_2, \dots, a_n$.

Chú ý. Nếu m và m' là những BCNN của các số $a_1, a_2, \dots, a_n$ thì $m = \pm m'$. Trong trường hợp $m > 0$ ta ký hiệu

$$m = \text{BCNN}(a_1, a_2, \dots, a_n), \text{ hoặc } m = [a_1, a_2, \dots, a_n]$$

và quy ước gọi nó là BCNN của $a_1, a_2, \dots, a_n$. Trong cuốn sách này chúng ta sẽ dùng ký hiệu sau cho đơn giản.

Định lý 4.11 (Về sự tồn tại của bội chung nhỏ nhất). *Tồn tại bội chung nhỏ nhất của n số nguyên khác không $a_1, a_2, \dots, a_n$ ($n > 1$).*

Chứng minh. Gọi M là tập hợp tất cả các số dương chia hết cho mọi a_i ($i = 1, 2, \dots, n$). Khi đó dễ thấy M khác rỗng vì

$$|a_1 a_2 \dots a_n| \in M.$$

Do đó trong M tồn tại phần tử bé nhất m . Đó chính là BCNN của $a_1, a_2, \dots, a_n$. Thật vậy, giả sử số nguyên k là một bội chung của các

a_i ($i = 1, 2, \dots, n$), ta chứng tỏ k là một bội của m . Không mất tính tổng quát có thể coi $k > 0$. Chia k cho m ta được

$$k = mq + r, \quad 0 \leq r < m.$$

Do k và m đều chia hết cho a_i nên $r = k - mq$ cũng chia hết cho a_i , với $i = 1, 2, \dots, n$. Điều này chứng tỏ $r \in M$ nếu $r \neq 0$. Nhưng điều đó mâu thuẫn với tính nhỏ nhất của m . Bởi vậy $r = 0$ và k chia hết cho m . $\square$

Mệnh đề sau cho mối liên hệ giữa ước chung lớn nhất và bội chung nhỏ nhất của hai số nguyên a, b , đồng thời cho một cách tìm bội chung nhỏ nhất của hai số đó.

Mệnh đề 4.12. Với hai số nguyên dương a, b ta có

$$[a, b] = \frac{ab}{(a, b)}.$$

Chứng minh. Đặt $m = \frac{ab}{(a, b)}$. Rõ ràng

$$m = a \cdot \frac{b}{(a, b)} = b \cdot \frac{a}{(a, b)}$$

nên m là một bội chung của a và b .

Bây giờ nếu k là một bội chung nào đó của a và b thì $k = ak_1 = bk_2$, với $k_1, k_2 \in \mathbb{Z}$. Suy ra

$$\frac{a}{(a, b)}k_1 = \frac{b}{(a, b)}k_2.$$

Do $\frac{a}{(a, b)}$ và $\frac{b}{(a, b)}$ nguyên tố cùng nhau nên $\frac{b}{(a, b)}$ là ước của k_1 . Từ đó $m = \frac{ab}{(a, b)}$ là ước của $ak_1 = k$. Điều này chứng tỏ m là BCNN của a và b , nghĩa là $\frac{ab}{(a, b)} = [a, b]$. $\square$

Bội chung nhỏ nhất của n số ($n > 2$) được tính theo công thức

$$[a_1, a_2, \dots, a_n] = [[a_1, a_2, \dots, a_{n-1}], a_n].$$

Trong nhiều trường hợp BCNN của nhiều số còn được xác định nhờ tính chất sau

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

Số nguyên tố

Định nghĩa. Số tự nhiên lớn hơn 1 không có ước dương nào khác ngoài 1 và chính nó được gọi là *số nguyên tố*.

Chúng ta chỉ ra một số tính chất cơ bản thường gặp của các số nguyên tố.

Tính chất 4.13. Cho p là số nguyên tố. Khi đó với mọi số nguyên a thì hoặc a chia hết cho p hoặc a nguyên tố cùng nhau với p .

Chứng minh. Do (a, p) là một ước của p nên xảy ra hai trường hợp: hoặc $(a, p) = 1$ hoặc $(a, p) = p$. Trong trường hợp thứ hai a chia hết cho p . $\square$

Tính chất 4.14. Nếu số nguyên tố p chia hết tích ab của hai số tự nhiên thì hoặc p chia hết a hoặc p chia hết b .

Chứng minh. Thật vậy, ngược lại nếu p không chia hết cả a lẫn b thì nó nguyên tố với mỗi số đó. Khi đó tồn tại các số nguyên u, v, r, s sao cho

$$1 = pu + av, \quad 1 = pr + bs.$$

Từ đó, nhân từng vế của hai đẳng thức ta được

$$1 = (pu + av)(pr + bs) = px + (ab)y,$$

nghĩa là p nguyên tố với ab . Điều này là trái với giả thiết. $\square$

Từ tính chất 4.14 vừa nêu, bằng phép quy nạp theo n , ta có thể chứng minh hệ quả sau.

Hệ quả 4.15. Nếu số nguyên tố p chia hết tích n số thì nó phải chia hết ít nhất một trong các thừa số đó.

Bây giờ chúng ta sẽ phát biểu và chứng minh định lý cơ bản của số học.

Định lý 4.16. *Mỗi số tự nhiên lớn hơn 1 đều phân tích được thành tích những thừa số nguyên tố và sự phân tích đó là duy nhất, không kể đến thứ tự của các thừa số.*

Chứng minh. a) *Tính phân tích được.* Giả sử a là một số tự nhiên lớn hơn 1. Gọi p_1 là một ước nguyên tố của a , $a = p_1 a_1$.

Nếu $a_1 > 1$ thì a_1 có một ước nguyên tố p_2 ,

$$a_1 = a_2 p_2, \text{ và } a = p_1 p_2 a_2.$$

Tiếp tục lập luận trên, sau hữu hạn bước ta được

$$a_{n-2} = p_{n-1} a_{n-1}$$

(do $a_1 > a_2 > \dots$), với $a_{n-1} = p_n$ là một số nguyên tố. Khi đó

$$a = p_1 p_2 \dots p_n \quad (1)$$

là sự phân tích a thành tích của các thừa số nguyên tố.

b) *Tính duy nhất.* Giả sử số tự nhiên a còn có sự phân tích thành tích các thừa số nguyên tố

$$a = q_1 q_2 \dots q_m \quad (2)$$

Giả sử $m \neq n$. Không mất tính tổng quát ta giả sử $m < n$. Do q_1 là ước nguyên tố của a nên nó phải là ước của một thừa số p_i nào đó. Bằng cách đánh số thích hợp ta có $q_1 \mid p_1$. Nhưng do p_1 nguyên tố nên $q_1 = p_1$. Từ đó

$$q_2 \dots q_m = p_2 \dots p_n.$$

Tiếp tục lập luận trên sau hữu hạn bước ta được

$$1 = p_{m+1} \dots p_n.$$

Điều này là vô lý. Bởi vậy $m = n$ và với cách đánh số thích hợp $p_i = q_i$ với $i = 1, 2, \dots, n$. □

Chú ý. Sự phân tích dạng (1) có thể viết dưới dạng

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

trong đó $p_1, p_2, \dots, p_k$ là những số nguyên tố khác nhau và $\alpha_1, \alpha_2, \dots, \alpha_k$ là những số nguyên dương. Cách viết này được gọi là *sự phân tích tiêu chuẩn của a* .

Bài tập

Tính chia hết

- 4.1. Chứng minh rằng nếu $m - n$ chia hết $mp + nq$ thì $m - n$ chia hết $mq + np$ (ở đó $m, n, p, q \in \mathbb{Z}$).
- 4.2. Chứng minh rằng nếu $(a^3 + b^3 + c^3):9$ thì một trong ba số a, b, c chia hết cho 3.
- 4.3. Chứng minh rằng không có cặp số nguyên x, y nào thoả mãn đẳng thức:
 - a) $x^2 + 1 = 3y$.
 - b) $x^2 + 2 = 5y$.
- 4.4. Chứng minh rằng với mọi số tự nhiên $n \geq 1$ ta có tích

$$(n+1)(n+2)\dots(n+n)$$

chia hết cho 2^n .

Ước chung lớn nhất

- 4.5. Chứng minh rằng nếu a và c là hai số nguyên tố cùng nhau thì $a|m$ và $c|m$ kéo theo $ac|m$.
- 4.6. Nếu $a > 0$ chứng minh rằng $(ab, ac) = a(b, c)$.
- 4.7. Chứng minh rằng với hai số nguyên dương a và b tập hợp tất cả các số dạng $am + bn$ (m, n nguyên dương) chứa tất cả các bội của (a, b) lớn hơn ab .
- 4.8. Chứng minh rằng:

$$(3a + 5b, 8a + 13b) = (a, b).$$
- 4.9. Tìm $(a + b, a - b)$ biết $(a, b) = d$.
- 4.10. Chứng minh rằng $(a, b) = 1$ với:
 - a) $a = 21m + 4, b = 14m + 3$;

$$b) a = m^3 + 2m, b = m^4 + 3m^2 + 1;$$

$$c) a = m^2n + 2m, b = mn + 1,$$

trong đó $m, n \in \mathbb{Z}$.

4.11. Cho $(a, b) = 1$ và n là ước chung của $a - b$ và $ac - bd$. Chứng minh rằng n là ước của $c - d$.

4.12. Cho a, m, n là những số nguyên dương, trong đó $a > 1$ và $(m, n) = 1$. Chứng minh rằng:

$$(a - 1)(a^{mn} - 1) : (a^m - 1)(a^n - 1).$$

4.13. Chứng minh rằng các số $2^p - 1$ và $2^q - 1$ là nguyên tố cùng nhau khi và chỉ khi hai số p và q nguyên tố cùng nhau.

Bội chung nhỏ nhất

4.14. a) Tìm $[2^n - 1, 2^n + 1]$ với $n \in \mathbb{N}$;

b) Tìm $[a, a + 2]$ với $a \in \mathbb{N}$.

4.15. Tìm bội chung nhỏ nhất của ba số nguyên liên tiếp.

4.16. Đặt $[a, b] = m$. Chứng minh rằng:

$$(a + b, m) = (a, b).$$

4.17. Cho m là một bội chung của $a_1, a_2, \dots, a_n$, trong đó $a_i \in \mathbb{N}^*$, $n \geq 2$. Ta đặt

$$M_i = \frac{M}{a_i} \text{ và } D = (M_1, M_2, \dots, M_n).$$

Chứng minh rằng: $[a_1, a_2, \dots, a_n] = \frac{M}{D}$.

4.18. Cho k và n là hai số nguyên lớn hơn 1. Chứng minh rằng:

a) $(n!)^k$ và $(k!)^n$ là ước của $(nk)!$

b) $[(n!)^k, (k!)^n]$ là ước của $(nk)!$

Số nguyên tố

4.19. Cho $p \geq 5$ là một số nguyên tố và $2p + 1$ cũng là một số nguyên tố. Chứng minh rằng $4p + 1$ là một hợp số.

4.20. Tìm số nguyên tố p sao cho hai số $p + 4$ và $p + 8$ cũng là những số nguyên tố.

4.21. Chứng minh rằng tích của những số dạng $4m + 1$ lại là một số có dạng ấy. Từ kết quả này suy ra rằng có vô số số nguyên tố dạng $4m + 3$.

Giải bài toán tương tự cho số nguyên tố có dạng $6m + 5$.

4.22. Chứng minh rằng với $m > 2$, giữa m và $m!$ có ít nhất một số nguyên tố. Từ đó suy ra rằng có vô số số nguyên tố.

4.23. Chứng minh rằng nếu tổng của ba số chính phương là một số chính phương thì có ít nhất hai số trong ba số này là chẵn.

Chương II

NHÓM - ĐỒNG CẤU NHÓM

1. Đại số hai ngôi
2. Nhóm
3. Nhóm con
4. Nhóm con chuẩn tắc - nhóm thương
5. Đồng cấu nhóm

1. Đại số hai ngôi

Lịch sử phát triển của đại số được chia thành hai thời kỳ phân biệt. Đại số được hình thành trước thế kỷ thứ 19 được gọi là đại số cổ điển, trong khi hầu hết những kiến thức đại số sau đó được gọi là đại số hiện đại hay đại số trừu tượng.

Phương pháp dựa vào một ký hiệu, chẳng hạn như x , để đại diện cho một số chưa biết trong khi giải các bài toán đã được biết đến từ thời Hy Lạp cổ đại. Đại số cổ điển có thể được đặc trưng bởi khẳng định rằng mỗi ký hiệu luôn thay thế cho một số. Số này có thể là số nguyên, số thực hoặc số phức. Tuy nhiên, vào thế kỷ thứ 17 và 18, các nhà toán học đã nghi ngờ rằng liệu căn bậc hai của -1 có phải là một số hay không. Câu trả lời là không cho đến tận thế kỷ thứ 19 và sự bắt đầu của đại số hiện đại là dựa ra được giải thích thỏa đáng về các số phức.

Mục tiêu chủ yếu của đại số cổ điển là giải các phương trình đại số. Đại số cổ điển đã thành công trong việc đưa ra các thuật toán để giải tất cả các phương trình đại số một ẩn có bậc không vượt quá 4. Tuy nhiên, Niels Henrik Abel (1802 - 1829) bằng các kỹ thuật đại số hiện đại đã chỉ ra rằng phương trình đại số bậc 5 hoặc cao hơn không phải

luôn luôn giải được bằng các phép khai căn bậc n . Đại số cổ điển đã có những đóng góp vô cùng quan trọng. Trong khoa học tự nhiên, khoa học kỹ thuật và khoa học xã hội đó là phương pháp giải hệ phương trình tuyến tính cũng như toàn bộ đại số tuyến tính liên quan tới nó.

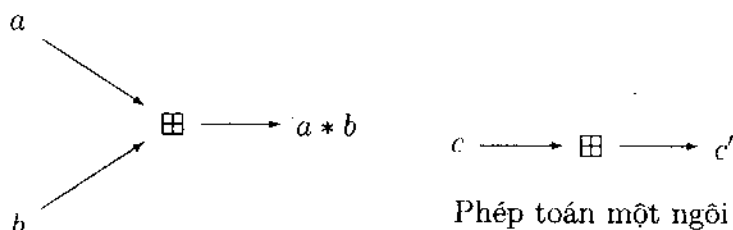
Trong thế kỷ thứ 19, người ta đã dần dần nhận ra rằng các ký hiệu toán học không nhất thiết phải là đại diện cho các số, mà thực ra chúng không nhất thiết phải đại diện cho bất kỳ cái gì cả. Từ sự phát hiện này đã nảy sinh ra cái mà người ta biết ngày nay đó là *đại số hiện đại* hay *đại số trừu tượng*.

Đại số hiện đại có hai lợi ích cơ bản. Một là để mô tả các mô hình hay các cấu trúc nảy sinh trong tự nhiên và trong toán học. Lợi ích thứ hai của đại số hiện đại là cho những phương pháp mở rộng các hệ thống số phổ biến một cách tự nhiên thành những hệ thống số mới tiện lợi hơn.

Đại số hai ngôi

Hệ đại số là một khái niệm cơ bản của đại số hiện đại. Một hệ như vậy là một *tập hợp các phần tử* mà trên đó có thể thực hiện các *phép toán* tựa như phép cộng hay phép nhân các số.

Như được chỉ ra trong hình dưới đây, ta có thể hình dung một phép toán như là một "hộp đen" với các đầu vào khác nhau lấy từ một tập S và một đầu ra chính là sự kết hợp của các đầu vào bằng một cách đã được chỉ rõ nào đó.



Phép toán hai ngôi

Nếu hộp đen có hai đầu vào thì phép toán kết hợp hai phần tử của tập hợp đó để tạo thành một phần tử thứ ba. Phép toán như vậy

được gọi là *phép toán hai ngôi*. Nếu chỉ có một đầu vào thì phép toán được gọi là *một ngôi*. Ví dụ về phép toán một ngôi là tìm nghịch đảo của một số thực khác không.

Định nghĩa. Cho tập hợp S . Một *phép toán hai ngôi* trên S là một ánh xạ

$$\begin{aligned}\varphi: S \times S &\rightarrow S \\ (a, b) &\mapsto \varphi(a, b).\end{aligned}$$

Như vậy, phép toán hai ngôi là một quy tắc cho tương ứng hai phần tử $x, y \in S$ với một phần tử của S là ảnh của (x, y) qua φ .

Thông thường ta biểu diễn phép toán hai ngôi như phép nhân và thay cho $\varphi(x, y)$ ta viết $x \circ y$ hay $x * y$, hoặc đơn giản là xy , và gọi là *tích* của x và y . Đôi khi ta cũng ký hiệu phép toán hai ngôi bởi dấu $+$ và gọi $x + y$ là *tổng* của x và y .

Tập hợp S cùng với phép toán hai ngôi $\circ$ cho trên nó được gọi là một *dại số hai ngôi*, ký hiệu bởi $(S, \circ)$.

Ví dụ

Giả sử $\mathbb{N}^* = \{1, 2, 3, \dots\}$ là tập các số nguyên dương. Phép cộng và phép nhân thông thường đều là những phép toán hai ngôi trên $\mathbb{N}^*$, bởi vì nếu $x, y \in \mathbb{N}^*$ thì $x + y \in \mathbb{N}^*$ và $xy \in \mathbb{N}^*$. Tuy nhiên, phép trừ không phải là phép toán hai ngôi trên $\mathbb{N}^*$ vì chẳng hạn $1 - 2$ không thuộc $\mathbb{N}^*$.

Ta có thể nêu một vài phép toán hai ngôi tự nhiên khác trên $\mathbb{N}^*$, đó là phép mũ hóa và phép lấy ước chung lớn nhất, vì với bất kỳ hai số nguyên dương x và y thì x^y và (x, y) là những phần tử được xác định của $\mathbb{N}^*$.

Phép cộng, phép nhân và phép trừ đều là những phép toán hai ngôi trên $\mathbb{R}$ vì $x + y, xy$ và $x - y$ là những số thực với mọi cặp số thực x và y . Ký hiệu $-$ trong một biểu thức $x - y$ thay cho phép toán hai ngôi là phép trừ, nhưng trong biểu thức $-x$ ký hiệu này lại thay cho phép toán một ngôi là phép lấy số đối.

Phép chia không phải là một phép toán hai ngôi trên $\mathbb{R}$ vì phép chia cho 0 là không xác định. Tuy nhiên, nó là một phép toán hai ngôi trên tập $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ các số thực khác 0.

Một phép toán hai ngôi trên một tập hữu hạn, để thuận tiện, thường được biểu diễn bằng một *bảng*. Chẳng hạn, xét tập $T = \{a, b, c\}$

gồm ba phần tử. Một phép toán hai ngôi $*$ trên T được xác định bởi bảng dưới đây. Trong bảng này, $x * y$ là phần tử trên dòng x và cột y . Ví dụ, $b * c = b$ và $c * b = a$.

Bảng phép toán hai ngôi trên $\{a, b, c\}$

$*$	a	b	c
a	b	a	a
b	c	a	b
c	c	a	b

Một tập hợp cùng với một hoặc nhiều phép toán trên nó được gọi là một *cấu trúc đại số*. Tập hợp đó được gọi là *tập nền* của cấu trúc. Đại số hiện đại nghiên cứu các cấu trúc đó. Trong cuốn sách này chúng ta sẽ nghiên cứu một số kiểu cấu trúc đại số cơ bản nhất.

Bằng những ví dụ cụ thể ta có thể thấy rằng có thể xảy ra các tình huống $xy \neq yx$ hoặc $x(yz) \neq (xy)z$ trong một đại số hai ngôi, nghĩa là một phép toán đại số hai ngôi nói chung không có tính chất giao hoán hay kết hợp.

Nửa nhóm

Định nghĩa. 1) Đại số hai ngôi $(S, \circ)$ được gọi là một *nửa nhóm* nếu phép nhân trên S thỏa mãn luật kết hợp, nghĩa là

$$a \circ (b \circ c) = (a \circ b) \circ c$$

với mọi $a, b, c \in S$.

2) Nửa nhóm S được gọi là *vị nhóm* nếu trong S có phần tử e , gọi là *phần tử đơn vị*, sao cho

$$e \circ a = a \circ e = a$$

với mọi $a \in S$.

Phần tử đơn vị còn được gọi là *phần tử trung hoà*. Trong trường hợp phép toán được ký hiệu bởi *phép cộng* thì phần tử này ký hiệu bởi 0.

Ví dụ

1. Tập hợp $\mathbb{N}$ các số tự nhiên cùng với phép toán cộng thông thường là một nửa nhóm, hơn nữa là một vị nhóm với phần tử trung hoà là số 0.

2. Tập hợp các ánh xạ từ tập hợp X đến chính nó cùng với phép hợp thành các ánh xạ là một vị nhóm với phần tử đơn vị là ánh xạ đồng nhất của X .

3. Ký hiệu tập các ma trận thực cỡ $n \times n$ là $M_n(\mathbb{R})$. Phép nhân ma trận là một phép toán có tính chất kết hợp trên $M_n(\mathbb{R})$ nhưng không giao hoán (trừ trường hợp $n = 1$). Ma trận I mà giá trị ở vị trí thứ (i, j) của nó bằng 1 nếu $i = j$ và bằng 0 trong trường hợp ngược lại là phần tử đơn vị của phép nhân.

Đối với dãy $a_1, a_2, \dots, a_n (n \geq 2)$ những phần tử của nửa nhóm nhân M ta định nghĩa tích bội n bằng quy nạp theo n như sau

$$\prod_{i=1}^2 a_i = a_1 a_2, \quad \prod_{i=1}^{n+1} a_i = \left(\prod_{i=1}^n a_i \right) a_{n+1}$$

Mệnh đề 1.1. *Đối với dãy $m + n$ phần tử của nửa nhóm M ta có*

$$\left(\prod_{i=1}^m a_i \right) \left(\prod_{j=1}^n a_{m+j} \right) = \prod_{k=1}^{m+n} a_k.$$

Chứng minh. Ta chứng minh đẳng thức trên bằng quy nạp theo n . Với $n = 1$ công thức đúng theo định nghĩa của tích bội.

Với $n \geq 2$, ta giả sử công thức đúng cho $n - 1$. Khi đó ta có

$$\begin{aligned} \left(\prod_{i=1}^m a_i \right) \left(\prod_{j=1}^n a_{m+j} \right) &= \left(\prod_{i=1}^m a_i \right) \left[\left(\prod_{j=1}^{n-1} a_{m+j} \right) a_{m+n} \right] \\ &= \left[\left(\prod_{i=1}^m a_i \right) \left(\prod_{j=1}^{n-1} a_{m+j} \right) \right] a_{m+n} \\ &= \left(\prod_{k=1}^{m+n-1} a_k \right) a_{m+n} = \prod_{k=1}^{m+n} a_k. \quad \square \end{aligned}$$

Bây giờ ta xét tới tính chất cơ đơn vị của nửa nhóm.

Mệnh đề 1.2. Trong nửa nhóm M nếu tồn tại phần tử u sao cho $ua = a$ với mọi $a \in M$ (ta nói u là đơn vị trái) và phần tử v sao cho $av = a$ với mọi $a \in M$ (ta nói v là đơn vị phải) thì $u = v$ và là phần tử đơn vị của M . Nói riêng, phần tử đơn vị của nửa nhóm (nếu có) là duy nhất.

Chứng minh. Ta có

$$u = uv \text{ (do định nghĩa của } u),$$

$$v = uv \text{ (do định nghĩa của } v).$$

Bởi vậy $u = v$ và là phần tử đơn vị của M . □

Vị nhóm xyclic

Trong một vị nhóm bất kỳ M lũy thừa của phần tử $a \in M$ được xác định bằng quy nạp theo $n \in \mathbb{N}$ như sau:

$$a^0 = e, a^1 = a, a^2 = aa, \dots, a^{n+1} = a^n a \quad (1)$$

Định nghĩa. Vị nhóm M được gọi là *xyclic* nếu nó chỉ gồm các lũy thừa c^n của phần tử c nào đó. Khi đó ta nói rằng vị nhóm M được sinh bởi c .

Mệnh đề 1.3. Trong vị nhóm bất kỳ $a^m a^n = a^{m+n}$ đối với mọi số tự nhiên m, n .

Chứng minh. Với $n = 0$ rõ ràng ta có

$$a^m a^0 = a^m e = a^m.$$

Với $n > 0$ mệnh đề là trường hợp riêng của mệnh đề 1.1. □

Định nghĩa. Nửa nhóm M được gọi là *giao hoán* (hay *abel*) nếu $ab = ba$ với mọi $a, b \in M$.

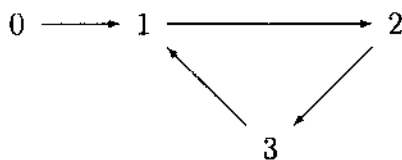
Hiển nhiên mọi vị nhóm xyclic đều giao hoán.

Chú ý về ký hiệu. Đối với nửa nhóm giao hoán ta thường ký hiệu phép toán bởi dấu $+$ (và khi đó phần tử trung hoà ký hiệu bởi 0 như đã nói ở trên).

Ví dụ

1. Vĩ nhóm $(\mathbb{N}, +)$ là xyclic với phần tử trung hoà 0 và sinh bởi phần tử 1.

2. Cho $A = \{0, 1, 2, 3\}$. Xét ánh xạ $\varphi : A \rightarrow A$ cho bởi biểu đồ



Tất cả các lũy thừa $\varphi^0 = id, \varphi^1 = \varphi, \varphi^2, \varphi^3$ khác nhau nhưng $\varphi^4 = \varphi$. Vì vậy vĩ nhóm xyclic gồm tất cả các lũy thừa của φ được cho bởi bảng

	1	φ	φ^2	φ^3
1	1	φ	φ^2	φ^3
φ	φ	φ^2	φ^3	φ
φ^2	φ^2	φ^3	φ	φ^2
φ^3	φ^3	φ	φ^2	φ^3

Nửa nhóm con

Để tìm hiểu một cấu trúc nào đó, ta thường bắt đầu bằng việc khảo sát các *cấu trúc con* của nó. Tập nền của một cấu trúc con là một tập con của tập nền của cấu trúc đó, và các phép toán trên cả hai tập hợp là như nhau.

Tập con H của nửa nhóm $(N, \circ)$ được gọi là *đóng* (hay *ổn định*) đối với phép toán trong N nếu với mọi $a, b \in H$ ta đều có $ab \in H$.

Nếu tập con H đóng thì H là nửa nhóm với phép toán $H \times H \rightarrow H$, thu hẹp của phép toán trong N . Khi đó ta nói rằng phép toán trong H là *cảm sinh* bởi phép toán trong N và H là *nửa nhóm con* của N .

Ví dụ tập hợp tất cả các số tự nhiên $\mathbb{N}$ là nửa nhóm con của nửa nhóm cộng các số nguyên $\mathbb{Z}$.

Đồng cấu nửa nhóm

Hai cấu trúc đại số có cùng dạng nào đó có thể được so sánh dựa vào các ánh xạ bảo toàn cấu trúc, mà ta gọi là các đồng cấu. Khái niệm đồng cấu là một trong những khái niệm cơ bản của đại số hiện đại. Ta sẽ gặp nó trong mọi cấu trúc đại số mà ta xét.

Định nghĩa. Ánh xạ $f : N \rightarrow N'$ từ nửa nhóm N tới nửa nhóm N' được gọi là *đồng cấu nửa nhóm* nếu

$$f(ab) = f(a)f(b)$$

với mọi $a, b \in N$. Đồng cấu f được gọi là *đơn cấu* (tương ứng *toàn cấu*, *dẳng cấu*) nếu ánh xạ f là đơn ánh (tương ứng toàn ánh, song ánh). Trường hợp $N' = N$ thì f được gọi là một *tự đồng cấu* của N .

Mệnh đề 1.4. Nếu $f : N \rightarrow N'$ là đồng cấu nửa nhóm và N có đơn vị e thì $f(e)$ là đơn vị của Imf .

Chứng minh. Lấy phần tử bất kỳ $y \in Imf$. Khi đó tồn tại $x \in N$ sao cho $y = f(x)$. Do e là phần tử đơn vị của N nên ta có

$$yf(e) = f(x)f(e) = f(xe) = f(x) = y$$

$$f(e)y = f(e)f(x) = f(ex) = f(x) = y.$$

Điều này chứng tỏ $f(e)$ là đơn vị của $f(N)$. □

Chú ý. Nếu $f : N \rightarrow N'$ là một đồng cấu của các nửa nhóm và N có đơn vị e thì có thể $f(e)$ không phải là đơn vị của N' . Chẳng hạn nếu $f : \mathbb{N} \rightarrow \mathbb{N}$ là ánh xạ biến số tự nhiên bất kỳ thành 0 thì f là một tự đồng cấu của nửa nhóm nhân $\mathbb{N}$, nhưng $f(1)$ không phải là phần tử đơn vị của $\mathbb{N}$.

Bây giờ ta hãy xét cấu trúc của một vị nhóm xyclic bất kỳ C sinh bởi phần tử c . Nếu tất cả các lũy thừa của c đều khác nhau thì ta có ánh xạ

$$\begin{aligned} f : \mathbb{N} &\rightarrow C \\ n &\mapsto c^n \end{aligned}$$

là một đẳng cấu.

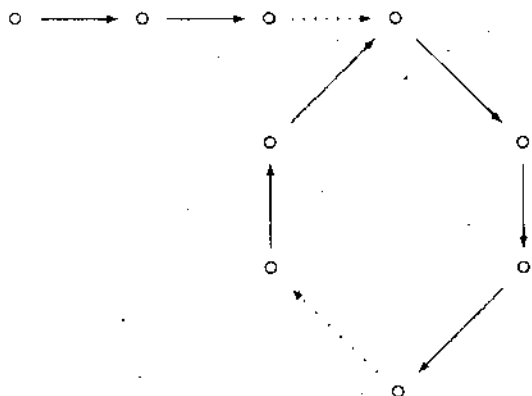
Trong trường hợp ngược lại, sẽ tồn tại số nguyên dương bé nhất

s sao cho $c^s = c^m$ đối với m nào đó, $m < s$. Khi đó $C = \{1, c, \dots, c^s\}$ và bằng quy nạp theo j ta có thể chứng tỏ rằng

$$c^i c^j = c^{i+j-kn},$$

trong đó $n = s - m$ và k là số tự nhiên bé nhất thỏa mãn $i + j - kn < s$ (đặc biệt nếu $i + j < s$ thì $k = 0$). Trong trường hợp này ta nói C là vị nhóm kiểu (m, n) .

Một vị nhóm C kiểu (m, n) có thể biểu diễn bởi đồ thị gồm đoạn đầu có độ dài m và tiếp đó là một vòng xích (hay một thông lọng) độ dài n như hình vẽ dưới đây:



Mệnh đề 1.5. Trong mỗi vị nhóm xyclic kiểu (m, n) , $m \neq 0$, có đúng một phần tử $a \neq 1$ sao cho $a^2 = a$. Khi đó ta gọi a là phần tử lũy đẳng.

Chứng minh. Trước hết ta thấy rằng nếu c là phần tử sinh của vị nhóm xyclic C kiểu (m, n) thì

$$c^i c^k = c^j \Leftrightarrow n \mid k \text{ và } m \leq i < m + n.$$

Bây giờ ta chọn k là số duy nhất trong tập hợp

$$\{m, m+1, \dots, m+n-1\}$$

chia hết cho n , và đặt $i = k$ ta được $c^k c^k = c^k$. □

Bài tập

Đối với các bài tập từ 1.1 đến 1.7 hãy xét các tính chất kết hợp, giao hoán, có đơn vị của phép toán trên đại số hai ngôi đã cho.

1.1. $(M_n(\mathbb{R}), +)$.

1.2. $(\{1, 2, 3, 6, 12\}, \text{UCLN})$.

1.3. $(\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}, +)$.

1.4. $(\{\frac{a}{b} \in \mathbb{Q} \mid a, b \in \mathbb{Z}, b = 2k + 1\}, +)$.

1.5. $(\{z \in \mathbb{C} \mid |z| = 1\}, +)$.

1.6. $(\{z \in \mathbb{C} \mid |z| = 1, \cdot\})$.

1.7. $(\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}, \times)$.

1.8. Giả thiết rằng phép toán hai ngôi $*$ trên tập X có đơn vị và thỏa mãn đẳng thức: $x * (y * z) = (x * z) * y$.

Chứng minh rằng phép toán $*$ là kết hợp và giao hoán.

1.9. Những phép toán nào trong số các phép toán hai ngôi $(m, n) \mapsto m * n$ trên tập các số nguyên $\mathbb{Z}$ sau đây là kết hợp? giao hoán?

$$m * n = m - n; \quad m * n = m^2 + n^2; \quad m * n = 2(m + n).$$

1.10. Giả sử X là một tập hợp tùy ý. Xét ánh xạ

$$X^2 \rightarrow X$$

cho bởi $(x, y) \mapsto x$. Chứng minh X là một nửa nhóm với phép toán hai ngôi này. Nửa nhóm đó có giao hoán hay không? có đơn vị hay không?

1.11. Cho các đồng cấu nửa nhóm $\alpha : A \rightarrow B; \beta : B \rightarrow C$. Chứng minh rằng:

a) Nếu $\beta \circ \alpha$ là toàn cấu thì β là toàn cấu.

b) Nếu $\beta \circ \alpha$ là đơn cấu thì α là đơn cấu.

1.12. Cho $f : X \rightarrow Y$ là một đồng cấu của các nửa nhóm. Chứng minh rằng:

a) Nếu A là một nửa nhóm con của X thì ảnh $f(A)$ là nửa nhóm con của Y .

b) Nếu B là nửa nhóm con của Y thì tạo ảnh toàn phần $f^{-1}(B)$ là nửa nhóm con của X .

- 1.13.** Cho A, B là những vị nhóm và $f : A \rightarrow B$ là đồng cấu nửa nhóm. Chứng minh rằng các điều sau tương đương:
- $f(e_A) = e_B$, trong đó e_A, e_B lần lượt là các phần tử đơn vị của A, B .
 - Ảnh $f(A)$ là vị nhóm con của B .
 - Tạo ảnh $f^{-1}(e_B)$ là vị nhóm con của A .
- Ngoài ra, nếu $f^{-1}(e_B) = \{e_A\}$ thì f có là đơn cấu hay không?
- 1.14.** Giả sử a và b là hai phần tử của một nửa nhóm X sao cho $(ab)^2 = a^2b^2$. Chứng minh rằng $(ab)^n = a^n b^n$ với mọi số tự nhiên $n > 1$. Nếu a và b là hai phần tử sao cho $(ab)^2 = a^2b^2$ thì có suy ra $ab = ba$ hay không?

2. Nhóm

Định nghĩa. Vị nhóm $(G, \circ)$ được gọi là *nhóm* nếu với mỗi phần tử $a \in G$ đều tồn tại một phần tử $a' \in G$ sao cho

$$a \circ a' = a' \circ a = e.$$

Nói cách khác, tập hợp G cùng với phép toán hai ngôi $\circ$ được gọi là một *nhóm* nếu các điều kiện sau được thoả mãn:

(i) Phép toán kết hợp:

$$a \circ (b \circ c) = (a \circ b) \circ c,$$

với mọi a, b, c thuộc G .

(ii) Trong G có phần tử e (gọi là đơn vị) sao cho

$$e \circ a = a \circ e = a,$$

với mọi $a \in G$.

(iii) Đối với mỗi $a \in G$ tồn tại phần tử $a' \in G$ sao cho

$$a \circ a' = a' \circ a = e.$$

Nhóm G được gọi là *giao hoán* hay *abel* (lấy tên nhà toán học Niels Abel) nếu $ab = ba$ với mọi $a, b \in G$.

Bổ đề 2.1. Giả sử nửa nhóm G có đơn vị e . Khi đó phần tử a' có tính chất $aa' = a'a = e$ là duy nhất đối với mỗi $a \in G$.

Chứng minh. Giả sử ngoài phần tử a' còn có phần tử a'' sao cho $aa'' = a''a = e$. Khi đó

$$a'' = a''e = a''(aa') = (a''a)a' = ea' = a'. \quad \square$$

Phần tử duy nhất a' được gọi là *nghịch đảo* của a và ký hiệu bởi a^{-1} . Bây giờ ta có thể nói rằng *một nhóm G là một vị nhóm mà mọi phần tử của nó đều có nghịch đảo* (hay mọi phần tử đều *khả nghịch*).

Ví dụ

1. Đại số hai ngôi $(\mathbb{Z}, +)$ là một nhóm với phần tử đơn vị 0, và đóng vai trò của phần tử a' chính là số đối $-a$ của a .

2. Giả sử G là tập hợp các số phức $\{1, -1, i, -i\}$ và phép nhân các phần tử trên G là phép nhân các số phức. Thế thì G là một nhóm abel. Thật vậy, tích hai phần tử của G là một phần tử thuộc G . Phép nhân trong G là kết hợp, giao hoán do tính kết hợp, giao hoán của phép nhân các số phức. Phần tử đơn vị là 1, còn nghịch đảo của a là $1/a$, cụ thể

$$(-1)^{-1} = -1, i^{-1} = -i, (-i)^{-1} = i.$$

3. Tập hợp $S(X)$ tất cả các song ánh từ tập hợp X tới chính nó lập thành một nhóm với phép toán hai ngôi là phép hợp thành các ánh xạ. Phần tử đơn vị của $S(X)$ là ánh xạ đồng nhất id_X và đối với song ánh $f \in S(X)$ thì phần tử nghịch đảo f' ở đây chính là ánh xạ ngược của f . Mỗi phần tử $f \in S(X)$ được gọi là một *phép thế* của X và $S(X)$ được gọi là *nhóm tất cả các phép thế* của X , hay *nhóm đối xứng* của X .

Bây giờ ta xét một trường hợp riêng có nhiều ứng dụng quan trọng, khi tập hợp X có hữu hạn phần tử. Ta ký hiệu nhóm đối xứng của tập $X = \{1, 2, \dots, n\}$ là S_n , và gọi là *nhóm đối xứng của n phần tử*.

Mỗi song ánh từ X lên chính nó được gọi là một *phép thế bậc n* và được ký hiệu bởi

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix} \quad (1)$$

trong đó mỗi phần tử ở dòng dưới là ảnh của phần tử tương ứng ở dòng trên. Một cách tổng quát, mỗi phép thế f có thể viết dưới dạng

$$f = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ f(i_1) & f(i_2) & \dots & f(i_n) \end{pmatrix}$$

trong đó $i_1, i_2, \dots, i_n$ là một hoán vị của tập X .

Nếu f, g là hai phép thế thì tích $g \circ f$ là phép thế thu được bởi việc thực hiện liên tiếp phép thế f rồi tới phép thế g . (Cũng có tác giả quy ước tích $g \circ f$ được thực hiện bởi g trước rồi đến f). Ví dụ cho hai phép thế bậc 3:

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Do

$$\begin{aligned} (g \circ f)(1) &= g(f(1)) = g(2) = 2, \\ (g \circ f)(2) &= g(f(2)) = g(3) = 1, \\ (g \circ f)(3) &= g(f(3)) = g(1) = 3, \end{aligned}$$

nên

$$g \circ f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Do mỗi phần tử của S_n là một hoán vị bậc n nên nhóm S_n có cấp $n!$.

Phép thế $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ biến các phần tử theo một vòng xích, và được viết một cách đơn giản là $(1\ 3\ 2)$. Ta hiểu điều này như sau: $1 \mapsto 3, 3 \mapsto 2, 2 \mapsto 1$. Phép thế f cũng có thể viết theo ký hiệu vòng xích là $(3\ 2\ 1)$ hay $(2\ 1\ 3)$.

Một cách tổng quát, nếu $a_1, a_2, \dots, a_m, 1 \leq m \leq n$, là các phần tử phân biệt của tập hợp $\{1, 2, \dots, n\}$ thì phép thế f cho bởi $f(a_1) = a_2, f(a_2) = a_3, \dots, f(a_{m-1}) = a_m, f(a_m) = a_1$, và $f(x) = x$ nếu $x \notin \{a_1, a_2, \dots, a_m\}$, được gọi là một vòng xích độ dài m , hay một m -xích. Ta ký hiệu vòng xích này bởi $(a_1 a_2 \dots a_m)$.

Lưu ý rằng giá trị n không được thể hiện trong ký hiệu của vòng xích. Ví dụ,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = (1\ 3\ 4\ 2)$$

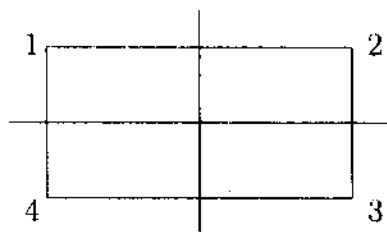
là 4 - vòng xích trong S_4 , còn

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 2 & 5 & 6 \end{pmatrix} = (1\ 3\ 4\ 2)$$

là 4 - vòng xích trong S_6 .

4. Nhóm đối xứng của hình chữ nhật không là hình vuông

Ta đánh dấu các đỉnh của hình chữ nhật bởi các số 1, 2, 3, 4 như ở hình vẽ sau:



Mỗi phép đối xứng của hình chữ nhật biến các đỉnh thành các đỉnh, và như vậy là một hoán vị giữa các đỉnh. Ta ký hiệu a là phép đối xứng qua trục hoành, thế thì

$$a(1) = 4, a(2) = 3, a(3) = 2, a(4) = 1.$$

Tương tự b là phép đối xứng qua trục tung. Phép đối xứng thứ ba c là phép quay 180° quanh gốc tọa độ. Phép đối xứng cuối cùng là phép đồng nhất e . Nhóm các phép đối xứng của hình chữ nhật được cho bởi bảng sau:

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Nhóm này thường được gọi là 4-nhóm Klein, mang tên nhà hình học người Đức Felix Klein (1849 - 1925).

Bổ đề 2.2. Đối với mọi phần tử a, b của nhóm G ta có

- (i) $(a^{-1})^{-1} = a$;
- (ii) $(ab)^{-1} = b^{-1}a^{-1}$.

Chứng minh. (i) Do $aa^{-1} = e$ nên a là phần tử nghịch đảo của a^{-1} . Từ tính duy nhất của nghịch đảo ta suy ra $(a^{-1})^{-1} = a$.

(ii) Rõ ràng ta có

$$\begin{aligned}(ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1} = aa^{-1} = e \\ (b^{-1}a^{-1})(ab) &= b^{-1}(a^{-1}a)b = b^{-1}b = e\end{aligned}$$

nên phần tử $b^{-1}a^{-1}$ là phần tử nghịch đảo của ab . $\square$

Hệ quả 2.3. Trong nhóm G luật giản ước luôn luôn thực hiện được, nghĩa là $ax = ay$ kéo theo $x = y$ và $xb = yb$ kéo theo $x = y$, với mọi $a, b \in G$.

Chứng minh. Nhân a^{-1} vào bên trái mỗi vế của đẳng thức thứ nhất ta được

$$\begin{aligned}a^{-1}(ax) &= a^{-1}(ay) \\ \Rightarrow (a^{-1}a)x &= (a^{-1}a)y \Rightarrow x = y.\end{aligned}$$

Điều còn lại được chứng minh tương tự. $\square$

Chúng ta đã ký hiệu $a^k, k \geq 1$ là tích của a với chính nó k lần. Tương tự, ta ký hiệu $a^{-k} = (a^{-1})^k$, với $k \geq 1$. Sau cùng ta viết a^0 là đơn vị. Như vậy ta đã xác định a^k với mọi $k \in \mathbb{Z}$, và ta có các luật lũy thừa:

$$a^k a^m = a^{k+m}, (a^k)^m = a^{km}$$

đối với mọi $a \in G$ và mọi $k, m \in \mathbb{Z}$.

Hơn nữa, nếu $ab = ba$ thì $(ab)^k = a^k b^k, k \in \mathbb{Z}$. Tuy nhiên điều này không đúng nếu $ab \neq ba$. Ví dụ, nếu

$$a = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, b = \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}$$

trong nhóm các ma trận khả nghịch cỡ 2×2 thì $(ab)^2 \neq a^2 b^2$.

Sau đây là những điều kiện tương đương với định nghĩa của nhóm.

Định lý 2.4. Một nửa nhóm G là nhóm nếu và chỉ nếu hai điều kiện sau được thoả mãn:

(i) Tồn tại phần tử $e \in G$ sao cho $ea = a$ với mọi $a \in G$ (e được gọi là đơn vị trái của G),

(ii) Với mỗi $x \in G$ tồn tại $x' \in G$ sao cho $x'x = e$ (x' gọi là nghịch đảo trái của x).

Chứng minh. ($\Rightarrow$) Điều này là hiển nhiên.

($\Leftarrow$) Giả sử e là một đơn vị trái của nửa nhóm G . Ta sẽ chứng tỏ e cũng là đơn vị phải của G và khi đó e là đơn vị của G theo Mệnh đề 1.2.

Lấy phần tử tùy ý $a \in G$. Khi đó theo (ii) tồn tại $b \in G$ để $ba = e$. Lại theo (ii) ta có phần tử $c \in G$ để $cb = e$. Khi đó

$$ab = eab = (cb)(ab) = c(ba)b = cb = e.$$

Điều này chứng tỏ b cũng là nghịch đảo phải của a . Khi đó ta cũng có

$$ae = a(ba) = (ab)a = ea = a.$$

Như vậy e cũng là đơn vị phải và do đó là đơn vị của G . Đồng thời mỗi nghịch đảo trái của phần tử tùy ý a cũng là nghịch đảo hai phía. Vậy G là nhóm. $\square$

Hệ quả 2.5. *Nửa nhóm G là 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. ($\Rightarrow$) Nếu G là nhóm thì các phương trình lần lượt có nghiệm là $x = a^{-1}b, y = ba^{-1}$.

($\Leftarrow$) Lấy phần tử $a \in G$. Gọi e là nghiệm của phương trình $ya = a$. Ta chứng tỏ e là đơn vị trái trong G . Thật vậy, nếu c là phần tử nào đó của G thì tồn tại phần tử $u \in G$ là nghiệm của phương trình $ax = c$. Khi đó

$$ec = e(au) = (ea)u = au = c.$$

Bây giờ với phần tử bất kỳ $a \in G$ nghiệm của phương trình $ya = e$ chính là nghịch đảo trái của a . Theo Định lý 2.4, G là một nhóm. $\square$

Bài tập

Đối với các bài từ 2.1 đến 2.4 hãy cho biết đâu là nhóm, đâu là nhóm abel. Hãy giải thích cho kết luận đưa ra.

2.1. $(M_n(\mathbb{R}) \setminus \{0\}, \cdot)$, trong đó 0 là ma trận không cỡ $n \times n$.

2.2. $(\{e, a\}, *)$, trong đó $e * e = e$, và $e * a = a * e = a * a = a$.

- 2.3. $(\mathbb{R}^*, \sim)$ trong đó $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ và $x \sim y$ là xy nếu $x > 0$, là x/y nếu $x < 0$.
- 2.4. $(\mathbb{Z}, *)$, trong đó $m * n$ là $m + n$ nếu m chẵn, và là $m - n$ nếu m lẻ.
- 2.5. Chứng minh rằng $\mathbb{Z}_6^* = \mathbb{Z}_6 \setminus \{\bar{0}\}$ không là nhóm đối với phép nhân $\bar{r} \cdot \bar{s} = \overline{rs}$.
- 2.6. Cho G là tập tất cả các cặp số thực (a, b) , trong đó $a \neq 0$. Trên G xác định phép toán hai ngôi cho bởi công thức

$$(a, b) * (c, d) = (ac, bc + d).$$

Chứng tỏ rằng khi đó G là một nhóm.

- 2.7. Chứng minh rằng trong nhóm G

$$(a_1 a_2 \dots a_n)^{-1} = a_n^{-1} \dots a_2^{-1} a_1^{-1}.$$

- 2.8. Chứng minh rằng trong nhóm G , $(a^{-1}ba)^k = a^{-1}b^k a$ đối với mỗi số nguyên k .
- 2.9. Chứng minh rằng nếu $a^2 = e$ với mọi phần tử a của nhóm G thì G là nhóm abel.
- 2.10. Nếu a không là đơn vị của nhóm và $a^4b = ba^5$, hãy chứng minh $ab \neq ba$.
- 2.11. Cho G là nửa nhóm. Với mỗi $a \in G$ ký hiệu

$$aG = \{ax \mid x \in G\} \quad (1)$$

$$Ga = \{xa \mid x \in G\}. \quad (2)$$

Chứng minh rằng G là nhóm khi và chỉ khi với mỗi a thì $aG = Ga = G$.

- 2.12. Chứng minh rằng G là một nhóm abel khi và chỉ khi G thỏa mãn các điều kiện sau:
- (i) $(ab)c = a(cb)$,
 - (ii) Tồn tại $e \in G$ sao cho $ea = a$ với mọi $a \in G$,
 - (iii) Với mỗi $a \in G$ tồn tại $a' \in G$ để $a'a = e$.
- 2.13. Chứng minh rằng một nửa nhóm hữu hạn X là nhóm nếu và chỉ nếu luật giản ước thực hiện được đối với mọi phần tử của nó.

3. Nhóm con

Ta thấy rằng có những tập con nào đó của một nhóm cũng là nhóm với chính phép toán này. Nhóm như vậy được gọi là nhóm con của nhóm đã cho. Ví dụ $(\mathbb{R}, +)$ là một nhóm con của nhóm $(\mathbb{C}, +)$. Bây giờ ta sẽ đưa ra định nghĩa chính xác của khái niệm nhóm con theo ngôn ngữ của phép toán đại số.

Ta nhắc lại rằng tập con khác rỗng H của nửa nhóm nhân G được gọi là *đóng* (hay *ổn định*) nếu $a, b \in H \Rightarrow ab \in H$, và khi đó H là nửa nhóm con của G với phép toán cảm sinh bởi phép toán trong G .

Định nghĩa. Tập con đóng H của nhóm nhân G được gọi là *nhóm con* của G nếu nó là một nhóm đối với phép toán cảm sinh bởi phép nhân trong G .

Ví dụ

1. Đối với mỗi nhóm G , bản thân G và tập $E = \{e\}$ là những nhóm con, chúng được gọi là những nhóm con *tâm thường* của G .

Chú ý rằng, để đơn giản, người ta thường ký hiệu $E = \{e\}$ bởi e mà không sợ có sự nhầm lẫn nào.

2. Trong nhóm $(\mathbb{Z}, +)$ tập $n\mathbb{Z} = \{x \mid x = na, a \in \mathbb{Z}\}$ là một nhóm con với mỗi $n \in \mathbb{N}$.

Bây giờ ta cho một đặc trưng của nhóm con.

Định lý 3.1. Tập con H của nhóm G là nhóm con khi và chỉ khi các điều kiện sau được thỏa mãn:

- (i) nếu $a, b \in H$ thì $ab \in H$,
- (ii) $e \in H$,
- (iii) nếu $a \in H$ thì $a^{-1} \in H$.

Chứng minh. ($\Leftarrow$) Điều kiện (i) chứng tỏ H là tập đóng đối với phép nhân trong G và do đó phép nhân cảm sinh trong H là kết hợp. Các điều kiện (ii) và (iii) chứng tỏ H là một nhóm, và do đó H là nhóm con của G .

($\Rightarrow$) Giả sử nhóm con H có đơn vị e_H . Khi đó $e_H^2 = e_H = ee_H$. Thực hiện luật giản ước trong G ta có $e_H = e$.

Bây giờ giả sử $a \in H$ có nghịch đảo trong G và nghịch đảo trong H lần lượt là a^{-1}, c . Khi đó $aa^{-1} = e = ac$.

Thực hiện luật giản ước trong G ta có $a^{-1} = c$. Cuối cùng, do H là nhóm con nên nó là tập con đóng và do đó có (i). $\square$

Mệnh đề 3.2. Nếu H là một tập con hữu hạn khác rỗng của nhóm G và $ab \in H$ với mọi $a, b \in H$, thì H là nhóm con của G .

Chứng minh. Chúng ta chứng tỏ rằng phần tử đơn vị e thuộc H , và đối với mỗi $a \in H$, nghịch đảo của nó cũng thuộc H . Do H là tập con đóng nên mọi phần tử $a, a^2, a^3, \dots$ thuộc vào H . Nhưng do H là tập hữu hạn nên những phần tử này không thật sự phân biệt, bởi vậy phải có $a^i = a^j$ đối với $1 \leq i < j$ nào đó. Giản ước hai vế cho a^i ta được $e = a^{j-i}$, điều này chứng tỏ $e \in H$. Bây giờ ta có $a^{-1} = a^{j-i-1} \in H$, do $j-i-1 \geq 0$. $\square$

Hệ quả 3.3. Giả sử H là tập con khác rỗng của nhóm G . Khi đó các điều kiện sau là tương đương:

- (i) H là nhóm con của G .
- (ii) Nếu $a, b \in H$ thì $a^{-1} \in H$ và $ab \in H$.
- (iii) Nếu $a, b \in H$ thì $ab^{-1} \in H$.

Chứng minh. (i) $\Rightarrow$ (ii) do Định lý 3.1.

(ii) $\Rightarrow$ (iii) Nếu $a, b \in H$ thì $b^{-1} \in H$ và do đó $ab^{-1} \in H$.

(iii) $\Rightarrow$ (i) Lấy phần tử bất kỳ $a \in H$. Khi đó theo (c) $e = aa^{-1} \in H$. Lại theo (c) với $e, a \in H$ ta có $a^{-1} = ea^{-1} \in H$. Cuối cùng, với $a, b \in H$ ta có $b^{-1} \in H$ và do đó theo (c)

$$ab = a(b^{-1})^{-1} \in A.$$

Vậy H là nhóm con của G theo Định lý 3.1. $\square$

Hệ quả 3.4. Trong nhóm G tập hợp tất cả các lũy thừa $a^n (n \in \mathbb{Z})$ của phần tử a lập thành một nhóm con, được gọi là nhóm cyclic sinh bởi a .

Định nghĩa. 1) Phần tử a của nhóm G gọi là có cấp vô hạn nếu không tồn tại số nguyên dương n nào sao cho $a^n = e$. Phần tử a được gọi là có cấp hữu hạn m nếu m là số nguyên dương bé nhất sao cho $a^m = e$.

2) Lực lượng của nhóm G , ký hiệu bởi $|G|$, được gọi là cấp của nhóm. G được gọi là nhóm hữu hạn nếu $|G|$ là hữu hạn, và được gọi là nhóm vô hạn nếu $|G|$ là vô hạn.

Ví dụ

1. Nhóm $\{1, -1, i, -i\}$ là nhóm xyclic cấp 4 sinh bởi i .
2. 4-Nhóm Klein K nói trong ví dụ ở mục 2 không là xyclic. Thật vậy, các phần tử khác đơn vị của nó đều có cấp 2. Nghĩa là K không có phần tử cấp 4, nên không là xyclic.
3. Nhóm các phép quay của một đa giác đều n đỉnh trong mặt phẳng là nhóm xyclic cấp n , sinh bởi phép quay góc $2\pi/n$ radian. Nhóm này ký hiệu bởi C_n .

Bổ đề 3.5. Cho G là nhóm với phần tử đơn vị e và $a \in G$ là phần tử có cấp n . Khi đó $a^k = e$ khi và chỉ khi k chia hết cho n .

Chứng minh. Điều kiện đủ là hiển nhiên. Bây giờ ta chứng minh điều kiện cần. Giả sử k là số nguyên sao cho $a^k = e$. Theo định lý về phép chia với dư trong $\mathbb{Z}$ ta có

$$k = nq + r, 0 \leq r < n.$$

Do $a^n = e$ nên từ đẳng thức trên suy ra $a^k = a^r$, và do đó $a^r = e$. Nếu $r \neq 0$ thì điều này trái với tính bé nhất của n . Bởi vậy phải có $r = 0$, và ta có điều phải chứng minh. $\square$

Tập hợp sinh

Bổ đề 3.6. Giao của một họ khác rỗng những nhóm con của nhóm G là một nhóm con của G .

Chứng minh. Giả sử $\{G_i \mid i \in I\}$, $I \neq \emptyset$ là một họ nhóm con của G và $\tilde{G} = \bigcap_i G_i$.

Vì $e \in G_i$ với mọi $i \in I$ nên $e \in \tilde{G}$, do đó $\tilde{G} \neq \emptyset$. Giả sử $a, b \in \tilde{G}$. Khi đó $a, b \in G_i, \forall i \in I$. Do G_i là nhóm con của G nên $ab^{-1} \in G_i$, với mọi $i \in I$. Từ đó $ab^{-1} \in \tilde{G}$. Điều này chứng tỏ $\tilde{G}$ là nhóm con của nhóm G . $\square$

Để thấy giao H của tất cả các nhóm con của nhóm G chứa tập U là nhóm con bé nhất chứa U . Từ đó ta có khái niệm sau.

Định nghĩa. Cho U là một tập hợp con của nhóm G . Khi đó, nhóm con bé nhất H chứa U được gọi là *nhóm con sinh bởi tập U* , còn U được gọi là *tập sinh* hay *tập các phần tử sinh* của H . Trường hợp $H = G$ ta nói rằng G *sinh bởi U* .

Rõ ràng nhóm con H là xyclic khi nó được sinh bởi tập gồm một phần tử.

Mệnh đề 3.7. *Nhóm con của một nhóm xyclic là xyclic.*

Chứng minh. Giả sử G là nhóm xyclic sinh bởi phần tử g và H là một nhóm con của nó. Nếu $H = \{e\}$ thì H là nhóm xyclic sinh bởi e . Trong trường hợp $H \neq \{e\}$, gọi s là số nguyên dương bé nhất sao cho $g^s \in H$.

Hiển nhiên, $g^{qs} = (g^s)^q \in H$ với mọi $q \in \mathbb{Z}$. Bây giờ ta chứng tỏ rằng mọi phần tử thuộc H đều là lũy thừa của g^s . Giả sử $g^k \in H$. Theo định lý về phép chia với dư trong vành số nguyên $\mathbb{Z}$ ta có $k = sq + r, 0 \leq r < s$. Từ đó,

$$r = k - sq, g^r = g^k \cdot (g^{sq})^{-1} \in H.$$

Nếu $r \neq 0$ thì điều này trái với tính bé nhất của s . Vậy $r = 0$ và do đó $g^k = (g^s)^q$. Bởi vậy H là nhóm xyclic sinh bởi phần tử g^s . $\square$

Hệ quả 3.8. *Mọi nhóm con của nhóm $(\mathbb{Z}, +)$ đều có dạng $A = m\mathbb{Z}$ với $m \in \mathbb{Z}$.*

Chứng minh. Nếu nhóm con $A = 0$ thì $A = 0\mathbb{Z}$. Nếu $A \neq 0$ theo chứng minh của mệnh đề trên A là nhóm xyclic sinh bởi phần tử $m.1 = m$. Khi đó $A = m\mathbb{Z}$. $\square$

Ví dụ. *Nhóm các phép tự trùng D_n của đa giác đều trong không gian.* Ta xét nhóm tất cả các phép dời hình trong không gian ba chiều biến một đa giác đều n đỉnh thành chính nó. Ngoài n phép quay trong mặt phẳng nó còn có n phép lật đa giác trong không gian quanh trục đối xứng (có n trục đối xứng). Gọi g là phép quay góc $2\pi/n$ radian và h là một phép lật, thế thì h là một phần tử cấp 2 và nhóm D_n sinh bởi hai phần tử g, h :

$$D_n = \{e, g, g^2, \dots, g^{n-1}, hg, hg^2, \dots, hg^{n-1}\}$$

Chú ý rằng nếu $n \geq 3$ thì $gh \neq hg$ nên D_n không là nhóm giao hoán và do đó không là xyclic.

Bài tập

3.1. Chứng minh rằng:

- a) Cấp của phần tử g^{-1} chính là cấp của g .
- b) Cấp của phần tử ab chính là cấp của ba .

3.2. Vẽ sơ đồ các nhóm con của nhóm C_6 .

3.3. Vẽ sơ đồ các nhóm con của nhóm S_3 .

3.4. Trong nhóm các phép thế S_4 chứng minh rằng các phép thế:

$$e, \quad a = (12)(34), \quad b = (13)(24), \quad c = (14)(23)$$

lập thành một nhóm con của S_4 . Nhóm con đó có giao hoán hay không?

3.5. Số phần tử sinh của nhóm xyclic C_n là bao nhiêu?

3.6. Tìm các nhóm con cấp 3 của nhóm S_3 .

3.7. Lập bảng nhân và tìm cấp của mỗi phần tử của nhóm

$$(\{\pm 1, \pm i, \pm j, \pm k\}, \cdot),$$

trong đó

$$i^2 = j^2 = k^2 = -1, \quad ij = k = -ji, \quad jk = i = -kj, \quad ki = j = -ik.$$

Nhóm này được gọi là *nhóm quaternion* Q , cấp 8.

3.8. Xây dựng bảng cho nhóm sinh bởi g và h , trong đó g và h thoả mãn các hệ thức $g^3 = h^2 = e$ và $gh = hg^2$.

3.9. Giả sử H là một nhóm con của nhóm G , và g là một phần tử bất kỳ thuộc G . Chứng minh rằng tập hợp

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\}$$

là một nhóm con của G . Nhóm con này được gọi là nhóm con *liên hợp* của H bởi g .

3.10. Chứng minh rằng nếu nhóm G có cấp 4 thì hoặc G là nhóm xyclic hoặc mọi phần tử khác đơn vị của G có cấp 2.

3.11. Chứng minh rằng tập con khác rỗng H của nhóm hữu hạn G là nhóm con nếu và chỉ nếu nó đóng đối với phép toán trong G .

- 3.12.** Chứng minh các phát biểu sau là tương đương:
 a) Nhóm G có nhiều hơn một phần tử và không có nhóm con thực sự.
 b) G là nhóm xyclic cấp nguyên tố.
- 3.13.** Cho A là một nhóm xyclic cấp n và d là một ước của n . Chứng minh rằng A có đúng một nhóm con cấp d và nhóm con này là xyclic.
- 3.14.** Chứng minh rằng mọi nhóm xyclic vô hạn đều có đúng hai phần tử sinh.
- 3.15.** Các số nguyên Gauss là các phần tử thuộc tập hợp

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}.$$

Nhóm $(\mathbb{Z}[i], +)$ có là xyclic không?

- 3.16.** Chứng minh rằng trong nhóm nhân abel A , tập hợp tất cả các phần tử $a \in A$ có tính chất $a^n = e$ với số nguyên dương n đã cho lập thành một nhóm con của A . Điều này còn đúng không đối với nhóm không abel?
- 3.17.** Chứng minh rằng hai nhóm con khác không bất kỳ của nhóm $(\mathbb{Q}, +)$ có giao khác không.
- 3.18.** Cho A là một nhóm con của nhóm X và $a \in X$. Chứng minh rằng tập hợp $aA = \{ax \mid x \in A\}$ là một nhóm con của X khi và chỉ khi $a \in A$.
- 3.19.** Giả sử X là một nhóm xyclic cấp n sinh bởi phần tử a . Xét phần tử $b = a^k \in X$. Chứng minh:
 a) Cấp của b bằng $\frac{n}{d}$, với d là ước chung lớn nhất của n và k .
 b) b là phần tử sinh của X khi và chỉ khi n và k nguyên tố cùng nhau (từ đó suy ra số phần tử sinh của X).
- 3.20.** Chứng minh rằng nhóm có cấp là số chẵn có ít nhất một phần tử cấp 2.

4. Nhóm con chuẩn tắc - nhóm thương

Lớp ghép

Định nghĩa. Cho H là một nhóm con của nhóm G . Khi đó tập hợp $gH = \{ga \mid a \in H\}$, với $g \in G$ được gọi là *lớp ghép trái* của nhóm G theo nhóm con H . Định nghĩa tương tự cho *lớp ghép phải* Hg .

Bổ đề 4.1. Cho H là nhóm con của nhóm G và $a, b \in G$. Khi đó

$$aH = bH \Leftrightarrow a^{-1}b \in H,$$

$$Ha = Hb \Leftrightarrow ab^{-1} \in H.$$

Chứng minh. Giả sử $aH = bH$. Khi đó tồn tại $u, v \in H$ sao cho $au = bv$. Suy ra $a^{-1}b = uv^{-1} \in H$.

Ngược lại, giả sử $a^{-1}b \in H$. Lấy $x \in aH, x = au$, với $u \in H$. Theo giả thiết $a^{-1}b = c \in H$. Từ đó $a = bc^{-1}$ và

$$x = au = (bc^{-1})u = b(c^{-1}u) = bv,$$

với $v = c^{-1}u \in H$. Nghĩa là $x \in bH$. Vậy $aH \subset bH$.

Hoàn toàn tương tự ta có $bH \subset aH$, và do đó $aH = bH$.

Phép tương đương thứ hai được suy ra tương tự. $\square$

Bổ đề nói trên cho phép chúng ta trình bày khái niệm lớp ghép bằng ngôn ngữ quan hệ tương đương. Trên G ta xác định một quan hệ hai ngôi $\sim$ như sau:

$$a \sim b \bmod H \Leftrightarrow a^{-1}b \in H.$$

Có thể thử lại rằng quan hệ $\sim$ này là một *quan hệ tương đương* trên G ; do đó nó cho một *phân hoạch* nhóm G theo các lớp không giao nhau và mỗi lớp như vậy là một lớp ghép trái theo H .

Thật vậy, với mỗi $a \in G$ thì $a^{-1}a \in H$ nên quan hệ có tính chất phản xạ. Nếu $a \sim b \bmod H$ thì $a^{-1}b \in H$, từ đó $b^{-1}a = (a^{-1}b)^{-1} \in H$, nghĩa là $b \sim a \bmod H$. Do đó quan hệ đã cho có tính đối xứng.

Nếu $a \sim b \bmod H$ và $b \sim c \bmod H$ thì $a^{-1}b, b^{-1}c \in H$, khi đó

$$a^{-1}c = (a^{-1}b)(b^{-1}c) \in H \text{ và } a \sim c \bmod H,$$

vì vậy quan hệ có tính bắc cầu, và do đó là một quan hệ tương đương.

Lớp tương đương chứa phần tử a là

$$\begin{aligned}\{g \in G \mid g \sim a \bmod H\} &= \{g \in G \mid a^{-1}g \in H\} \\ &= \{g \in G \mid g = ah, h \in H\} = aH.\end{aligned}$$

Tương tự, quan hệ hai ngôi $a \sim b \Leftrightarrow ab^{-1} \in H$ là một quan hệ tương đương trên G mà mỗi lớp tương đương là một lớp ghép phải theo H .

Ví dụ sau sẽ chỉ ra lớp ghép trái của một phần tử không nhất thiết trùng với lớp ghép phải.

Ví dụ. Tìm các lớp ghép trái và lớp ghép phải của mỗi nhóm $H = A_3$ và $K = \{(1), (12)\}$ trong S_3 .

Trước hết ta tính các lớp ghép phải của $H = A_3$ theo bảng sau

	<u>Các lớp ghép phải</u>		<u>Các lớp ghép trái</u>
H	$= \{(1), (123), (132)\}$	H	$= \{(1), (123), (132)\}$
$H(12)$	$= \{(12), (13), (23)\}$	$(12)H$	$= \{(12), (23), (13)\}$

Trong trường hợp này, các lớp ghép trái và các lớp ghép phải của H là như nhau.

Tuy nhiên, các lớp ghép trái và ghép phải của K không trùng nhau hoàn toàn.

	<u>Các lớp ghép phải</u>		<u>Các lớp ghép trái</u>
K	$= \{(1), (12)\}$	K	$= \{(1), (12)\}$
$K(13)$	$= \{(13), (132)\}$	$(13)K$	$= \{(13), (123)\}$
$K(23)$	$= \{(23), (123)\}$	$(23)K$	$= \{(23), (132)\}$

Nhận xét

1. Ta có thể thấy rằng tương ứng $gH \longleftrightarrow Hg^{-1}$ là một song ánh giữa tập các lớp ghép trái và tập các lớp ghép phải của nhóm G theo nhóm con H , do đó hai lớp ghép này là cùng lực lượng.

2. Nhóm con H và lớp ghép gH có cùng lực lượng do tương ứng $h \longleftrightarrow gh$ là song ánh.

Thật vậy, xét tương ứng $\varphi: H \rightarrow aH$ cho bởi $\varphi(h) = ah$. Rõ ràng φ là một toàn ánh. Giả sử $\varphi(h_1) = \varphi(h_2)$, nghĩa là $ah_1 = ah_2$. Nhân

a^{-1} vào bên trái mỗi vế ta được $h_1 = h_2$. Điều này nói lên φ là một đơn ánh, và do đó là một song ánh.

Định nghĩa. Số các lớp ghép trái của G theo nhóm con H được gọi là *chỉ số* của H trong G , và ký hiệu bởi $[G : H]$.

Định lý 4.2. (Định lý Lagrange). Nếu G là một nhóm hữu hạn và H là nhóm con của G thì cấp của H chia hết cấp của G .

Chứng minh. Giả sử cấp của nhóm con H và của nhóm G lần lượt là m và n . Nếu G được phân hoạch thành p lớp ghép trái theo H thì theo nhận xét trên ta có $n = p.m$. Bởi vậy $|H|$ chia hết $|G|$. $\square$

Hệ quả 4.3. Cấp của một phần tử tùy ý của nhóm hữu hạn G chia hết cấp của G .

Chứng minh. Giả sử $H = \{a^r \mid r \in \mathbb{Z}\}$ là nhóm con cyclic sinh bởi phần tử $a \in G$. Cấp của nhóm H bằng cấp của phần tử a . Do đó theo định lý Lagrange ta có cấp của a chia hết cấp của nhóm G . $\square$

Hệ quả 4.4. Nếu a là một phần tử của nhóm hữu hạn G thì $a^{|G|} = e$.

Chứng minh. Nếu m là cấp của a thì $|G| = mk$ với số tự nhiên k nào đó. Bởi vậy $a^{|G|} = a^{mk} = (a^m)^k = e^k = e$. $\square$

Hệ quả 4.5. Mọi nhóm cấp nguyên tố p là cyclic.

Chứng minh. Giả sử G là nhóm cấp nguyên tố p , gọi a là phần tử tùy ý khác đơn vị của G . Khi đó nhóm con cyclic A sinh bởi a có cấp $n > 1$ và n là ước của cấp p của G . Do p là số nguyên tố nên $n = p$, nghĩa là $A = G$. $\square$

Mệnh đề đảo của định lý Lagrange nói chung không đúng, nghĩa là nếu m là một ước của cấp của nhóm G thì không nhất thiết trong G có nhóm con cấp m . Trong mục sau này ta sẽ chứng minh A_4 là một nhóm cấp 12 nhưng nó không có nhóm con cấp 6.

Định lý Lagrange có thể mở rộng cho trường hợp các nhóm cyclic hữu hạn. Bổ đề sau đây là cần thiết.

Bổ đề 4.6. Cho g là một phần tử cấp n trong một nhóm và $m \geq 1$.

(i) Nếu $(n, m) = d$ thì g^m có cấp n/d .

(ii) Đặc biệt nếu m chia hết n thì g^m có cấp n/m .

Chứng minh. (i) Trước hết ta có

$$(g^m)^{n/d} = (g^n)^{m/d} = e^{m/d} = e.$$

Giả sử $g^k = e$, ta phải chỉ ra n/d chia hết k . Ta có $g^{mk} = e$, vì vậy n chia hết m/k . Do đó, n/d chia hết $(m/d)k$. Nhưng n/d và m/d nguyên tố cùng nhau, vì vậy n/d chia hết k .

(ii) Nếu m chia hết n , thì $(n, m) = m$, vì vậy từ (i) suy ra (ii). $\square$

Mệnh đề 4.7. Nếu G là một nhóm cyclic cấp n , và k chia hết n thì G có đúng một nhóm con H cấp k . Hơn nữa, nếu g sinh ra G , thì H được sinh bởi $g^{n/k}$.

Chứng minh. Giả sử G sinh bởi phần tử g . Gọi H là nhóm con sinh bởi $g^{n/k}$. Khi đó, $|H| = k$ bởi vì $g^{n/k}$ có cấp k . Bây giờ cho K là một nhóm con bất kỳ của G , có cấp k , và giả sử K được sinh bởi g^m có cấp k . Nếu $d = (m, n)$, thì g^m có cấp n/d theo bổ đề vừa nêu trên. Do đó, $k = n/d$ hay $d = n/k$. Ta biểu diễn số nguyên d dưới dạng $d = xm + yn$, $x, y \in \mathbb{Z}$. Khi đó,

$$g^{n/k} = g^d = (g^m)^x (g^n)^y = (g^m)^x \in K.$$

Vì $g^{n/k}$ sinh ra H , nên $H \subset K$. Từ đó do $|H| = |K|$ nên $H = K$. $\square$

Nhóm con chuẩn tắc

Định nghĩa. Nhóm con H của nhóm G được gọi là *nhóm con chuẩn tắc* nếu $gH = Hg$ với mọi $g \in G$. Khi đó ta cũng nói rằng H là nhóm con chuẩn tắc trong G .

Khái niệm nhóm con chuẩn tắc có một số đặc trưng cơ bản sau.

Định lý 4.8. Cho H là nhóm con của nhóm G . Khi đó các điều sau là tương đương:

- (i) H là chuẩn tắc trong G .
- (ii) $gHg^{-1} = H$ với mọi $g \in G$, trong đó $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$.
- (iii) $gag^{-1} \in H$ với $\forall g \in G, \forall a \in H$.

Phần tử gag^{-1} được gọi là liên hợp của a bởi g .

Chứng minh. (i) $\Rightarrow$ (ii) Nếu H là nhóm con chuẩn tắc trong G thì $gH = Hg$ với mọi $g \in G$. Bởi vậy nếu h là phần tử thuộc H thì tồn tại $h' \in H$ sao cho $gh = h'g$. Suy ra $ghg^{-1} = h' \in H$, nghĩa là $gHg^{-1} \subset H$.

Điều này đúng cho mọi $g \in G$ nên ta có

$$H = (gg^{-1})H(gg^{-1}) = g(g^{-1}Hg)g^{-1} \subset gHg^{-1} \subset H.$$

Từ đó suy ra b).

(ii) $\Rightarrow$ (iii). Hiển nhiên.

(iii) $\Rightarrow$ (i). Với $a \in H$ từ giả thiết suy ra $gag^{-1} = a' \in H$. Do đó $ga = a'g$. Điều này chứng tỏ $gH \subset Hg$. Tương tự, $g^{-1}ag = a'' \in H$ nên $ag = ga''$, và do đó $Hg \subset gH$.

Vậy $gH = Hg$, và H là chuẩn tắc trong G . □

Ví dụ

1. Trong mọi nhóm G , bản thân nhóm G và nhóm con đơn vị e là những nhóm con chuẩn tắc. Nhóm $G \neq \{e\}$ và không có nhóm con chuẩn tắc nào ngoài G và e được gọi là *nhóm đơn*. Có thể thấy mọi nhóm xyclic cấp nguyên tố đều là nhóm đơn.

2. Trong nhóm giao hoán A mọi nhóm con đều là nhóm con chuẩn tắc.

3. Mọi nhóm con có chỉ số 2 trong một nhóm G đều là nhóm con chuẩn tắc.

Chứng minh. Giả sử H là nhóm con có chỉ số 2 trong G . Khi đó trong G chỉ có hai lớp ghép trái theo H . Một trong hai lớp này là H và lớp khác là gH , với g là phần tử không thuộc vào H . Bây giờ ta chứng tỏ rằng $ghg^{-1} \notin H$, với mọi $g \in G, h \in H$.

Nếu $g \in H$ thì điều này là hiển nhiên. Bây giờ giả sử $g \notin H$, và giả sử rằng $ghg^{-1} \notin H$. Thế thì phần tử ghg^{-1} phải thuộc vào lớp ghép gH , và do đó ta có $ghg^{-1} = gh_1, h_1 \in H$. Từ đó $g = hh_1^{-1} \in H$, và điều này trái với giả thiết $g \notin H$. Bởi vậy $ghg^{-1} \in H$, với mọi $g \in G, h \in H$, và do đó H là nhóm con chuẩn tắc của G .

Ta cũng có thể lập luận một cách đơn giản như sau. Trong G có sự phân lớp theo lớp ghép trái $\{H, gH\}$ và sự phân lớp theo lớp ghép phải $\{H, Hg\}$ với g là một phần tử không thuộc vào H . Từ đó $gH = Hg$ và bởi vậy H là nhóm con chuẩn tắc của G . □

Nhóm thương

Giả sử H là nhóm con của nhóm G . Khi đó trong G có sự chia lớp tương đương theo các lớp ghép trái của H , và ta có tập

$$G/H = \{gH \mid g \in G\},$$

được gọi là *tập thương* của nhóm G theo H .

Bây giờ chúng ta sẽ xác định phép toán hai ngôi trên G/H , cảm sinh bởi phép toán trong G , và chứng tỏ rằng G/H cùng với phép toán này là một nhóm.

Bổ đề 4.9. Nếu H là nhóm con chuẩn tắc trong nhóm G thì tương ứng

$$\begin{aligned}(G/H) \times (G/H) &\rightarrow G/H \\ (aH, bH) &\mapsto (ab)H\end{aligned}$$

là một ánh xạ. Hơn nữa, tập thương G/H là một nhóm với phép toán $(aH)(bH) = (ab)H$.

Chứng minh. Giả sử H là nhóm con chuẩn tắc trong G và giả sử $aH = xH, bH = yH$. Ta cần chứng minh $(ab)H = (xy)H$. Từ giả thiết suy ra $x = au, y = bv$, với $u, v \in H$. Khi đó:

$$xy = (au)(bv) = ab(b^{-1}ub)v = (ab)h,$$

với $h = (b^{-1}ub)v$. Do H là nhóm con chuẩn tắc, và $b^{-1}ub$ là phần tử liên hợp của $u \in H$ nên $b^{-1}ub \in H$. Từ đó $h \in H$. Điều này chứng tỏ $(xy)H = (ab)H$. Bởi vậy tương ứng đã cho là một ánh xạ.

Theo định nghĩa của phép toán hai ngôi, ánh xạ vừa chứng minh xác định một phép toán hai ngôi *cảm sinh* trên tập thương G/H , cho bởi quy tắc $(xH)(yH) = xyH$. Luật kết hợp của phép toán cảm sinh suy ra từ luật kết hợp của phép toán trong G . Sau đó có thể kiểm tra một cách dễ dàng rằng G/H có phần tử đơn vị là $eH = H$ và gH có nghịch đảo là $g^{-1}H$. $\square$

Định nghĩa. Nhóm G/H nói trong Bổ đề 4.9 được gọi là *nhóm thương* của G theo H .

Nhận xét. Bạn đọc có thể tự kiểm tra rằng quy tắc $(aH)(bH) = (ab)H$ là một phép toán trên tập thương G/H chỉ khi H là nhóm con chuẩn tắc trong G .

Ví dụ

Xét nhóm $(\mathbb{Z}, +)$ và nhóm con $A = n\mathbb{Z}$. Ký hiệu lớp ghép $x+A$ bởi $\bar{x}$ ta có $\mathbb{Z}/A = \{\bar{x} \mid x \in \mathbb{Z}\}$ là nhóm thương với phép toán $\bar{x} + \bar{y} = \overline{x+y}$.

Từ nay ta sẽ ký hiệu nhóm thương $\mathbb{Z}/n\mathbb{Z}$ bởi $\mathbb{Z}_n$ và gọi là nhóm các lớp đồng dư theo môđun n .

Mệnh đề 4.10. Nếu G là nhóm abel hữu hạn và số nguyên tố p chia hết cấp của nhóm G thì G chứa phần tử cấp p và do đó chứa nhóm con cấp p .

Chứng minh. Chúng ta sẽ chứng minh kết quả này bằng quy nạp theo cấp của G . Giả sử $|G| = pk, k \geq 1$. Trước hết, với $k = 1$ thì theo Hệ quả 4.4, G là nhóm cyclic, và mệnh đề là hiển nhiên đúng.

Bây giờ giả sử $|G| = pk, k > 1$. Ta chọn một phần tử bất kỳ khác đơn vị $g \in G$. Giả sử g có cấp r , thế thì có thể xảy ra các trường hợp sau:

Trường hợp 1. Nếu p là ước của $r, r = pm$, thì phần tử g^m có cấp p do $g^m \neq e, p$ là số nguyên tố và $(g^m)^p = g^r = e$.

Trường hợp 2. Xét trường hợp còn lại, p không là ước của r . Gọi H là nhóm con cyclic sinh bởi g . Do G là nhóm abel nên H là nhóm con chuẩn tắc, và nhóm thương G/H có cấp $\frac{|G|}{r}$. Rõ ràng cấp này chia hết cho p , nên theo giả thiết quy nạp nhóm thương G/H có phần tử cấp p , chẳng hạn aH . Nếu n là cấp của a trong nhóm G thì $(aH)^n = a^nH = H$. Từ đó suy ra n là bội của p và ta quay về trường hợp 1. Như vậy mệnh đề đã cho đúng với k .

Bây giờ theo nguyên lý quy nạp ta có điều phải chứng minh. $\square$

Bài tập

- 4.1.** Trên một nhóm G cho quan hệ C bởi aCb nếu và chỉ nếu $ab = ba$. Đó có phải là quan hệ tương đương hay không? Nếu đó là quan hệ tương đương, hãy mô tả các lớp tương đương của nó.

- 4.2. Nếu H là nhóm con duy nhất với cấp cho trước của nhóm G , chứng minh rằng H là chuẩn tắc.
- 4.3. Nếu H là một nhóm con của nhóm G . Chứng minh rằng có tương ứng 1-1 giữa tập các lớp ghép trái của H trong G và tập các lớp ghép phải của H trong G .
- 4.4. Tìm các lớp ghép trái và lớp ghép phải của

$$H = \{(1), (12), (34), (12) \circ (34)\}$$

trong S_4 .

- 4.5. Nhóm con xyclic $\{(1), (123), (132)\}$ có là chuẩn tắc trong S_4 không?
- 4.6. Nhóm con

$$\{(1), (1234), (13) \circ (24), (1432), (13), (24), (14) \circ (23), (12) \circ (34)\}$$

có là chuẩn tắc trong S_4 không?

- 4.7. Tìm tất cả các nhóm con và nhóm con chuẩn tắc của nhóm các phép thế S_3 .
- 4.8. Giả sử S là một tập con của nhóm G . Chứng minh rằng tập con $C(S) = \{g \in G \mid gs = sg, \forall s \in S\}$ là một nhóm con của G . Nhóm con $C(S)$ được gọi là *cái tâm hoá* của S ; trường hợp đặc biệt $C(G)$ gọi là *tâm* của G . Chứng minh rằng $C(G)$ là nhóm con chuẩn tắc của G .
- 4.9. Tìm tâm của các nhóm D_3, D_4 .
- 4.10. Với hai phần tử a, b của nhóm G ta gọi $aba^{-1}b^{-1}$ là *giao hoán tử* của a và b . Chứng minh rằng:
- Nhóm con G' sinh bởi mọi giao hoán tử của G là một nhóm con chuẩn tắc của G (nhóm con này được gọi là *nhóm con giao hoán tử* của G).
 - Nhóm thương G/G' là nhóm abel.
 - Nếu A là nhóm con chuẩn tắc trong G thì nhóm thương G/A là abel khi và chỉ khi $G' \subset A$.
- 4.11. Tìm nhóm con giao hoán tử của nhóm các phép thế S_3 .
- 4.12. Cho G là một nhóm con cấp n , và $(n, m) = 1$. Chứng minh rằng mọi phần tử h của G có một căn bậc m ; nghĩa là $h = g^m$ với một $g \in G$ nào đó.

4.13. Chứng minh rằng mọi nhóm cấp p^m , trong đó p là số nguyên tố, đều chứa một nhóm con cấp p .

4.14. Chứng minh rằng:

a) Nếu M là một nhóm con của nhóm G , N là nhóm con chuẩn tắc của G thì tập hợp

$$MN = \{xy \mid x \in M, y \in N\}$$

là một nhóm con của G .

b) Nếu M cũng là nhóm con chuẩn tắc của G thì MN là nhóm con chuẩn tắc của G .

4.15. Cho S là một tập con của nhóm G và

$$N_S = \{g \in G \mid gSg^{-1} = S\}$$

a) Chứng tỏ rằng N_S là nhóm con của G (N_S được gọi là cái chuẩn hoá của S).

b) Nếu K là một nhóm con của G và H là một nhóm con chuẩn tắc của K thì $K \subset N_H$.

c) Nếu K là một nhóm con của N_H thì

$$KH = \{ab \mid a \in K, b \in H\}$$

là một nhóm và H là nhóm con chuẩn tắc của KH .

d) Cái chuẩn hoá N_H của nhóm con H là nhóm con lớn nhất của nhóm G nhận H làm nhóm con chuẩn tắc của nó.

4.16. Cho tập hợp $A = \{(x, y) \in \mathbb{R}^2, x \neq 0\}$ với $\mathbb{R}$ là tập các số thực. Trên A xác định một phép toán hai ngôi $\circ$ như sau:

$$(x, y) \circ (u, v) = (xu, yu + v).$$

Chứng minh rằng tập hợp $H = \{(1, y) \mid y \in \mathbb{R}\}$ là một nhóm con chuẩn tắc trong A .

4.17. Nhóm con chuẩn tắc H được gọi là nhóm con chuẩn tắc tối đại của nhóm G nếu $H \neq G$ và với mọi nhóm con chuẩn tắc K của G , $K \supset H$, $K \neq H$ thì $K = G$. Chứng minh rằng H là nhóm con chuẩn tắc tối đại của G khi và chỉ khi nhóm thương G/H là một nhóm đơn.

4.18. Gọi $\mathbb{C}^*$ là nhóm các số phức khác không với phép nhân và W là nhóm nhân các số phức theo môđun đơn vị. Mô tả $\mathbb{C}^*/W$.

4.19. Nhóm G được gọi là *mêta-Abel* nếu nó có một nhóm con chuẩn tắc K sao cho cả K và G/K đều giao hoán.

(a) Chứng minh rằng mọi nhóm con và nhóm thương của một nhóm mêta Abel là mêta Abel.

(b) Chứng minh rằng G là mêta Abel nếu và chỉ nếu nhóm giao hoán tử G' là giao hoán.

4.20. Nhắc lại rằng tâm $Z(G)$ của một nhóm G được định nghĩa bởi

$$Z(G) = \{zg = gz \mid \text{với mọi } g \in G\}.$$

Cho $K \subset Z(G)$ là một nhóm con.

(a) Chứng minh rằng K là chuẩn tắc trong G .

(b) Nếu G/K là xyclic, chứng minh rằng G là giao hoán.

5. Đồng cấu nhóm

Một trong những kết quả cơ bản của lý thuyết nhóm là định lý đồng cấu nhóm. Nó mô tả mối quan hệ sâu sắc giữa những đồng cấu với các nhóm con chuẩn tắc và các nhóm thương. Những kết quả tương tự cũng được phát biểu cho các vành, các không gian vectơ, cũng như cho phần lớn các hệ đại số khác.

Định nghĩa. Ánh xạ $f : G \rightarrow H$ từ nhóm G đến nhóm H được gọi là *đồng cấu nhóm* (hay một cách ngắn gọn là *đồng cấu*) nếu:

$$f(ab) = f(a)f(b) \text{ với mọi } a, b \in G.$$

Bổ đề 5.1. Nếu $f : G \rightarrow H$ là một đồng cấu nhóm thì:

(i) $f(e_G) = e_H$, với e_G, e_H lần lượt là các phần tử đơn vị của G, H .

(ii) $f(a^{-1}) = [f(a)]^{-1}$, với mọi $a \in G$.

Chứng minh. (i) Trước hết, thay cho các ký hiệu e_G, e_H ta sẽ viết đơn giản là e mà không sợ có sự nhầm lẫn nào.

Với phần tử tùy ý $a \in G$ ta có

$$f(a)e = f(a) = f(ae) = f(a)f(e)$$

Thực hiện luật giản ước trong nhóm H ta được $f(e) = e$.

(ii) Bây giờ ta có

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(e) = e.$$

Từ đó, $f(a^{-1}) = [f(a)]^{-1}$. □

Mệnh đề 5.2. *Hợp thành của hai đồng cấu $\alpha : A \rightarrow B, \beta : B \rightarrow C$ là một đồng cấu.*

Chứng minh. Có thể thử lại một cách dễ dàng. □

Định nghĩa. Đồng cấu $f : G \rightarrow H$ được gọi là *đơn cấu* (tương ứng *toàn cấu*, *đẳng cấu*), nếu f là một đơn ánh (tương ứng toàn ánh, song ánh).

Nếu $f : G \rightarrow H$ là một đẳng cấu thì nó là một song ánh. Ánh xạ ngược của nó cũng là một đồng cấu, và do đó là đẳng cấu. Khi đó ta nói G và H đẳng cấu với nhau và ký hiệu bởi $G \cong H$.

Ví dụ

1. Đối với các nhóm G, H ánh xạ $\theta : G \rightarrow H$, biến mọi phần tử của G thành phần tử đơn vị của H là một đồng cấu. Ta thường gọi đồng cấu này là đồng cấu tầm thường.

2. Nếu H là nhóm con của nhóm G thì ánh xạ

$$\begin{aligned} i : H &\rightarrow G \\ a &\mapsto a \end{aligned}$$

là một đơn cấu, gọi là *phép nhúng tự nhiên* hay *đơn cấu chính tắc*.

Nói riêng, phép đồng nhất $id_G : G \rightarrow G$ là một đơn cấu, hơn nữa là một đẳng cấu.

3) Nếu N là nhóm con chuẩn tắc của G thì ánh xạ

$$\begin{aligned} p : G &\rightarrow G/N \\ g &\mapsto gN = \bar{g} \end{aligned}$$

là một toàn cấu, gọi là *phép chiếu tự nhiên* hay *toàn cấu chính tắc*.

Định nghĩa. Với $f : G \rightarrow H$ là một đồng cấu, ta ký hiệu

$$\text{Ker } f = \{g \in G \mid f(g) = e_H\} = f^{-1}(e_H)$$

$$\text{Im } f = \{f(x) \mid x \in G\}$$

và lần lượt gọi $\text{Ker } f$ là *hạt nhân*, $\text{Im } f$ là *ảnh* của f .

Mệnh đề 5.3. Giả sử $f : G \rightarrow H$ là một đồng cấu nhóm, M là một nhóm con của G , N là nhóm con chuẩn tắc của H . Khi đó:

- (i) $f(M)$ là nhóm con của H ,
- (ii) $f^{-1}(N)$ là nhóm con chuẩn tắc của G .

Đặc biệt suy ra $\text{Im} f$ là nhóm con của H và $\text{Ker} f$ là nhóm con chuẩn tắc của G .

Chứng minh. (i) Giả sử $a, b \in f(M)$. Khi đó

$$a = f(x), b = f(y), x, y \in M.$$

Từ đó

$$ab^{-1} = f(x)[f(y)]^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in f(M),$$

do $xy^{-1} \in M$. Bởi vậy theo Hệ quả 3.2 ảnh $f(M)$ là nhóm con của H .

(ii) Trước hết ta chứng minh $f^{-1}(N)$ là nhóm con của nhóm G . Giả sử $x, y \in f^{-1}(N)$. Thế thì $a = f(x), b = f(y) \in N$. Từ đó

$$f(xy^{-1}) = f(x)[f(y)]^{-1} = ab^{-1} \in N.$$

Điều này kéo theo $xy^{-1} \in f^{-1}(N)$ và do đó $f^{-1}(N)$ là nhóm con của G . Còn lại ta chứng minh $f^{-1}(N)$ là nhóm con chuẩn tắc của G . Với mọi $x \in f^{-1}(N)$ và mọi $g \in G$ ta có $f(x) \in N$ và

$$f(g^{-1}xg) = [f(g)]^{-1}f(x)f(g) \in N.$$

Điều này kéo theo $g^{-1}xg \in f^{-1}(N)$.

Vậy $f^{-1}(N)$ là nhóm con chuẩn tắc trong G . Sau cùng, $\text{Im} f$ là nhóm con của H do G là nhóm con của chính nó, và $\text{Ker} f$ là nhóm con chuẩn tắc trong G do $\text{Ker} f = f^{-1}(e)$, còn $\{e\}$ là nhóm con chuẩn tắc trong H . □

Mệnh đề 5.4. (i) Đồng cấu $f : G \rightarrow H$ là đơn cấu khi và chỉ khi $\text{Ker} f = \{e\}$.

(ii) Nhóm con N của G là chuẩn tắc khi và chỉ khi N là hạt nhân của một đồng cấu $f : G \rightarrow H$ nào đó.

Chứng minh. (i) Nếu $f : G \rightarrow H$ là đơn cấu thì f là đơn ánh, do đó $\text{Ker } f = f^{-1}(e) = \{e\}$.

Ngược lại, giả sử $\text{Ker } f = \{e\}$. Nếu $a, b \in G$ sao cho $f(a) = f(b)$ thì $f(ab^{-1}) = f(a)[f(b)]^{-1} = e$ do $ab^{-1} \in \text{Ker } f$. Từ đó $ab^{-1} = e$, suy ra $a = b$.

(ii) Ta đã biết hạt nhân của một đồng cấu $f : G \rightarrow H$ là một nhóm con chuẩn tắc của G . Ngược lại, nếu N là một nhóm con chuẩn tắc của G thì N là hạt nhân của phép chiếu tự nhiên $p : G \rightarrow G/N$. $\square$

Định lý 5.5 (Định lý đồng cấu). Giả sử N là nhóm con chuẩn tắc của G . Khi đó với mỗi đồng cấu $\varphi : G \rightarrow H$ sao cho $N \subset \text{Ker } \varphi$ đều tồn tại duy nhất một đồng cấu $\psi : G/N \rightarrow H$ sao cho biểu đồ sau giao hoán

$$\begin{array}{ccc} G & \xrightarrow{p} & G/N \\ & \searrow \varphi & \swarrow \psi \\ & H & \end{array}$$

nghĩa là $\varphi = \psi \circ p$, trong đó p là phép chiếu tự nhiên. Hơn nữa, ψ đơn cấu khi và chỉ khi $N = \text{Ker } \varphi$.

Chứng minh. Xét tương ứng

$$\begin{aligned} \psi : G/N &\rightarrow H \\ \bar{g} &\mapsto \psi(\bar{g}) = \varphi(g). \end{aligned}$$

Tương ứng ψ được xác định trên một lớp ghép bằng việc sử dụng phần tử đại diện của lớp ghép đó, vì vậy chúng ta cần kiểm tra tính hợp lý của việc định nghĩa ψ , nghĩa là ψ không phụ thuộc vào phần tử đại diện. Thật vậy, nếu $\bar{x} = \bar{y}$ thì $xy^{-1} \in N$. Bởi vậy theo giả thiết

$$\varphi(xy^{-1}) = \varphi(x)[\varphi(y)]^{-1} = e.$$

Suy ra $\varphi(x) = \varphi(y)$.

Ảnh xạ ψ là một đồng cấu nhóm vì

$$\psi(\bar{a}\bar{b}) = \psi(\overline{ab}) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(\bar{a})\psi(\bar{b}).$$

Bây giờ với mọi $a \in G$ ta có $(\psi p)a = \psi(\bar{a}) = \varphi(a)$, nghĩa là $\psi \circ p = \varphi$.

Nếu $\psi' : G/N \rightarrow H$ là một đồng cấu sao cho $\psi' \circ p = \varphi$ thì với mọi $\bar{a} \in G/N$ ta có

$$\psi'(\bar{a}) = \psi'(p(a)) = (\psi' \circ p)a = \varphi(a) = (\psi \circ p)a = \psi(\bar{a}).$$

Vậy $\psi' = \psi$.

Cuối cùng do $\psi(\bar{a}) = \varphi(a)$ nên $\bar{a} \in \text{Ker}\psi$ khi và chỉ khi $a \in \text{Ker}\varphi$. Bởi vậy nếu $N = \text{Ker}\varphi$ thì $\text{Ker}\varphi = \{e\}$ và do đó ψ đơn cấu.

Ngược lại nếu ψ đơn cấu thì $\bar{a} = \bar{e}$ với mọi $a \in \text{Ker}\varphi$, nghĩa là $\text{Ker}\varphi \subset N$. $\square$

Hệ quả 5.6. Đối với đồng cấu nhóm $\varphi : G \rightarrow H$ ta có

$$G/\text{Ker}\varphi \cong \text{Im}\varphi.$$

Chứng minh. Theo định lý vừa chứng minh ánh xạ $\psi : G/\text{Ker}\varphi \rightarrow H$ là đơn cấu. Nếu xem ψ là ánh xạ từ $G/\text{Ker}\varphi$ đến $\text{Im}\varphi$ thì ψ là toàn cấu. Bởi vậy nó là một đẳng cấu. $\square$

Xem như một áp dụng của định lý đồng cấu ta có mệnh đề sau:

Mệnh đề 5.7. (i) Mỗi nhóm xyclic cấp vô hạn đẳng cấu với nhóm cộng các số nguyên $\mathbb{Z}$.

(ii) Mỗi nhóm xyclic cấp n đẳng cấu với nhóm cộng $\mathbb{Z}_n$ các lớp đồng dư theo môđun n .

Chứng minh. (i) Ký hiệu $A = \langle a \rangle$ là nhóm xyclic sinh bởi phần tử a có cấp vô hạn. Khi đó ánh xạ

$$\begin{aligned} \varphi : \mathbb{Z} &\rightarrow A \\ x &\mapsto a^x \end{aligned}$$

là một toàn ánh do mỗi phần tử của A là một lũy thừa của a . Do a có cấp vô hạn nên

$$\text{Ker}\varphi = \{x \in \mathbb{Z} \mid a^x = e\} = \{0\}.$$

Điều này chứng tỏ φ đơn cấu và do đó là đẳng cấu.

(ii) Nếu $A = \langle a \rangle$ là nhóm xyclic cấp n thì ánh xạ

$$\begin{aligned} \varphi : \mathbb{Z} &\rightarrow A \\ x &\mapsto a^x \end{aligned}$$

là toàn cầu với hạt nhân

$$\text{Ker } \varphi = \{x \in \mathbb{Z} \mid a^x = e\} = \{x \in \mathbb{Z} \mid x \cdot n\} = n\mathbb{Z}$$

(do $a^x = e$ khi và chỉ khi x chia hết cho n). Bởi vậy

$$A \cong \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n. \quad \square$$

Chúng ta cũng có thể chứng minh sự đẳng cấu của hai nhóm xyclic có cùng cấp một cách trực tiếp, không cần thông qua định lý đồng cấu.

Trong cuốn sách này chúng ta thường nói tới hai nhóm xyclic $(\mathbb{Z}_n, +)$ và $(C_n, \circ)$ với số nguyên dương n nào đó. Theo mệnh đề vừa chứng minh ta có

$$(\mathbb{Z}_n, +) \cong (C_n, \circ).$$

Mệnh đề 5.8. Nếu G và H là các nhóm hữu hạn có cấp là các số nguyên tố cùng nhau thì chỉ có duy nhất một đồng cấu từ G đến H , đó là đồng cấu tầm thường.

Chứng minh. Cho K là hạt nhân của đồng cấu f từ G vào H . Khi đó $G/K \cong \text{Im } f$, là một nhóm con của H . Ta lại có

$$|G/K| = |G| / |K|$$

là một ước của $|G|$. Theo Định lý Lagrange, $|\text{Im } f|$ là một ước của $|H|$. Vì $|G|$ và $|H|$ là nguyên tố cùng nhau nên ta có $|G/K| = |\text{Im } f| = 1$. Bởi vậy $K = G$, vì vậy $f : G \rightarrow H$ là đồng cấu tầm thường. $\square$

Ví dụ. Nếu a và b là các phần tử sinh của các nhóm xyclic $C_{12} = \langle a \rangle$ và $C_6 = \langle b \rangle$ tương ứng, ta xét ánh xạ $f : C_{12} \rightarrow C_6$ cho bởi $f(a^r) = b^{2r}$. Trước hết ta chứng tỏ rằng định nghĩa là hợp lý. Thật vậy, nếu $a^r = a^{r_1}$ thì 12 chia hết $r - r_1$ theo mệnh đề 3.5, vì vậy $b^{2r} = b^{2r_1}$.

Dễ dàng kiểm tra được f là một đồng cấu và f có hạt nhân là

$$K = \{a^r \mid f(a^r) = b^{2r} = e\} = \{e, a^3, a^6, a^9\}$$

bởi vì nếu a^r thuộc K thì $b^{2r} = e$, do đó $2r$ chia hết cho 6, hay r chia hết cho 3. Bởi vậy $C_{12}/K \cong C_6$ và đẳng cấu này thu được qua ánh xạ từ lớp ghép $a^r K$ đến b^{2r} .

Mệnh đề 5.9. Giả sử A, B là hai nhóm con chuẩn tắc của nhóm G và $A \subset B$. Khi đó có đẳng cấu chính tắc

$$(G/A)(B/A) \cong G/B.$$

Chứng minh. Xét tương ứng

$$\begin{aligned}\varphi: G/A &\rightarrow G/B \\ gA &\mapsto gB.\end{aligned}$$

Có thể kiểm tra được φ là một ánh xạ, hơn nữa là một toàn cấu. Nếu $gA \in \text{Ker}\varphi$ thì $\varphi(gA) = gB = e$.

Điều này xảy ra khi và chỉ khi $g \in B$, và do đó $\text{Ker}\varphi = B/A$. Theo Hệ quả 5.6 ta có điều phải chứng minh. $\square$

Hệ quả 5.10. Nếu A là nhóm con chuẩn tắc của nhóm G và B là một nhóm con của G thì tập

$$AB = \{ab \mid a \in A, b \in B\}$$

là một nhóm con của G và ta có đẳng cấu

$$AB/B \cong B/(A \cap B).$$

Chứng minh. Giả sử $a_1, a_2 \in A$ và $b_1, b_2 \in B$. Khi đó

$$\begin{aligned}(a_1b_1)(a_2b_2)^{-1} &= a_1b_1b_2^{-1}a_2^{-1} = a_1ba_2^{-1} \\ &= a_1(ba_2^{-1}b^{-1})b = a_1a'b = ab,\end{aligned}$$

với $b = b_1b_2^{-1} \in B, a' = ba_2^{-1}b^{-1} \in A$. Bởi vậy $ab \in AB$ và do đó AB là nhóm con của G . Mặt khác ta có A là nhóm con chuẩn tắc của AB . Bây giờ xét ánh xạ

$$\begin{aligned}\varphi: B &\rightarrow AB/A \\ b &\mapsto bA\end{aligned}$$

Dễ thấy φ là một đồng cấu. Hơn nữa với phần tử tùy ý $ab \in AB$ ta có:

$$ab = b(b^{-1}ab) = ba', a' = b^{-1}ab \in A$$

nên $abA = bA$ và do đó φ là một toàn cấu. Nếu $b \in \text{Ker}\varphi$ thì $\varphi(b) = eA \Leftrightarrow b \in A$, nghĩa là $\text{Ker}\varphi = A \cap B$ và khi đó theo Hệ quả 5.6 ta có điều phải chứng minh. $\square$

Nhờ khái niệm đẳng cấu ta có thể phân lớp các nhóm có cùng cấp. Ví dụ về điều này được trình bày ở chương sau khi chúng ta đã có khái niệm tích trực tiếp.

Bài tập

Trong các bài tập từ 5.1 đến 5.4, kiểm tra định nghĩa của mỗi ánh xạ là hợp lý. Xác định trong số đó đâu là đồng cấu nhóm, và khi đó hãy tìm hạt nhân và ảnh của nó. Phần tử của $\mathbb{Z}_n$ chứa x được ký hiệu là $[x]_n$.

- 5.1. $f : \mathbb{Z}_{12} \rightarrow \mathbb{Z}_{12}$, trong đó $f([x]_{12}) = [x + 1]_{12}$.
- 5.2. $f : C_{12} \rightarrow C_{12}$, trong đó $f(g) = g^3$.
- 5.3. $f : \mathbb{Z} \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_4$, ở đó $f(x) = ([x]_2, [x]_4)$.
- 5.4. $f : \mathbb{Z}_8 \rightarrow \mathbb{Z}_2$, ở đó $f([x]_8) = [x]_2$.
- 5.5. Chứng minh rằng mỗi ảnh toàn cấu của một nhóm xyclic là xyclic.
- 5.6. Cho vị nhóm cộng $\mathbb{N}$, nhóm cộng $\mathbb{Z}$ và phép nhúng tự nhiên $i : \mathbb{N} \rightarrow \mathbb{Z}$. Nếu A là một nhóm và $f : \mathbb{N} \rightarrow A$ là đồng cấu của các vị nhóm thì tồn tại duy nhất đồng cấu nhóm $f' : \mathbb{Z} \rightarrow A$ sao cho $f = f' \circ i$.
- 5.7. Cho đồng cấu nhóm

$$\varphi : \mathbb{Z} \rightarrow \mathbb{Z}$$

xác định bởi $x \mapsto 6x$. Hãy tìm $\text{Ker } \varphi$ và $\varphi^{-1}(12\mathbb{Z})$.

- 5.8. Tìm mọi đồng cấu từ $(\mathbb{Z}, +)$ đến $(\mathbb{Q}, +)$.
- 5.9. $(\mathbb{Z}, +)$ có đẳng cấu với $(\mathbb{Q}^*, \times)$ hay không, trong đó $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$. Hãy giải thích.
- 5.10. $(\mathbb{R}, +)$ có đẳng cấu với $(\mathbb{R}^+, \times)$ hay không, trong đó $\mathbb{R}^+$ là tập các số thực dương? Cho giải thích.
- 5.11. Cho hai nhóm xyclic $A = \langle a \rangle$, $B = \langle b \rangle$ lần lượt sinh bởi các phần tử a, b , có cấp tương ứng là m, n . Cho $f : A \rightarrow B$ là một đồng cấu.
 - a) Chứng minh rằng $f(A)$ là nhóm xyclic sinh bởi $f(a)$ và cấp

của $f(a)$ là một ước chung của m và n .

b) Hãy chỉ ra các tự đẳng cấu của nhóm $\mathbb{Z}_6$.

5.12. Ký hiệu $\text{Aut}(G)$ là nhóm tất cả các tự đẳng cấu của nhóm G .

Chứng minh rằng:

a) $\text{Aut}(\mathbb{Z}_6) \cong \mathbb{Z}_2$.

b) $\text{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

c) $(\mathbb{Z}_7^*, \times) \cong (\mathbb{Z}_6, +)$.

5.13. Chứng minh rằng đối với phần tử g của nhóm G , tương ứng $n \mapsto g^n$ là một đồng cấu nhóm từ $\mathbb{Z}$ tới G và là đồng cấu duy nhất $\mathbb{Z} \rightarrow G$ với $1 \mapsto g$.

5.14. Hãy tìm tất cả các đồng cấu từ:

a) Một nhóm xyclic cấp n đến chính nó;

b) Một nhóm xyclic cấp 6 đến một nhóm xyclic cấp 18;

c) Một nhóm xyclic cấp 18 đến một nhóm xyclic cấp 6.

5.15. Tìm tất cả các đồng cấu nhóm từ:

a) C_3 vào C_4 .

b) $\mathbb{Z}$ vào $\mathbb{Z}_4$.

c) $\mathbb{Z}$ vào D_4 .

5.16. Chứng minh nếu hợp thành của hai đồng cấu $g : G \rightarrow H, h : H \rightarrow K$ là một đẳng cấu thì

a) g là một đơn cấu,

b) h là một toàn cấu,

c) $H = (\text{Im}g)(\text{Ker}h) = (\text{Ker}h)(\text{Im}g)$ và $\text{Im}g \cap \text{Ker}h = e$.

5.17. Đối với toàn cấu $f : G \rightarrow H$ và nhóm con B của H hãy chứng tỏ B chuẩn tắc trong H khi và chỉ khi $f^{-1}(B)$ là chuẩn tắc trong G và khi đó hãy chứng minh

$$G/f^{-1}(B) \cong H/B.$$

5.18. Cho X là nhóm xyclic cấp nguyên tố p . Chứng minh rằng mọi phần tử của X , khác đơn vị, đều là phần tử sinh của X và mọi ánh xạ

$$\begin{aligned}\varphi_k : X &\rightarrow X, \\ x &\mapsto x^k\end{aligned}$$

đều là tự đẳng cấu của X , với k là số nguyên dương thoả mãn $0 < k < p$.

5.19. Cho nhóm X . Với mỗi phần tử $a \in X$ ta xét ánh xạ

$$\begin{aligned} f : X &\rightarrow X \\ x &\mapsto axa^{-1} \end{aligned}$$

Chứng minh rằng:

- a) f_a là một tự đẳng cấu của X , gọi là tự đẳng cấu trong xác định bởi phần tử a .
 - b) Tập hợp các tự đẳng cấu trong của X lập thành một nhóm con của nhóm các tự đẳng cấu của X . Chứng minh rằng nhóm con H của X là chuẩn tắc nếu và chỉ nếu $f_a(H) = H$ với mọi tự đẳng cấu trong f_a của X .
 - c) Nhóm các tự đẳng cấu trong của X đẳng cấu với nhóm thương $X/C(X)$ với $C(X)$ là tâm của nhóm X .
- 5.20. Cho X và Y là hai nhóm cyclic có các phần tử sinh theo thứ tự là x và y , với các cấp tương ứng là s và t .
- a) Chứng minh quy tắc φ cho tương ứng mỗi phần tử $x^n \in X$ với phần tử $(y^k)^n \in Y$, trong đó k là một số tự nhiên khác 0 cho trước, là một đồng cấu khi và chỉ khi sk là bội của t .
 - b) Chứng minh nếu $sk = mt$ và φ là đơn cấu thì $(s, m) = 1$.
- 5.21. Chứng minh rằng có một đồng cấu duy nhất từ nhóm cộng các số hữu tỷ $\mathbb{Q}$ đến nhóm cộng các số nguyên $\mathbb{Z}$. Từ đó suy ra $\mathbb{Q}$ không phải là một nhóm cyclic.
- 5.22. Tìm nhóm các tự đẳng cấu của 4-nhóm Klein.
- 5.23. Tìm nhóm các tự đẳng cấu lần lượt của nhóm S_5 .
- 5.24. Chứng minh rằng mọi nhóm cấp 6 hoặc đẳng cấu với $\mathbb{Z}_6$ hoặc đẳng cấu với nhóm các phép thế S_3 .
- 5.25. Tìm bốn nhóm con khác nhau của S_4 , đẳng cấu với S_3 .
- 5.26. Cho G là một nhóm abel hữu hạn và p là một số nguyên tố sao cho $g^p = e$ với mọi $g \in G$, chứng minh rằng G đẳng cấu với $\mathbb{Z}_p^n$ với số nguyên n nào đó.
- 5.27. Cho A là một nhóm cộng abel. Ký hiệu $\text{End}(A)$ là tập tất cả các tự đồng cấu của nhóm A . Chứng minh:
- a) $\text{End}(A)$ là một nhóm abel với phép cộng sau:

$$\forall f, g \in \text{End}(A), (f + g)(a) = f(a) + g(a), \forall a \in A.$$

- b) $\text{End}(\mathbb{Z}) \cong \mathbb{Z}$, với $\mathbb{Z}$ là nhóm cộng các số nguyên.

c) $\text{End}(\mathbb{Q}) \cong \mathbb{Q}$, với $\mathbb{Q}$ là nhóm cộng các số hữu tỷ.

5.28. Cho các đồng cấu nhóm $f : K \rightarrow H, g : G \rightarrow K$, trong đó f là một toàn cấu. Chứng minh rằng các điều kiện sau đây là tương đương:

a) Tồn tại một đồng cấu $h : H \rightarrow K$ sao cho $g = h \circ f$;

b) $\text{Ker} f \subset \text{Ker} g$.

Nếu một trong các điều kiện đó được thoả mãn thì:

c) h là duy nhất;

d) h là đơn ánh nếu và chỉ nếu $\text{Ker} f = \text{Ker} g$;

e) h là toàn ánh nếu và chỉ nếu g là toàn ánh.

5.29. Cho

$$G_p = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_p) \mid ad - bc = 1 \right\}.$$

Nếu p là một số nguyên tố, chứng minh rằng G_p là một nhóm có cấp $p(p^2 - 1)$ và tìm một nhóm đẳng cấu với G_2 .

5.30. Cho G là nhóm sinh bởi các ma trận $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ và $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

với phép nhân ma trận. Chứng tỏ rằng G là nhóm không abel cấp 8. Nó có đẳng cấu với nhóm D_4 hay với nhóm quaternion Q hay không?

Chương III

CẤU TRÚC NHÓM

1. Tích trực tiếp
2. Nhóm đối xứng
3. Nhúng nửa nhóm vào một nhóm
4. Tác động của một nhóm trên một tập hợp

1. Tích trực tiếp

Từ hai nhóm đã cho chúng ta có thể xây dựng một nhóm mới nhờ tích trực tiếp mà ta sẽ trình bày dưới đây.

Mệnh đề 1.1. Nếu A và B là hai nhóm thì tích Đề-các

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

lập thành một nhóm cùng với phép toán hai ngôi cho bởi

$$(a, b)(x, y) = (ax, by).$$

Nhóm $A \times B$ được gọi là tích trực tiếp của A và B .

Ví dụ, viết tích trực tiếp $C_2 \times C_2$ dưới dạng bảng ta thấy rằng tích này đẳng cấu với 4-nhóm Klein của các phép đối xứng của một hình chữ nhật.

Mệnh đề 1.2. Nếu m, n là hai số nguyên tố cùng nhau thì

$$C_{mn} = C_m \times C_n.$$

Chứng minh. Gọi g, h và k tương ứng là các phần tử sinh của C_{mn}, C_m và C_n . Xét tương ứng $f: C_{mn} \rightarrow C_m \times C_n$ cho bởi

$$f(g^r) = (h^r, k^r), r \in \mathbb{Z}.$$

Định nghĩa này là hợp lý bởi vì nếu $g^r = g^{r'}$ thì $r - r'$ là bội của mn , vì vậy $r - r'$ là bội của m và của n . Do đó, $h^r = h^{r'}$ và $k^r = k^{r'}$. Hơn nữa, f là một đồng cấu nhóm bởi vì

$$\begin{aligned} f(g^r \cdot g^s) &= f(g^{r+s}) = (h^{r+s}, k^{r+s}) = (h^r \cdot h^s, k^r \cdot k^s) \\ &= (h^r, k^r) \cdot (h^s, k^s) = f(g^r) \cdot f(g^s) \end{aligned}$$

Nếu $g^r \in \text{Ker } f$ thì $h^r = e$ và $k^r = e$. Bởi vậy, r chia hết cho cả m và n , và vì $(m, n) = 1$ nên r chia hết cho mn . Do đó, $\text{Ker } f = \{e\}$, và ảnh của f đẳng cấu với C_{mn} .

Mặt khác do

$$|C_{mn}| = mn, \quad |C_m \times C_n| = |C_m| \cdot |C_n| = mn,$$

nên $\text{Im } f = C_m \times C_n$, và bởi vậy f là một đẳng cấu. $\square$

Lưu ý rằng nếu m và n không nguyên tố cùng nhau thì C_{mn} không đẳng cấu với $C_m \times C_n$. Ví dụ, $C_2 \times C_2$ không đẳng cấu với C_4 vì tích trực tiếp không chứa phần tử có cấp 4.

Tổng quát, cấp của phần tử (h, k) trong $H \times K$ là bội chung nhỏ nhất của cấp của h và của k , bởi vì

$$(h, k)^r = (h^r, k^r) = (e, e)$$

nếu và chỉ nếu $h^r = e$ và $k^r = e$. Do đó, nếu $(m, n) > 1$ thì cấp của (h, k) trong $C_m \times C_n$ luôn luôn nhỏ hơn mn .

Định nghĩa tích trực tiếp được mở rộng một cách tự nhiên cho một họ $(G_i \mid i \in I)$ các nhóm, với tập chỉ số I tùy ý. Tích Đề-các $\prod_i G_i$ gồm tất cả các họ (a_i) , với $a_i \in G_i, i \in I$, là một nhóm với phép toán nhân theo từng thành phần, nghĩa là

$$(a_i)(b_i) = (a_i b_i)$$

Ta gọi nhóm này là *tích trực tiếp* của họ các nhóm (G_i) .

Nhóm con của $\prod_i G_i$ gồm tất cả các họ (a_i) , sao cho chỉ có một số hữu hạn a_i khác đơn vị, được gọi là *tích trực tiếp yếu* của họ G_i . Hiển nhiên rằng, tích trực tiếp yếu của họ G_i trùng với tích trực tiếp của chúng khi và chỉ khi tập chỉ số I hữu hạn.

Trong trường hợp các nhóm G_i là aben ta thường nói *tổng trực tiếp* thay cho tích trực tiếp yếu.

Tích trực tiếp có thể được dùng để phân lớp tất cả các nhóm aben hữu hạn. Có thể chứng minh rằng một nhóm aben hữu hạn bất kỳ đẳng cấu với tích trực tiếp của các nhóm xyclic. Các kết quả trên có thể được sử dụng để phân loại các tích của các nhóm xyclic đó sai khác một đẳng cấu. Ví dụ, có ba nhóm aben cấp 24 không đẳng cấu là:

$$C_{24} = C_8 \times C_3$$

$$C_2 \times C_3 \times C_4 = C_6 \times C_4 = C_2 \times C_{12}$$

$$C_2 \times C_2 \times C_2 \times C_3 = C_2 \times C_2 \times C_6$$

Bây giờ chúng ta sẽ nói tới sự phân tích một nhóm thành tích trực tiếp của hai nhóm con của nó. Những khảo sát sau đây là cần thiết.

Các ánh xạ:

$$\begin{aligned} i_A : A &\rightarrow A \times B, & i_B : B &\rightarrow A \times B \\ a &\mapsto (a, e) & b &\mapsto (e, b) \end{aligned}$$

là những đơn cấu, được gọi là những *phép nhúng tự nhiên*.

Các ánh xạ:

$$\begin{aligned} p_A : A \times B &\rightarrow A, & p_B : A \times B &\rightarrow B \\ (a, b) &\mapsto a & (a, b) &\mapsto b \end{aligned}$$

là những toàn cấu, được gọi là những *phép chiếu tự nhiên*.

Các đồng cấu nói trên thỏa mãn các quan hệ

$$\text{Im } i_A = \text{Ker } p_A, \quad \text{Im } i_B = \text{Ker } p_B.$$

Từ đó suy ra $\overline{A} = i_A(A)$, $\overline{B} = i_B(B)$ là những nhóm con chuẩn tắc của $A \times B$. Hơn nữa, dễ thấy

$$A \times B = \overline{AB} \text{ và } \overline{A} \cap \overline{B} = e.$$

Điều này gợi ý cho chúng ta định nghĩa sau.

Định nghĩa. Giả sử A, B là hai nhóm con chuẩn tắc của nhóm G . Ta nói rằng G *phân tích được thành tích trực tiếp* của A và B nếu

$G = AB$ và $A \cap B = e$. Khi đó ta cũng nói rằng các nhóm A, B là các *hạng tử trực tiếp* của nhóm G .

Ví dụ. Cho $G = \langle g \rangle$ là nhóm xyclic cấp 6. Khi đó gọi $A = \langle a \rangle$, $B = \langle b \rangle$ là các nhóm xyclic lần lượt sinh bởi $a = g^2, b = g^3$ thì G phân tích được thành tích trực tiếp của A và B .

Mệnh đề 1.3. Nếu G phân tích được thành tích trực tiếp của hai nhóm con chuẩn tắc A, B thì mỗi phần tử của A đều giao hoán được với mỗi phần tử của B và mỗi phần tử của G viết được một cách duy nhất dưới dạng $ab, a \in A, b \in B$.

Chứng minh. Với các phần tử tùy ý $a \in A, b \in B$ ta cần chứng minh $ab = ba$. Muốn vậy ta xét phần tử $c = aba^{-1}b^{-1}$. Do A là nhóm con chuẩn tắc nên $ba^{-1}b^{-1} \in A$, và do đó $c \in A$.

Tương tự, $c \in B$ và do đó $c \in A \cap B$. Do $A \cap B = e$ nên $c = e$, nghĩa là $ab = ba$.

Do $G = AB$ nên mỗi phần tử g của G viết được dưới dạng $g = ab$ với $a \in A, b \in B$. Giả sử g cũng có biểu diễn $g = uv, u \in A, v \in B$. Khi đó $ab = uv$. Từ đó, $bv^{-1} = a^{-1}u$ là phần tử thuộc $A \cap B$ và do đó bằng e . Điều đó chứng tỏ $a = u, b = v$. $\square$

Định lý sau cho ta mối liên hệ giữa sự phân tích một nhóm thành tích trực tiếp với tích trực tiếp của hai nhóm.

Định lý 1.4. Nhóm G phân tích được thành tích trực tiếp của các nhóm con chuẩn tắc A và B nếu và chỉ nếu ánh xạ

$$\begin{aligned}\varphi: A \times B &\rightarrow G \\ (a, b) &\mapsto ab\end{aligned}$$

là một đẳng cấu.

Chứng minh. ($\Rightarrow$) Giả sử G phân tích được thành tích trực tiếp của các nhóm con chuẩn tắc A và B . Trước hết có thể thử lại φ là một đồng cấu. Do $G = AB$ nên φ là một toàn cấu. Nếu (a, b) là phần tử thuộc hạt nhân $\text{Ker } \varphi$ thì $ab = e$.

Do cách viết duy nhất của $e \in G$ (Mệnh đề 6.1) ta suy ra $a = b = e$. Bởi vậy $\text{Ker } \varphi = \{(e, e)\}$, và do đó φ là đơn cấu.

($\Leftarrow$) Bây giờ giả sử φ là một đẳng cấu. Nếu g là một phần tử tùy ý thuộc G thì tồn tại $(a, b) \in A \times B$ sao cho $\varphi((a, b)) = ab = g$.

Điều này có nghĩa là $G = AB$. Nếu c là phần tử thuộc giao $A \cap B$ thì $\varphi((c, c^{-1})) = cc^{-1} = e$.

Do φ đơn cấu nên điều này kéo theo $c = c^{-1} = e$. Vậy $A \cap B = e$, và G phân tích được thành tích trực tiếp của A và B . $\square$

Chú ý về thuật ngữ và ký hiệu

1) Do định lý nói trên, khi G phân tích được thành tích trực tiếp của A và B ta cũng nói rằng G là tích trực tiếp của A và B và ký hiệu $A \times B$ mà không sợ có sự hiểu lầm nào. Sự phân biệt hai khái niệm này sẽ được hiểu trong từng tình huống cụ thể.

2) Nếu G là một nhóm aben và phép toán trong nhóm G ký hiệu bởi $+$ thì ta ký hiệu $G = A \oplus B$ thay cho $A \times B$ và gọi G là *tổng trực tiếp* của A và B .

Mệnh đề 1.5. Nếu $f : A \rightarrow X, g : B \rightarrow Y$ là hai đồng cấu nhóm thì ánh xạ

$$\begin{aligned} A \times B &\rightarrow X \times Y \\ (a, b) &\mapsto (f(a), g(b)) \end{aligned}$$

cũng là một đồng cấu và được ký hiệu bởi $f \times g$.

Chứng minh. Có thể thử lại một cách dễ dàng. $\square$

Mệnh đề 1.6. Nếu A, B lần lượt là nhóm con chuẩn tắc của các nhóm X, Y thì tích trực tiếp $A \times B$ là nhóm con chuẩn tắc của tích trực tiếp $X \times Y$ và

$$(X \times Y)/(A \times B) \cong (X/A) \times (Y/B).$$

Chứng minh. Xét các phép chiếu tự nhiên

$$\begin{aligned} \alpha : X &\rightarrow X/A, & \beta : Y &\rightarrow Y/B \\ x &\mapsto \bar{x} & y &\mapsto \bar{y} \end{aligned}$$

Khi đó kiểm tra được ngay

$$\begin{aligned} \gamma = \alpha \times \beta : X \times Y &\rightarrow (X/A) \times (Y/B) \\ (x, y) &\mapsto (\bar{x}, \bar{y}) \end{aligned}$$

là một đồng cấu. Hơn nữa, dễ thấy γ là toàn cấu. Cặp (x, y) thuộc hạt nhân $\text{Ker}\gamma$ khi và chỉ khi

$$\gamma(x, y) = (\bar{x}, \bar{y}) = (e_A, e_B).$$

Điều này nghĩa là $x \in A, y \in B$. Vậy $\text{Ker}\gamma = A \times B$. Theo định lý đồng cấu ta có $(X \times Y)/\text{Ker}\gamma \cong \text{Im}\gamma$. Đó là điều phải chứng minh. $\square$

Ví dụ. Mô tả tất cả các đồng cấu nhóm từ C_{10} đến $C_2 \times C_5$. Đồng cấu nào trong số đó là đẳng cấu?

Vì C_{10} là nhóm cyclic sinh bởi phần tử g nên một đồng cấu từ C_{10} được xác định bởi ảnh của g . Cho h và k tương ứng là các phần tử sinh của C_2 và C_5 , và xét hàm $f_{r,s} : C_{10} \rightarrow C_2 \times C_5$, biến g thành phần tử $(h^r, k^s) \in C_2 \times C_5$. Khi đó, nếu $f_{r,s}$ là một đồng cấu, thì

$$f_{r,s}(g^n) = (h^{rn}, k^{sn})$$

với $0 \leq n \leq 9$. Tuy nhiên điều này là đúng với mọi n , bởi vì nếu $g^n = g^m$, thì $10 \mid n - m$, Do đó $2 \mid n - m$ và $5 \mid n - m$ và $h^{rn} = h^{rm}$ và $k^{sn} = k^{sm}$.

Ta kiểm tra lại $f_{r,s}$ là một đồng cấu với r và s bất kỳ. Ta có.

$$\begin{aligned} f_{r,s}(g^a g^b) &= f_{r,s}(g^{a+b}) = (h^{(a+b)r}, k^{(a+b)s}) \\ &= (h^{ar}, k^{as})(h^{br}, k^{bs}) = f_{r,s}(g^a) f_{r,s}(g^b). \end{aligned}$$

Bởi vậy có mười đồng cấu $f_{r,s}$ từ C_{10} đến $C_2 \times C_5$ tương ứng với mười phần tử (h^r, k^s) của $C_2 \times C_5$. Ta có

$$\begin{aligned} \text{Ker} f_{r,s} &= \{g^n \mid (h^{rn}, k^{sn}) = (e, e)\} \\ &= \{g^n \mid rn \equiv 0 \pmod{2} \text{ và } sn \equiv 0 \pmod{5}\}. \end{aligned}$$

Do đó, $\text{Ker} f_{r,s} = \{e\}$ nếu $(r, s) = (1, 1), (1, 2), (1, 3)$, hoặc $(1, 4)$. Trong khi đó

$$\text{Ker} f_{0,0} = C_{10}, \text{Ker} f_{1,0} = \{e, g^2, g^4, g^6, g^8\}, \text{ và}$$

$$\text{Ker} f_{0,s} = \{e, g^5\}, \text{ nếu } s = 1, 2, 3, 4.$$

Nếu $\text{Ker} f_{r,s}$ chứa nhiều hơn một phần tử thì $f_{r,s}$ là một đơn ánh nhưng không thể là một đẳng cấu. Theo định lý đồng cấu, ta có

$$|C_{10}/\text{Ker} f_{r,s}| = |\text{Im} f_{r,s}|,$$

và nếu $\text{Ker } f_{r,s} = e$, thì $|\text{Im } f_{r,s}| = 10$, vì vậy $f_{r,s}$ là toàn cấu. Bởi vậy, các đẳng cấu là $f_{1,1}, f_{1,2}, f_{1,3}$ và $f_{1,4}$.

Xem như một áp dụng của khái niệm tích trực tiếp ta kết thúc mục này bằng một ví dụ chỉ ra tất cả các lớp đẳng cấu có thể có của các nhóm với sáu phần tử. Trước hết ta chứng minh các bổ đề sau.

Bổ đề 1.7. *Giả sử a và b là các phần tử trong một nhóm aben, lần lượt có cấp là r và s với r và s nguyên tố cùng nhau. Khi đó ab có cấp rs .*

Chứng minh. Gọi A và B tương ứng là các nhóm con sinh bởi a và b . Vì $ab = ba$, ta có

$$(ab)^{rs} = a^{rs}b^{rs} = (a^r)^s(b^s)^r = e^s e^r = e.$$

Giả sử $(ab)^k = e$, ta cần chỉ ra rs chia hết k . Rõ ràng $a^k = b^{-k} \in A \cap B$. Vì $A \cap B$ là nhóm con của cả A và B nên cấp của nó chia hết $|A| = r$ và $|B| = s$, theo định lý Lagrange. Vì r và s là nguyên tố cùng nhau nên $|A \cap B| = 1$. Từ đó suy ra $a^k = e$ và $b^{-k} = e$, vì vậy r chia hết k và s chia hết k . Do đó, rs chia hết k (bởi vì r và s nguyên tố cùng nhau). $\square$

Bổ đề 1.8. *Nếu $(G, \cdot)$ là một nhóm hữu hạn mà mọi phần tử $g \in G$ thoả mãn $g^2 = e$, thì $|G| = 2^n$ với mọi $n \geq 0$, và G đẳng cấu với tích trực tiếp n -bản sao của C_2 ,*

$$C_2^n = C_2 \times C_2 \times \dots \times C_2.$$

Chứng minh. Mọi phần tử trong G có cấp 1 hoặc 2, và chỉ có đơn vị có cấp 1. Bởi vậy mọi phần tử của G là nghịch đảo của chính nó. Nhóm G là giao hoán bởi vì với $g, h \in G$ bất kỳ thì

$$gh = (gh)^{-1} = h^{-1}g^{-1} = hg.$$

Chọn các phần tử $a_1, a_2, \dots, a_n \in G$ sao cho $a_i \neq e$ và a_i không thể được viết như là tích của các lũy thừa của $a_1, a_2, \dots, a_{i-1}$. Hơn nữa, chọn n là số lớn nhất sao cho mọi phần tử được biểu diễn qua các phần tử a_i . Nếu C_2 được sinh ra bởi g , ta chứng tỏ ánh xạ $f: C_2^n \rightarrow G$, xác định bởi

$$f(g^{r_1}, g^{r_2}, \dots, g^{r_n}) = a_1^{r_1} a_2^{r_2} \dots a_n^{r_n}$$

là một đẳng cấu. Trước hết, định nghĩa đó là hợp lý vì với mọi số nguyên r_i , bởi vì nếu $g^{r_i} = g^{q_i}$ thì $a_i^{r_i} = a_i^{q_i}$. Ta có

$$\begin{aligned} f((g^{r_1}, \dots, g^{r_n}) \cdot (g^{s_1}, g^{s_2}, \dots, g^{s_n})) &= f(g^{r_1+s_1}, g^{r_2+s_2}, \dots, g^{r_n+s_n}) \\ &= a_1^{r_1+s_1} \dots a_n^{r_n+s_n} \\ &= (a_1^{r_1} \dots a_n^{r_n}) \cdot (a_1^{s_1} \dots a_n^{s_n}) \\ &= f(g^{r_1}, g^{r_2}, \dots, g^{r_n}) \cdot f(g^{s_1}, \dots, g^{s_n}). \end{aligned}$$

Do đó f là một đồng cấu nhóm.

Gọi $(g^{r_1}, \dots, g^{r_n}) \in \text{Ker } f$. Giả sử r_i là số mũ lẻ cuối cùng, sao cho tất cả các số $r_{i+1}, r_{i+2}, \dots, r_n$ là số chẵn. Khi đó $a_1^{r_1} \dots a_{i-1}^{r_{i-1}} a_i = e$ và

$$a_i = a_i^{-1} = a_1^{r_1} \dots a_{i-1}^{r_{i-1}},$$

nó là một mâu thuẫn. Bởi vậy, tất cả các số mũ đều chẵn, và f là một đơn ánh. Việc chọn các phần tử a_i đảm bảo f là một toàn ánh. Do đó, f là một song ánh. $\square$

Với các kết quả này bây giờ ta có thể mô tả các nhóm có cấp 6.

Giả sử G là một nhóm cấp 6. Mỗi phần tử của G có cấp 1, 2, 3 hoặc 6.

Trường hợp 1. Nếu có một phần tử cấp 6 thì nhóm đó là cyclic.

Trường hợp 2. Nếu trong G không có phần tử cấp 6 thì theo Bổ đề 1.7, không thể tất cả các phần tử khác đơn vị đều có cấp 2. Do đó, có một phần tử, ký hiệu là a , có cấp 3. Nhóm con $H = \{e, a, a^2\}$ có chỉ số 2 và nếu $b \notin H$ thì tập các phần tử của nhóm G là

$$H \cup bH = \{e, a, a^2, b, ab, a^2b\}$$

Do H là nhóm con có chỉ số 2 trong G nên nó là chuẩn tắc, và nhóm thương theo H là nhóm cyclic cấp 2. Do đó

$$b^r \in b^r H = (bH)^r = \begin{cases} H & \text{nếu } r \text{ chẵn} \\ bH & \text{nếu } r \text{ lẻ} \end{cases}$$

Bởi vậy, b có cấp chẵn. Nó không thể là 6, vì vậy nó phải là 2. Vì H là chuẩn tắc nên $bab^{-1} \in H$. Do $a \neq e$ nên $bab^{-1} = e$.

Nếu $bab^{-1} = a$ thì $ba = ab$, và do đó theo Bổ đề 1.7, ab sẽ có cấp 6. Điều này là trái với giả thiết. Bởi vậy $bab^{-1} = a^2$, và nhóm G được

sinh bởi hai phần tử a và b , thoả mãn các quan hệ

$$a^3 = b^2 = e \text{ và } ba = a^2b.$$

Nhóm này là đẳng cấu với D_3 và S_3 .

Bài tập

Trong các bài tập từ 1.1 đến 1.4, cặp nhóm nào là đẳng cấu? Vì sao?

1.1. $\mathbb{Z}_6$ và $\mathbb{Z}_2 \times \mathbb{Z}_3$.

1.2. C_{60} và $C_{10} \times C_6$.

1.3. D_n và $C_n \times C_2$.

1.4. $\mathbb{Z}_4 \times \mathbb{Z}_2$ và $\{\pm 1, \pm i, \pm(1+i)/\sqrt{2}, \pm(1-i)/\sqrt{2}\}$.

1.5. Chứng minh rằng nếu $G \times H$ là nhóm xyclic thì G và H là xyclic.

1.6. Cho X và Y là những nhóm xyclic có cấp là m và n . Chứng minh rằng $X \times Y$ là một nhóm xyclic khi và chỉ khi m và n nguyên tố cùng nhau.

1.7. Với các nhóm G và H bất kỳ, chứng minh rằng

$$(G \times H)/G' = H \text{ và } (G \times H)/H' = G,$$

ở đó

$$G' = \{(g, e) \in G \times H \mid g \in G\}$$

$$H' = \{(e, h) \in G \times H \mid h \in H\}.$$

1.8. Tìm tất cả các lớp đẳng cấu của nhóm có cấp 10.

1.9. Chứng tỏ rằng $\mathbb{Z}_2 \times \mathbb{Z}_2$ có 6 tự đẳng cấu và $\text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$.

1.10. Chứng minh rằng mọi nhóm cấp 4 hoặc đẳng cấu với $\mathbb{Z}_4$ hoặc đẳng cấu với $\mathbb{Z}_2 \times \mathbb{Z}_2$.

1.11. Có thể phân tích $\mathbb{Z}$ thành tổng trực tiếp của hai nhóm aben không?

- 1.12. Chứng minh rằng đối với mỗi nhóm L và mỗi cặp đồng cấu nhóm $g : L \rightarrow G, g' : L \rightarrow G'$ đều tồn tại đồng cấu duy nhất $h : L \rightarrow G \times G'$ sao cho biểu đồ sau giao hoán

$$\begin{array}{ccccc} & & L & & \\ & \swarrow g & \downarrow h & \searrow g' & \\ G & \xleftarrow{p} & G \times G' & \xrightarrow{p'} & G' \end{array}$$

nghĩa là $g = p \circ h, g' = p' \circ h$, trong đó p, p' là các phép chiếu tự nhiên.

- 1.13. Chứng minh rằng nếu $f : G \rightarrow H$ là một toàn cấu nhóm và nếu A là một nhóm con chuẩn tắc của G sao cho *cái thu hẹp* $k = f|_A$ là một đẳng cấu thì G phân tích được thành tích trực tiếp của A và hạt nhân $B = \text{Ker } f$.
- 1.14. Cho B, C là những nhóm aben. Chứng minh rằng nếu $\beta : B \rightarrow C$ và $\gamma : C \rightarrow B$ là những đồng cấu sao cho $\beta \circ \gamma = \text{id}_C$ thì $B = \text{Ker } \beta \oplus \text{Im } \gamma$.
- 1.15. Giả sử $(X_i)_{i \in I}$ là một họ khác rỗng các nhóm.
 $X = \prod_{i \in I} X_i$ là tích trực tiếp của họ $(X_i)_{i \in I}$. Các ánh xạ $p_i, i \in I$ cho bởi

$$\begin{aligned} p_i : X &\rightarrow X_i \\ x &\mapsto x_i. \end{aligned}$$

- a) Chứng minh rằng p_i là toàn cấu với mọi $i \in I$.
 b) Cho nhóm Y và cho một họ đồng cấu $(f_i : Y \rightarrow X_i, i \in I)$. Chứng minh rằng tồn tại duy nhất đồng cấu $\bar{f} : Y \rightarrow X$ sao cho với mọi $i \in I$ ta có $f_i = p_i \circ \bar{f}$.

2. Nhóm đối xứng

Trong mục 3 chương II chúng ta đã cho ví dụ về nhóm đối xứng S_n của n phần tử. Nhóm này có nhiều ứng dụng quan trọng trong đại số trừu tượng. Trong phần này chúng ta sẽ tìm hiểu sâu sắc hơn về cấu trúc của nhóm này và trình bày định lý Keli(Cayley) về sự đẳng cấu của một nhóm bất kỳ với một nhóm con của nhóm các phép thế của nó.

Trước hết ta nhắc lại khái niệm *vòng xích*. Nếu $a_1, a_2, \dots, a_m, 1 \leq m \leq n$, là các phần tử phân biệt của tập hợp $\{1, 2, \dots, n\}$ thì phép thế f cho bởi $f(a_1) = a_2, f(a_2) = a_3, \dots, f(a_{m-1}) = a_m, f(a_m) = a_1$, và $f(x) = x$ nếu $x \notin \{a_1, a_2, \dots, a_m\}$, được gọi là một vòng xích độ dài m , hay một m -xích. Ta ký hiệu vòng xích này bởi $(a_1 a_2 \dots a_m)$. Mệnh đề sau là hiển nhiên:

Mệnh đề 2.1. *Mỗi m -vòng xích trong nhóm S_n có cấp m .*

Một vòng xích có độ dài 2, $f = (i j)$, được gọi là một *chuyển trí*. Hai vòng xích được gọi là *độc lập* nếu chúng không có phần tử chung.

Bổ đề 2.2. *Mỗi phép thế khác phép đồng nhất là tích của những vòng xích độc lập.*

Chứng minh. Xét phép thế

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

Ở dòng thứ nhất ta lấy một phần tử tùy ý, chẳng hạn i_1 rồi lấy ảnh liên tiếp ta được i_2 là ảnh của i_1 , i_3 là ảnh của $i_2, \dots, i_m$ là ảnh của i_{m-1} và i_1 là ảnh của i_m . Thế thì ta được một vòng xích $(i_1 i_2 \dots i_m)$. Tiếp tục cách làm đó với các phần tử còn lại của tập $\{1, 2, \dots, n\}$ cho tới hết ta thu được các vòng xích độc lập mà tích của chúng bằng phép thế f . $\square$

Bổ đề 2.3. *Mỗi phép thế đều có thể phân tích được thành tích những phép chuyển trí.*

Chứng minh. Không mất tính tổng quát, ta chỉ cần chứng minh mệnh đề cho một vòng xích. Khi đó ta có

$$(i_1 i_2 \dots i_m) = (i_1 i_m) \dots (i_1 i_3)(i_1 i_2). \quad \square$$

Nói chung có thể phân tích một phép thế thành tích của các chuyển trí theo nhiều cách khác nhau, chẳng hạn

$$(j\ k)(i\ k) = (i\ j)(j\ k) \quad \text{nếu } i \neq j \quad (1)$$

$$(i\ j)(i\ k) = (i\ k)(j\ k) \quad \text{nếu } j \neq k \quad (2)$$

Tuy nhiên ta có tính chất quan trọng sau.

Bổ đề 2.4. Nếu tích của các chuyển trí nào đó bằng phép thế đồng nhất thì số các chuyển trí này là chẵn.

Chứng minh. Ta có thể chứng minh bổ đề này theo s , là số các số khác nhau chứa trong cách viết của tích các chuyển trí đã cho.

Nếu $s = 2$ thì tích đã cho là lũy thừa của một chuyển trí nào đó. Nhưng do $(i\ j)(i\ j) = id$, với id ký hiệu cho phép đồng nhất, nên số mũ của lũy thừa này phải là số chẵn. Với $s > 2$ giả sử ta có tích

$$(i_1\ i_2)(i_3\ i_4) \dots (i_{2q-1}\ i_{2q}) = id \quad (3)$$

trong đó có đúng s số khác nhau. Giả sử i là một trong số các số này. Do tích các chuyển trí độc lập là giao hoán và do quan hệ (1) ta có thể "đời về phía trước" tất cả các chuyển trí mà trong cách viết của nó có chứa i , tức là biến tích (3) thành

$$(i\ j_1)(i\ j_p)(k_1\ k_2) \dots (k_{2r-1}\ k_{2r}) \quad (4)$$

trong đó các số $k_1, k_2, \dots, k_{2r}$ khác với i . Do quan hệ (2) và do

$$(i\ j)(i\ j) = id \quad (5)$$

nên có thể chuyển tích (4) về một tích cũng có dạng như vậy nhưng với p nhỏ hơn (nếu $p > 1$).

Sau một dãy các phép biến đổi như vậy ta được một tích mà số chuyển trí có chứa i là 0 hoặc 1. Nếu xảy ra tình huống thứ hai ta có tích

$$(i\ j)(l_1\ l_2) \dots (l_{2t-1}\ l_{2t})$$

Tích này biến j thành i và vì vậy không là phép đồng nhất. Bởi vậy chỉ có thể xảy ra tình huống thứ nhất, khi mà trong cách viết của tích không chứa i . Bởi vậy theo quy nạp tích này gồm một số chẵn các chuyển trí.

Còn lại, ta thấy rằng trong các phép biến đổi nói trên số các chuyển trí hoặc không thay đổi (khi sử dụng các quan hệ (1), (2)) hoặc giảm bớt hai đơn vị (khi sử dụng quan hệ (5)). Vì vậy tích ban đầu (3) cũng gồm một số chẵn các chuyển trí.

Bổ đề đã được chứng minh hoàn toàn. $\square$

Mệnh đề 2.5. Trong mọi dạng phân tích một phép thế đã cho thành tích các chuyển trí thì tính chẵn lẻ của số các chuyển trí là không thay đổi.

Chứng minh. Thật vậy, giả sử phép thế f có hai cách phân tích thành tích các chuyển trí

$$f = (i_1 i_2) \dots (i_{2p-1} i_{2p}) = (j_1 j_2) \dots (j_{2q-1} j_{2q}).$$

Khi đó

$$id = f \circ f^{-1} = (i_1 i_2) \dots (i_{2p-1} i_{2p})(j_{2q-1} j_{2q}) \dots (j_2 j_1).$$

Theo Bổ đề 2.4 ta có $p + q$ là số chẵn. Do đó các số p, q cũng là hai số chẵn hoặc cùng lẻ. $\square$

Định nghĩa. Một phép thế được gọi là *chẵn* nếu nó được phân tích thành tích của một số chẵn các chuyển trí và được gọi là *lẻ* trong trường hợp ngược lại.

Tích chẵn, lẻ của phép thế còn có thể được định nghĩa nhờ khái niệm nghịch thế.

Mệnh đề 2.6. Tập hợp A_n tất cả các phép thế chẵn bậc n lập thành một nhóm con của nhóm đối xứng S_n . Nhóm con này được gọi là nhóm thay phiên.

Chứng minh. Hiển nhiên. $\square$

Mệnh đề 2.7. Nhóm thay phiên A_n là nhóm con chỉ số 2 trong S_n và do đó là nhóm con chuẩn tắc của S_n .

Chứng minh. Ta nhận thấy rằng trong nhóm đối xứng S_n đối với hai phép thế lẻ a, b thì tích ab^{-1} là phép thế chẵn. Bởi vậy mọi phép thế lẻ lập thành một lớp ghép theo nhóm con A_n . Nghĩa là A_n là nhóm con chỉ số 2 trong S_n và do đó là nhóm con chuẩn tắc của S_n . $\square$

Định lý 2.8 (Định lý Cayley). *Mỗi nhóm G đều đẳng cấu với một nhóm con của nhóm đối xứng $S(G)$ của nó.*

Chứng minh. Đối với mỗi phần tử $a \in G$ ta xác định $f_a : G \rightarrow G$ cho bởi $f_a(x) = ax$. Ta chứng tỏ rằng f_a là một song ánh. Nó là toàn ánh do với $y \in G$ thì $f_a(a^{-1}y) = a(a^{-1}y) = y$. Nó là đơn ánh vì nếu $f_a(x) = f_a(y)$ thì $ax = ay$, và do đó $x = y$. Như vậy $f_a \in S(G)$.

Giả sử $H = \{f_a \mid a \in G\}$. Ta chứng tỏ rằng H là nhóm con của $S(G)$ đẳng cấu với G . Để làm điều đó ta sẽ chứng tỏ rằng ánh xạ $\varphi : G \rightarrow H$, cho bởi $\varphi(a) = f_a$, là một đẳng cấu. Tính toàn ánh là hiển nhiên. Nó cũng là đơn ánh do

$$\begin{aligned}\varphi(a) = \varphi(b) &\Rightarrow f_a = f_b \\ \Rightarrow f_a(e) = f_b(e) &\Rightarrow a = b.\end{aligned}$$

Bây giờ ta chứng tỏ φ là một đồng cấu, và do đó là đẳng cấu. Với $a, b, x \in G$ ta có

$$f_a \circ f_b(x) = f_a(bx) = a(bx) = (ab)x = f_{ab}(x).$$

Nghĩa là $f_a \circ f_b = f_{ab}$, hay $\varphi(a) \circ \varphi(b) = \varphi(ab)$. □

Bài tập

- 2.1. Tìm cấp của mỗi phần tử của nhóm thay phiên A_4 .
- 2.2. Nhóm con cyclic $\{(1), (123), (132)\}$ có là chuẩn tắc trong A_4 không?
- 2.3. Tìm nhóm con của nhóm A_4 đẳng cấu với 4-nhóm Klein.
- 2.4. Hai nhóm D_6 và A_4 có đẳng cấu không? Hãy giải thích.
- 2.5. Cho π là r -vòng xích trong S_n , chứng minh rằng $\rho^{-1} \circ \pi \circ \rho$ cũng là một r -vòng xích đối với mỗi ρ thuộc S_n .
- 2.6. Tìm tất cả 10 nhóm con của A_4 và vẽ biểu đồ quan hệ theo quan hệ bao hàm.
- 2.7. Cho G là một nhóm con của S_n và G chứa một phép thế lẻ, chứng minh rằng G chứa một nhóm con chuẩn tắc có chỉ số 2.

2.8. Chứng minh rằng

$$K = \{(1), (12) \circ (34), (13) \circ (24), (14) \circ (23)\}$$

là một nhóm con của S_4 đẳng cấu với 4-nhóm Klein. Chứng minh rằng K là chuẩn tắc và $S_4/K \cong S_3$.

2.9. Cho K là nhóm được cho trong bài tập 2.8, chứng minh rằng K là chuẩn tắc trong A_4 và $A_4/K \cong C_3$. Điều này chứng tỏ A_4 không phải là nhóm đơn.

2.10. Cho $f: S_n \rightarrow S_{n+1}$, ở đó $f(\pi)$ là phép thế trên $\{1, 2, \dots, n+1\}$ xác định bởi $f(\pi)(i) = \pi(i)$ nếu $i \leq n$ và $f(\pi)(n+1) = n+1$. Hãy cho biết f có phải là một đồng cấu hay không? Tìm ảnh và hạt nhân của nó (nếu có).

2.11. Chứng tỏ rằng S_n sinh bởi các phần tử

$$(1\ 2), (2\ 3), \dots, (n-1\ n).$$

2.12. Chứng tỏ rằng S_n sinh bởi các phần tử $(1\ 2\ 3 \dots n)$ và $(1\ 2)$.

2.13. Chứng tỏ rằng tập hợp $\{f_1, f_2, \dots, f_6\}$ các hàm từ $\mathbb{R} \setminus \{0, 1\}$ đến chính nó với phép toán hợp thành là đẳng cấu với S_3 , trong đó

$$\begin{aligned} f_1(x) &= x, & f_2(x) &= 1-x, & f_3(x) &= \frac{1}{x}, \\ f_4(x) &= 1-\frac{1}{x}, & f_5(x) &= \frac{1}{1-x}, & f_6(x) &= \frac{x}{1-x}. \end{aligned}$$

3. Nhúng một nửa nhóm vào nhóm

Trong mục này ta muốn xét xem với điều kiện nào thì có thể có một ánh xạ đơn cấu, hay còn gọi là một *nhúng*, từ một nửa nhóm đã cho vào một nhóm nào đó.

Trước hết dễ thấy rằng nếu có thể nhúng nửa nhóm S vào nhóm

G thì S phải thoả mãn luật giản ước:

Từ $ac = bc$ cũng như từ $ca = cb$ suy ra $a = b$.

Điều kiện cần này cũng là điều kiện đủ trong trường hợp nửa nhóm giao hoán.

Mệnh đề 3.1. Giả sử A là nửa nhóm aben và S là nửa nhóm con của A gồm các phần tử chính quy theo nghĩa

$$ax = bx \Rightarrow a = b, \text{ với } x \in S; a, b \in A.$$

Khi đó có thể nhúng A vào vị nhóm aben G sao cho mọi phần tử của S đều có phần tử nghịch đảo trong G .

Chứng minh. Xét tập tích Đề-các $A \times S$ cùng với quan hệ hai ngôi trên nó

$$(a, x) \sim (b, y) \Leftrightarrow ay = bx.$$

Dễ thấy quan hệ này là phản xạ và đối xứng. Nó còn là bắc cầu. Thật vậy, nếu có $(a, x) \sim (b, y)$, $(b, y) \sim (c, z)$ thì $ay = bx$, $bz = cy$, và do đó $ayz = bxz = cyx$.

Sau khi giản ước cho y ta được $az = cx$ hay $(a, x) \sim (c, z)$.

Bởi vậy quan hệ $\sim$ vừa định nghĩa là một quan hệ tương đương. Nó tạo nên một sự phân lớp trên $A \times S$ và ta được tập thương

$$G = A \times S / \sim,$$

mà mỗi phần tử là một lớp $\overline{(a, x)}$. Để đơn giản ta ký hiệu lớp $\overline{(a, x)}$ bởi phân số hình thức $\frac{a}{x}$. Trên G ta định nghĩa một phép toán hai ngôi cho bởi

$$\frac{a}{x} \circ \frac{b}{y} = \frac{ab}{xy}.$$

Quy tắc này có nghĩa vì $xy \in S$ và nó không phụ thuộc vào các cặp đại diện cho mỗi lớp. Thật vậy, nếu

$$\frac{a}{x} = \frac{a'}{x'}, \quad \frac{b}{y} = \frac{b'}{y'},$$

thì $ax' = a'x$, $by' = b'y$ nên $abx'y' = a'b'xy$. Từ đó $\frac{ab}{xy} = \frac{a'b'}{x'y'}$.

Có thể kiểm tra một cách dễ dàng rằng $(G, \circ)$ là một vị nhóm giao hoán với phần tử đơn vị $1 = \frac{x}{x}$, trong đó x là phần tử tùy ý thuộc S .

Xét tương ứng $\varphi : A \rightarrow G$ cho bởi $a \mapsto \frac{ax}{x}$, với phần tử tùy ý $x \in S$. Do $\frac{ax}{x} = \frac{ay}{y}$ với mọi $y \in S$ nên φ là một ánh xạ. Hơn nữa có thể thấy φ là một đồng cấu do

$$\varphi(ab) = \frac{abxy}{xy} = \frac{ax}{x} \circ \frac{by}{y} = \varphi(a) \circ \varphi(b).$$

Đồng cấu φ là một đơn cấu do

$$\varphi(a) = \varphi(b) \Leftrightarrow \frac{ax}{x} = \frac{by}{y} \Leftrightarrow axy = byx \Leftrightarrow a = b.$$

Như vậy ta có thể nhúng A vào G nhờ đơn cấu φ . Đồng nhất A với $\varphi(A)$ bởi $a \equiv \frac{ax}{x}$, với $x \in S$ ta có thể chỉ ra phần tử nghịch đảo của phần tử $s \in S$ là phần tử $\frac{x}{sx}$. $\square$

Định lý 3.2. *Mỗi nửa nhóm aben A với luật giản ước đều có thể nhúng vào một nhóm aben G . Khi đó mỗi phần tử của G viết được dưới dạng ab^{-1} , với a, b thuộc A .*

Chứng minh. Giả sử A là một nửa nhóm aben với luật giản ước. Áp dụng mệnh đề trên cho trường hợp $S = A$ ta được G là một nhóm. Thật vậy, khi đó phần tử bất kỳ của G có dạng a/b với $a, b \in A$, nên nó có nghịch đảo là b/a . Hơn nữa khi đó

$$\frac{a}{b} = \frac{axy}{bxy} = \frac{ax}{x} \circ \frac{y}{by} = \frac{ax}{x} \circ \left(\frac{by}{y}\right)^{-1} = ab^{-1}. \quad \square$$

Bài tập

- 3.1.** Cho M là vị nhóm giao hoán thỏa mãn luật giản ước. Hãy chứng minh rằng tồn tại nhóm aben A và đồng cấu $k : M \rightarrow A$ của các vị nhóm với tính chất phổ dụng sau: Với mỗi nhóm B và mỗi đồng cấu vị nhóm $f : M \rightarrow B$ tồn tại đồng cấu nhóm duy nhất $f' : A \rightarrow B$ sao cho $f = f' \circ k$.

4. Tác động của nhóm trên một tập hợp

Cho G là một nhóm với đơn vị e và X là một tập hợp nào đó.

Định nghĩa. Nhóm $(G, \cdot)$ được gọi là *tác động* lên tập X nếu có một ánh xạ

$$\begin{aligned} G \times X &\rightarrow X, \\ (g, x) &\mapsto gx \end{aligned}$$

sao cho với mọi $g, h \in G$ và mọi $x \in X$ ta có

$$\begin{aligned} (gh)x &= g(hx) \\ ex &= x. \end{aligned}$$

Khi đó X được gọi là một G -tập.

Mệnh đề 4.1. *Mỗi tác động của nhóm G lên tập X hoàn toàn được xác định khi và chỉ khi đã cho một đồng cấu nhóm*

$$\varphi : G \rightarrow S(X)$$

trong đó $S(X)$ ký hiệu cho nhóm đối xứng của tập X .

Chứng minh. Xét G -tập X . Mỗi phần tử $g \in G$ cảm sinh một phép thế $\varphi_g : X \rightarrow X$, cho bởi hệ thức

$$\varphi_g(x) = gx$$

Trước hết ta chứng tỏ φ_g là một phần tử thuộc nhóm đối xứng $S(X)$.

Ánh xạ φ_g là một đơn ánh bởi vì nếu $gx = gy$ thì $g^{-1}gx = g^{-1}gy$, từ đó $ex = ey$, hay $x = y$. Nó là một toàn ánh vì nếu $z \in X$ thì

$$g(g^{-1}z) = gg^{-1}z = ez = z.$$

Do đó φ_g là một song ánh và được xem như là một phần tử của $S(X)$, nhóm các phép đối xứng của X .

Bây giờ ta chứng tỏ ánh xạ $\varphi : G \rightarrow S(X)$ biến mỗi phần tử $g \in G$ thành song ánh $\varphi_g : X \rightarrow X$, là một đồng cấu nhóm. Thật vậy, đối với $x \in X$ và với $g, h \in G$ ta có

$$\varphi_{gh}(x) = (gh)x = \varphi_g(\varphi_h(x)) = (\varphi_g \circ \varphi_h)(x)$$

Từ đó $\varphi(gh) = \varphi(g) \circ \varphi(h)$.

Ngược lại, nếu đã cho đồng cấu $\varphi : G \rightarrow S(X)$ thì X sẽ là một G -tập với tác động được xác định bởi hệ thức

$$gx = \varphi(g)(x), g \in G, x \in X. \quad \square$$

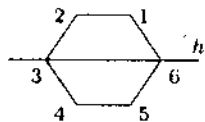
Nhóm G được gọi là tác động *trung thành* lên tập X nếu đồng cấu nhóm $\varphi : G \rightarrow S(X)$ là một đơn cấu. Khi đó phần tử của G , giữ cố định mọi phần tử của X chỉ là đơn vị e của G . Do φ đơn cấu nên G đẳng cấu với ảnh $\text{Im} \varphi$, và vì vậy ta có thể đồng nhất G với $\text{Im} \varphi$ và xem G như một nhóm con của $S(X)$.

Ví dụ, nhóm xyclic cấp 2, $C_2 = \{e, h\}$ tác động lên hình lục giác ở Hình A, ở đó h quay hình lục giác theo đường thẳng nối đỉnh 3 và đỉnh 6. Khi đó, C_2 tác động trung thành và có thể đồng nhất với nhóm con $\{(1), (15) \circ (24)\}$ của D_6 .

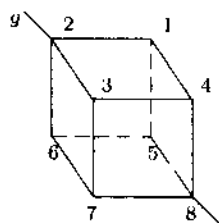
Nhóm xyclic $C_3 = \{e, g, g^2\}$ tác động trung thành lên khối lập phương trong Hình B, ở đó g quay khối lập phương thông qua 3 phép quay có trục là đường thẳng đi qua hai đỉnh đối diện. Nhóm tác động này có thể xem như nhóm con

$$\{(1), (1\ 6\ 3) \circ (4\ 5\ 7), (1\ 3\ 6) \circ (4\ 7\ 5)\}$$

của nhóm đối xứng của khối lập phương.



Hình A.



Hình B.

Mệnh đề 4.2. Nếu G tác động lên tập X và $x \in X$ thì tập

$$G_x = \{g \in G \mid gx = x\}$$

là một nhóm con của G . Nhóm con G_x được gọi là cái ổn định của x . Nó là tập các phần tử của G , giữ nguyên x .

Chứng minh. Ta chứng tỏ G_x là một nhóm con của nhóm G . Nếu $g, h \in G_x$ thì

$$(gh)x = g(hx) = gx = x$$

Bởi vậy $gh \in G_x$.

Mặt khác, nếu $g \in G_x$ thì $gx = x$. Từ đó,

$$g^{-1}x = g^{-1}(gx) = (g^{-1}g)x = ex = x,$$

nghĩa là $g^{-1} \in G_x$. □

Định nghĩa. Tập của tất cả các ảnh của một phần tử $x \in X$ dưới tác động của nhóm G được gọi là *quỹ đạo* của x theo G và được ký hiệu bởi

$$Gx = \{gx \mid g \in G\}.$$

Ví dụ. Cho nhóm G và gọi X là tập tất cả các nhóm con của nó. Ta xác định một tác động của nhóm G lên tập X , cho bởi

$$\begin{aligned}(G \times X) &\rightarrow X \\ (g, H) &\rightarrow gHg^{-1}.\end{aligned}$$

Nhóm con gHg^{-1} được gọi là *liên hợp* với H bởi g . Ta thấy rằng mỗi một quỹ đạo của H gồm tất cả các nhóm con của G liên hợp với H . Nhóm con ổn định đối với H là

$$G_H = \{g \in G \mid gHg^{-1} = H\}$$

Nhóm con này được gọi là *cái chuẩn hoá* của H , và H là nhóm con chuẩn tắc của nhóm này.

Mệnh đề 4.3. Cho X là một G -tập. Khi đó X được phân hoạch bởi các quỹ đạo $Gx, x \in X$.

Chứng minh. Trên X có một quan hệ hai ngôi cảm sinh bởi tác động của nhóm G như sau:

$$x \approx y \text{ khi và chỉ khi } y = gx, g \in G.$$

Ta chứng tỏ rằng đây là một quan hệ tương đương. Rõ ràng $x \approx x$ do $x = ex$. Nếu $x \approx y$ thì $y = gx$. Thế thì $x = g^{-1}y$ và do đó $y \approx x$. Sau cùng, quan hệ $\approx$ là bắc cầu. Thật vậy, nếu $x \approx y$ và $y \approx z$ thì $x = gy, y = hz$. Bởi vậy, $x = ghz$ và do đó $x \approx z$.

Quan hệ tương đương $\approx$ tạo nên một phân hoạch trên tập X . Lớp tương đương của phần tử $x \in X$ chính là quỹ đạo Gx của nó. □

Khi nhóm cyclic C_2 tác động lên một lục giác trong Hình A. nói trên ta nhận được các quỹ đạo là $\{1,5\}$, $\{2,4\}$, $\{3\}$ và $\{6\}$.

Có một mối liên kết quan trọng giữa số các phần tử trong một quỹ đạo của phần tử x và cái ổn định của điểm này.

Bổ đề 4.4. Nếu nhóm G tác động lên tập X thì với mọi $x \in X$ có một song ánh

$$p: G/G_x \rightarrow Gx.$$

Chứng minh. Gọi $H = G_x$ và xác định ánh xạ

$$p: G/H \rightarrow Gx$$

bởi $p(gH) = gx$. Định nghĩa này trên các lớp ghép là hợp lý bởi vì nếu $gH = kH$ thì $k = gh$ với $h \in H$. Do đó $kx = g(hx) = gx$, vì h là ổn định đối với x .

Ánh xạ p là một toàn ánh theo định nghĩa của quỹ đạo của x . Nó cũng là một đơn cấu, bởi vì nếu $p(gH) = p(kH)$ thì $gx = kx$. Do đó $g^{-1}kx = x$, và bởi vậy $g^{-1}k \in H$. Điều này tương đương với $gH = kH$. Bởi vậy, p là một song ánh. $\square$

Hệ quả sau được suy ra trực tiếp từ Bổ đề 4.4.

Hệ quả 4.5. Nếu nhóm hữu hạn G tác động lên tập X , thì với mỗi phần tử $x \in X$, ta có

$$|G| = |G_x| \cdot |Gx|.$$

Ví dụ. Tìm số các phép quay thực sự của một khối lập phương.

Lời giải. Gọi G là nhóm của các phép quay thực sự của một khối lập phương; nghĩa là các phép quay này có thể được thực hiện trong không gian ba chiều. Cái ổn định của đỉnh 1 trong Hình B là

$$G_1 = \{(1), (2\ 4\ 5) \circ (3\ 8\ 6), (2\ 5\ 4) \circ (3\ 6\ 8)\}.$$

quỹ đạo của 1 là tập tất cả các đỉnh, vì có một phần tử của G , biến 1 thành đỉnh khác. Bởi vậy theo Hệ quả 4.5. ta có

$$|G| = |G_1| \cdot |G1| = 3 \cdot 8 = 24.$$

$\square$

Nhóm đối xứng đầy đủ của một khối lập phương sẽ gồm cả những phép quay không thực sự, chẳng hạn phép phản xạ qua một mặt phẳng

được thể hiện trong Hình B. Nhóm này có phép thế $(24) \circ (68)$ trên các đỉnh và nó không thể thu được phép quay mang tính vật lý khối lập phương trong không gian ba chiều. Theo nhóm này, ta có

$$G_1 = \{(1), (2\ 4\ 5) \circ (3\ 6\ 8), (2\ 4) \circ (6\ 8), (2\ 5) \circ (3\ 8), (4\ 5) \circ (3\ 6)\}.$$

Vì vậy cấp của nhóm đối xứng đầy đủ của khối lập phương là

$$|G_1| = |G_1| = 6 \cdot 8 = 48.$$

Bởi vậy có 24 phép quay thực sự và 24 phép quay không thực sự của một khối lập phương.

Ta kết thúc chương này bằng việc đề cập đến tác động của nhóm đối xứng S_n lên tập hợp các đa thức n biến $x_1, x_2, \dots, x_n$. Một phép thế $\sigma \in S_n$ tác động lên một đa thức $f = f(x_1, x_2, \dots, x_n)$ bằng việc hoán vị các biến:

$$\sigma(f) = f(x_{\sigma 1}, x_{\sigma 2}, \dots, x_{\sigma n}).$$

Bài tập

4.1. Chứng minh rằng $(\mathbb{R}^*, \cdot)$ tác động lên $\mathbb{R}^{n+1}$ bởi phép nhân vô hướng. quỹ đạo của các tác động này là gì?

Với các Bài tập 4.2, 4.3, gọi

$$\mathbb{Z}_m^* = \{[x] \in \mathbb{Z}_m \mid \text{UCLN}(x, m) = 1\}.$$

Số các phần tử trong tập hợp này được ký hiệu là $\phi(m)$ và được gọi là ϕ -hàm Euler. Ví dụ, $\phi(4) = 2$ và $\phi(8) = 4$.

4.2. Tìm các nhóm trong số C_7 , C_8 , $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_4 , S_3 đẳng cấu với $(\mathbb{Z}_8^*, \cdot)$, $(\mathbb{Z}_9^*, \cdot)$, $(\mathbb{Z}_{10}^*, \cdot)$ và $(\mathbb{Z}_{15}^*, \cdot)$ và mô tả các đẳng cấu đó.

4.3. Chứng minh rằng nếu $\text{UCLN}(a, m) = 1$ thì $a^{\phi(m)} \equiv 1 \pmod{m}$. [Kết quả này được tìm ra bởi Leonhard Euler (1707 - 1783).]

4.4. Chứng minh rằng nếu p là số nguyên tố thì với mọi số nguyên a , $a^p \equiv a \pmod{p}$.

[Kết quả này được tìm ra bởi Pierre Fermat (1601 - 1665).]

- 4.5. Nếu G là một nhóm có cấp 35 tác động lên một tập hợp có 13 phần tử, hãy chứng minh rằng G phải có một điểm cố định, nghĩa là một điểm $x \in S$ sao cho $g(x) = x$ với mọi $g \in G$.
- 4.6. Cho G là một nhóm có cấp p^r tác động lên một tập hợp có m phần tử, chứng minh rằng G có một điểm cố định nếu p không chia hết m .

Chương IV

VÀNH VÀ TRƯỜNG

1. Định nghĩa và ví dụ
2. Idêan, vành thương
3. Đồng cấu vành
4. Trường các thương
5. Vành, trường sắp thứ tự

1. Định nghĩa và ví dụ

Vành

Định nghĩa. Tập hợp R cùng với hai phép toán hai ngôi, được viết như phép cộng (+) và phép nhân ($\times$) thông thường, được gọi là một *vành* nếu các điều kiện sau được thoả mãn:

- (i) $(R, +)$ là một nhóm aben,
- (ii) $(R, \times)$ là một nửa nhóm,
- (iii) Phép nhân phân phối về hai phía đối với phép cộng, nghĩa là:

$$\begin{aligned}a \times (b + c) &= a \times b + a \times c \\(b + c) \times a &= b \times a + c \times a\end{aligned}$$

với mọi a, b, c thuộc R .

Vành R được gọi là *giao hoán* nếu phép nhân trong R có tính chất giao hoán: $a \times b = b \times a$, với mọi $a, b \in R$. Vành R được gọi là *có đơn vị* nếu phép nhân có đơn vị.

Chú ý. 1. Phần tử trung hoà của phép cộng được gọi là *phần tử không* của vành R và ký hiệu bởi 0.

2. Nếu R là vành có đơn vị thì phần tử đơn vị được ký hiệu bởi e hoặc 1 .

Ví dụ

1. Tập hợp các số nguyên $\mathbb{Z}$ với phép cộng và phép nhân thông thường là một vành giao hoán, có đơn vị.

2. Nhóm aben $(\mathbb{Z}_n, +)$ là một vành giao hoán, có đơn vị với phép nhân cho bởi

$$\bar{x} \cdot \bar{y} = \overline{xy}.$$

Do phép nhân của các lớp được định nghĩa qua các đại diện nên ta phải chứng tỏ rằng định nghĩa này là hợp lý. Giả sử $\bar{x} = \overline{x_1}, \bar{y} = \overline{y_1}$. Thế thì $x \equiv x_1 \pmod{n}, y \equiv y_1 \pmod{n}$. Điều này kéo theo

$$x = x_1 + kn, y = y_1 + sn.$$

Từ đó, $xy = x_1y_1 + tn$, nghĩa là $xy \equiv x_1y_1 \pmod{n}$.

3. $(\mathbb{Q}(\sqrt{2}), +, \times)$ là một vành giao hoán, có đơn vị, trong đó $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

Trước hết chúng ta chứng tỏ rằng phép cộng và phép nhân hai số thực đóng kín đối với tập $\mathbb{Q}(\sqrt{2})$, và do đó chúng là những phép toán đại số hai ngôi trên $\mathbb{Q}(\sqrt{2})$. Với $a, b, c, d \in \mathbb{Q}$ ta có

$$\begin{aligned}(a + b\sqrt{2}) + (c + d\sqrt{2}) &= (a + c) + (b + d)\sqrt{2} \in \mathbb{Q}(\sqrt{2}) \\ (a + b\sqrt{2}) \cdot (c + d\sqrt{2}) &= (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Q}(\sqrt{2})\end{aligned}$$

Sau đó ta có thể kiểm tra các tiên đề của vành. Phần tử trung hoà và đơn vị của $\mathbb{Q}(\sqrt{2})$ lần lượt là

$$0 = 0 + 0\sqrt{2}, \quad 1 = 1 + 0\sqrt{2}.$$

4. Tập hợp $M_n(\mathbb{R}), (n \geq 2)$, các ma trận thực vuông cấp n với phép cộng và phép nhân ma trận là một vành có đơn vị, không giao hoán.

5. Cho A là một nhóm cộng aben và $\text{End}(A)$ là tập hợp các tự đồng cấu của nó. Khi đó $\text{End}(A)$ trở thành một vành với phép nhân là phép hợp thành các ánh xạ và phép cộng được cho bởi

$$(f + g)(a) = f(a) + g(a)$$

với mọi $f, g \in \text{End}(A), a \in A$. Ta gọi $\text{End}(A)$ là vành các tự đồng cấu của nhóm aben A .

Tính chất của vành

Mỗi vành R đều có tất cả các tính chất của một nhóm cộng giao hoán và thoả mãn một số tính chất cơ bản sau:

1) Với mọi $a \in R$, $0 \times a = a \times 0 = 0$.

Thật vậy, với $x \in R$ ta có

$$x \times a = (0 + x) \times a = 0 \times a + x \times a,$$

điều này chứng tỏ $0 \times a = 0$. Tương tự ta có $a \times 0 = 0$.

2) Nếu vành R có đơn vị 1 và có nhiều hơn một phần tử thì $1 \neq 0$.
Thật vậy, khi đó trong R tồn tại phần tử $a \neq 0$ và ta có

$$a \times 0 = 0, a \times 1 = a.$$

Từ đó, do $a \neq 0$ nên $1 \neq 0$.

Từ nay về sau để thuận tiện ta ký hiệu tích $a \times b$ của hai phần tử trong vành R đơn giản bởi ab .

3) Với mọi a, b, c thuộc R ta có:

$$a(b - c) = ab - ac$$

$$(b - c)a = ba - ca.$$

Thật vậy, ta có thể viết $b = (b - c) + c$. Nhân hai vế của đẳng thức với a về bên trái ta được

$$ab = a(b - c) + ac$$

Từ đó, do R là nhóm đối với phép cộng nên

$$a(b - c) = ab - ac.$$

Tương tự ta có $(b - c)a = ba - ca$.

4) Trong R có luật phân phối suy rộng, nghĩa là với mọi phần tử $a, b_1, b_2, \dots, b_n$ ($n \geq 2$) thuộc R ta có:

$$a \sum_{i=1}^n b_i = \sum_{i=1}^n ab_i \quad (1),$$

$$\left(\sum_{i=1}^n b_i \right) a = \sum_{i=1}^n ab_i \quad (2).$$

Ta sẽ chứng minh đẳng thức (1) bằng quy nạp theo n . Với $n = 2$, theo tiên đề (iii) ta có

$$a(b_1 + b_2) = ab_1 + ab_2$$

nghĩa là tính chất này đúng với $n = 2$.

Giả sử đẳng thức (1) đúng với $n = k$, tức là

$$a \sum_{i=1}^k b_i = \sum_{i=1}^k ab_i.$$

Ta chứng minh đẳng thức (1) đúng với $n = k + 1$. Khi đó theo giả thiết quy nạp ta có

$$\begin{aligned} a \sum_{i=1}^{k+1} b_i &= a \left(\sum_{i=1}^k b_i + b_{k+1} \right) = a \sum_{i=1}^k b_i + ab_{k+1} \\ &= \sum_{i=1}^k ab_i + ab_{k+1} = \sum_{i=1}^{k+1} ab_i \end{aligned}$$

nghĩa là đẳng thức (1) đúng với $n = k + 1$, và do đó đúng với mọi $n \geq 2$.

5) *Quy tắc về dấu:* Với mọi a, b thuộc R

$$a(-b) = (-a)b = -ab; \quad (-a)(-b) = ab.$$

Thật vậy,

$$b + (-b) = 0 \Rightarrow a(b + (-b)) = ab + a(-b) = 0,$$

từ đó suy ra $-ab = a(-b)$.

Chứng minh tương tự ta được $(-a)b = -ab$. Bây giờ áp dụng hai lần tính chất trên ta có

$$(-a)(-b) = -[(-a)b] = -[-ab] = ab.$$

6) *Đối với mọi số nguyên n và mọi phần tử a, b thuộc vành R*

$$n(ab) = (na)b = a(nb).$$

Thật vậy, với $n > 0$ ta có

$$\begin{aligned} n(ab) &= ab + ab + \dots + ab \text{ (tổng của } n \text{ hạng tử)} \\ &= (a + a + \dots + a)b = (na)b. \end{aligned}$$

Tương tự $n(ab) = a(nb)$. Với $n = 0$ các đẳng thức là hiển nhiên (theo tính chất 1) vừa nêu trên. Với $n < 0$ thì $-n > 0$ và do đó theo định nghĩa bội nguyên âm của một phần tử và theo trường hợp $n > 0$ ta có

$$n(ab) = -((-n)(ab)) = -((-n)a)b = -(-(na)b) = (na)b.$$

Miền nguyên và trường

Một tính chất khá tiện lợi của các hệ thống số quen thuộc là nếu $ab = 0$ thì nhất thiết $a = 0$ hoặc $b = 0$. Tính chất này cho phép giản ước các phần tử khác không. Thế nhưng tính chất này không còn đúng với mọi vành. Ví dụ trong vành $\mathbb{Z}_4$ ta có $\bar{2} \cdot \bar{2} = \bar{0}$.

Định nghĩa. Phần tử $a \neq 0$ thuộc vành R được gọi là một *ước bên trái* (tương ứng *bên phải*) của *không* nếu tồn tại $b \in R, b \neq 0$, sao cho $ab = 0$ (tương ứng $ba = 0$). Nếu a vừa là ước bên trái, vừa là ước bên phải của không thì a được gọi là *ước của không*.

Ví dụ. Trong vành $M_2(\mathbb{R})$ các ma trận vuông cấp 2 trên tập các số thực, các ma trận

$$A = \begin{bmatrix} 0 & 0 \\ 1 & 2 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix}$$

theo thứ tự là ước bên trái, ước bên phải của không.

Định lý 1.1. Cho R là một vành giao hoán, có đơn vị $1 \neq 0$. Khi đó hai tính chất sau là tương đương:

- (i) R không có ước của không.
- (ii) Phép nhân trong R có luật giản ước cho những phần tử khác không.

Chứng minh. (i) $\Rightarrow$ (ii). Giả sử R không có ước của không. Giả sử ta có $ab = ac$, với a, b, c thuộc R , và $a \neq 0$. Khi đó

$$a(b - c) = 0.$$

Đó $a \neq 0$ và R không có ước của 0 nên $b - c = 0$. Từ đó $b = c$, nghĩa là phép nhân trong R là giản ước được.

(ii) $\Rightarrow$ (i). Giả sử phép nhân trong R có luật giản ước cho những phần tử khác không. Giả sử $a, b \in R$ là hai phần tử bất kỳ mà $ab = 0$ và $a \neq 0$. Khi đó ta có thể viết $ab = a0$ và sau đó áp dụng luật giản ước ta được $b = 0$. Điều này chứng tỏ vành R không có ước của không. $\square$

Định nghĩa. Vành R được gọi là một *miền nguyên* nếu nó là vành giao hoán, có đơn vị $1 \neq 0$ và không có ước của không.

Ví dụ

1. Vành số nguyên $\mathbb{Z}$, vành số hữu tỷ $\mathbb{Q}$ đều là những miền nguyên.
2. Tập hợp $(\mathbb{Z}_4, +, \times)$ là một vành giao hoán, có đơn vị, nhưng không là miền nguyên do có $\bar{2}$ là ước của không.
3. Đối với miền nguyên $\mathbb{Z}$, tích trực tiếp $\mathbb{Z} \times \mathbb{Z}$ của nhóm abel $(\mathbb{Z}, +)$ với chính nó cùng với phép nhân cho bởi

$$(a, b)(c, d) = (ac, bd)$$

là một vành. Tuy nhiên, có thể thấy rằng tích trực tiếp $R = \mathbb{Z} \times \mathbb{Z}$ là một vành giao hoán, có đơn vị nhưng không là miền nguyên do $(a, 0) \cdot (0, b) = (0, 0)$ với mọi a, b thuộc $\mathbb{Z}$.

Định nghĩa. Vành F được gọi là một *trường* nếu F là một vành giao hoán, có đơn vị $1 \neq 0$ và mọi phần tử khác 0 của nó đều khả nghịch (theo nghĩa có nghịch đảo đối với phép nhân).

Một cách tương đương, tập hợp F cùng với hai phép toán ký hiệu bởi $+$, $\times$ là một trường nếu:

- (i) $(F, +)$ là một nhóm giao hoán với phần tử trung hoà 0,
- (ii) $(F^*, \times)$ là một nhóm giao hoán, trong đó $F^* = F \setminus \{0\}$,
- (iii) Phép nhân phân phối với phép cộng.

Ví dụ

1. Tập hợp các số hữu tỷ $\mathbb{Q}$, (hoặc tập các số thực $\mathbb{R}$, hoặc tập các số phức $\mathbb{C}$) với phép cộng và nhân thông thường là một trường.
2. Tập $(\mathbb{Z}_3, +, \cdot)$ là một trường. Trong trường này $(\bar{2})^{-1} = \bar{2}$. Trong phần sau chúng ta sẽ chứng minh rằng vành $(\mathbb{Z}_p, +, \times)$ là một trường khi và chỉ khi p là số nguyên tố.

3. $(\mathbb{Q}(\sqrt{2}), +, \times)$ là một trường. Thật vậy, ta đã biết đó là một vành giao hoán có đơn vị. Nếu $a + b\sqrt{2} \neq 0$ thì $a \neq 0$ hoặc $b \neq 0$, kéo

theo $a - b\sqrt{2} \neq 0$. Do đó

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} =$$

$$\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

và $(\mathbb{Q}(\sqrt{2}), +, \times)$ là một trường.

Định lý 1.2. *Mỗi trường đều là một miền nguyên.*

Chứng minh. Giả sử F là một trường. Khi đó F là một vành giao hoán có đơn vị $1 \neq 0$. Mặt khác giả sử a, b, c là ba phần tử bất kỳ thuộc F sao cho $ab = ac$ (1) và $a \neq 0$. Vì $a \neq 0$ nên tồn tại $a^{-1} \in F$ sao cho $a^{-1} \cdot a = 1$. Từ (1) suy ra

$$a^{-1} \cdot (ab) = a^{-1} \cdot (ac) \Rightarrow b = c.$$

Vậy trong F có luật giản ước cho những phần tử khác 0 và do đó F là một miền nguyên. $\square$

Định lý 1.3. *Một miền nguyên hữu hạn là một trường.*

Chứng minh. Giả sử $D = \{a_0, a_1, a_2, \dots, a_n\}$ là một miền nguyên với $a_0 = 0, a_1 = 1$. Ta chứng tỏ rằng mọi phần tử khác không của D có nghịch đảo đối với phép nhân. Giả sử $a \in D, a \neq 0$. Khi đó tập hợp

$$aD = \{aa_0, aa_1, aa_2, \dots, aa_n\}$$

trùng với D . Thật vậy, nếu $aa_i = aa_j$ thì sau khi giản ước cho a ta được $a_i = a_j$, bởi vậy mọi phần tử của aD là phân biệt và do đó aD chính là D . Từ đó suy ra tồn tại a_s sao cho $aa_s = 1$, nghĩa là $a_s = a^{-1}$. Vậy D là một trường. $\square$

Hệ quả 1.4. *Vành $\mathbb{Z}_n$ là trường khi và chỉ khi n là một số nguyên tố.*

Chứng minh. ($\Leftarrow$) Giả sử n là một số nguyên tố và giả sử $\bar{a}\bar{b} = \bar{0}$ trong $\mathbb{Z}_n$. Thế thì $n|ab$, và do đó $n|a$ hoặc $n|b$. Bởi vậy $\bar{a} = \bar{0}$ hoặc $\bar{b} = \bar{0}$, và $\mathbb{Z}_n$ là một miền nguyên. Do $\mathbb{Z}_n$ có hữu hạn phần tử nên nó là một trường (Định lý 1.3).

($\Rightarrow$) Bây giờ giả sử n không là số nguyên tố. Thế thì n có sự phân tích $n = r.s$, trong đó $1 < r, s < n$. Như vậy ta có $\bar{r}, \bar{s}$ là những phần tử khác không trong $\mathbb{Z}_n$ nhưng tích của chúng $\bar{r}.\bar{s} = \overline{rs} = \bar{0}$. Bởi vậy $\mathbb{Z}_n$ không là miền nguyên, và do đó nó không là trường. $\square$

Vành con, trường con

Định nghĩa. Cho A là một tập con ổn định đối với phép cộng và phép nhân của vành R . Nếu A cùng với các phép toán cảm sinh là một vành (tương ứng, là một trường) thì A được gọi là một *vành con* (tương ứng, là một *trường con*) của vành (trường) R .

Từ định nghĩa ta thấy ngay rằng nếu A là vành con của R thì A chứa phần tử 0 của R và nếu A là trường con thì A chứa các phần tử 0 và đơn vị 1 của R .

Nếu A là vành con (trường con) của vành (trường) R thì R còn được gọi là một *mở rộng* của vành (trường) A .

Ví dụ

1. Vành các số nguyên $\mathbb{Z}$ là vành con của vành các số hữu tỷ $\mathbb{Q}$.
2. Tập $m\mathbb{Z}$ các số nguyên là bội của một số nguyên m cho trước là một vành con của vành các số nguyên $\mathbb{Z}$.
3. Trường số hữu tỷ $\mathbb{Q}$ là một trường con của trường số thực $\mathbb{R}$; trường các số thực $\mathbb{R}$ là trường con của trường số phức $\mathbb{C}$.
4. Cho A là một vành có đơn vị. Khi đó tập U các phần tử khả nghịch lập thành một vành con của A . Hơn nữa, U là một trường (xem phần bài tập).
5. $(\mathbb{Q}(\sqrt{2}), +, \times)$ là trường con của trường số phức $\mathbb{C}$.

Bây giờ ta cho một tính chất đặc trưng của vành con.

Định lý 1.5. Tập con A của vành R là một vành con của R khi và chỉ khi thỏa mãn các điều kiện sau:

- (i) $0 \in A$,
- (ii) $\forall a, b \in A \Rightarrow a - b \in A$ và $ab \in A$.

Chứng minh. Thật vậy, tập con A của vành R là ổn định đối với phép toán nhân khi và chỉ khi $a, b \in A$ kéo theo $ab \in A$. Đồng thời tập con

A là nhóm con theo phép toán cộng khi và chỉ khi nó thoả mãn (i) và phần còn lại của (ii). Luật phân phối trong A suy ra từ luật phân phối trong R . $\square$

Đối với khái niệm trường con ta có đặc trưng sau.

Định lý 1.6. *Tập con A của trường F là trường con của F khi và chỉ khi thoả mãn các điều kiện sau:*

- (i) $0 \in A, 1 \in A$,
- (ii) $\forall a, b \in A \Rightarrow a - b \in A$,
- (iii) $\forall a, b \in A, b \neq 0 \Rightarrow ab^{-1} \in A$.

Chứng minh. Phép suy luận tương tự như phép suy luận trong chứng minh định lý 1.5. $\square$

Theo định lý 1.6 để chứng minh $\mathbb{Q}(\sqrt{2})$ là một trường ta có thể chứng minh nó là trường con của trường số thực $\mathbb{R}$. Khi đó thay cho việc kiểm tra tất cả các tiên đề của một trường ta chỉ cần thử lại ba điều kiện nói trong định lý vừa nêu trên.

Trong định nghĩa của chúng ta một vành không nhất thiết phải có đơn vị. Tuy nhiên chúng ta có khẳng định sau.

Mệnh đề 1.7. *Cho R là một miền nguyên và A là một vành con của nó. Nếu A có đơn vị thì đơn vị đó trùng với đơn vị của R .*

Chứng minh. Gọi e, e' tương ứng là đơn vị của R, A . Khi đó

$$e.e' = e' = e'.e'.$$

Từ đó $(e - e').e' = 0$. Do R là miền nguyên và do $e' \neq 0$ nên $e - e' = 0$, hay $e = e'$. $\square$

Bài tập

1.1. Hãy viết các bảng cộng và bảng nhân của mỗi vành $\mathbb{Z}_4, \mathbb{Z}_3$.

Hãy cho biết những tập hợp nào trong các bài tập từ 1.2 đến 1.6 có là vành với phép cộng và phép nhân hay không? Nói rõ vì sao.

1.2. Mọi số hữu tỷ với mẫu số là số lẻ.

- 1.3. $\{a + b\sqrt{5} | a, b \in \mathbb{Z}\}$
 1.4. $\{a + b\sqrt{2} + c\sqrt{3} | a, b, c \in \mathbb{Z}\}$
 1.5. $\{a + b\sqrt[3]{2} | a, b \in \mathbb{Q}\}$.
 1.6. Mọi ma trận thực cỡ 2×2 với định thức bằng không.
 1.7. Hệ $(\mathbb{Z}, +, \times)$ có phải là vành không, trong đó phép cộng là thông thường, còn phép nhân được cho bởi $a \times b = 0$ với mọi $a, b \in \mathbb{Z}$.
 1.8. Chứng minh rằng trong định nghĩa của vành có đơn vị, tiên đề về tính giao hoán của phép toán cộng có thể suy ra được từ các tiên đề còn lại.
 1.9. Cho R là một vành. Đặt:

$$I = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in R \right\}$$

Chứng minh rằng I là vành con của vành $M_2(\mathbb{R})$.

- 1.10. Xác định các vành con của vành $\mathbb{Z}_n$.

Những vành nào trong các bài tập từ 1.11 đến 1.13 là miền nguyên? là trường?

- 1.11. $\mathbb{Z}_2 \times \mathbb{Z}_2$.
 1.12. $\{a + bi | a, b \in \mathbb{Q}\}$.
 1.13. $\{a + b\sqrt{2} | a, b \in \mathbb{Z}\}$.

Tìm mọi ước của không trong các vành ở các bài tập từ 1.14 đến 1.18.

- 1.14. $\mathbb{Z}_{10}$.
 1.15. $\mathbb{Z}_4 \times \mathbb{Z}_2$.
 1.16. $M_2(\mathbb{Z}_2)$.
 1.17. $(S(X), \Delta, \cap)$.
 1.18. $M_n(\mathbb{R})$.
 1.19. Chứng minh rằng vành R là giao hoán nếu $x^2 - x \in Z(R)$, $\forall x \in R$, trong đó $Z(R)$ là tập tất cả các phần tử giao hoán được với mọi phần tử của R .
 1.20. Vành R được gọi là một vành *Bool* nếu $x^2 = x$ với mọi $x \in R$. Chứng minh rằng:
 a) $x = -x$ với mọi $x \in R$;
 b) R là vành giao hoán;

c) Nếu R là vành không có ước của không, có nhiều hơn một phần tử, thì R là miền nguyên.

1.21. Giả sử vành R có nhóm cộng $(R, +)$ là xyclic. Chứng minh rằng R là vành giao hoán.

1.22. Chứng minh rằng trường các số hữu tỷ không có trường con nào khác ngoài bản thân nó.

1.23. Chứng minh rằng bộ phận

$$A = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$$

là một trường con của trường số thực $\mathbb{R}$.

1.24. Cho hai phần tử $a, b \in R$. Chứng minh rằng $1 - ab$ là khả nghịch khi và chỉ khi $1 - ba$ là khả nghịch. Trong trường hợp đó hãy tìm $(1 - ab)^{-1}$.

1.25. Phần tử a của vành R được gọi là *lũy linh* nếu tồn tại số nguyên dương n sao cho $a^n = 0$. Chứng minh rằng nếu a là một phần tử lũy linh của vành R thì $1 - a$ là khả nghịch.

2. Idean, vành thương

Định nghĩa và ví dụ

Định nghĩa. Vành con J của vành R được gọi là *idean trái* (tương ứng, *phải*) của R nếu $xa \in J$ (tương ứng, $ax \in J$) với mọi $a \in J, x \in R$. Nếu J vừa là idean trái vừa là idean phải của vành R thì J được gọi là *idean* của R .

Mệnh đề 2.1. Cho J là tập con khác rỗng của vành R . Khi đó các điều sau là tương đương:

(i) J là idean của R .

(ii) Nếu $a, b \in J$ và $x \in R$ thì $a - b \in J$ và $ax, xa \in J$.

Chứng minh. Trước hết ta thấy rằng điều kiện $a - b \in J$ với mọi $a, b \in J$ tương đương với khẳng định rằng J là một nhóm con đối với

phép cộng. Từ đó hiển nhiên $(i) \Rightarrow (ii)$.

Ngược lại, nếu $ax, xa \in J$ với mọi $a \in J, x \in R$ thì ta suy ra J đóng kín đối với phép nhân khi ta lấy $x \in J$, do đó J là vành con của R , và do đó $(ii) \Rightarrow (i)$. $\square$

Từ Mệnh đề 2.1 ta có thể nói rằng một ideal J của vành R là một nhóm con cộng, có tính chất $ax, ax \in J$ với mọi $a \in J, x \in R$.

Ví dụ

1. Đối với vành R tùy ý ta luôn có $\{0\}$ và R là những ideal của R . Các ideal này được gọi là những ideal tầm thường của R . Ideal $\{0\}$ thường được ký hiệu đơn giản là 0 . Nếu R là một trường thì R chỉ gồm những ideal tầm thường là 0 và R (xem Định lý 2.6).

2. Tập $m\mathbb{Z}$, với m là số nguyên cho trước, là ideal của vành số nguyên $\mathbb{Z}$.

3. Tập hợp các ma trận thực J có dạng

$$J = \left\{ \begin{bmatrix} 0 & 0 \\ a & b \end{bmatrix} \mid a, b \in \mathbb{R} \right\}$$

là ideal phải của vành các ma trận thực vuông cấp 2.

Mệnh đề 2.2. Cho I là ideal của vành R . Nếu I chứa đơn vị, thì I trùng với vành R .

Chứng minh. Giả sử $1 \in I$. Khi đó với mọi $r \in R$ ta có $r = r \cdot 1 \in I$, do đó $I = R$. $\square$

Idéal sinh bởi một tập hợp

Định lý 2.3. Giao của một họ khác rỗng những ideal của vành R là một ideal của vành R .

Chứng minh. Cho họ $(J_i)_{i \in I}$ là một họ những ideal của vành R chỉ số hoá bởi tập $I \neq \emptyset$. Đặt

$$J = \bigcap_{i \in I} J_i$$

Ta chứng minh J là ideal. Vì $0 \in J_i, \forall i \in I$, nên $0 \in J$.

Giả sử $a, b \in J$, khi đó $a, b \in J_i, \forall i \in I$. Từ đó suy ra $a - b \in J_i, \forall i \in I$, và vì vậy $a - b \in J$.

Bây giờ giả sử $a \in J$ và $x \in R$. Khi đó $a \in J_i, \forall i \in I$ nên ta có

$$ax \in J_i, xa \in J_i \text{ với } \forall i \in I.$$

Vậy $ax \in J$ và $xa \in J$, nghĩa là J là ideal của R . □

Định nghĩa. Cho M là một tập con của vành R . Giao của họ tất cả các ideal của R chứa M là một ideal bé nhất của R , chứa M . Ideal này được gọi là ideal *sinh bởi* M , ký hiệu (M) .

Nếu M là một tập hữu hạn thì ideal sinh bởi M được gọi là *ideal hữu hạn sinh*. Nếu $M = \{a\}$ thì ideal sinh bởi M được gọi là *ideal chính* sinh bởi phần tử a và ký hiệu đơn giản là (a) . Đặc biệt khi $M = \emptyset$ thì ideal sinh bởi tập rỗng là 0 .

Ví dụ, mọi ideal của vành $\mathbb{Z}$ đều là ideal chính. Thật vậy, nếu A là một ideal của vành $\mathbb{Z}$ thì trước hết nó là nhóm con cộng của $\mathbb{Z}$ và do đó nó có dạng $m\mathbb{Z}, m \in \mathbb{Z}$. Ngược lại như trong ví dụ vừa nêu thì $m\mathbb{Z}$ là ideal của $\mathbb{Z}$.

Ví dụ ta vừa xét là trường hợp riêng của mệnh đề sau.

Mệnh đề 2.4. Cho a là một phần tử của vành giao hoán R . Tập $\{ar | r \in R\}$ tất cả các bội của a là ideal chính sinh bởi a .

Chứng minh. Cho $ar, as \in (a)$ và $t \in R$. Khi đó

$$ar - as = a(r - s) \in (a) \text{ và } (ar)t = a(rt) \in (a).$$

Do đó (a) là một ideal của R . □

Mở rộng mệnh đề này cho tập sinh hữu hạn ta có:

Định lý 2.5. Cho R là một vành giao hoán có đơn vị và $a_1, a_2, \dots, a_n$ là n phần tử thuộc R . Khi đó ideal sinh bởi tập hợp $\{a_1, a_2, \dots, a_n\}$ là tập hợp

$$A = \{x_1a_1 + x_2a_2 + \dots + x_na_n | x_i \in R\}$$

Chứng minh. Xét tập hợp

$$A = \{x_1a_1 + x_2a_2 + \dots + x_na_n | x_i \in R\}$$

Có thể thử lại rằng R là một ideal của R , và A chứa các phần tử $a_1, a_2, \dots, a_n$.

Bây giờ giả sử J là một ideal của R chứa các phần tử $a_1, a_2, \dots, a_n$. Khi đó

$$x_1 a_1 + x_2 a_2 + \dots + x_n a_n \in J,$$

trong đó $x_i \in R$. Do đó $A \subset J$. Điều này chứng tỏ A là một ideal bé nhất chứa các a_i , nghĩa là A sinh bởi tập $\{a_1, a_2, \dots, a_n\}$. $\square$

Kết quả sau đây chứng tỏ rằng một trường có thể được đặc trưng bởi các ideal của nó.

Định lý 2.6. *Một vành giao hoán không tầm thường R là một trường nếu và chỉ nếu 0 và R là tất cả các ideal của nó.*

Chứng minh. Cho I là một ideal của trường R . Giả sử rằng $I \neq 0$. Khi đó tồn tại một phần tử khác 0 , $a \in I$. Vì $a^{-1} \in R$, nên $a \cdot a^{-1} = 1 \in I$. Do đó theo Mệnh đề 2.2, $I = R$. Bởi vậy, R chỉ có các ideal tầm thường.

Ngược lại, giả sử rằng 0 và R là tất cả các ideal trong vành R . Gọi a là một phần tử khác 0 của R và xét (a) là ideal chính sinh bởi a . Do $1 \cdot a \in (a)$ nên $(a) \neq 0$, và do đó $(a) = R$. Bởi vì $1 \in R = (a)$, nên tồn tại một số $b \in R$ nào đó sao cho $ab = 1$. Do đó, $b = a^{-1}$ và R là một trường. $\square$

Các phép toán trên các ideal

Định lý 2.7. *Cho I_1 và I_2 là hai ideal của vành R . Khi đó*

$$I_1 + I_2 = \{a_1 + a_2 : a_1 \in I_1, a_2 \in I_2\}$$

là một ideal của R .

Chứng minh. Đặt $I = I_1 + I_2$. Khi đó có $0 = 0 + 0 \in I$. Giả sử $a = a_1 + a_2 \in I$, $b = b_1 + b_2 \in I$, với $a_1, b_1 \in I_1$; $a_2, b_2 \in I_2$. Thế thì

$$a - b = (a_1 - b_1) + (a_2 - b_2) \in I.$$

Giả sử $a = a_1 + a_2 \in I$, $x \in R$ ta có:

$$xa = x(a_1 + a_2) = xa_1 + xa_2 \in I_1 + I_2$$

$$ax = (a_1 + a_2)x = a_1x + a_2x \in I_1 + I_2.$$

Vậy $I_1 + I_2$ là một ideal của R . □

Định nghĩa. Ideal $I_1 + I_2$ được gọi là *tổng* của hai ideal I_1, I_2 .

Định lý 2.8. Cho I, J là hai ideal của vành R . Khi đó

$$IJ = \left\{ \sum_{i=1}^n a_i b_i \mid a_i \in I, b_i \in J, n \geq 1 \right\}$$

là một ideal của R .

Chứng minh. Trước hết ta có $0 = 0.0 \in IJ$. Giả sử

$$a = \sum_{i=1}^m a_i b_i, \quad a' = \sum_{j=1}^n a'_j b'_j$$

là những phần tử thuộc IJ . Khi đó ta có:

$$a + b = \sum_{i=1}^m a_i b_i + \sum_{j=1}^n a'_j b'_j \in IJ.$$

Bây giờ với $a = \sum_{i=1}^m a_i b_i \in IJ$, $x \in R$ ta có

$$xa = x \sum_{i=1}^m a_i b_i = \sum_{i=1}^m (xa_i) b_i \in IJ,$$

$$ax = \left(\sum_{i=1}^m a_i b_i \right) x = \sum_{i=1}^m a_i (b_i x) \in IJ.$$

Vậy IJ là một ideal của R . □

Định nghĩa. Ideal IJ nói trong Định lý 2.8 được gọi là *tích* của hai ideal I, J .

Nhận xét. Rõ ràng đối với hai ideal I, J ta luôn có $IJ \subset I \cap J$.

Ví dụ

1. Trong vành các số nguyên $\mathbb{Z}$ tổng $m\mathbb{Z} + n\mathbb{Z}$ là ideal chính $d\mathbb{Z}$, với d là ước chung lớn nhất của m và n .

Thật vậy, nếu $d = (m, n)$ thì tồn tại các số nguyên u, v sao cho $d = mu + nv$, và do đó $d\mathbb{Z} \subset m\mathbb{Z} + n\mathbb{Z}$. Mặt khác, do d là ước của m và n nên $m\mathbb{Z}$ và $n\mathbb{Z}$ cùng chứa trong $d\mathbb{Z}$, do đó $m\mathbb{Z} + n\mathbb{Z} \subset d\mathbb{Z}$.

2. Giao $m\mathbb{Z} \cap n\mathbb{Z}$ là ideal chính $b\mathbb{Z}$, với b là bội chung nhỏ nhất của m và n .

Thật vậy, giả sử $m\mathbb{Z} \cap n\mathbb{Z} = b\mathbb{Z}$. Thế thì $b\mathbb{Z}$ chứa trong $m\mathbb{Z}$ và $n\mathbb{Z}$, và do đó b là bội của m và n . Bây giờ nếu k là một bội chung của m và n thì k thuộc $m\mathbb{Z} \cap n\mathbb{Z} = b\mathbb{Z}$, do đó k là bội của b . Điều này chứng tỏ b là bội chung nhỏ nhất của m và n .

Hơn nữa, trong vành $\mathbb{Z}$ ta còn có $(m\mathbb{Z})(n\mathbb{Z}) = mn\mathbb{Z}$, và do đó

$$m\mathbb{Z} \cap n\mathbb{Z} = (m\mathbb{Z})(n\mathbb{Z})$$

khi và chỉ khi m, n nguyên tố cùng nhau.

Vành thương

Cho J là một ideal của vành R . Do nhóm cộng R là aben nên J là một nhóm con chuẩn tắc của R , và ta có nhóm thương

$$R/J = \{\bar{x} = x + J \mid x \in R\}$$

với phép cộng cho bởi

$$(x + J) + (y + J) = (x + y) + J.$$

Hơn nữa đó là một nhóm aben. Bây giờ ta sẽ chỉ ra rằng phép nhân trên R cảm sinh một phép nhân trong R/J , biến nhóm aben R/J thành một vành.

Định lý 2.9. *Giả sử J là một ideal của vành R . Khi đó tương ứng*

$$\begin{aligned} (R/J) \times (R/J) &\rightarrow R/J \\ (x + J, y + J) &\mapsto xy + J \end{aligned}$$

là một ánh xạ. Hơn nữa, nhóm thương R/J trở thành một vành với phép nhân

$$(x + J)(y + J) = xy + J.$$

Chứng minh. Để chứng minh quy tắc nói trong mệnh đề là một ánh xạ ta cần chứng tỏ rằng nó không phụ thuộc vào đại diện của các lớp. Thật vậy, giả sử

$$x + J = x' + J, \quad y + J = y' + J,$$

khi đó $x - x' \in J$ và $y - y' \in J$. Bởi vậy,

$$x' = x + a, \quad y' = y + b, \quad a, b \in J.$$

Từ đó suy ra

$$x'y' = xy + xb + ay + ab = xy + c, \quad c \in J.$$

Vậy, $x'y' + J = xy + J$.

Ánh xạ nói trên xác định một phép toán hai ngôi trên tập thương R/J cho bởi

$$(x + J)(y + J) = xy + J.$$

Có thể kiểm tra được rằng nhóm cộng giao hoán R/J cùng với phép nhân vừa định nghĩa là một vành. $\square$

Định nghĩa. Vành R/J nói trong Định lý 2.9 được gọi là *vành thương* của vành R theo idêan J .

Hai phép toán trong vành thương R/J thường được ký hiệu bởi

$$\bar{x} + \bar{y} = \overline{x + y}, \quad \bar{x} \cdot \bar{y} = \overline{xy}$$

Nhận xét. 1. Nếu R là vành giao hoán thì vành thương R/J cũng là vành giao hoán. Nếu vành R có đơn vị e thì R/J là vành có đơn vị $\bar{e} = e + J$.

2. Chúng ta có thể kiểm tra được rằng, tương ứng nói trong Định lý 2.9 là ánh xạ chỉ khi J là idêan của R .

Ví dụ. Trong phần trước chúng ta đã chứng minh nhóm cộng $\mathbb{Z}_m$ là một vành đối với phép nhân $\bar{x} \cdot \bar{y} = \overline{xy}$. Bây giờ ta có thể nhận được điều này khi xem

$$\mathbb{Z}_m = \{\bar{a} = a + m\mathbb{Z} : a \in \mathbb{Z}\}$$

là vành thương của vành $\mathbb{Z}$ theo idêan $m\mathbb{Z}$.

Idêan nguyên tố và idêan tối đại

Định nghĩa. Cho R là vành giao hoán, có đơn vị 1.

1) Idêan P của R được gọi là *idêan nguyên tố* nếu $P \neq R$ và từ $ab \in P$ suy ra $a \in P$ hoặc $b \in P$ với mọi $a, b \in R$.

2) Idêan M được gọi là *idêan tối đại* của R nếu $M \neq R$ và nếu với bất kỳ idêan B của R sao cho $M \subset B \subset R$ thì $B = R$ hoặc $B = M$.

Ví dụ

1. 0 là idêan nguyên tố của vành số nguyên $\mathbb{Z}$ nhưng không là idêan tối đại của $\mathbb{Z}$.

2. Trong vành số nguyên $\mathbb{Z}$ mọi idêan đều có dạng $m\mathbb{Z}$. Chúng là idêan nguyên tố của $\mathbb{Z}$ khi và chỉ khi m là nguyên tố. Khi đó $m\mathbb{Z}$ cũng là idêan tối đại của $\mathbb{Z}$ (xem phần bài tập).

3. Nếu F là một trường thì 0 vừa là idêan nguyên tố, vừa là idêan tối đại của F .

Định lý 2.10. Cho vành R giao hoán có đơn vị và J là một idêan của nó. Khi đó:

(i) J là idêan nguyên tố trong vành R khi và chỉ khi vành thương R/J là một miền nguyên;

(ii) J là một idêan tối đại trong vành R khi và chỉ khi vành thương R/J là một trường.

Chứng minh. (i) Giả sử J là một idêan nguyên tố của vành R ,

$$R/J = \{\bar{x} = x + J | x \in R\}$$

là vành thương của vành R trên J . Vì J nguyên tố nên $J \neq R$, do đó R/J có nhiều hơn một phần tử. Đơn vị của R/J là $\bar{1} = 1 + J$ với 1 là đơn vị của R . Do R là vành giao hoán nên R/J cũng là vành giao hoán. Bây giờ giả sử $\bar{x}$ và $\bar{y}$ là hai phần tử tùy ý của R/J . Nếu

$$\bar{x} \cdot \bar{y} = \bar{0}$$

thì $xy \in J$. Vì J là idêan nguyên tố nên hoặc $x \in J$ hoặc $y \in J$. Từ đó suy ra $\bar{x} = \bar{0}$ hoặc $\bar{y} = \bar{0}$. Vậy R/J không có ước của không, và do đó R/J là một miền nguyên.

Ngược lại, giả sử R/J là một miền nguyên. Khi đó R/J có nhiều hơn một phần tử, do đó $J \neq R$. Giả sử x, y là hai phần tử thuộc R

sao cho $xy \in J$. Khi đó

$$\bar{x} \cdot \bar{y} = \bar{0}.$$

Vì R/J không có ước của $\bar{0}$ nên suy ra $\bar{x} = \bar{0}$ hoặc $\bar{y} = \bar{0}$. Từ đó $x \in J$ hoặc $y \in J$. Vậy J là ideal nguyên tố.

(ii) Giả sử J là ideal tối đại trong vành R , và giả sử $u \in R/J, u \neq 0$. Thế thì tồn tại $r \in R/J$ sao cho

$$u = \bar{r} = r + J.$$

Khi đó $J + rR = R$, do đó

$$1 = y + rx, \quad y \in J, x \in R.$$

Từ đó

$$\bar{1} = \bar{0} + \bar{r} \cdot \bar{x}$$

nghĩa là $\bar{r}$ có nghịch đảo. Vậy R/J là một trường.

Ngược lại, giả sử R/J là một trường. Thế thì R/J không có ideal thực sự. Khi đó nếu B là một ideal của R sao cho

$$J \subset B \subset R$$

thì B/J là ideal của R/J . Do trong R/J không có ideal thực sự nên $B/J = 0$ hoặc $B/J = R/J$, nghĩa là $B = J$ hoặc $B = R$. Điều này chứng tỏ J là ideal tối đại trong R . $\square$

Mệnh đề trên cho thấy mọi ideal tối đại đều là ideal nguyên tố. Điều ngược lại nói chung không đúng. Tuy nhiên ta có mệnh đề sau.

Mệnh đề 2.11. Trong vành số nguyên $\mathbb{Z}$ mọi ideal nguyên tố khác không đều là tối đại.

Chứng minh. Giả sử $m\mathbb{Z} \neq 0$ là một ideal nguyên tố. Nếu $n\mathbb{Z} \supset m\mathbb{Z}$ thì $m \in n\mathbb{Z}$ và $m = nr$. Theo định nghĩa của ideal nguyên tố nếu $n \notin m\mathbb{Z}$ thì $r \in m\mathbb{Z}$, nghĩa là $r = mt$ với $t \in \mathbb{Z}$ nào đó. Từ đó

$$m = nr = ntm.$$

Do $m \neq 0$ nên $nt = 1$, suy ra $n\mathbb{Z} = \mathbb{Z}$. Vậy $m\mathbb{Z}$ là ideal tối đại của vành $\mathbb{Z}$. $\square$

Bài tập

Với các bài tập từ 2.1 đến 2.5, tìm tất cả các ideal của vành đã cho.

2.1. $\mathbb{Z}_2 \times \mathbb{Z}_2$.

2.2. $\mathbb{Z}_{18}$.

2.3. $\mathbb{Q}$.

2.4. $\mathbb{Z}_7$.

2.5. $\mathbb{Z}[i]$.

2.6. Tìm các ước của không trong vành $\mathbb{Z}/6\mathbb{Z}$.

Với các bài tập 2.7, 2.8, xác định bảng cộng và nhân cho các vành đã cho. Tìm tất cả các ước của 0 trong mỗi vành. Vành nào trong các vành này là trường?

2.7. $\mathbb{Z}_6/(3)$.

2.8. $\mathbb{Z}_3 \times \mathbb{Z}_3/((1, 2))$.

2.9. Chứng minh $\mathbb{Z}/n\mathbb{Z}$ (với $n > 0$) là một miền nguyên khi và chỉ khi n là một số nguyên tố.

2.10. Cho R là một vành tùy ý, n là số nguyên cho trước. Chứng minh $A = \{x \in R \mid nx = 0\}$ là một ideal của R .

2.11. Cho vành R và $a \in R$. Chứng minh rằng các bộ phận

$$aR = \{ax \mid x \in R\}$$

$$Ra = \{xa \mid x \in R\}$$

lần lượt là ideal phải, ideal trái của R .

2.12. Cho R là vành giao hoán có đơn vị là 1, I và J là hai ideal của R . Hãy chứng minh nếu $I + J = R$ thì $IJ = I \cap J$.

2.13. a) Chứng minh rằng đối với hai số nguyên dương m và n

$$m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$$

khi và chỉ khi m và n nguyên tố cùng nhau.

b) Chứng minh trực tiếp rằng

$$m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z}$$

khi và chỉ khi m và n nguyên tố cùng nhau.

- 2.14.** Giả sử R là một miền nguyên với phần tử đơn vị e và n là cấp của e trong nhóm cộng R . Chứng minh:
- n là một số nguyên tố.
 - Mọi phần tử khác không $x \in R$ có cấp n .
 - Bộ phận $mR = \{mx | x \in R\}$ với m là số nguyên cho trước là một ideal của R .
 - $R/mR \cong R$ nếu m là bội của n ; $R/mR \cong \{0\}$ nếu m không là bội của n .
- 2.15.** Trong vành đa thức $\mathbb{Z}[x]$ xét ideal I sinh bởi $n \in \mathbb{N}$ và x . Chứng minh rằng I là một ideal nguyên tố nếu và chỉ nếu n là một số nguyên tố.
- 2.16.** Cho R là vành giao hoán có đơn vị $1 \neq 0$. Chứng minh rằng nếu mọi ideal của R , khác R , đều là ideal nguyên tố thì R là một trường.
- 2.17.** Cho R là một vành giao hoán có đơn vị và I là ideal thực sự của vành R . Chứng minh rằng tồn tại một ideal tối đại của R chứa I .
- 2.18.** Cho R là vành giao hoán có đơn vị 1. Chứng minh rằng với mỗi phần tử không khả nghịch $a \in R$ đều chứa trong một ideal tối đại chứa a .
- 2.19.** Giả sử I là một ideal thực sự của $\mathbb{Z}$. Chứng minh rằng I là một ideal tối đại của $\mathbb{Z}$ khi và chỉ khi $I = p\mathbb{Z}$, với p là một số nguyên tố.
- 2.20.** Chứng minh rằng mọi ideal tối đại trong vành $\mathbb{Z}_n$ đều có dạng $p\mathbb{Z}_n$, trong đó p là một ước nguyên tố của n .
- 2.21.** Cho R là vành giao hoán, có đơn vị. Chứng minh hai khẳng định sau là tương đương với nhau:
- R chỉ có một ideal tối đại duy nhất.
 - Tập các phần tử không khả nghịch của R lập thành một ideal của R .
- 2.22.** Cho R, S là hai vành. Trên tích $R \times S$ ta định nghĩa phép nhân và phép cộng như sau:

$$\begin{aligned}(x, y)(a, b) &= (xa, yb) \\ (x, y) + (a, b) &= (x + a, y + b).\end{aligned}$$

Chứng minh rằng $R \times S$ là một vành và X là một ideal của

$R \times S$ khi và chỉ khi $X = A \times B$ với A là một ideal của R , B là một ideal của S .

2.23. Cho R là một vành giao hoán. Một phần tử $a \in R$ được gọi là lũy linh nếu $a^n = 0$ với $n \geq 0$ nào đó trong $\mathbb{Z}$. Tập $N(R)$ tất cả các phần tử lũy linh trong R được gọi là căn của R .

a) Chứng minh rằng $N(R)$ là một ideal của R .

b) Chứng minh rằng $N[R/N(R)] = 0$.

c) Chứng minh rằng $N(R)$ bằng giao của tất cả các ideal nguyên tố của R .

2.24. Cho R là một vành giao hoán có đơn vị. Chứng minh rằng:

a) $N(R) = \{x \in R \mid \exists n \in \mathbb{N}^*, x^n = 0\}$ là một ideal của R .

b) Tập $N(R)$ là giao của mọi ideal nguyên tố của R .

2.25. Tìm nhóm các ước của đơn vị trong vành $\mathbb{Z}/n\mathbb{Z}$. Từ đó chứng minh $a^{p-1} \equiv 1 \pmod{p}$ với p là một số nguyên tố và a không chia hết cho p .

2.26. Một vành giao hoán R được gọi là một vành địa phương nếu tồn tại một ideal thực sự lớn nhất P (theo nghĩa với mọi ideal thực sự $I \subset R$ ta có $I \subset P$). Chứng minh rằng các mệnh đề sau là tương đương:

a) R là một vành địa phương.

b) Tập các phần tử không khả nghịch của R là một ideal.

c) Tồn tại một ideal tối đại Q sao cho $1 + a$ khả nghịch với mọi $a \in Q$.

2.27. Nếu F là trường, chứng minh rằng $R = M_2(F)$ có đúng hai ideal là 0 và R . (Bởi vì điều này, R được gọi là vành đơn.).

2.28. Cho vành địa phương R với $J(R)$ là ideal gồm tất cả các phần tử không khả nghịch của R .

a) Chứng minh rằng mọi vành $\mathbb{Z}_p$ với mỗi số nguyên tố p và

$n \geq 1$, là địa phương, nhưng $\mathbb{Z}_6$ thì không là địa phương.

b) Chứng minh rằng

$$\mathbb{Z}_{(p)} = \left\{ \frac{r}{s} \in \mathbb{Q} \mid p \text{ không chia hết } s, (r, s) = 1 \right\}$$

là một vành con địa phương của $\mathbb{Q}$ với mỗi số nguyên tố p .

c) Nếu R là địa phương, chứng minh rằng $R/J(R)$ là một trường.

d) Chứng minh rằng R là địa phương nếu $R/N(R)$ là một trường (Lưu ý rằng nếu a lũy linh thì $1 - a$ khả nghịch).

3. Đồng cấu vành

Định nghĩa và ví dụ

Định nghĩa. Cho hai vành R và S . Ánh xạ $f : R \rightarrow S$ được gọi là một *đồng cấu* từ vành R đến vành S nếu:

$$\begin{aligned}f(a + b) &= f(a) + f(b) \\f(ab) &= f(a)f(b).\end{aligned}$$

với mọi $a, b \in R$.

Trong trường hợp $R = S$ đồng cấu f được gọi là một *tự đồng cấu* của R . Nếu f là một đơn ánh (tương ứng toàn ánh, song ánh) thì đồng cấu f được gọi là một *đơn cấu* (tương ứng *toàn cấu*, *đẳng cấu*).

Nếu có một ánh xạ đẳng cấu từ vành R đến vành S thì ta nói rằng R và S *đẳng cấu* với nhau và ký hiệu $R \cong S$.

Ví dụ

1. Cho R và S là hai vành tùy ý. Ánh xạ $\theta : R \rightarrow S$ biến mọi phần tử $x \in R$ thành phần tử $0 \in S$ là một đồng cấu vành, được gọi là *đồng cấu không*.

2. Cho A là một vành con của vành R . Ánh xạ đồng nhất

$$\mu : A \rightarrow R, \quad x \mapsto x$$

là một đơn cấu, được gọi là *phép nhúng tự nhiên* của A vào R . Đặc biệt, khi $A = R$ thì phép nhúng μ trở thành một tự đẳng cấu của R , được gọi là *phép đồng nhất* của R .

3. Cho I là một ideal của vành R . Ánh xạ

$$p : R \rightarrow R/I, \quad x \mapsto x + I$$

là một toàn cấu từ vành R đến vành thương R/I , được gọi là *phép chiếu tự nhiên* từ R lên R/I .

4. Cho trường số phức $\mathbb{C}$. Ánh xạ

$$p : \mathbb{C} \rightarrow \mathbb{C}, \quad a + bi \mapsto a - bi$$

là một tự đẳng cấu của trường số phức $\mathbb{C}$.

Ví dụ. Các phép biến đổi tuyến tính từ $\mathbb{R}^n$ đến chính nó là vành $(L(\mathbb{R}^n, \mathbb{R}^n), +, \circ)$ với phép cộng và phép hợp thành ánh xạ. Khi đó ánh xạ

$$f : L(\mathbb{R}^n, \mathbb{R}^n) \rightarrow M_n(\mathbb{R})$$

là một đồng cấu vành, ở đó f đặt tương ứng mỗi phép biến đổi tuyến tính α với ma trận chính tắc của nó, tức là ma trận cỡ $n \times n$ các hệ tử đối với cơ sở chính tắc của $\mathbb{R}^n$.

Thật vậy, nếu α là một phép biến đổi tuyến tính từ $\mathbb{R}^n$ đến chính nó thì

$$\alpha \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} a_{11}x_1 + \dots + a_{1n}x_n \\ \vdots \\ a_{n1}x_1 + \dots + a_{nn}x_n \end{bmatrix} \quad \text{và} \quad f(\alpha) = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix}$$

Phép cộng và phép nhân ma trận đã được xác định sao cho

$$\begin{aligned} f(\alpha + \beta) &= f(\alpha) + f(\beta) \\ f(\alpha \circ \beta) &= f(\alpha)f(\beta) \end{aligned}$$

Ngoài ra, nếu i là phép biến đổi tuyến tính đồng nhất của $\mathbb{R}^n$ thì $f(i)$ là ma trận đơn vị.

Mỗi một ma trận xác định một phép biến đổi tuyến tính, do đó f là một toàn cấu. Hơn thế, f còn là một đơn cấu do mỗi ma trận chỉ xác định đúng một ánh xạ tuyến tính. Cụ thể, cột thứ j của ma trận chính là ảnh của vectơ cơ sở thứ j . Bởi vậy f là một đẳng cấu vành.

Tính chất của đồng cấu

Cho $f : R \rightarrow S$ là một đồng cấu từ vành R đến vành S . Khi đó:

1. f là một đồng cấu từ nhóm cộng R đến nhóm cộng S nên nó có các tính chất của một đồng cấu nhóm. Cụ thể là

a) $f(0) = 0$,

$$b) f(-a) = -f(a), \quad \forall a \in R.$$

Tuy nhiên cần lưu ý rằng nếu R và S là những vành có đơn vị thì không nhất thiết xảy ra $f(1) = 1$.

2. Nếu A là một vành con của R thì $f(A)$ là một vành con của S .

Thật vậy, giả sử A là vành con của R . Do mỗi đồng cấu vành là đồng cấu nhóm và mỗi vành con là một nhóm con nên $f(A)$ là nhóm con. Giả sử y_1, y_2 thuộc $f(A)$. Khi đó tồn tại a_1, a_2 thuộc A sao cho $f(a_1) = y_1, f(a_2) = y_2$. Từ đó suy ra

$$y_1 y_2 = f(a_1) f(a_2) = f(a_1 a_2) \in f(A).$$

Vậy $f(A)$ là vành con của S .

3. Nếu I là một ideal của S thì $f^{-1}(I)$ là một ideal của R .

Trước hết, $f^{-1}(I)$ là một nhóm con đối với phép cộng. Bây giờ, giả sử $x \in f^{-1}(I)$ và $r \in R$. Thế thì $f(x) \in I$, và do đó

$$f(xr) = f(x)f(r) \in I,$$

tức là $xr \in f^{-1}(I)$. Vậy I là một ideal của vành R .

Ảnh và hạt nhân của đồng cấu

Nếu f là một đồng cấu từ vành R đến vành S thì nó là một đồng cấu nhóm, và khi đó ta đã có khái niệm ảnh đồng cấu $Im f = f(R)$, và hạt nhân đồng cấu $Ker f = f^{-1}(0)$.

Nhận xét. Từ tính chất 2) và 3) vừa nêu trên ta suy ra rằng $Im f$ là một vành con của S và $Ker f$ là một ideal của R .

Mệnh đề 3.1. Vành con J là một ideal của vành R khi và chỉ khi J là hạt nhân của đồng cấu vành nào đó.

Chứng minh. Theo nhận xét trên, hạt nhân của một đồng cấu vành $f : R \rightarrow S$ là một ideal của R . Ngược lại, nếu J là một ideal của vành R thì J là hạt nhân của phép chiếu tự nhiên $p : R \rightarrow R/J$. $\square$

Tương tự như định lý đồng cấu nhóm, trong lý thuyết vành chúng ta có định lý đồng cấu vành, hay còn gọi là *định lý về tính phổ dụng của vành thương*.

Định lý 3.2. Cho f là một đồng cấu vành từ R đến vành S . Khi đó tồn tại duy nhất đồng cấu vành $\varphi : R/\text{Ker } f \rightarrow S$ sao cho tam giác sau là giao hoán

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ & \searrow p \quad \nearrow \varphi & \\ & R/\text{Ker } f & \end{array}$$

và $\text{Im } \varphi = \text{Im } f$, trong đó $p : R \rightarrow R/\text{Ker } f$ là phép chiếu tự nhiên. Hơn nữa φ là đơn cấu.

Chứng minh. Đặt $K = \text{Ker } f$. Từ định lý đồng cấu nhóm suy ra quy tắc φ đặt tương ứng mỗi lớp $\bar{x} = x + K \in R/K$ với phần tử $f(x) \in S$, là một đơn cấu nhóm duy nhất thỏa mãn $f = \varphi \circ p$. Bây giờ ta còn phải thử lại rằng φ là một đồng cấu vành. Ta có

$$\begin{aligned} \varphi(\bar{x} \cdot \bar{y}) &= \varphi(\overline{xy}) = f(xy) \\ &= f(x)f(y) = \varphi(\bar{x}) \cdot \varphi(\bar{y}). \end{aligned} \quad \square$$

Định lý 3.2 còn có thể phát biểu ở dạng tổng quát hơn, như đã làm với các đồng cấu nhóm ở Định lý 5.5 Chương II. Bạn đọc có thể tự làm điều này và thực hiện phép chứng minh một cách không khó khăn gì.

Từ Định lý 3.2 ta suy ra ngay hệ quả sau.

Hệ quả 3.3. Nếu $f : R \rightarrow S$ là một đồng cấu vành thì vành thương $R/\text{Ker } f$ đẳng cấu với $\text{Im } f$.

Chứng minh. Theo định lý 3.2, ta có đơn cấu $\varphi : R/\text{Ker } f \rightarrow S$. Có thể xem φ là đồng cấu từ $R/\text{Ker } f$ đến $\text{Im } f$ và khi đó hiển nhiên φ là một toàn cấu. Bởi vậy φ là ánh xạ đẳng cấu

$$R/\text{Ker } f \cong \text{Im } f \quad \square$$

Định lý 3.4. Cho I và J là hai idêan của vành R . Khi đó

$$(I + J)/J \cong I/(I \cap J).$$

Chứng minh. Theo Định lý 2.7 ta có $I + J$ là một vành con của R , ngoài ra J là một idêan của $I + J$, và $I \cap J$ là idêan của I . Xét ánh xạ

$$\begin{aligned} \varphi : I &\rightarrow (I + J)/J \\ a &\mapsto a + J \end{aligned}$$

Theo phép chứng minh Hệ quả 5.10, Chương II, thì φ là một toàn cấu nhóm với hạt nhân $\text{Ker } \varphi = I \cap J$. Bây giờ, có thể thấy rằng φ còn là một đồng cấu vành. Từ đó theo Hệ quả 3.3 ta có đẳng cấu vành

$$I/(I \cap J) \cong (I + J)/J. \quad \square$$

Tích trực tiếp

Đối với hai vành $(R, +, \times)$ và $(S, +, \times)$, tổng trực tiếp của hai nhóm aben $(R, +)$ và $(S, +)$ là một vành với phép nhân cho bởi

$$(a, x)(b, y) = (ab, xy).$$

Vành này được gọi là *tích trực tiếp* của hai vành R và S , và ký hiệu bởi $R \times S$.

Một cách tổng quát ta cũng có thể định nghĩa tích trực tiếp $\prod_I R_i$ của một họ những vành $(R_i | i \in I)$. Mỗi phần tử của tích trực tiếp là một họ (a_i) , với $a_i \in R_i, i \in I$. Hai phép toán cộng và nhân được xác định bởi phép cộng và phép nhân theo từng thành phần, nghĩa là

$$\begin{aligned}(a_i) + (b_i) &= (a_i + b_i) \\ (a_i)(b_i) &= (a_i b_i)\end{aligned}$$

Vành con của tích trực tiếp $\prod_I R_i$ gồm tất cả các họ (a_i) , sao cho chỉ có một số hữu hạn thành phần $a_i \neq 0$, được gọi là *tổng trực tiếp* của các vành R_i , và ký hiệu bởi $\bigoplus_I R_i$.

Tổng trực tiếp $\bigoplus_I R_i$ trùng với tích trực tiếp $\prod_I R_i$ khi và chỉ khi I là tập hữu hạn. Do vậy,

$$R_1 \times R_2 \times \dots \times R_n = R_1 \oplus R_2 \oplus \dots \oplus R_n$$

Trong trường hợp các vành R_i đều là vành có đơn vị thì tích trực tiếp $\prod_I R_i$ có đơn vị là (e_i) , với e_i là đơn vị của vành R_i .

Mệnh đề 3.5. Các vành $\mathbb{Z}_{mn}$ và $\mathbb{Z}_m \times \mathbb{Z}_n$ đẳng cấu khi và chỉ khi m, n là hai số nguyên tố cùng nhau.

Chứng minh. Nếu $(m, n) = 1$ thì ánh xạ

$$f: \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$$

cho bởi

$$f(x + mn\mathbb{Z}) = (x + m\mathbb{Z}, x + n\mathbb{Z})$$

là một đẳng cấu nhóm. Ta có thể thử lại rằng f cũng là một đồng cấu vành. Thật vậy,

$$\begin{aligned} f[(x + mn\mathbb{Z})(y + mn\mathbb{Z})] &= f(xy + mn\mathbb{Z}) \\ &= (xy + m\mathbb{Z}, xy + n\mathbb{Z}) \\ &= (x + m\mathbb{Z}, x + n\mathbb{Z})(y + m\mathbb{Z}, y + n\mathbb{Z}) \\ &= f(x + mn\mathbb{Z})f(y + mn\mathbb{Z}) \end{aligned}$$

Nếu $(m, n) \neq 1$ ta đã chỉ ra rằng các nhóm cộng $\mathbb{Z}_{mn}$ và $\mathbb{Z}_m \times \mathbb{Z}_n$ không đẳng cấu và bởi vậy không thể có một đẳng cấu vành giữa chúng. $\square$

Biểu diễn thặng dư

Bây giờ chúng ta nêu một ứng dụng của dạng biểu diễn của một vành nào đó thành tích trực tiếp của các vành.

Cho $m = m_1 m_2 \dots m_r$, với m_i là các số nguyên tố cùng nhau từng đôi một. Chúng ta biết rằng có một đẳng cấu vành

$$\mathbb{Z}_m \cong \prod_i \mathbb{Z}_{m_i}$$

Qua đẳng cấu này mỗi x trong $\mathbb{Z}_m$ được biểu diễn duy nhất dưới dạng một bộ r số $(a_1, a_2, \dots, a_r)$, trong đó $x \equiv a_i \pmod{m_i}$. Khi đó ta nói rằng $(a_1, a_2, \dots, a_r)$ là một *biểu diễn thặng dư* của x .

Ví dụ, với $m = 30$ ta có đẳng cấu

$$\mathbb{Z}_{30} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

Do đó mỗi số nguyên từ 0 đến 29 có thể được biểu diễn một cách duy nhất theo các môđun thặng dư 2, 3 và 5 như trong bảng dưới đây.

Biểu diễn thặng dư các số nguyên từ 0 đến 29

x	Thặng dư môđun:			x	Thặng dư môđun:			x	Thặng dư môđun:		
	2	3	5		2	3	5		2	3	5
0	0	0	0	10	0	1	0	20	0	2	0
1	1	1	1	11	1	2	1	21	1	0	1
2	0	2	2	12	0	0	2	22	0	1	2
3	1	0	3	13	1	1	3	23	1	2	3
4	0	1	4	14	0	2	4	24	0	0	4
5	1	2	0	15	1	0	0	25	1	1	0
6	0	0	1	16	0	1	1	26	0	2	1
7	1	1	2	17	1	2	2	27	1	0	2
8	0	2	3	18	0	0	3	28	0	1	3
9	1	0	4	19	1	1	4	29	1	2	4

Nhờ đẳng cấu vành, phép cộng và phép nhân trong $\mathbb{Z}_m$ được biểu diễn một cách đơn giản bởi phép cộng và phép nhân của các biểu diễn thặng dư theo từng thành phần. Ví dụ, để cộng 4 và 7 sử dụng biểu diễn thặng dư, chúng ta có

$$(0, 1, 4) + (1, 1, 2) = (0 + 1, 1 + 1, 4 + 2) = (1, 2, 1).$$

Tương tự, nhân 4 và 7, chúng ta có

$$(0, 1, 4) \cdot (1, 1, 2) = (0 \cdot 1, 1 \cdot 1, 4 \cdot 2) = (0, 1, 3).$$

Biểu diễn thặng dư có ứng dụng quan trọng trong việc thiết kế các bộ cộng nhanh, bởi vì tất cả các thặng dư có thể được cộng cùng lúc. Các số có thể được dễ dàng chuyển thành dạng thặng dư; tuy nhiên, các chương trình ngược lại để tìm một số có biểu diễn thặng dư cho trước đòi hỏi sử dụng định lý dư Trung Hoa. Chúng ta có thể tìm hiểu sâu hơn về việc sử dụng biểu diễn thặng dư trong các tài liệu thuộc lĩnh vực khoa học máy tính.

Bài tập

3.1. Cho f là một đồng cấu vành từ R đến S (R và S là những vành giao hoán có đơn vị).

a) Chứng minh rằng nếu f là một toàn cấu và I là một ideal

của R thì $f(I)$ là idêan của S . Nếu f không là toàn cấu thì tính chất này còn đúng không? Tại sao?

b) Chứng minh rằng nếu P là một idêan nguyên tố của S thì $f^{-1}(P)$ là một idêan nguyên tố của R . Kết quả này còn đúng không nếu thay giả thiết "nguyên tố" bằng giả thiết "tối đại"? Tại sao?

3.2. Giả sử A là một vành, B là một tập hợp với hai phép toán cộng và nhân, $f: A \rightarrow B$ là một song ánh thỏa mãn:

$$(i) \forall a, b \in A, f(a+b) = f(a) + f(b).$$

$$(ii) \forall a, b \in A, f(ab) = f(a)f(b).$$

Chứng minh rằng B là một vành, hơn nữa B đẳng cấu với A .

3.3. Chứng minh rằng phương trình $x^3 - 5x^2 - x - 17 = 0$ không có nghiệm trong $\mathbb{Z}$.

3.4. Vành R được gọi là một vành *Bool* nếu $a^2 = a$ với mọi $a \in R$. Chứng minh rằng mỗi idêan nguyên tố P của vành Bool R là một idêan tối đại và $R/P \cong \mathbb{Z}_2$.

3.5. Chứng minh rằng

$$S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$$

là vành con của vành $M_2(\mathbb{R})$, đẳng cấu với $\mathbb{C}$.

3.6. Cho S là một vành. Đặt

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in S \right\};$$

$$A = \left\{ \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \mid a \in S \right\}$$

Chứng minh rằng A là một idêan của R và $R/A \cong S \times S$.

3.7. Giả sử $f: R \rightarrow R$ là một tự đồng cấu của vành R . Chứng minh rằng tập hợp

$$A = \{x \in R \mid f(x) = x\}$$

là một vành con của R .

3.8. Cho m và n là hai số nguyên, m chia hết n . Tìm idêan A của $\mathbb{Z}_n$ sao cho $\mathbb{Z}_n/A \cong \mathbb{Z}_m$.

3.9. Tìm tất cả các tự đồng cấu của vành $\mathbb{Z}[\sqrt{2}]$.

- 3.10. Chứng minh rằng có duy nhất một đồng cấu vành từ vành các số hữu tỷ $\mathbb{Q}$ đến vành các số nguyên $\mathbb{Z}$.
- 3.11. Hãy tìm tất cả các tự đồng cấu của vành các số nguyên $\mathbb{Z}$.
- 3.12. Tìm mọi tự đồng cấu của vành

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

- 3.13. Tìm mọi tự đồng cấu của vành

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

- 3.14. Tìm mọi đồng cấu từ vành từ $\mathbb{Z}$ đến $\mathbb{Z}_{10}$.
- 3.15. Tìm mọi đồng cấu từ $\mathbb{Z}_{15}$ đến $\mathbb{Z}_3$.
- 3.16. Tìm mọi tự đồng cấu của vành $\mathbb{Z} \times \mathbb{Z}$.
- 3.17. Tìm mọi đồng cấu từ $\mathbb{Z}_7$ đến $\mathbb{Z}_4$.
- 3.18. Hãy xác định vành các tự đồng cấu $\text{End}(\mathbb{Z}_2 \times \mathbb{Z}_2)$. Nó có là vành giao hoán không?
- 3.19. Chứng minh rằng $10^n \equiv 1 \pmod{9}$ đối với mọi số tự nhiên n . Từ đó chứng minh rằng một số nguyên là bội của 9 nếu và chỉ nếu tổng các chữ số của nó là bội của 9.
- 3.20. Tìm số các vành đẳng cấu có 3 phần tử.
- 3.21. Trên vành $(R, +, \times)$ xác định hai phép toán cho bởi

$$\begin{aligned} r \oplus s &= r + s + 1 \\ r \circ s &= r.s + r + s. \end{aligned}$$

Chứng tỏ rằng $(R, \oplus, \circ)$ là một vành đẳng cấu với vành $(R, +, \times)$.

- 3.22. Giả sử R là một vành tùy ý, $\mathbb{Z}$ là vành các số nguyên. Trên $R \times \mathbb{Z}$ ta định nghĩa các phép toán như sau:

$$\begin{aligned} (x_1, n_1) + (x_2, n_2) &= (x_1 + x_2, n_1 + n_2), \\ (x_1, n_1)(x_2, n_2) &= (x_1x_2 + n_1x_2 + n_2x_1, n_1n_2). \end{aligned}$$

Chứng minh rằng $R \times \mathbb{Z}$ là một vành có đơn vị, chứa một vành con đẳng cấu với R .

3.23. Cho $R = A \times B$ là tích Đề-các của hai vành A và B tùy ý. Chứng minh:

- a) R là một vành với phép cộng và nhân theo từng thành phần;
b) Các bộ phận

$$\begin{aligned}\overline{A} &= \{(a, 0) \mid a \in A\} \\ \overline{B} &= \{(0, b) \mid b \in B\}\end{aligned}$$

là những vành con của R theo thứ tự đẳng cấu với A và B ;

c) $\overline{A}$ và $\overline{B}$ là hai idêan của R thoả mãn các hệ thức:

$$\overline{A} \cap \overline{B} = \{(0, 0)\}, \quad R = \overline{A} + \overline{B}.$$

d) Giả sử A và B là những vành có đơn vị, hãy tìm các đơn vị của R , $\overline{A}$ và $\overline{B}$.

3.24. Tìm tập các tự đẳng cấu của trường

$$\mathbb{Q}(\sqrt{i}) = \{a + b\sqrt{i} \mid a, b \in \mathbb{Q}\},$$

với một giá trị xác định của $\sqrt{i}$.

3.25. Tìm tập các tự đẳng cấu của trường

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}.$$

3.26. Giả sử R là một vành và $a \in R$. Chứng minh rằng:

a) Ánh xạ

$$\begin{aligned}h_a : R &\rightarrow R \\ x &\mapsto ax\end{aligned}$$

là một tự đẳng cấu của nhóm cộng aben R .

b) Ánh xạ

$$\begin{aligned}h : R &\rightarrow \text{End}(R) \\ a &\mapsto h(a) = h_a\end{aligned}$$

là một đồng cấu vành từ R đến vành các tự đẳng cấu $\text{End}(R)$ của nhóm cộng giao hoán R .

c) Tìm $\text{Ker}h$. Chứng minh rằng h là đơn cấu khi R có đơn vị.

3.25. Giả sử $f : X \rightarrow Y$ là một đồng cấu từ vành X đến vành Y , A và B theo thứ tự là hai ideal của X và Y sao cho $f(A) \subset B$;

$$p : X \rightarrow X/A, \quad p' : Y \rightarrow Y/B$$

là các toàn cấu chính tắc. Chứng minh rằng tồn tại một đồng cấu duy nhất $\bar{f}$ từ X/A đến Y/B sao cho hình vuông

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ p \downarrow & & \downarrow p' \\ X/A & \xrightarrow{\bar{f}} & Y/B \end{array}$$

là giao hoán, tức là $\bar{f} \circ p = p' \circ f$.

3.26. Hãy tìm các tự đồng cấu của:

- a) trường các số hữu tỷ;
- b) trường các số thực;
- c) trường các số phức, giữ nguyên mọi số thực.

3.29. Cho I và J là hai ideal của vành giao hoán, có đơn vị R , và cho ánh xạ

$$\begin{aligned} p : R &\rightarrow (R/I) \times (R/J) \\ a &\mapsto (a + I, a + J) \end{aligned}$$

Hãy chứng minh:

- a) p là một đồng cấu;
- b) p là một toàn cấu khi và chỉ khi $I + J = R$;
- c) Hãy mở rộng các kết quả trên cho tập $I_1, I_2, \dots, I_n$ (với $n > 2$) những ideal của vành R .

3.30. Giả sử R là vành giao hoán, có đơn vị; A, B là hai ideal của R sao cho $R = A + B$. Chứng minh rằng

$$R/AB \cong (R/A) \times (R/B).$$

3.31. Cho m và n là hai số tự nhiên nguyên tố cùng nhau. Chứng minh đẳng cấu vành

$$\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$$

- 3.32.** Giả sử $f : V \rightarrow R$, $g : V \rightarrow Y$ là hai đồng cấu vành, với f là toàn cấu. Chứng minh các điều kiện sau đây là tương đương:
- Tồn tại đồng cấu $h : R \rightarrow Y$ sao cho $g = h \circ f$.
 - $\text{Ker } f \subseteq \text{Ker } g$.
 - Khi một trong các điều kiện trên được thoả mãn thì:
 - h là duy nhất;
 - h là đơn ánh nếu và chỉ nếu $\text{Ker } f = \text{Ker } g$.
 - h là toàn ánh nếu và chỉ nếu g là toàn ánh.

3.33. Cho $d = 7$ hoặc $d = 11$. Chứng minh

- Bộ phận

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$$

là một trường con của trường số thực $\mathbb{R}$;

- Các trường $\mathbb{Q}(\sqrt{11})$ và $\mathbb{Q}(\sqrt{7})$ không đẳng cấu với nhau.

4. Trường các thương

Trong mục này vành R được giả thiết là một miền nguyên.

Miền nguyên $\mathbb{Z}$ được chứa trong trường số hữu tỷ $\mathbb{Q}$. Hơn nữa $\mathbb{Q}$ là trường số bé nhất chứa $\mathbb{Z}$. Mở rộng điều này chúng ta sẽ chứng tỏ rằng mỗi miền nguyên đều nhúng được vào một trường tối thiểu, gọi là trường các thương của miền nguyên đó.

Trước hết ta hãy xét tình huống miền nguyên R chứa trong một trường F nào đó. Khi đó giao Q của tất cả các trường con của F , chứa R là trường con bé nhất của F chứa R . Trường con này được đặc trưng bởi mệnh đề sau.

Mệnh đề 4.1. Trường Q gồm tất cả các phần tử có dạng ab^{-1} , với $a, b \in R, b \neq 0$.

Chứng minh. Dễ thấy $0, 1 \in Q$. Bây giờ ta chứng tỏ Q đóng kín đối với phép trừ và phép nhân. Thật vậy,

$$\begin{aligned} ab^{-1} - cd^{-1} &= ad(bd)^{-1} - cb(bd)^{-1} = (ad - bc)(bd)^{-1} \in Q \\ (ab^{-1}).(cd^{-1}) &= (ac)(bd)^{-1} \in Q. \end{aligned}$$

Bởi vậy Q là một trường con của K . Hơn nữa, với mọi $r \in R$ thì $r = r1^{-1} \in Q$ nên $R \subset Q$.

Nếu F là một trường con của K và chứa R thì rõ ràng F cũng chứa Q . Điều này chứng tỏ Q là trường con bé nhất của K , chứa R . $\square$

Bây giờ ta xét bài toán: *Đối với mỗi miền nguyên R có hay không một trường tối thiểu Q chứa R như một vành con?* Câu trả lời là có và chúng ta có thể xây dựng trường Q xuất phát từ R như sau.

Giả sử R là một miền nguyên. Xét tập hợp

$$R \times R^* = \{(a, b) | a, b \in R, b \neq 0\}$$

gồm các cặp phần tử của R có thành phần thứ hai khác không. Dựa trên sự kiện, trong trường số hữu tỷ $\frac{a}{b} = \frac{c}{d}$ nếu và chỉ nếu $ad = bc$, ta xác định quan hệ hai ngôi trên R cho bởi

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Ta thử lại rằng đây là một quan hệ tương đương:

(i) $(a, b) \sim (a, b)$ do $ab = ba$.

(ii) Nếu $(a, b) \sim (c, d)$ thì $ad = bc$. Điều này kéo theo $cb = da$ và do đó $(c, d) \sim (a, b)$.

(iii) Nếu $(a, b) \sim (c, d)$ và nếu $(c, d) \sim (e, f)$ thì $ad = bc$ và $cf = de$. Điều này kéo theo

$$(af - be)d = (ad)f - b(ed) = bcf - bcf = 0.$$

Do R không có ước của không và $d \neq 0$, đẳng thức trên cho ta $af - be = 0$, nghĩa là $(a, b) \sim (e, f)$.

Như vậy quan hệ $\sim$ là phản xạ, đối xứng, bắc cầu, và do đó là một quan hệ tương đương. Để cho gọn ta sẽ ký hiệu lớp tương đương (a, b) chứa cặp (a, b) của $R \times R^*$ là $\frac{a}{b}$ và ký hiệu tập thương gồm các lớp tương đương đó là Q .

Được gợi ý bởi các phép toán cộng và nhân trong trường số hữu tỷ Q ta xây dựng hai phép toán trong Q để Q trở thành một trường như sau.

Định lý 4.2. *Tập thương Q cùng với hai phép toán*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

là một trường. Hơn nữa Q chứa R như một vành con.

Ta gọi Q là trường các thương của R .

Chứng minh. Trước hết có thể chứng minh được rằng các quy tắc cộng và nhân nói trên không phụ thuộc vào đại diện $(a, b), (c, d)$ của các lớp. Ta chứng minh điều này cho phép cộng. Giả sử

$$(a, b) \sim (a', b') \text{ và } (c, d) \sim (c', d')$$

Thế thì $ab' = ba'$ và $cd' = dc'$. Do đó

$$\begin{aligned}(ad + bc)(b'd') &= (ab')dd' + bb'(cd') = (a'b)dd' + bb'(c'd) \\ &= (a'd' + b'c')(bd)\end{aligned}$$

và như vậy

$$\frac{ad + bc}{bc} = \frac{a'd' + b'c'}{b'd'}$$

Điều này chứng tỏ rằng định nghĩa của phép cộng là hợp lý. Cũng như vậy, $acb'd' = a'c'bd$, nghĩa là

$$\frac{ac}{bd} = \frac{a'c'}{b'd'}$$

và định nghĩa của phép nhân là hợp lý.

Sau đó có thể kiểm tra được rằng với hai phép toán này Q là một vành giao hoán, có đơn vị. Trong vành Q phần tử không là $\frac{0}{1}$, phần tử đối của $\frac{a}{b}$ là $-\frac{a}{b} = \frac{-a}{b}$, và phần tử đơn vị là $\frac{b}{b} = \frac{1}{1}$ với mọi $b \in R^*$, phần tử nghịch đảo của phần tử khác không $\frac{a}{b}$ là $\frac{b}{a}$, do $a \neq 0$. Bởi vậy Q là một trường. (Các chứng minh chi tiết xin dành cho bạn đọc).

Bây giờ chúng ta sẽ chứng tỏ rằng có một đơn cấu vành từ R đến Q . Xét ánh xạ

$$\varphi: R \rightarrow Q, r \mapsto \frac{r}{1}$$

Dễ thấy đó là một đồng cấu vành. Ta có

$$\begin{aligned}\text{Ker } \varphi &= \{r \mid \frac{r}{1} = 0\} = \{r \mid \overline{(r, 1)} = \overline{(0, 1)}\} \\ &= \{r \mid (r, 1) \sim (0, 1)\} = \{r \mid r.1 = 1.0\} = \{0\}\end{aligned}$$

Điều này chứng tỏ φ là một đơn cấu. Do φ là một đơn cấu nên ta có thể đồng nhất R với ảnh của nó bởi $a \equiv \varphi(a)$ và xem R như là một vành con của Q . $\square$

Nhận xét. Mỗi phần tử của trường các thương Q viết được dưới dạng ab^{-1} , với $a, b \in R, b \neq 0$. Thật vậy,

$$\frac{a}{b} = \frac{a}{1} \times \frac{1}{b} = \frac{a}{1} \times \left(\frac{b}{1}\right)^{-1} \equiv ab^{-1}.$$

Từ đó ta có ngay các hệ quả sau.

Hệ quả 4.3. Trường số hữu tỷ $\mathbb{Q}$ là trường các thương của vành các số nguyên $\mathbb{Z}$.

Chứng minh. Điều này suy ra trực tiếp từ Định lý 4.1 khi ta lấy $R = \mathbb{Z}$. Khi đó hai cặp $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}^*$ là tương đương khi và chỉ khi hai phân số $\frac{a}{b}, \frac{c}{d}$ là bằng nhau. $\square$

Hệ quả 4.4. Trường các thương của miền nguyên R là trường tối thiểu chứa R .

Chứng minh. Thật vậy, giả sử A là một trường con của F , chứa trường các thương Q của miền nguyên $\mathbb{R}$. Khi đó nếu $x \in Q$ thì $x = ab, a, b \in \mathbb{R}, a \neq 0$. Do A là trường chứa $\mathbb{R}$ nên từ đó suy ra $x \in A$ và bởi vậy $Q \subset A$. $\square$

Mệnh đề này có nghĩa là nếu F là một trường nào đó chứa miền nguyên R thì F chứa một trường các thương của R .

Đặc số

Định nghĩa. Cho R là một vành giao hoán, có đơn vị e . R được gọi là vành có đặc số 0 (tương ứng, đặc số $n, 0 < n < \infty$) nếu trong nhóm cộng R , phần tử e có cấp vô hạn (tương ứng, có cấp n).

Chú ý. Từ định nghĩa cấp của một phần tử ta suy ra rằng:

a) Nếu vành R có đặc số 0 thì $n = 0$ là số tự nhiên duy nhất sao cho $ne = 0$.

b) Nếu vành R có đặc số n thì n là số nguyên bé nhất trong các số nguyên dương k sao cho $ke = 0$.

Ví dụ

1. Vành số nguyên $\mathbb{Z}$ và mọi vành mở rộng của $\mathbb{Z}$ đều là những vành có đặc số 0.

2. Vành $\mathbb{Z}_m$ ($m \geq 2$) là vành có đặc số m .

Định lý 4.5. (i) Trong vành R có đặc số $n \neq 0$ thì $nx = 0$ với mọi $x \in R$.

(ii) Nếu miền nguyên có đặc số $n \neq 0$ thì n là số nguyên tố.

Chứng minh. Giả sử $n \neq 0$ là đặc số của vành R . Gọi e là đơn vị của vành R . Khi đó ta có $ne = 0$. Với mọi $x \in R$, $x = ex$, suy ra

$$nx = \underbrace{x + \dots + x}_n = \underbrace{ex + \dots + ex}_n = \underbrace{(e + \dots + e)}_n x = (ne)x = 0.$$

Bây giờ giả sử R là miền nguyên, có đặc số $n \neq 0$. Nếu n không phải là số nguyên tố thì n là một hợp số, $n = pq$, $1 < p, q < n$. Do $p, q < n$ nên $pe \neq 0$ và $qe \neq 0$. Tuy nhiên, khi đó

$$(pe)(qe) = \underbrace{(e + \dots + e)}_p \underbrace{(e + \dots + e)}_q = \underbrace{e + \dots + e}_{pq} = ne = 0.$$

Điều đó có nghĩa là R có ước của 0, trái với giả thiết R là một miền nguyên. Vậy n phải là một số nguyên tố. $\square$

Khái niệm đặc số cho ta một mô tả về cấu trúc của trường thông qua hai trường quen thuộc $\mathbb{Z}_p$ và $\mathbb{Q}$.

Định lý 4.6. Cho F là một trường. Nếu F có đặc số 0 thì F chứa trường con đẳng cấu với trường số hữu tỷ $\mathbb{Q}$. Nếu F có đặc số $p \neq 0$ thì F chứa trường con đẳng cấu với trường $\mathbb{Z}_p$ các lớp thặng dư theo môđun p .

Chứng minh. Giả sử F là một trường với đơn vị e . Xét ánh xạ

$$\begin{aligned} f: \mathbb{Z} &\rightarrow F, \\ n &\mapsto ne. \end{aligned}$$

Dễ thấy f là một đồng cấu vành. Nếu F có đặc số 0 thì

$$\text{Ker } f = \{x \in \mathbb{Z} \mid xe = 0\} = \{0\}.$$

bởi vậy f là một đơn cấu. Từ đó suy ra $\mathbb{Z}$ đẳng cấu với $f(\mathbb{Z})$. Hơn nữa do F là một trường nên F chứa trường các thương của $f(\mathbb{Z})$. Trường này đẳng cấu với trường các thương của $\mathbb{Z}$ là trường các số hữu tỷ $\mathbb{Q}$.

Nếu F có đặc số nguyên tố p thì

$$\text{Ker } f = \{x \in \mathbb{Z} \mid xe = 0\} = \{x \in \mathbb{Z} \mid x:p\} = p\mathbb{Z}.$$

Theo định lý đồng cấu

$$\text{Im } f \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p.$$

□

Bài tập

4.1. Cho I là một ideal của vành giao hoán R . Chứng minh rằng I là ideal nguyên tố khi và chỉ khi I là hạt nhân của một đồng cấu vành từ R vào một trường.

4.2. Giả sử R là một trường với phần tử đơn vị e . Xét bộ phận

$$A = \{ne \mid n \in \mathbb{Z}\}.$$

a) Chứng minh A là một vành con của vành R , A có phải là một miền nguyên không?

b) Chứng minh A đẳng cấu với vành các số nguyên $\mathbb{Z}$ khi R có đặc số 0, và đẳng cấu với trường các số nguyên $\text{mod } p$, khi R có đặc số p .

4.3. Giả sử A là một vành con của một trường F . Chứng minh rằng nếu A có nhiều hơn một phần tử và A có đơn vị thì phần tử đơn vị của A trùng với phần tử đơn vị của F , và lúc đó A là một miền nguyên.

4.4. Giả sử p là một số nguyên tố. Chứng minh rằng tập hợp các số hữu tỷ có dạng m/n , trong đó n nguyên tố với p , là một miền nguyên. Tìm trường các thương của miền nguyên này.

5. Vành, trường sắp thứ tự

Trong mục này vành R đã cho được giả thiết là vành giao hoán và có đơn vị 1.

Định nghĩa và ví dụ

Định nghĩa. Cho R là một vành giao hoán có đơn vị 1. Nếu trong R có một quan hệ thứ tự toàn phần $\leq$ thoả mãn các điều kiện sau với mọi $a, b, c \in R$:

- (i) $a \leq b$ kéo theo $a + b \leq b + c$,
- (ii) $0 < a$ và $0 < b$ kéo theo $0 < ab$,

thì R được gọi là một *vành sắp thứ tự*.

Một trường được gọi là *sắp thứ tự* nếu nó là một vành sắp thứ tự.

Ví dụ

1. Vành số nguyên $\mathbb{Z}$ với quan hệ $\leq$ được xác định bởi điều kiện " $a \leq b$ khi và chỉ khi tồn tại số tự nhiên c sao cho $a + c = b$ " là một vành sắp thứ tự.
2. Trường số hữu tỷ $\mathbb{Q}$ với quan hệ $\leq$ được xác định bởi điều kiện " $a \leq b$ khi và chỉ khi $b - a$ là số dương" là một trường sắp thứ tự.

Phần tử dương, phần tử âm

Định nghĩa. Phần tử a thuộc vành sắp thứ tự R được gọi là *phần tử dương* nếu $0 < a$ và gọi là *phần tử âm* nếu $a < 0$.

Đặt $P = \{a \in R \mid 0 < a\}$ là tập các phần tử dương của vành sắp thứ tự R , và đặt $-P = \{-a \in R \mid a \in P\}$

Khi đó ta có các tính chất sau:

1. $0 < a$ khi và chỉ khi $-a < 0$, và do đó

$$P \cap (-P) = \emptyset, \quad P \cup \{0\} \cup (-P) = R$$

2. Nếu $a, b \in P$ thì $a + b \in P$ và $ab \in P$.

3. Với mọi $a, b \in R$, với mọi $c \in P, a \leq b$ kéo theo $ac \leq bc$.

Từ những tính chất vừa nêu chúng ta có thể đưa ra một điều kiện đủ để một vành là sắp thứ tự.

Định lý 5.1. Nếu trong vành R có một tập con P thỏa mãn các điều kiện:

- (i) $a, b \in P$ kéo theo $a + b \in P$,
- (ii) $a, b \in P$ kéo theo $ab \in P$,
- (iii) $P \cap (-P) = \emptyset, P \cup \{0\} \cup (-P) = R$

thì trong R có một quan hệ thứ tự để R trở thành một vành sắp thứ tự.

Chứng minh. Quan hệ $\leq$ trong R được xác định như sau

$$a \leq b \Leftrightarrow \exists c \in P \text{ sao cho } a + c = b$$

Ta có thể chứng minh được $\leq$ là một quan hệ thứ tự toàn phần và R cùng với quan hệ $\leq$ là một vành sắp thứ tự. Việc chứng minh chi tiết xin dành cho bạn đọc. $\square$

Bổ đề 5.2. Cho $(R, \leq)$ là một vành sắp thứ tự. Khi đó:

- (i) $x^2 \geq 0$ với mọi $x \in R$, và $1 > 0$.
- (ii) R là vành có đặc số 0.

Chứng minh. (i) Nếu $x > 0$ thì $x^2 > 0$, còn nếu $x = 0$ thì $x^2 = 0$. Sau cùng, nếu $x < 0$ thì $-x > 0$. Từ đó, theo quy tắc nhân dấu ta có $x^2 = (-x)^2 > 0$.

Đặc biệt ta có $1 = 1^2 > 0$.

(ii) Ta chứng minh bởi $n1$ là phần tử dương với mọi số nguyên dương n bằng quy nạp theo n . Trường hợp $n = 1$ đã được xét tới trong câu a). Giả sử $n1 > 0$ với $n = k > 0$. Khi đó ta có

$$(k+1)1 = k1 + 1 > 0 + 1 = 1 > 0.$$

Từ đó suy ra $n1 > 0$ với mọi $n > 0$. Điều đó chứng tỏ vành R có đặc số 0. $\square$

Nhận xét. Từ câu (ii) suy ra rằng mọi trường sắp thứ tự đều chứa một trường con đẳng cấu với trường số hữu tỷ $\mathbb{Q}$.

Từ câu (i) suy ra rằng không có một quan hệ thứ tự nào trong tập các số phức $\mathbb{C}$ để trường này trở thành một trường sắp thứ tự, vì $i^2 = -1 < 0$.

Định lý 5.3. *Giả sử R là một miền nguyên sắp thứ tự. Q là trường các thương của miền nguyên R . Khi đó trong Q có duy nhất một tập các phần tử dương P sao cho Q là một trường sắp thứ tự và $P \cap R$ là tập các phần tử dương của R .*

Chứng minh. Tính duy nhất. Trước hết ta nhắc lại rằng

$$Q = \left\{ \frac{a}{b} \mid a, b \in R; b \neq 0 \right\}$$

trong đó

$$\begin{aligned} \frac{a}{b} &= \overline{(a, b)} \\ \overline{(a, b)} &= \overline{(c, d)} \Leftrightarrow ad = bc. \end{aligned}$$

Giả sử quan hệ thứ tự trên miền nguyên R đã được kéo dài tới một quan hệ thứ tự trên trường các thương Q của nó. Rõ ràng

$$\frac{a}{b} > 0 \Rightarrow \frac{a}{b} b^2 = ab > 0$$

Ngược lại, nếu $ab > 0$ trong R thì

$$ab(b^{-1})^2 = \frac{a}{b} > 0.$$

Điều này nói lên tính duy nhất của sự kéo dài quan hệ thứ tự từ R lên Q .

Sự tồn tại. Ta định nghĩa phần tử dương trong Q bởi

$$\frac{a}{b} > 0 \Leftrightarrow ab > 0.$$

Định nghĩa nói trên là không phụ thuộc vào đại diện. Thật vậy, nếu $\frac{a}{b} = \frac{c}{d}$ thì $ad = bc$.

Từ đó $(ab)d^2 = (cd)b^2$. Vì $d^2 > 0, b^2 > 0$ nên $ab > 0$, kéo theo $cd > 0$, nghĩa là $\frac{c}{d} > 0$.

Bây giờ ta chứng minh tập

$$\overline{P} = \left\{ \frac{a}{b} \in R \mid ab > 0 \right\}$$

thoả mãn các điều kiện của tập các số dương nói trong Định lý 5.1. Nếu $a, b \in R$ là những phần tử khác không thì chỉ một trong hai phần tử $ab, (-ab)$ là dương, vì vậy hoặc $\frac{a}{b} > 0$ hoặc $-\frac{a}{b} = \frac{-a}{b} > 0$, và chỉ xảy ra một trong hai trường hợp.

Nếu $\frac{a}{b} > 0$ thì $ab > 0, cd > 0$. Khi đó

$$abd^2 > 0, cdb^2 > 0$$

Từ đó

$$(ad + bc)bd = abd^2 + cdb^2 > 0,$$

nghĩa là $\frac{a}{b} + \frac{c}{d} > 0$. Sau cùng ta có

$$(ac)(bd) = (ab)(cd) > 0,$$

nghĩa là $\frac{a}{b} \cdot \frac{c}{d} > 0$.

Đối với trường hợp $-\frac{a}{b} > 0$ chúng ta lập luận tương tự.

Quan hệ thứ tự vừa xác định trên Q là kéo dài của quan hệ thứ tự đã cho trên R . Thật vậy với $a \in R$ thì $a = \frac{a}{1}$, do đó

$$\frac{a}{1} > 0 \Leftrightarrow a \cdot 1 = a > 0,$$

nghĩa là $a > 0$ trong R khi và chỉ khi $a = \frac{a}{1} > 0$ trong Q . □

Định nghĩa. Vành R được gọi là một *vành sắp thứ tự Acsimet* nếu $(R, \leq)$ là một vành sắp thứ tự và với mọi a, b thuộc R , $0 < a$, tồn tại số tự nhiên n sao cho $b < na$.

Trường F được gọi là *trường sắp thứ tự Acsimet* nếu $(F, \leq)$ là một vành sắp thứ tự Acsimet.

Ví dụ

1. Vành số nguyên là một vành sắp thứ tự Acsimet.

2. Trường số hữu tỷ, trường số thực là những trường sắp thứ tự Acsimet. Ta có nhận xét rằng nếu R là một trường sắp thứ tự thì nó có đặc số 0 và vì vậy có thể nhúng trường số hữu tỷ $\mathbb{Q}$ vào R như một trường con. Với nhận xét này ta có thể phát biểu mệnh đề sau.

Định lý 5.4. Mọi trường sắp thứ tự Acsimet F đều trù mật hữu tỷ theo nghĩa với mọi a, b thuộc F , $a < b$, đều tồn tại số hữu tỷ q sao cho $a < q < b$.

Chứng minh. Giả sử $a, b \in F$, $a < b$. Khi đó $b - a > 0$. Do F sắp thứ tự Acsimet nên tồn tại $n \in \mathbb{N}$ sao cho

$$1 < n(b - a) = nb - na \Rightarrow 1 + na < nb.$$

Xét tập hợp

$$A = \{x \in F \mid na < x\}$$

Đối với hai phần tử 1 và na tồn tại số tự nhiên m (do F sắp thứ tự Acsimet) sao cho $m = m1 > na$. Điều này chứng tỏ $m \in A$ và do đó $A \neq \emptyset$. Hơn nữa, A bị chặn dưới nên A có phần tử bé nhất k . Ta chứng tỏ $k < nb$. Thật vậy, nếu ngược lại, $k \geq nb$, thì

$$k > na + 1 \Rightarrow k - 1 > na.$$

Điều này chứng tỏ $k - 1 \in F$, trái với giả thiết về tính bé nhất của k . Như vậy ta có

$$na < k < nb \Rightarrow a < \frac{k}{n} < b.$$

Do $\frac{p}{q} \in \mathbb{Q}$ nên ta có điều phải chứng minh. □

Bài tập

5.1. Chứng minh các tính chất sau đây trong vành sắp thứ tự R :

- a) $a + x < a + y \Rightarrow x < y$;
- b) $a - x < a - y \Rightarrow x > y$;
- c) Với $c > 0$, từ $a \leq b$ suy ra $ac \leq bc$;
- d) Với $c < 0$, từ $a \leq b$ suy ra $bc \leq ac$;
- e) Với $a > 0$, từ $ax < ay$ suy ra $x < y$;
- f) Với $a < 0$, từ $ax < ay$ suy ra $y < x$;
- g) Nếu $a \neq 0$ thì $a^2 > 0$.

5.2. Cho R là một vành sắp thứ tự với P là tập các phần tử dương của R , và A là một vành con chứa đơn vị của R . Chứng minh rằng A là một vành sắp thứ tự với tập con dương là $A \cap P$.

5.3. Trong một vành sắp thứ tự, định nghĩa giá trị tuyệt đối của phần tử a là một phần tử $|a|$ cho bởi

$$\begin{aligned}|a| &= a \text{ nếu } a > 0, \\|a| &= 0 \text{ nếu } a = 0, \\|a| &= -a \text{ nếu } a < 0.\end{aligned}$$

Chứng minh các quy tắc sau:

$$\begin{aligned}|ab| &= |a| \cdot |b|; \\|a + b| &\leq |a| + |b|; \\-|a| &\leq a \leq |a|; \\|a| - |b| &\leq |a - b|.\end{aligned}$$

5.4. Cho R là một trường sắp thứ tự; $x, y \in R$ là hai phần tử mà $x < y$. Chứng minh tồn tại phần tử $z \in R$ sao cho $x < z < y$.

Chương V

VÀNH ĐA THỨC VÀ VÀNH OCLIT

1. *Vành đa thức*
2. *Thuật toán chia trong miền nguyên*
3. *Vành chính*
4. *Vành Oclit (Euclide)*

Trong lý thuyết vành, vành các số nguyên $\mathbb{Z}$ là một trong những vành cụ thể, được biết rõ nhất. Ngoài vai trò là ví dụ minh họa cho nhiều khái niệm, sự kiện, nó còn là một mô hình cơ sở để từ đó khái quát thành những lớp vành mới có nhiều ứng dụng rộng rãi. Trong chương này chúng ta sẽ đề cập tới một lớp vành cụ thể khác, đóng vai trò cơ bản trong đại số cũng như trong nhiều ngành toán học, là vành các đa thức. Vành các đa thức $F(x)$ trên một trường F có nhiều tính chất giống với vành các số nguyên $\mathbb{Z}$, trong đó đặc biệt phải kể đến tính nhân tử hoá và thuật toán Oclit. Những lớp vành tổng quát có thuật toán này sẽ được trình bày với những nét cơ bản nhất.

1. Vành đa thức

Cho R là một vành giao hoán có đơn vị $1 \neq 0$. Một đa thức của x trên vành R là một biểu thức dạng

$$f(x) = a_0 + a_1x + \cdots + a_nx^n,$$

trong đó $a_0, \dots, a_n \in R$ và $a_n \neq 0$ nếu $n > 0$. Phần tử a_i được gọi là hệ tử của x^i trong $f(x)$. Nếu hệ tử của x^i là 0 thì hạng tử $0x^i$ có thể bỏ đi, và nếu hệ tử của x^i là 1 thì ta viết x^i thay cho $1x^i$. Phần tử a_n được gọi là hệ tử cao nhất của $f(x)$.

Hai đa thức $f(x)$ và $g(x)$ được gọi là *bằng nhau* nếu các hệ tử tương ứng của x^i trong cả hai đa thức bằng nhau. Đặc biệt

$$a_0 + a_1x + \cdots + a_nx^n = 0$$

nếu và chỉ nếu $a_0 = a_1 = \cdots = a_n = 0$. Nếu n là số tự nhiên lớn nhất sao cho $a_n \neq 0$ thì ta sẽ nói n là bậc của $f(x)$, và ký hiệu $n = \deg f(x)$. Nếu mọi hệ tử của $f(x)$ đều bằng không thì $f(x)$ được gọi là *đa thức không*, và bậc của nó không được định nghĩa.

Như vậy, các đa thức bậc 0 là mọi phần tử khác không a thuộc R , chúng còn được gọi là các *đa thức hằng*.

Tập hợp tất cả các đa thức của x trên vành giao hoán R ký hiệu bởi $R[x]$. Đối với hai đa thức trên R

$$a(x) = \sum_{i=0}^n a_i x^i, \quad b(x) = \sum_{i=0}^m b_i x^i$$

phép cộng và phép nhân được xác định bởi

$$a(x) + b(x) = \sum_{i=0}^s (a_i + b_i) x^i, \quad \text{với } s = \max(m, n);$$

$$a(x) \cdot b(x) = \sum_{i=0}^{m+n} c_i x^i, \quad \text{ở đó } c_k = \sum_{i+j=k} a_i b_j$$

Một cách không khó khăn ta có thể thử lại rằng tập hợp $R[x]$ cùng với hai phép toán vừa nêu thoả mãn mọi tiên đề của một vành giao hoán có đơn vị. Đóng vai trò phần tử không là đa thức không 0 và phần tử đơn vị là đa thức hằng 1.

Ví dụ trong vành $\mathbb{Z}_5[x]$ ta có

$$(2x^3 + 2x^2 + 1) + (3x^2 + 4x + 1) = 2x^3 + 4x + 1, \text{ và}$$

$$(2x^3 + 2x^2 + 1)(3x^2 + 4x + 1) = x^5 + 4x^4 + 4x + 1.$$

(Ta lưu ý rằng trong vành đa thức $\mathbb{Z}_m[x]$ các hệ tử được rút gọn theo môđun m .)

Phép dựng vành đa thức của ẩn x có thể mở rộng cho đa thức n biến $x_1, x_2, \dots, x_n$ với hệ tử trên vành R . Chúng ta có thể định nghĩa bằng quy nạp

$$R[x_1, x_2, \dots, x_n] = R[x_1, x_2, \dots, x_{n-1}][x_n]$$

Chẳng hạn trong vành đa thức hai biến $R[x, y] = R[x][y]$ mỗi đa thức $f(x, y)$ có dạng

$$f = k_0 + k_1 y + k_2 y^2 + \dots + k_n y^n$$

trong đó $k_i = k_i(x)$ là những đa thức của ẩn x .

Bây giờ chúng ta quay về với vành đa thức một ẩn $R[x]$.

Bổ đề 1.1. Nếu R là một miền nguyên và $f(x), g(x)$ là hai đa thức khác không của vành $R[x]$ thì

$$\deg(f(x).g(x)) = \deg f(x) + \deg g(x).$$

Chứng minh. Giả sử

$$f(x) = a_0 + a_1 x + \dots + a_n x^n, \quad a_n \neq 0$$

$$g(x) = b_0 + b_1 x + \dots + b_m x^m, \quad b_m \neq 0$$

Khi đó

$$f(x).g(x) = c_0 + c_1 x + \dots + c_{n+m} x^{n+m}$$

trong đó $c_k = \sum_{i+j=k} a_i b_j$, nói riêng $c_{n+m} = a_n b_m$. Do R là miền nguyên nên từ $a_n \neq 0, b_m \neq 0$ suy ra $c_{n+m} \neq 0$.

Đó là điều phải chứng minh. □

Nếu vành hệ tử R không là miền nguyên thì bậc của tích có thể nhỏ hơn tổng các bậc. Ví dụ trong $\mathbb{Z}_6[x]$ thì $(2x^3 + 3)(3x) = 3x$.

Hệ quả 1.2. Nếu R là một miền nguyên thì vành đa thức $R[x]$ cũng là miền nguyên.

Chứng minh. Thật vậy, nếu $f(x) \neq 0$ và $g(x) \neq 0$ thì

$$\deg(f(x).g(x)) = \deg f(x) + \deg g(x).$$

Từ đó $f(x).g(x) \neq 0$. Điều này chứng tỏ $R[x]$ là miền nguyên. □

Hệ quả 1.3. Nếu R là một trường thì trong vành $R[x]$ các hằng khác không là những phần tử khả nghịch và chỉ có chúng.

Chứng minh. Thật vậy, nếu $f(x)$ khả nghịch thì tồn tại $g(x) \in R[x]$ sao cho $f(x).g(x) = 1$, do đó

$$\deg f(x) + \deg g(x) = 0 \Rightarrow \deg f(x) = 0,$$

hay $f(x)$ là hằng. Điều ngược lại là hiển nhiên.

Chú ý. Giả sử $f(x)$ là một đa thức trên vành R . Khi thay ẩn x bởi một phần tử bất kỳ $c \in R$ ta được một phần tử xác định thuộc R . Như vậy có thể xem đa thức $f(x)$ như một hàm từ R tới R .

Ta cần lưu ý rằng hai đa thức $f(x), g(x)$ được xem là hai hàm bằng nhau nếu và chỉ nếu $f(c) = g(c)$ với mọi $c \in R$. Ta có thể nêu ví dụ hai đa thức khác nhau nhưng lại là hai hàm bằng nhau. Thật vậy, với $R = \mathbb{Z}_3$ thì hai đa thức $f(x) = x^3 - x$ và $g(x) = 0$ cùng xác định một hàm là hàm *đồng nhất không*. Bởi vậy tương ứng đa thức $f(x)$ với hàm

$$\begin{aligned} f : R &\rightarrow R \\ c &\mapsto f(c) \end{aligned}$$

không là 1-1. □

Phép chia và phép chia với dư

Vành đa thức $F(x)$ trên trường F có một tính chất quan trọng, tương tự như trong vành các số nguyên $\mathbb{Z}$, là thuật toán *chia với dư*. Trong vành này khái niệm đa thức bất khả quy là một khái niệm có vai trò giống như các số nguyên tố.

Định lý 1.4. Cho R là một miền nguyên và $a(x), b(x)$ là hai đa thức trong $R[x]$, ngoài ra hệ tử cao nhất của $b(x)$ khả nghịch trong R . Khi đó tồn tại duy nhất cặp đa thức $q(x), r(x) \in R[x]$ sao cho

$$a(x) = b(x).q(x) + r(x),$$

với $\deg r(x) < \deg b(x)$ nếu $r(x) \neq 0$.

Chứng minh. a) Sự tồn tại. Giả sử

$$\begin{aligned} a(x) &= a_0 + a_1x + \cdots + a_nx^n, \quad a_n \neq 0 \\ b(x) &= b_0 + b_1x + \cdots + b_mx^m, \quad b_m \neq 0. \end{aligned}$$

Nếu $n < m$ ta đặt $q(x) = 0$, $r(x) = a(x)$.

Nếu $n \geq m$ ta đặt

$$\begin{aligned}a_1(x) &= a(x) - b_m^{-1}a_n x^{n-m}b(x) \\ &= a(x) - q_1(x)b(x).\end{aligned}$$

Bậc của đa thức này không lớn hơn $m-1$ bởi vì các hệ tử cao nhất của $a(x)$ và $q_1(x)b(x)$ trùng nhau và bằng $b_m^{-1}a_nb_m = a_n$. Tiếp tục quá trình trên ta được

$$a_k(x) = a_{k-1}(x) - q_k(x)b(x), \quad k = 1, 2, 3, \dots$$

Rõ ràng sau không quá $n-m+1$ bước ta sẽ được đa thức $a_k(x) = 0$. Khi đó

$$q(x) = q_1(x) + q_2(x) + \dots + q_k(x); \quad r(x) = a_{k-1}(x).$$

b) *Tính duy nhất.* Giả sử còn có

$$a(x) = q'(x)b(x) + r'(x),$$

với $\deg r'(x) < \deg b(x)$ nếu $r'(x) \neq 0$. Khi đó

$$r(x) - r'(x) = (q'(x) - q(x))b(x).$$

Nếu $r(x) \neq r'(x)$ thì ta cũng có $q'(x) \neq q(x)$ và khi đó

$$\deg(r(x) - r'(x)) = \deg(q'(x) - q(x)) + \deg b(x) \geq \deg b(x).$$

Điều này là vô lý vì

$$\deg(r(x) - r'(x)) \leq \max(\deg r(x), \deg r'(x)) < \deg b(x).$$

Bởi vậy phải có $r(x) = r'(x)$. Do $R[x]$ là miền nguyên nên từ đó $q(x) = q'(x)$. $\square$

Hệ quả đầu tiên được suy ra từ định lý quan trọng này là:

Bổ đề 1.5. Mọi ideal trong vành đa thức $F[x]$ trên trường F đều là ideal chính.

Chứng minh. Giả sử I là ideal của vành $R[x]$. Nếu $I = 0$ thì I sinh bởi phần tử 0. Bây giờ giả sử $I \neq 0$. Chọn trong I phần tử $p(x)$ có bậc nhỏ nhất. Khi đó với phần tử $f(x)$ bất kỳ thuộc I ta có

$$f(x) = p(x)q(x) + r(x),$$

với $r = 0$ hoặc $\deg r < \deg p$ nếu $r \neq 0$. Bởi vì

$$r(x) = f(x) - p(x)q(x) \in I$$

và do giả thiết về $p(x)$ nên ta phải có $r(x) = 0$. Điều này chứng tỏ

$$f(x) = p(x)q(x) \in p(x)R[x].$$

Bởi vậy $I \subset p(x)R[x]$. Bao hàm thức ngược lại là hiển nhiên do ta có $p(x) \in I$. Do đó $I = p(x)R[x]$. $\square$

Nếu trên vành R các đa thức $p(x), a(x) \neq 0$ thỏa mãn đẳng thức $p(x) = a(x)b(x)$, với $b(x) \in R[x]$ thì $a(x)$ được gọi là *ước* của $p(x)$, còn $p(x)$ là *bội* của $a(x)$. Ta cũng nói $a(x)$ *chia hết* $p(x)$, còn $p(x)$ *chia hết* cho $a(x)$.

Định nghĩa. Đa thức $p(x)$ trong vành $R[x]$ gọi là *khả quy* (trên R) nếu $p(x) = a(x)b(x)$ đối với các đa thức không khả nghịch $a(x), b(x)$ nào đó thuộc $R[x]$. Đa thức $p(x)$ được gọi là *bất khả quy* nếu $p(x)$ không khả nghịch và không khả quy.

Nói riêng, khi vành R là một trường F thì đa thức $f(x) \in F[x]$ là khả quy nếu $f(x) = a(x)b(x)$ với các đa thức $a(x), b(x)$ không là hằng.

Chú ý. Tính khả quy và bất khả quy của đa thức $p(x)$ đã cho hoàn toàn phụ thuộc vào vành cơ sở R . Chẳng hạn trên trường số thực $\mathbb{R}$ đa thức $x^2 + 1$ là bất khả quy nhưng trên $\mathbb{C}$ nó trở thành khả quy,

$$x^2 + 1 = (x + i)(x - i).$$

Đa thức $x^2 - 2$ bất khả quy trên $\mathbb{Q}$ và trên $\mathbb{Z}_3$, nhưng trên $\mathbb{R}$ thì

$$x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2}).$$

Đa thức $x^2 + x + 1$ bất khả quy trên $\mathbb{Q}$ và trên $\mathbb{Z}_2$, nhưng trên $\mathbb{Z}_3$ nó có sự phân tích

$$x^2 + x + 1 = (x + 2)^2.$$

Từ đẳng thức

$$\deg(ab) = \deg a + \deg b$$

đối với hai đa thức $a(x), b(x)$ trên trường F ta suy ra rằng các đa thức tuyến tính là bất khả quy trên một trường bất kỳ.

Khái niệm đa thức bất khả quy sẽ được nghiên cứu trong tình huống tổng quát ở mục sau. Bây giờ ta nêu một tính chất cơ bản của đa thức bất khả quy.

Mệnh đề 1.6. *Giả sử E là một trường mở rộng của trường F , u là một phần tử thuộc E , và $f(x)$ là đa thức bất khả quy trong $F[x]$ nhận u là nghiệm. Giả sử $g(x) \in F[x]$ cũng nhận u là nghiệm. Khi đó trong $F[x]$:*

- (i) $f(x)$ là đa thức có bậc thấp nhất nhận u là nghiệm.
- (ii) $g(x)$ chia hết cho $f(x)$.

Chứng minh. (i) Giả sử $h(x)$ là đa thức trong $F[x]$ có bậc thấp nhất, nhận u làm nghiệm. Khi đó

$$f(x) = h(x)q(x) + r(x),$$

với $r(x) = 0$ hoặc $\deg r(x) < \deg h(x)$ nếu $r(x) \neq 0$. Nếu $r(x) \neq 0$ thay $x = u$ vào đẳng thức trên ta được $r(u) = 0$ và điều này trái với giả thiết về bậc của $h(x)$. Do đó $r(x) = 0$ và $f(x) = h(x)q(x)$. Từ đó do $f(x)$ bất khả quy nên $q(x)$ phải là phần tử khả nghịch, nghĩa là bậc của $q(x)$ bằng 0 và $\deg f(x) = \deg h(x)$.

(ii) Theo định lý về phép chia với dư ta có

$$g(x) = f(x)q(x) + r(x),$$

Do $f(x)$ có bậc thấp nhất nên lặp lại lập luận trên ta được $r(x) = 0$ và do đó $g(x) = f(x)q(x)$. □

Nghiệm của đa thức

Định nghĩa. Giả sử R là vành con của vành V , và $f(x) \in R[x]$ có dạng

$$f(x) = a_0 + a_1x + \cdots + a_nx^n.$$

Phần tử $c \in V$ được gọi là *ng nghiệm* của $f(x)$ nếu

$$f(c) = a_0 + a_1c + \cdots + a_nc^n = 0.$$

Phần tử $u \in V$ gọi là *đại số trên R* nếu u là nghiệm của một đa thức $g(x) \neq 0$ nào đó của $R[x]$. Trong trường hợp trái lại u được gọi là phần tử *siêu việt trên R* .

Ví dụ

1. Hiển nhiên các phần tử thuộc vành cơ sở R đều đại số trên chính nó.

2. $\sqrt{2}$ là đại số trên trường các số hữu tỷ $\mathbb{Q}$. Nó là nghiệm của đa thức $x^2 - 2 \in \mathbb{Q}[x]$.

3. Số phức $a + bi$ là đại số trên trường các số thực $\mathbb{R}$, do nó là nghiệm của $x^2 - 2ax + a^2 + b^2 \in \mathbb{R}[x]$.

Đối với các nghiệm thuộc vành cơ sở R ta có một số kết quả cơ bản sau:

Định lý 1.7 (Định lý nhân tử). *Giả sử R là một miền nguyên, $c \in R$. Khi đó $x - c$ là ước của đa thức $p(x) \in R[x]$ khi và chỉ khi $p(c) = 0$.*

Chứng minh. Chia $p(x)$ cho $x - c$ ta được

$$p(x) = (x - c)q(x) + r(x)$$

với $\deg r(x) < 1$ nếu $r(x) \neq 0$, nghĩa là $r(x) \in R[x]$. Từ đó $p(c) = r$. Bởi vậy $x - c$ là ước của $p(x)$ khi và chỉ khi $r = p(c) = 0$. $\square$

Định lý nhân tử chứng tỏ rằng $x - c$ là một nhân tử của $f(x)$ nếu và chỉ nếu c là một nghiệm của $f(x)$.

Định lý 1.8. *Một đa thức bậc n trên một miền nguyên R có nhiều nhất n nghiệm trong R .*

Chứng minh. Chúng ta chứng minh định lý bằng quy nạp theo bậc n của đa thức.

Một đa thức bậc 0 chỉ là một hằng số khác không và do đó không có nghiệm.

Giả sử rằng định lý đúng với mọi đa thức bậc $n - 1$ trên R , và giả sử $f(x) \in R[x]$ là một đa thức bậc n . Nếu $f(x)$ không có nghiệm, thì

định lý đúng. Nếu $f(x)$ có nghiệm, ta gọi α là một nghiệm của nó. Theo định lý nhân tử, chúng ta có thể viết

$$f(x) = (x - \alpha)g(x),$$

và dễ thấy $\deg g(x) = n - 1$.

Do miền nguyên R không có ước của không nên $f(c) = 0$ nếu và chỉ nếu $(c - \alpha) = 0$ hoặc $g(c) = 0$. Do đó, mỗi nghiệm của $f(x)$ hoặc là bằng α hoặc là một nghiệm của $g(x)$. Theo giả thiết quy nạp, $g(x)$ có, nhiều nhất $n - 1$ nghiệm, do đó $f(x)$ có nhiều nhất n nghiệm. $\square$

Chú ý rằng nếu R không là miền nguyên thì kết quả không còn đúng nữa. Ví dụ đa thức $f(x) = x^3$ trong vành $\mathbb{Z}_8[x]$ có tới 4 nghiệm là 0, 2, 4, 6.

Vành thương của vành đa thức

Nếu F là một trường thì vành thương của vành các đa thức $F[x]$ tạo nên một lớp vành quan trọng, mà chúng ta thường sử dụng để xây dựng các trường mới. Nhắc lại rằng $F[x]$ là một vành idêan chính, và mỗi vành thương có dạng $F[x]/(p(x))$, với một đa thức $p(x) \in F[x]$. Bây giờ chúng ta xem xét cấu trúc của một vành thương như thế.

Các phần tử của vành $F[x]/(p(x))$ là các lớp tương đương theo quan hệ tương đương trên $F[x]$ được định nghĩa bởi

$$f(x) \equiv g(x) \pmod{(p(x))} \text{ nếu và chỉ nếu } f(x) - g(x) \in (p(x)).$$

Do $f(x) = q(x).p(x) + r(x)$, trong đó $r(x)$ bằng 0 hoặc có bậc nhỏ hơn bậc của $p(x)$, nên mọi lớp tương đương của $F[x]$ theo idêan $(p(x))$ chứa đa thức 0 hoặc đa thức có bậc nhỏ hơn bậc của $p(x)$.

Định lý 1.9. *Giả sử F là một trường, và $P = p(x)$ là idêan trong $F[x]$ sinh bởi đa thức $p(x)$ có bậc $n > 0$. Khi đó mỗi phần tử của vành thương $F[x]/(p(x))$ biểu diễn được một cách duy nhất dưới dạng*

$$a_0 + a_1x + \dots + a_{n-1}x^{n-1} + P,$$

trong đó $a_0, a_1, \dots, a_{n-1} \in F$.

Chứng minh. Gọi $f(x) + P$ là một phần tử của $F[x]/(p(x))$. Theo định lý về phép chia với dư ta có

$$f(x) = q(x)p(x) + r(x),$$

trong đó $r(x)$ bằng 0 hoặc có bậc nhỏ hơn bậc của $p(x)$. Khi đó

$$f(x) + P = r(x) + P,$$

và đây là biểu diễn đòi hỏi.

Để chứng minh tính duy nhất của biểu diễn nói trên ta giả sử rằng $r(x) + P = t(x) + P$, trong đó $r(x)$ và $t(x)$ bằng 0 hoặc có bậc nhỏ hơn n . Khi đó

$$r(x) \equiv t(x) \pmod{p(x)}.$$

Từ đó $r(x) - t(x)$ chia hết cho $p(x)$. Nếu $r(x) - t(x) \neq 0$ thì bậc của nó không nhỏ hơn bậc của $p(x)$; điều này không thể xảy ra. Vậy $r(x) - t(x) = 0$, và do đó $r(x) = t(x)$. $\square$

Ví dụ. Cho $P = x^2 - 2$ là ideal chính của $\mathbb{Q}[x]$ sinh bởi $x^2 - 2$. Tìm tổng và tích của $3x + 4 + P$ và $5x - 6 + P$ trong vành

$$\mathbb{Q}[x]/(x^2 - 2) = \{a_0 + a_1x + P \mid a_0, a_1 \in \mathbb{Q}\}.$$

Lời giải.

$$\begin{aligned}(3x + 4 + P) + (5x - 6 + P) &= (3x + 4) + (5x - 6) + P = 8x - 2 + P; \\ (3x + 4 + P)(5x - 6 + P) &= (3x + 4)(5x - 6) + P = 15x^2 + 2x - 24 + P.\end{aligned}$$

Theo thuật toán chia,

$$15x^2 + 2x - 24 = 15(x^2 - 2) + 2x + 6.$$

Do đó,

$$15x^2 + 2x - 24 + P = 2x + 6 + P.$$

Thường có những cách để tìm phần dư của $f(x)$ khi chia cho $p(x)$ dễ hơn cách áp dụng trực tiếp thuật toán chia. Nếu $\deg p(x) = n$ và $P = (p(x))$, bài toán tìm phần dư trong phép chia dẫn đến bài toán tìm một đa thức $r(x)$ có bậc nhỏ hơn n thỏa mãn $f(x) \equiv r(x) \pmod{P}$. Phương trình này thường được giải bằng thao tác đồng dư, sử dụng

kết quả $p(x) \equiv 0 \pmod{P}$.

Trong ví dụ vừa nêu trên, P là idêan sinh bởi $x^2 - 2$. Khi đó

$$x^2 - 2 \equiv 0 \pmod{P} \text{ và } x^2 \equiv 2 \pmod{P}.$$

Bởi vậy, trong mỗi phương trình đồng dư theo môđun P , chúng ta có thể thay x^2 bởi 2. Chẳng hạn,

$$\begin{aligned} 15x^2 + 2x - 24 &\equiv 15 \cdot 2 + 2x - 24 \pmod{P} \\ &= 2x + 6 \pmod{P}, \end{aligned}$$

do đó, $15x^2 + 2x - 24 + P = 2x + 6 + P$.

Bài tập

1.1. Trong vành $\mathbb{Z}_6[x]$ hãy thực hiện phép nhân

$$(2x^3 + 4x^2 + x)(3x^2 + 3x + 2)$$

Vành này có ước của 0 hay không?

1.2. Trong vành $\mathbb{Z}_7[x]$ hãy xác định p để $x^3 + px + 5$ chia hết cho $x^2 + 5x + 6$.

Với các bài tập từ 1.3 đến 1.8, tìm thương và phần dư.

1.3. Chia $3x^4 + 4x^3 - x^2 + 5x - 1$ cho $2x^2 + x + 1$ trong $\mathbb{Q}[x]$.

1.4. Chia $x^6 + x^4 - 4x^3 + 5x$ cho $x^3 + 2x^2 + 1$ trong $\mathbb{R}[x]$.

1.5. Chia $x^7 + x^6 + x^4 + x + 1$ cho $x^3 + x + 1$ trong $\mathbb{Z}_2[x]$.

1.6. Chia $2x^5 + x^4 + 2x^3 + x^2 + 2$ cho $x^3 + 2x + 2$ trong $\mathbb{Z}_3[x]$.

1.7. Chia $17 + 11i$ cho $3 + 4i$ trong $\mathbb{Z}[i]$.

1.8. Chia $20 + 8i$ cho $7 - 2i$ trong $\mathbb{Z}[i]$.

1.9. Trong vành $\mathbb{Z}[x]$ xét xem các đa thức sau có phải là bất khả quy hay không?

a) $f(x) = 2x + 3$;

b) $g(x) = x^2 + 1$;

c) $h(x) = x^2 + 2x - 2$.

1.10. Cho K là một trường con của trường F và u là một phần tử của F . Xét đồng cấu vành

$$\begin{aligned}\varphi: K[x] &\rightarrow F \\ f(x) &\mapsto f(u)\end{aligned}$$

Chứng minh rằng $\text{Ker } \varphi$ là một ideal nguyên tố của $K[x]$. Kết quả còn đúng không nếu K là vành con chứa đơn vị của một miền nguyên F ?

1.11. Giả sử $p(x)$ là một đa thức với hệ số nguyên và bất khả quy trong $\mathbb{Z}[x]$. Chứng minh rằng trong $\mathbb{Z}[x]$ nếu $p(x)$ chia hết tích $f(x)g(x)$ thì hoặc $p(x)$ chia hết $f(x)$ hoặc $p(x)$ chia hết $g(x)$.

1.12. Chứng minh rằng đa thức $x^2 + 14 \in \mathbb{Z}_{15}[x]$ có 4 nghiệm trong $\mathbb{Z}_{15}$.

1.13. Trong vành $\mathbb{Q}[x]$ chứng minh rằng đa thức

$$(x+1)^{2n} - x^{2n} - 2x - 1$$

chia hết cho các đa thức: a) $2x+1$; b) $x+1$; c) x .

1.14. Giả sử F là trường các thương của miền nguyên R , $\alpha \in F$ là một nghiệm của đa thức

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0, \quad a_i \in R.$$

Khi đó $\alpha \in R$.

1.15. Giả sử đa thức

$$f(x) = (x-a_1)(x-a_2)\cdots(x-a_n) - 1,$$

có các hệ số a_i là những số nguyên phân biệt. Chứng minh rằng $f(x)$ là bất khả quy trong $\mathbb{Q}[x]$.

1.16. Cho đa thức với các hệ số nguyên

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0.$$

Chứng minh rằng nếu phân số tối giản $\frac{p}{q}$, với $p, q \in \mathbb{Z}$, là nghiệm của $f(x)$ thì

a) $p|a_0$ và $q|a_n$.

b) $p - mq$ là ước của $f(m)$ với m nguyên; đặc biệt $p - q$ là ước

của $f(1)$, $p + q$ là ước của $f(-1)$.

Áp dụng: Tính nghiệm hữu tỷ của đa thức

$$10x^5 - 81x^4 + 90x^3 - 102x^2 + 80x - 21.$$

- 1.17.** Chứng minh trực tiếp rằng nếu u là đại số trên F thì đa thức bậc nhỏ nhất có hệ tử cao nhất bằng 1, với nghiệm u , là bất khả quy trên F .
- 1.18.** Chứng minh trực tiếp rằng nếu u là một phần tử bất kỳ của trường F và K là một trường con bất kỳ của F thì tập hợp tất cả các đa thức $g(x)$ với các hệ tử trong K nhận u làm nghiệm là một ideal của $K[x]$.
- 1.19.** Tìm hạt nhân và ảnh của cấu xạ vành $\psi : \mathbb{R}[x] \rightarrow \mathbb{C}$ được định nghĩa bởi $\psi(p(x)) = p(i)$, trong đó $i = \sqrt{-1}$.
- 1.20.** Tìm hạt nhân và ảnh của cấu xạ vành $\psi : \mathbb{R}[x] \rightarrow \mathbb{C}$ được định nghĩa bởi $\psi(p(x)) = p(1 + i\sqrt{3})$.
- 1.21.** Tìm một đa thức trong $\mathbb{Q}[x]$ nhận $\sqrt{2} + \sqrt{3}$ là nghiệm. Từ đó chứng minh rằng $\sqrt{2} + \sqrt{3}$ là số vô tỷ.
- 1.22.** Nếu r/s là một nghiệm hữu tỷ, ở dạng tối giản, của một đa thức $p(x)$ với hệ số nguyên, chứng minh rằng $p(x) = (sx - r)g(x)$ với một đa thức $g(x)$ nào đó với hệ số nguyên.
- 1.23.** Chứng minh rằng r/s , ở dạng tối giản, không thể là một nghiệm của đa thức nguyên $p(x)$ trừ khi $(s - r) \mid p(1)$. Điều này có thể được sử dụng để rút ngắn danh sách các nghiệm hữu tỷ có thể có của một đa thức nguyên.

Với các bài tập từ 1.24 đến 1.27, tính tổng và tích của các phần tử trong vành thương đã cho.

- 1.24.** $3x + 4$ và $5x - 2$ trong $\mathbb{Q}[x]/(x^2 - 7)$.
- 1.25.** $x^2 + 3x + 1$ và $-2x^2 + 4$ trong $\mathbb{Q}[x]/(x^3 + 2)$.
- 1.26.** $x^2 + 1$ và $x + 1$ trong $\mathbb{Z}_2[x]/(x^3 + x + 1)$.
- 1.27.** $ax + b$ và $cx + d$ trong $\mathbb{R}[x]/(x^2 + 1)$, trong đó $a, b, c, d \in \mathbb{R}$.

Với các bài tập từ 1.28 đến 1.36, chứng minh các đẳng thức.

- 1.28.** $\mathbb{R}[x]/(x^2 + 5) \cong \mathbb{C}$.
- 1.29.** $\mathbb{Z}[x]/(x^2 + 1) \cong \mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$.

- 1.30. $\mathbb{Q}[x]/(x^2 - 7) \cong \mathbb{Q}(\sqrt{7}) = \{a + b\sqrt{7} | a, b \in \mathbb{Q}\}$.
- 1.31. $\mathbb{Z}[x]/(2x - 1) \cong \{a/b \in \mathbb{Q} | a \in \mathbb{Z}, b = 2^r, r \geq 0\}$, một vành con của $\mathbb{Q}$.
- 1.32. $\mathbb{Z}_{14}/(7) \cong \mathbb{Z}_7$.
- 1.33. $\mathbb{Z}_{14}/(2) \cong \mathbb{Z}_2$.
- 1.34. $\mathbb{R}[x, y]/(x + y) \cong \mathbb{R}[y]$.
- 1.35. $(R \times S)/((1, 0)) \cong S$.
- 1.36. Cho I là tập tất cả các đa thức trong $\mathbb{R}[x, y]$, không có hạng tử tự do. Tìm một đồng cấu vành từ $\mathbb{R}[x, y]$ đến $\mathbb{R}$ có hạt nhân là ideal I . Chứng minh rằng I không phải là một ideal chính.
- 1.37. $\{p(x) \in \mathbb{Q}[x] | p(0) = 3\}$ có phải là một ideal của $\mathbb{Q}[x]$ không?

2. Thuật toán chia trong miền nguyên

Định nghĩa. Cho a và b là hai phần tử của miền nguyên R . Phần tử a được gọi là *chia hết* b nếu tồn tại $c \in R$ sao cho $b = ac$. Khi đó ta cũng nói rằng a là *ước* của b , ký hiệu $a|b$.

Thay cho ký hiệu $a|b$ ta còn viết $b : a$, và nói rằng b *chia hết cho* a hay b là *bội* của a .

Tính chất

1) Với mọi $a \in R$:

$$a|0; a|a; 1|a; (-a)|a; a|(-a).$$

Thật vậy, ta có

$$0 = a0; a = a1;$$

$$a = (-a)(-1); -a = a(-1);$$

2) Với mọi $a, b, c \in R$, $a|b$ và $b|c$ kéo theo $a|c$. Thật vậy, ta có $b = ax$, $c = by$. Từ đó

$$c = (ax)y = a(xy),$$

nghĩa là $a|c$.

3) Nếu a là ước của $a_1, a_2, \dots, a_n$ thì a là ước của

$$x_1a_1 + x_2a_2 + \dots + x_na_n,$$

với $x_1, x_2, \dots, x_n \in R$.

4) Nếu a và b là hai ước của 1 thì ab cũng là ước của 1.

Thật vậy, vì a và b là hai ước của 1 nên tồn tại u và v thuộc R sao cho $au = 1$ và $bv = 1$. Suy ra

$$(au)(bv) = 1 \text{ hay } (ab)(uv) = 1$$

Vậy ab là ước của 1.

Từ tính chất 4) suy ra rằng

5) Tập các ước của 1 trong miền nguyên R là một nhóm aben với phép nhân trong R . Nó được gọi là *nhóm nhân các ước của đơn vị* của miền nguyên R . Các ước của đơn vị còn được gọi là các *phần tử khả nghịch*.

Ví dụ trong vành các số nguyên $\mathbb{Z}$, các phần tử khả nghịch là ± 1 . Nếu F là một trường thì các đa thức khả nghịch trong vành các đa thức $F[x]$ là các đa thức hằng khác không (đó là các đa thức bậc 0). Tập các phần tử khả nghịch trong vành số nguyên Gauss $\mathbb{Z}[i]$ là $\pm 1, \pm i$.

Định nghĩa. Phần tử a được gọi là *liên kết* với phần tử b nếu tồn tại phần tử khả nghịch u sao cho $a = bu$.

Mệnh đề dưới đây cho thấy quan hệ *liên kết* là một quan hệ tương đương trên miền nguyên R . Ta ký hiệu quan hệ này bởi dấu $\sim$.

Mệnh đề 2.1. *Quan hệ liên kết trên miền nguyên R là một quan hệ tương đương.*

Chứng minh. Do $a = a1$ nên $a \sim a$, bởi vậy quan hệ $\sim$ là phản xạ.

Nếu $a \sim b$ thì $a = bu$ với u khả nghịch. Thế thì tồn tại phần tử v sao cho $uv = 1$. Ta có $av = (bu)v = b$, nghĩa là $b \sim a$ và quan hệ $\sim$ là đối xứng.

Nếu $a \sim b$ và $b \sim c$ thì $a = bu, b = cv$, với u, v là những phần tử khả nghịch. Khi đó tích uv cũng khả nghịch và

$$a = bu = (cv)u = c(uv).$$

Bởi vậy, $a \sim c$ và quan hệ $\sim$ là bắc cầu. □

Hệ quả 2.2. Cho $a, b, c \in R$. Khi đó các điều sau tương đương.

- (i) a liên kết với c ,
- (ii) $a|c$ và $c|a$,
- (iii) $aR = cR$.

Chứng minh. (i) $\Rightarrow$ (ii) là hiển nhiên theo định nghĩa của liên kết.

(ii) $\Rightarrow$ (iii). Điều này suy ra từ tính tương đương của $a|c$ với $cR \subset aR$.

(iii) $\Rightarrow$ (i). Từ giả thiết suy ra sự tồn tại của các phần tử $u, v \in R$ sao cho $a = cu, c = av$. Khi đó

$$a = cu = (av)u = a(vu).$$

Do R là miền nguyên nên thực hiện luật giản ước ta được $1 = vu$, nghĩa là u, v là những phần tử khả nghịch, do đó a, b là liên kết. $\square$

Định nghĩa. Cho a là phần tử thuộc miền nguyên R . Các phần tử liên kết với a và các phần tử khả nghịch được gọi là các ước không thực sự của a . Các ước còn lại của a được gọi là ước thực sự.

Định nghĩa. 1) Phần tử $p \neq 0$, không khả nghịch của miền nguyên R được gọi là phần tử bất khả quy nếu nó không có ước thực sự.

2) Phần tử $p \neq 0$, không khả nghịch, được gọi là phần tử nguyên tố nếu với mọi $a, b \in R$, p là ước của tích ab kéo theo p hoặc là ước của a , hoặc là ước của b .

Ví dụ, trong vành số nguyên mỗi số nguyên tố đều là bất khả quy.

Định lý 2.3. Trong miền nguyên R mọi phần tử nguyên tố đều là phần tử bất khả quy.

Chứng minh. Giả sử $p \in R$ là một phần tử nguyên tố. Khi đó $p \neq 0$, và p không là ước của 1. Để chứng minh p là phần tử bất khả quy ta chỉ cần chứng minh p không có ước thực sự. Thật vậy, giả sử $p = uv$. Do p là phần tử nguyên tố nên từ p là ước của tích uv suy ra $p|u$ hoặc $p|v$. Nếu $p|u$ thì do $u|p$ nên p liên kết với u và do đó v là ước của đơn vị. Tương tự, nếu $p|v$ thì p liên kết với v và u là ước của đơn vị. $\square$

Ví dụ sau đây cho ta những phần tử bất khả quy mà không là phần tử nguyên tố. Đặt

$$\mathbb{Z}[\sqrt{3}i] = \{a + b\sqrt{3}i | a, b \in \mathbb{Z}\}.$$

Để thấy $\mathbb{Z}[\sqrt{3}i]$ là một miền nguyên với đơn vị là 1. Trong miền nguyên này 2 là một phần tử bất khả quy, nhưng không là phần tử nguyên tố. Việc chứng minh xin dành cho độc giả.

Định nghĩa. Cho a, b là những phần tử của vành R . Khi đó phần tử $d \in R$ được gọi là *ước chung lớn nhất* của a và b nếu d là ước chung của a và b , và d chia hết cho mọi ước chung của a và b .

Ước chung lớn nhất của a và b được ký hiệu bởi

$$d = (a, b) \text{ hoặc } \text{UCLN}(a, b).$$

Nhận xét. Ước chung lớn nhất của hai phần tử a và b nói chung không duy nhất. Hai phần tử d và d' cùng là ước chung lớn nhất của a và b khi và chỉ khi chúng liên kết với nhau, nghĩa là sai khác nhau một nhân tử khả nghịch.

Định nghĩa. Các phần tử a và b được gọi là *nguyên tố cùng nhau* nếu ước chung lớn nhất của chúng là ước của đơn vị. Trong trường hợp này ta thường viết $(a, b) = 1$.

Ví dụ

1. Trong vành số nguyên $\mathbb{Z}$, 2 và -2 đều là ước chung lớn nhất của 6 và 8. Chúng liên kết với nhau.

2. Trong vành $\mathbb{Z}[x]$ có $d_1(x) = x - 1$ và $d_2(x) = 2x - 2$ đều là ước chung lớn nhất của

$$f(x) = x^2 - 1 \text{ và } g(x) = x^2 - 3x + 2.$$

Trong mục tới chúng ta sẽ xét một số lớp vành, trong đó ước chung lớn nhất của hai phần tử luôn luôn tồn tại.

Bài tập

Các đa thức bất khả quy nói trong các bài tập dưới đây được hiểu là những phần tử bất khả quy của vành đang xét.

2.1. Trong vành đa thức $\mathbb{R}[x]$, với $\mathbb{R}$ là trường số thực, chứng minh các đa thức $ax^2 + bx + c$ với $b^2 - 4ac < 0$ là những đa thức bất khả quy. Điều đó có còn đúng nữa không nếu thay trường số thực $\mathbb{R}$ bởi trường số phức $\mathbb{C}$.

2.1. Xét vành $F[x]$ với F là một trường.

a) Chứng minh rằng mọi đa thức bậc nhất của $F[x]$ đều là bất khả quy. Nếu F là một miền nguyên thì điều đó còn đúng nữa không?

b) Chứng minh rằng các đa thức bậc hai và bậc ba của $F[x]$ là bất khả quy khi và chỉ khi chúng không có nghiệm trong trường F .

2.3. Trong vành $\mathbb{Z}[x]$ xét xem các đa thức sau đây có phải là bất khả quy hay không:

$$f(x) = 2x + 8; g(x) = x^2 + 1; h(x) = x^2 + 2x - 2$$

2.4. Cho $f(x) = x^5 - x^4 - 3x^3 + 2x + 4$. Phân tích $f(x)$ thành một tích những đa thức bất khả quy trên các trường số $\mathbb{Z}$; $\mathbb{Z}(\sqrt{2})$; $\mathbb{Q}$ và $\mathbb{R}$.

2.5. Tìm tất cả các đa thức bất khả quy bậc 2 trên $\mathbb{Z}_2$.

2.6. Tìm tất cả các đa thức bất khả quy bậc 2 trên $\mathbb{Z}_5$.

2.7. Tìm tất cả các đa thức bất khả quy bậc 2 trên $\mathbb{Z}_7$.

Trong các bài tập từ 2.8 đến 2.13, những đa thức đã cho có bất khả quy trong vành đã cho hay không? Tại sao?

2.8. $x^3 + x^2 + x + 1$ trong $\mathbb{Q}[x]$.

2.9. $x^4 + x^2 - 6$ trong $\mathbb{Q}[x]$.

2.10. $4x^3 + 3x^2 + x + 1$ trong $\mathbb{Z}_5[x]$.

2.11. $x^4 - 2x^3 + x^2 + 1$ trong $\mathbb{R}[x]$.

2.12. 5 có bất khả quy trong $\mathbb{Z}[i]$ hay không?

3. Vành chính

Trong các phần trước chúng ta thấy rằng trong vành các số nguyên $\mathbb{Z}$ và vành các đa thức $F(x)$ trên trường F mọi ideal đều là ideal chính. Điều đó gợi ý cho chúng ta xét một lớp vành tổng quát hoá của hai lớp vành nói trên theo định nghĩa sau.

Định nghĩa. Miền nguyên D được gọi là một vành chính nếu mọi idêan của D đều là idêan chính.

Ví dụ vành đa thức $F(x)$ trên trường F là một vành chính (theo Mệnh đề 1.5), tuy nhiên vành đa thức $\mathbb{Z}[x]$ không là vành chính (xem phần bài tập).

Định nghĩa. Một dãy chuyền (hay một dãy) tăng những idêan của miền nguyên R

$$J_1 \subset J_2 \subset J_3 \subset \cdots \subset J_n \cdots \quad (1)$$

được gọi là *dừng* nếu tồn tại số nguyên dương n_0 sao cho

$$J_n = J_{n_0} \text{ với mọi } n > n_0.$$

Dễ thấy dãy (1) dừng khi và chỉ khi nó chỉ có một số hữu hạn các J_i khác nhau.

Bổ đề 3.1. Trong vành chính R mọi dãy tăng những idêan đều dừng.

Chứng minh. Giả sử

$$J_1 \subset J_2 \subset J_3 \subset \cdots \subset J_n \cdots \quad (1)$$

là một dãy chuyền tăng những idêan của vành chính R . Khi đó

$$J = \bigcup_{i=1}^{\infty} J_i$$

là một idêan của R . Thật vậy, hiển nhiên $0 \in J$. Bây giờ nếu $a, b \in J$ thì tồn tại J_k, J_l sao cho $a \in J_k, b \in J_l$. Giả sử $l \geq k$ thế thì a, b đều thuộc J_l do đó $a - b \in J_l$ và bởi vậy $a - b \in J$.

Giả sử $x \in R$ và $a \in J$ thế thì $a \in J_k$ với k nào đó và vì vậy $ax \in J_k$, suy ra $ax \in J$.

Vì R là một vành chính nên tồn tại $d \in J$ sao cho $J = dR$. Theo định nghĩa của hợp tồn tại số tự nhiên m sao cho $d \in J_m$. Khi đó $J \subset J_m$. Mặt khác ta luôn có $J_m \subset J$ nên $J = J_m$. Vậy dãy chuyền (1) dừng. $\square$

Chúng ta thấy rằng trong vành các số nguyên $\mathbb{Z}$ và vành các đa thức $F[x]$ trên trường F thì ước chung lớn nhất của hai phần tử khác không luôn tồn tại. Bây giờ ta sẽ chứng tỏ rằng kết quả đó và một

số kết quả quen thuộc khác trong vành $\mathbb{Z}$ cũng đúng trong một vành chính bất kỳ.

Định lý 3.2. Trong vành chính R mọi cặp phần tử khác không a, b đều có ước chung lớn nhất d , và d là một tổ hợp tuyến tính của a, b :

$$d = as + bt,$$

với $s, t \in R$

Chứng minh. Giả sử R là một vành chính, a, b là hai phần tử thuộc R . Đặt

$$J = \{ax + by | x, y \in R\}$$

Do $J = aR + bR$ nên nó là một ideal của R . Vì R là vành chính nên tồn tại $d \in J$ sao cho $J = dR$. Ta sẽ chứng minh d là UCLN của a và b . Thật vậy, vì a, b thuộc J nên

$$a = da_1 \text{ và } b = db_1 \text{ với } a_1, b_1 \in R.$$

Vì $d \in J$ nên có

$$d = as + bt \text{ với } s, t \in R$$

Bây giờ nếu c là một ước chung của a và b thì c sẽ là ước của $d = as + bt$. $\square$

Do vành đa thức $F[x]$ trên trường F là vành chính nên ta có:

Hệ quả 3.3. Trong vành đa thức $F[x]$ trên một trường F ước chung lớn nhất của hai đa thức khác không luôn tồn tại.

Một tính chất quan trọng khác trong vành số nguyên là mỗi số tự nhiên $n \geq 2$ đều phân tích được một cách duy nhất thành tích các thừa số nguyên tố. Kết quả này cũng sẽ được khái quát hoá cho các vành chính trong định lý về nhân tử hoá.

Trước hết ta chứng minh một số tính chất của phần tử bất khả quy trong vành chính. Những tính chất này được sử dụng trong chứng minh định lý về nhân tử hoá trong vành chính.

Bổ đề 3.4. Cho R là một vành chính. Nếu a, b, c là những phần tử thuộc R sao cho $(a, b) = 1$ và $a|bc$ thì $a|c$.

Chứng minh. Do $(a, b) = 1$ nên tồn tại các phần tử s, t thuộc R sao cho $1 = as + bt$. Khi đó $c = acs + bct$, và do đó $a|c$, bởi vì ta đã có $a|bc$. $\square$

Bổ đề 3.5. Nếu p là phần tử bất khả quy trong vành chính R và c là một phần tử bất kỳ thuộc R thì hoặc $p|c$, hoặc $(p, c) = 1$.

Chứng minh. Thật vậy, ta giả sử $d = (p, c)$. Do p là bất khả quy nên d khả nghịch hoặc d liên kết với p . Từ đó suy ra c nguyên tố cùng nhau với p hoặc c chia hết cho p . $\square$

Do vành đa thức $F[x]$ trên một trường F là một vành chính nên ta có ngay kết quả thường được sử dụng sau đây.

Hệ quả 3.6. Trong vành đa thức $F[x]$ trên một trường F nếu $p(x)$ là một đa thức bất khả quy và $f(x)$ là một đa thức bất kỳ trên F thì hoặc $p(x)$ chia hết $f(x)$ hoặc chúng là nguyên tố cùng nhau.

Bổ đề 3.7. Nếu p là phần tử bất khả quy trong vành chính R và nếu $p|ab$ thì $p|a$ hoặc $p|b$.

Chứng minh. Nếu a không chia hết cho p thì a nguyên tố cùng nhau với p (do Bổ đề 3.5). Bây giờ theo Bổ đề 3.4 từ $p|ab$ suy ra $p|b$. $\square$

Ví dụ. Chứng minh rằng $\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}(\sqrt{2})$.

Lời giải. Xét đồng cấu vành $\psi : \mathbb{Q}[x] \rightarrow \mathbb{Q}(\sqrt{2})$ được xác định bởi $\psi(f(x)) = f(\sqrt{2})$. Hạt nhân là tập các đa thức có một nhân tử là $x^2 - 2$, tức là ideal chính $(x^2 - 2)$. Ảnh của ψ là $\mathbb{Q}(\sqrt{2})$, do đó theo định lý đồng cấu vành,

$$\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}(\sqrt{2}).$$

Trong đẳng cấu này, phần tử $a_0 + a_1x \in \mathbb{Q}[x]/(x^2 - 2)$ biến thành $a_0 + a_1\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Phép cộng và phép nhân của các phần tử $a_0 + a_1x$ và $b_0 + b_1x$ trong $\mathbb{Q}[x]/(x^2 - 2)$ tương ứng với phép cộng và phép nhân của các số thực $a_0 + a_1$ và $b_0 + b_1$.

Ví dụ. Chứng minh rằng $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

Lời giải. Ta xác định đồng cấu vành $\psi : \mathbb{R}[x] \rightarrow \mathbb{C}$ bởi $\psi(f(x)) = f(i)$, trong đó $i^2 = -1$. Mỗi đa thức trong $\text{Ker}\psi$ nhận i là nghiệm, do đó cũng nhận $-i$ là nghiệm và chứa nhân tử $x^2 + 1$. Bởi vậy $\text{Ker}\psi = (x^2 + 1)$.

Bây giờ $\psi(a + bx) = a + ib$ nên ψ là toàn ánh. Theo định lý đồng cấu vành, $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

Định lý cơ bản của lý thuyết số khẳng định rằng mỗi số tự nhiên $n > 1$ đều phân tích được thành tích các thừa số nguyên tố. Ta hãy

mở rộng kết quả này cho vành chính (Định lý 3.10) và gọi đó là tính chất nhân tử hoá của vành chính.

Trước hết chúng ta chứng minh hai bổ đề sau

Bổ đề 3.8. Trong vành chính R mỗi phần tử khác không và không khả nghịch đều chứa trong một ideal tối đại.

Chứng minh. Giả sử $a \neq 0$ là một phần tử không khả nghịch, thuộc vành chính R . Thế thì ideal chính sinh bởi a là thực sự chứa trong R . Xét dãy tăng những ideal của vành chính R

$$aR = J_1 \subset J_2 \subset \dots \subset J_n \dots$$

Theo Bổ đề 3.1 dãy này dừng, chẳng hạn tại J_k . Thế thì J_k là ideal tối đại chứa a . $\square$

Ví dụ trong vành số nguyên $\mathbb{Z}$ số 6 chứa trong các ideal tối đại là $2\mathbb{Z}$ và $3\mathbb{Z}$.

Bổ đề 3.9. Trong vành chính R phần tử a là bất khả quy khi và chỉ khi ideal aR tối đại.

Chứng minh. Theo định nghĩa của phần tử bất khả quy thì $a \neq 0$ và không khả nghịch. Vì vậy, theo Bổ đề 3.8, a chứa trong một ideal tối đại B . Do R là vành chính và B thực sự chứa trong R nên $B = bR$ với phần tử b không khả nghịch nào đó trong R . Từ $a \in bB$ suy ra b là một ước của a . Do a là bất khả quy nên b liên kết với a , và do đó $aR = B$, và là tối đại trong R .

Ngược lại, giả sử aR là ideal tối đại trong R . Do $aR \neq R$ nên a không khả nghịch. Nếu a có ước thực sự b thì aR thực sự chứa trong bR , trái với tính tối đại của aR . $\square$

Định lý 3.10 (Định lý nhân tử hoá). Mỗi phần tử khác 0 và không khả nghịch trong vành chính R đều phân tích được một cách duy nhất thành tích các nhân tử bất khả quy, sai khác một thứ tự các nhân tử và một nhân tử khả nghịch.

Chứng minh. Giả sử $0 \neq a \in R$ và a không khả nghịch. Theo Bổ đề 3.8 thì a chứa trong một ideal tối đại q_1R do đó $a = q_1 \cdot a_1$. Theo Bổ đề 3.9, q_1 bất khả quy. Nếu a_1 khả nghịch ta có điều phải chứng minh. Nếu a_1 không khả nghịch lập luận tương tự như đối với a ta có

$$a_1 = q_2 \cdot a_2, \text{ với } q_2 \text{ bất khả quy.}$$

Tiếp tục quá trình này sau hữu hạn bước ta được

$$a_{n-1} = q_n \cdot a_n, \text{ với } q_n \text{ bất khả quy và } a_n \text{ khả nghịch.}$$

Thật vậy, nếu dãy các ước thực sự

$$a, a_1, a_2, \dots, a_n, \dots$$

là vô hạn thì dãy tăng các idêan tương ứng

$$aR \subset a_1R \subset a_2R \subset \dots \subset a_nR \subset \dots$$

cũng là dãy vô hạn, trái với Bổ đề 3.1. Bây giờ đặt $p = a_{n-1} = q_n \cdot a_n$ ta được p là bất khả quy, và có sự phân tích a thành tích những phần tử bất khả quy:

$$a = q_1 q_2 \dots q_{n-1} \cdot p.$$

Để chứng minh tính duy nhất, giả sử rằng

$$a = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m, \quad (*)$$

trong đó mỗi p_i và q_i là bất khả quy. Hơn nữa, không mất tính tổng quát ta giả sử rằng $m \geq n$. Từ đẳng thức (*) suy ra

$$p_1 \mid q_1 q_2 \dots q_m.$$

Thế thì theo Bổ đề 1.7, ta có p_1 là ước của một q_k nào đó. Bằng cách đánh số lại các chỉ số ta có thể giả thiết $p_1 \mid q_1$. Do q_1 là phần tử bất khả quy nên q_1 liên kết với p_1 hay $q_1 = u_1 p_1$. Như vậy

$$p_1 p_2 \dots p_n = u_1 q_1 q_2 \dots q_m.$$

Sau khi giản ước hai vế cho p_1 ta được

$$p_2 \dots p_n = u_1 q_2 \dots q_m.$$

Tiếp tục lập luận trên sau hữu hạn bước ta được

$$1 = u_1 u_2 \dots u_n q_{n+1} \dots q_m.$$

Điều này lại không thể xảy ra, bởi vì một phần tử bất khả quy không thể chia hết 1. Do đó $m = n$, và các số nguyên tố $p_1, p_2, \dots, p_n$ trùng với $q_1, q_2, \dots, q_m$, sai khác về thứ tự và sai khác phép nhân với các phần tử khả nghịch. Định lý được chứng minh. $\square$

Khi vành chính là vành các số nguyên $\mathbb{Z}$, định lý trên cho ta định lý cơ bản của số học đã được nói đến lúc trước.

Do vành các đa thức $F[x]$ trên một trường F là vành chính nên từ Định lý 3.10 ta có:

Hệ quả 3.11. Cho trường F . Khi đó mọi đa thức $f(x) \in F[x]$, bậc $n \geq 1$ đều phân tích được một cách duy nhất thành tích những đa thức bất khả quy.

Trong một ví dụ ở mục sau chúng ta sẽ thấy vành các số nguyên Gauss

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$$

cũng có tính chất nhân tử hoá duy nhất như các vành $\mathbb{Z}$ và vành $F[x]$. Tuy nhiên, ví dụ sau chỉ ra rằng có những miền nguyên không có tính chất này. Xét miền nguyên

$$\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$$

Trong miền nguyên này số 4 có hai sự phân tích:

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}),$$

trong đó 2, $1 + \sqrt{-3}$, $1 - \sqrt{-3}$ đều bất khả quy.

Bài tập

3.1. Cho F là trường. Chứng minh trực tiếp rằng

a) $F[x]$ là vành chính.

b) Nếu $p(x)$ là đa thức bất khả quy trên F thì ideal chính sinh bởi $p(x)$ là tối đại trong $F[x]$ và suy ra vành thương $\overline{F} = F[x]/(p(x))$ là một trường.

3.2. a) Chứng minh rằng hai đa thức bất khả quy trên cùng một trường không thể có nghiệm chung.

b) Nếu $f(x)$ và $g(x)$ có nghiệm chung và $f(x)$ là bất khả quy trên F thì $f(x) \mid g(x)$.

3.3. Nếu $f(x)$ là đa thức bất khả quy trên trường F , có bậc $n \geq 1$ thì không tồn tại trong F hai đa thức khác không có bậc nhỏ hơn n mà tích của chúng chia hết cho $f(x)$.

- 3.4. Giả sử a và b là hai phần tử nguyên tố cùng nhau của vành chính A . Chứng minh idêan sinh ra bởi a và b là vành A .
- 3.5. Cho p là một phần tử khác 0 của một vành chính A . Chứng minh p là bất khả quy khi và chỉ khi Ap là một idêan tối đại của A .
- 3.6. Chứng minh rằng trong một vành chính, các idêan nguyên tố khác 0 đều là các idêan tối đại.
- 3.7. Chứng minh một trường là một vành chính.
- 3.8. Vành thương của một vành chính có phải là một vành chính không?
- 3.9. Vành con của một vành chính có phải là một vành chính không?
- 3.10. Vành $\mathbb{Z}[x]$ có phải là một vành chính không?
- 3.11. Giả sử $A = \{a + b\sqrt{3}i | a, b \in \mathbb{Z}\}$.
 a) Chứng minh rằng A cùng với phép cộng và phép nhân các số phức là một miền nguyên.
 b) Chứng minh rằng $2, 1 + \sqrt{3}i, 1 - \sqrt{3}i$ là những phần tử bất khả quy của A nhưng không phải là những phần tử nguyên tố. Từ đó suy ra A không phải là một vành chính.
- 3.12. Chứng minh rằng vành

$$A = \{a + b\sqrt{2}i | a, b \in \mathbb{Z}\}$$

là một vành chính.

- 3.13. Chứng minh rằng vành $\mathbb{Z}[x]$ không là vành chính, nhưng vành thương $\mathbb{Z}(x)/(9x^2 + 2)$ là một vành chính.
- 3.14. Chứng minh rằng vành $A[x]$ trên miền nguyên A là một vành chính khi và chỉ khi A là một trường.

Phân tích các đa thức trong các bài tập từ 3.15 đến 3.26 thành các nhân tử bất khả quy trong vành đã cho

- 3.15. $x^5 - 1$ trong $\mathbb{Q}[x]$.
- 3.16. $x^5 + 1$ trong $\mathbb{Z}_2[x]$.
- 3.17. $x^4 + 1$ trong $\mathbb{Z}_5[x]$.
- 3.18. $2x^3 + x^2 + 4x + 2$ trong $\mathbb{Q}[x]$.
- 3.19. $x^4 - 9x + 3$ trong $\mathbb{Q}[x]$.
- 3.20. $2x^3 + x^2 + 4x + 2$ trong $\mathbb{C}[x]$.

3.21. $x^3 - 4x + 1$ trong $\mathbb{Q}[x]$.

3.22. $x^4 + 3x^3 + 9x - 9$ trong $\mathbb{Q}[x]$.

3.23. $x^8 - 16$ trong $\mathbb{C}[x]$.

3.24. $x^8 - 16$ trong $\mathbb{R}[x]$.

3.25. $x^8 - 16$ trong $\mathbb{Q}[x]$.

3.26. $x^8 - 16$ trong $\mathbb{Z}_{17}[x]$.

3.28. Chứng minh rằng $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}$ không có tính chất nhân tử hoá duy nhất.

Miền nguyên R được gọi là thỏa mãn điều kiện có ước chung lớn nhất (viết tắt là UCLN) nếu trong R mọi cặp phần tử a, b đều có ước chung lớn nhất. Chứng minh các mệnh đề từ 3.29 đến 3.32 sau.

3.29. Cho a, b, c thuộc miền nguyên R thỏa mãn điều kiện có UCLN. Khi đó ta có:

1) $c(a, b) = (ca, cb)$,

2) Nếu $(a, b) = 1$ và $(a, c) = 1$ thì $(a, bc) = 1$.

3.30. Cho R là một miền nguyên thỏa mãn điều kiện có UCLN, p là phần tử bất khả quy thuộc R . Khi đó với mọi a thuộc R , hoặc a chia hết cho p hoặc a và p nguyên tố cùng nhau.

3.31. Trong vành R thỏa mãn điều kiện có UCLN, một phần tử là bất khả quy khi và chỉ khi nó là nguyên tố.

3.32. Cho R là miền nguyên thỏa mãn điều kiện có UCLN, $p \in R$ là phần tử bất khả quy. Nếu $a_1, a_2, \dots, a_n (n \geq 2)$ là những phần tử của R sao cho $p | a_1 a_2 \dots a_n$ thì tồn tại a_k sao cho $p | a_k$.

3.33. Cho R là một miền nguyên, thỏa mãn điều kiện dừng những ước thực sự. Nếu và $a \in R, a \neq 0$ không khả nghịch thì a có một ước bất khả quy.

Miền nguyên R được gọi là vành nhân tử hoá (hay vành Gauss) nếu mọi phần tử khác 0 và không khả nghịch của nó đều phân tích được một cách duy nhất thành một tích những nhân tử bất khả quy, sai khác thứ tự các nhân tử và sai khác các nhân tử khả nghịch. Chứng minh các mệnh đề từ 3.34 đến 3.37 sau.

3.34. Cho R là một miền nguyên thỏa mãn điều kiện dừng những ước thực sự và điều kiện có UCLN. Khi đó R là một vành nhân tử hoá (hay vành Gauss). Từ đó suy ra mọi vành chính đều là vành Gauss.

3.35. Vành nhân tử hoá thỏa mãn điều kiện dừng những ước thực sự và điều kiện có ƯCLN.

3.36. Cho A là một vành Gauss, $\bar{A}$ là trường các thương của A .

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x]$$

được gọi là một đa thức *nguyên bản* nếu ước chung lớn nhất của các hệ tử $a_0, a_1, \dots, a_n$ bằng 1. Chứng minh rằng:

a) Tích của hai đa thức nguyên bản là một đa thức nguyên bản.

b) Nếu đa thức $f(x) \in A[x]$ khả quy trong $\bar{A}[x]$ thì nó cũng khả quy trong $A[x]$.

3.37. Chứng minh rằng nếu A là một vành Gauss thì vành $A[x]$ cũng là vành Gauss. Tính chất này còn đúng không nếu thay giả thiết "vành Gauss" bằng giả thiết "vành chính".

4. Vành Ôclit

Định lý về phép chia với dư trong vành số nguyên và trong vành các đa thức trên một trường đóng vai trò quan trọng trong các lớp vành này. Bây giờ chúng ta hãy nghiên cứu một lớp vành tổng quát có thuật toán chia này.

Định nghĩa. Một miền nguyên R được gọi là *vành Ôclit* nếu có một ánh xạ

$$\begin{aligned} \delta: R^* &\rightarrow \mathbb{N} \\ x &\mapsto \delta(x) \end{aligned}$$

từ tập các phần tử khác 0 của R đến tập các số tự nhiên $\mathbb{N}$ thỏa mãn các điều kiện:

(i) $\forall a, b \in R^*, a|b$ kéo theo $\delta(a) \leq \delta(b)$.

(ii) $\forall a, b \in R, b \neq 0$ tồn tại $q, r \in R$ sao cho $a = bq + r$ với $r = 0$, hoặc nếu $r \neq 0$ thì $\delta(r) < \delta(b)$.

Ánh xạ δ được gọi là *ánh xạ Ôclit*.

Ví dụ

1. Từ định lý về phép chia với dư trong vành số nguyên $\mathbb{Z}$ ta suy

ra rằng vành $\mathbb{Z}$ là một vành Ôclit với ánh xạ

$$\begin{aligned}\delta: \mathbb{Z}^* &\rightarrow \mathbb{N} \\ n &\mapsto \delta(n) = |n|\end{aligned}$$

2. Cho F là một trường. Khi đó F cùng với ánh xạ

$$\begin{aligned}\delta: F^* &\rightarrow \mathbb{N} \\ a &\mapsto \delta(a) = c,\end{aligned}$$

với c là một số tự nhiên cho trước, là một vành Ôclit.

3. Từ định lý về phép chia với dư trong vành đa thức một ẩn $F[x]$ trên trường F suy ra $F[x]$ là một vành Ôclit với ánh xạ

$$\begin{aligned}\delta: F[x]^* &\rightarrow \mathbb{N} \\ f(x) &\mapsto \delta(f(x)) = \deg f(x)\end{aligned}$$

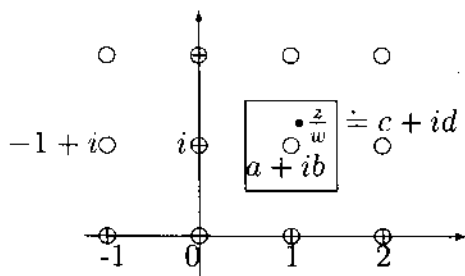
4. Vành các số nguyên Gauss

$$\mathbb{Z}[i] = \{a + ib | a, b \in \mathbb{Z}\}$$

là một vành Ôclit với ánh xạ Ôclit cho bởi $\delta(a + ib) = a^2 + b^2$.

Thật vậy, $\mathbb{Z}[i]$ là vành con của $\mathbb{C}$, và do đó là một miền nguyên. Nếu $z \in \mathbb{Z}[i]$, thì $\delta(z) = z\bar{z}$, trong đó $\bar{z}$ là liên hợp của z trong trường số phức $\mathbb{C}$. Với mỗi số phức khác không z , $\delta(z) > 0$, và với hai số nguyên Gauss khác không z và w , $\delta(z.w) = \delta(z).\delta(w)$.

Để chứng minh thuật toán chia trong $\mathbb{Z}[i]$, gọi z và w là các số nguyên Gauss với $w \neq 0$, thì $\frac{z}{w}$ là một số phức $c + id$, trong đó $c, d \in \mathbb{Q}$. Chọn các số nguyên a, b như trong hình vẽ (trong hình vẽ này các phần tử của $\mathbb{Z}[i]$ được khoanh tròn).



sao cho $|c - a| \leq \frac{1}{2}$ và $|d - b| \leq \frac{1}{2}$. Khi đó

$$\frac{z}{w} = a + ib + [(c - a) + i(d - b)],$$

do đó

$$z = (a + ib)w + [(c - a) + i(d - b)]w.$$

Bây giờ

$$\begin{aligned} \delta([(c - a) + i(d - b)]w) &= \delta((c - a) + i(d - b))\delta(w) \\ &= [(c - a)^2 + (d - b)^2]\delta(w) \leq \left(\frac{1}{4} + \frac{1}{4}\right)\delta(w) < \delta(w). \end{aligned}$$

Do đó $\mathbb{Z}[i]$ là vành Oclit.

Bây giờ ta cho một vài kết quả đơn giản của vành Oclit.

Bổ đề 4.1. Trong vành Oclit E đối với $x, y \in E^*$, $\delta(xu) = \delta(x)$ nếu u khả nghịch và $\delta(xu) > \delta(x)$ trong trường hợp ngược lại.

Chứng minh. Nếu u khả nghịch thì

$$\delta(x) = \delta(xuu^{-1}) \geq \delta(xu)$$

và vì vậy $\delta(x) = \delta(xu)$.

Tính khả nghịch của u tương đương với $xu|x$. Bởi vậy nếu u không khả nghịch thì xu không là ước của x . Khi đó

$$x = q(xu) + r \text{ với } \delta(r) = \delta(xu).$$

Ngoài ra,

$$r = x - qxu = x(1 - qu)$$

nên $\delta(r) \geq \delta(x)$. Bởi vậy $\delta(xu) > \delta(r) > \delta(x)$. □

Từ bổ đề trên dễ dàng suy ra hệ quả sau.

Hệ quả 4.2. Trong vành Oclit E phần tử u khả nghịch khi và chỉ khi $\delta(u) = \delta(1)$, và nếu hai phần tử a, b liên kết thì $\delta(a) = \delta(b)$.

Định lý sau cho ta mối quan hệ giữa lớp vành Oclit và lớp vành chính.

Định lý 4.3. Mọi vành Oclit đều là vành chính.

Chứng minh. Giả sử E là một vành Öclit với ánh xạ

$$\begin{aligned}\delta: E^* &\rightarrow \mathbb{N} \\ x &\mapsto \delta(x)\end{aligned}$$

Giả sử J là một ideal của E . Nếu $J = 0$ thì $J = (0)$. Nếu $J \neq 0$ thì tồn tại phần tử $a \in J, a \neq 0$. Đặt

$$J^* = J \setminus \{0\}$$

và a_0 là phần tử thuộc J^* sao cho $\delta(a_0) \leq \delta(x)$ với mọi $x \in J^*$. Ta sẽ chứng tỏ rằng $J = (a_0)$.

Thật vậy, vì $a_0 \in J$ nên $(a_0) \subset J$. Bây giờ giả sử $a \in J$. Do $a_0 \neq 0$ và do E là một vành Öclit nên tồn tại $q, r \in E$ sao cho

$$a = a_0q + r,$$

trong đó $r = 0$ hoặc $\delta(r) < \delta(a_0)$ nếu $r \neq 0$. Do $a, a_0q \in J$ nên

$$r = a - a_0q \in J.$$

Nếu $r \neq 0$ thì theo định nghĩa của δ ta có $\delta(r) < \delta(a_0)$, trái với giả thiết về a_0 . Vậy $r = 0$ và do đó $a = a_0q \in (a_0)$. Điều này chứng tỏ $J = (a_0)$ và do đó E là vành chính. $\square$

Do một vành Öclit là vành chính nên ước chung lớn nhất của hai phần tử khác không luôn tồn tại. Hơn nữa, ước chung lớn nhất đó có thể tìm được nhờ một thuật toán tương tự như thuật toán đã trình bày cho vành các số nguyên $\mathbb{Z}$. Trước hết ta có bổ đề sau.

Bổ đề 4.4 Trong vành Öclit E

$$a = bq + c \Rightarrow (a, b) = (b, c).$$

Chứng minh. Thật vậy, gọi I, J lần lượt là các ideal sinh bởi các tập hợp $\{a, b\}, \{b, c\}$. Hiển nhiên a thuộc J nên $I \subset J$.

Mặt khác, từ $c = a - bq$ suy ra c thuộc I , và do đó $J \subset I$. Vậy $I = J$. Theo chứng minh mệnh đề trên thì I, J theo thứ tự sinh bởi các phần tử $(a, b), (b, c)$ nên hai phần tử này liên kết và bởi vậy ta có thể chọn ước chung lớn nhất (a, b) của a và b chính là (b, c) . $\square$

Bây giờ chúng ta có thể trình bày thuật toán để tìm ước chung lớn nhất của hai phần tử khác không a, b trong vành Oclit E như sau.

Nếu $a = bq$ thì hiển nhiên $(a, b) = b$.

Nếu $a = bq_0 + r_0$, với $\delta(r_0) < \delta(b)$ thì theo bổ đề vừa chứng minh ta có

$$(a, b) = (b, r_0).$$

Tiếp tục quá trình này sau hữu hạn bước ta được

$$\begin{aligned} b &= r_0q_1 + r_1, \text{ với } \delta(r_1) < \delta(r_0) \\ \dots &= \dots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n, \text{ với } \delta(r_n) < \delta(r_{n-1}) \\ r_{n-1} &= r_nq_n, \end{aligned}$$

Quá trình này dừng sau hữu hạn bước do

$$\delta(b), \delta(r_0), \delta(r_1), \dots$$

là một dãy giảm thực sự những số tự nhiên. Bởi vậy theo bổ đề ta được

$$(a, b) = (b, r_1) = \dots = (r_{n-1}, r_n) = r_n,$$

nghĩa là ước chung lớn nhất của a, b bằng số dư cuối cùng r_n trong thuật toán nói trên.

Ví dụ. Tìm UCLN $g(x)$ của $a(x) = 2x^4 + 2$ và $b(x) = x^5 + 2$ trong $\mathbb{Z}_3[x]$, và tìm $s(x), t(x) \in \mathbb{Z}_3[x]$, sao cho

$$g(x) = s(x).(2x^4 + 2) + t(x).(x^5 + 2).$$

Lời giải. Lập lại việc sử dụng thuật toán chia (như sau đây), chúng ta có

$$\begin{aligned} \text{(i)} \quad x^5 + 2 &= (2x)(2x^4 + 2) + (2x + 2). \\ \text{(ii)} \quad 2x^4 + 2 &= (x^3 + 2x^2 + x + 2)(2x + 2) + 1. \\ \text{(iii)} \quad 2x + 2 &= (2x + 2).1 + 0. \end{aligned}$$

Do đó, $g(x) = 1$ và ta có thể tìm các đa thức $s(x), t(x)$ dựa vào thuật toán trên như sau:

$$\begin{aligned} 1 &= a(x) - (x^3 + 2x^2 + x + 2)(2x + 2) \\ &= a(x) - (x^3 + 2x^2 + x + 2)[b(x) - (2x)a(x)] \\ &= a(x).(2x^4 + x^3 + 2x^2 + x + 1) + b(x)(2x^3 + x^2 + 2x + 1). \end{aligned}$$

Từ đó ta có

$$\begin{aligned}s(x) &= 2x^4 + x^3 + 2x^2 + x + 1, \text{ và} \\ t(x) &= 2x^3 + x^2 + 2x + 1.\end{aligned}$$

Ví dụ. Tìm UCLN của $a(x) = x^4 + x^3 + 3x - 9$ và $b(x) = 2x^3 - x^2 + 6x - 3$ trong $\mathbb{Q}[x]$.

Lời giải. Theo thuật toán chia chúng ta có :

$$\begin{aligned}a(x) &= \left(\frac{1}{2}x + \frac{3}{4}\right)b(x) - \frac{9}{4}x^2 - \frac{27}{4} \\ b(x) &= \left(-\frac{8}{9} + \frac{4}{9}\right)\left(-\frac{9}{4}x^2 - \frac{27}{4}\right).\end{aligned}$$

Do đó

$$\text{UCLN}(a(x), b(x)) = -\frac{9}{4}x^2 - \frac{27}{4}.$$

Bây giờ chúng ta xác định khi nào thì thương của một vành Oclit là một trường. Kết quả này cho phép chúng ta xác định nhiều trường mới.

Định lý 4.5. Cho a là một phần tử của vành Oclit E . Vành thương $E/(a)$ là một trường nếu và chỉ nếu a bất khả quy trong E .

Chứng minh. Giả sử rằng a là một phần tử bất khả quy của E và $b + (a)$ là một phần tử khác 0 của $E/(a)$. Khi đó b không phải là bội của a , và do a là bất khả quy nên $\text{UCLN}(a, b) = 1$. Do đó tồn tại $s, t \in E$ sao cho $sa + bt = 1$.

Bây giờ, do $sa \in (a)$, nên

$$[t + (a)].[b + (a)] = 1 + (a)$$

là phần tử đơn vị của vành thương $E/(a)$. Bởi vậy $t + (a)$ là nghịch đảo của $b + (a)$ trong $E/(a)$ và $E/(a)$ là một trường.

Bây giờ giả sử rằng a khả quy trong E , nghĩa là tồn tại các phần tử s và t không khả nghịch, thoả mãn $st = a$. Ta có

$$\delta(s) < \delta(st) = \delta(a), \text{ và } \delta(t) < \delta(st) = \delta(a).$$

Do đó s không chia hết cho a , và $s \notin (a)$. Tương tự, $t \notin (a)$, và không có phần tử nào trong hai phần tử $(a) + s$ và $(a) + t$ là phần tử 0 trong $E/(a)$. Tuy nhiên

$$[s + (a)].[t + (a)] = st + (a) = (a),$$

là phần tử 0 của vành thương $E/(a)$. Bởi vậy, vành $E/(a)$ có ước của 0 và không thể là một trường. $\square$

Ví dụ trong vành thương $\mathbb{Q}[x]/P$, với $P = (x^2 - 1)$, các phần tử $x + 1 + P$ và $x - 1 + P$ là các ước của 0 bởi vì

$$(x + 1 + P)(x - 1 + P) = x^2 - 1 + P = P$$

là phần tử 0.

Hệ quả 4.6. $\mathbb{Z}_p = \mathbb{Z}/(p)$ là một trường nếu và chỉ nếu p nguyên tố.

Một trường hợp riêng khác của Định lý 4.5 là định lý quan trọng sau đây.

Định lý 4.7. Vành $F[x]/(p(x))$ là một trường nếu và chỉ nếu đa thức $p(x)$ bất khả quy trên trường F . Hơn nữa, vành $F[x]/(p(x))$ luôn chứa một vành con đẳng cấu với trường F .

Chứng minh. Xét vành đa thức $F[x]$ và gọi I là ideal của $F[x]$ sinh bởi $p(x)$. Theo Định lý 4.5, vành thương $E = F[x]/I$ là một trường. Xét phép chiếu

$$\begin{aligned}\varphi: F[x] &\rightarrow F[x]/I = E \\ f(x) &\mapsto f(x) + I\end{aligned}$$

Cái thu hẹp $\varphi|_F = \varphi_0$ là đơn cấu. Thật vậy, với $a, b \in F$ mà $\bar{a} = \bar{b}$ thì $a - b$ chia hết cho $p(x)$. Vậy $a - b = 0$.

Vì φ_0 là đơn cấu nên ta có thể đồng nhất F với trường con $\varphi_0(F)$ của E qua đơn cấu φ_0 , nghĩa là $a \equiv \bar{a}$ với $a \in F$. $\square$

Chúng ta có thể chứng minh đa thức $x^2 - 2$ không có nghiệm trong $\mathbb{Q}$, do đó nó là một đa thức bất khả quy trên $\mathbb{Q}$. Nghiệm của nó là một số thực, ký hiệu bởi $\sqrt{2}$. Bây giờ chúng ta sẽ xem xét tình huống tổng quát của sự kiện này, cho trước một đa thức bất khả quy $p(x) \in F[x]$, khi đó có hay không một mở rộng E của F chứa nghiệm u của $p(x)$? Câu trả lời là có và bây giờ chúng ta sẽ chỉ ra cách xây dựng một trường mở rộng của trường đã cho để một đa thức cho trước có nghiệm.

Định lý 4.8. Giả sử $p(x) = a_0 + a_1x + \dots + a_nx^n$ ($n > 1$) là một đa thức bất khả quy trên trường F . Khi đó tồn tại một trường E là mở rộng của F và chứa một nghiệm c của $p(x)$.

Chứng minh. Xét vành đa thức $F[x]$ và gọi I là ideal của $F[x]$ sinh bởi $p(x)$. Theo Định lý 4.7, vành thương $E = F[x]/I$ là một trường, và ta có thể đồng nhất F với một trường con của E bởi $a \equiv \bar{a}$ với $a \in F$. Với phép đồng nhất này trong $E = F[x]/I$ ta có

$$\overline{p(x)} = \bar{a}_0 + \bar{a}_1\bar{x} + \cdots + \bar{a}_n\bar{x}^n = \bar{0}$$

hay

$$a_0 + a_1c + \cdots + a_nc^n = 0, \quad \text{với } c = \bar{x}.$$

Vậy $c \in E$ và c là một nghiệm của đa thức $p(x)$. □

Ví dụ. Lập bảng nhân cho trường $\mathbb{Z}_3[x]/(x^2 + 1)$.

Lời giải. Nếu $x = 0, 1$ hoặc 2 trong $\mathbb{Z}_3$, thì $x^2 + 1 = 1, 2$ hoặc 2 ; do đó $x^2 + 1$ không có nhân tử tuyến tính. Bởi vậy, $x^2 + 1$ bất khả quy trên $\mathbb{Z}_3$ và theo Định lý 4.7, vành thương $\mathbb{Z}_3[x]/(x^2 + 1)$ là một trường. Theo Định lý 1.10, các phần tử của trường này có thể viết được dưới dạng

$$\mathbb{Z}_3[x]/(x^2 + 1) = \{a_0 + a_1x \mid a_0, a_1 \in \mathbb{Z}_3\}.$$

Do đó trường chứa 9 phần tử. Bảng phép nhân các đa thức trong $\mathbb{Z}_3[x]$ có thể tính được bằng cách thay x^2 bởi -1 hoặc 2 , vì

$$x^2 \equiv -1 \equiv 2 \pmod{x^2 + 1}.$$

Ví dụ. Chứng minh rằng $\mathbb{Q}[x]/(x^3 - 5) = \{a_0 + a_1x + a_2x^2 \mid a_i \in \mathbb{Q}\}$ là một trường và tìm nghịch đảo của phần tử $x + 1$.

Lời giải. Đa thức $(x^3 - 5)$ không có nhân tử tuyến tính và do đó là bất khả quy trên $\mathbb{Q}$. Bởi vậy, theo Định lý 4.7, $\mathbb{Q}[x]/(x^3 - 5)$ là một trường.

Nếu $s(x)$ là nghịch đảo của $x + 1$, thì

$$(x + 1)s(x) \equiv 1 \pmod{x^3 - 5};$$

tức là

$$(x + 1)s(x) + (x^3 - 5)t(x) = 1 \text{ với } t(x) \in \mathbb{Q}[x].$$

Chúng ta có thể tìm được những đa thức $s(x)$ và $t(x)$ như vậy bằng thuật toán Oclit. Chúng ta có

$$\begin{aligned} x^3 - 5 &= (x^2 - x + 1)(x + 1) - 6 \\ \Rightarrow 6 &\equiv (x^2 - x + 1)(x + 1) \pmod{x^3 - 5} \\ \Rightarrow 1 &\equiv \frac{1}{6}(x^2 - x + 1)(x + 1) \pmod{x^3 - 5}. \end{aligned}$$

Vì vậy trong $\mathbb{Q}[x]/(x^3 - 5)$ ta có

$$(x+1)^{-1} = \frac{1}{6}x^2 - \frac{1}{6}x + \frac{1}{6}$$

Ví dụ. Chứng minh rằng $\mathbb{Z}_3[x]/(x^3 + 2x + 1)$ là một trường có 27 phần tử và tìm nghịch đảo của phần tử x^2 .

Lời giải. Nếu $x = 0, 1$, hoặc 2 trong $\mathbb{Z}_3$, thì $x^3 + 2x + 1 = 1$; do đó $x^3 + 2x + 1$ không có nhân tử tuyến tính và là bất khả quy. Do đó

$$\mathbb{Z}_3[x]/(x^3 + 2x + 1) = \{a_0 + a_1x + a_2x^2 \mid a_i \in \mathbb{Z}_3\}$$

là một trường có $3^3 = 27$ phần tử.

Như trong ví dụ trên, để tìm nghịch đảo của x^2 , chúng ta áp dụng thuật toán Oclit cho $x^3 + 2x + 1$ và x^2 trong $\mathbb{Z}_3[x]$. Chúng ta có

$$\begin{aligned}x^3 + 2x + 1 &= x(x^2) + (2x + 1), \\x^2 &= (2x + 2)(2x + 1) + 1.\end{aligned}$$

Do đó

$$\begin{aligned}1 &= x^2 - (2x + 2)[(x^3 + 2x + 1) - x \cdot x^2] \\&= x^2(2x^2 + 2x + 1) - (2x + 2)(x^3 + 2x + 1).\end{aligned}$$

nên

$$1 \equiv x^2(2x^2 + 2x + 1) \pmod{(x^3 + 2x + 1)}$$

và nghịch đảo của x^2 trong $\mathbb{Z}_3[x]/(x^3 + 2x + 1)$ là $2x^2 + 2x + 1$.

Bài tập

4.1. Chứng minh rằng các vành sau là vành Oclit:

- a) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$;
- b) $\mathbb{Z}[x]/(x^2 + 2)$;
- c) $A = \{a + b\sqrt{2}i \mid a, b \in \mathbb{Z}\}$.

4.2. Chứng minh rằng mỗi trường là một vành Oclit.

4.3. Giả sử A là một vành Oclit. Chứng minh rằng A là một trường khi và chỉ khi $\delta(x)$ là hằng với mọi $x \in A^*$.

4.4. Giả sử

$$f(x) = x^5 + x^3 + x^2 + x + 1,$$

$$g(x) = x^3 + 2x^2 + x + 1.$$

Tìm ước chung lớn nhất của $f(x)$ và $g(x)$ trong $\mathbb{Z}[x]$.

Với các bài tập từ 4.5 đến 4.11, tìm UCLN của các phần tử a, b trong vành $\mathcal{O}$ lit đã cho, và tìm các phần tử s, t trong vành đó thoả mãn $as + bt = UCLN(a, b)$.

4.5. $a = 33, b = 42$ trong $\mathbb{Z}$.

4.6. $a = 2891, b = 1589$ trong $\mathbb{Z}$.

4.7. $a = 2x^3 - 4x^2 - 8x + 1, b = 2x^3 - 5x^2 - 5x + 2$ trong $\mathbb{Q}[x]$.

4.8. $a = x^6 - x^3 - 16x^2 + 12x - 2, b = x^5 - 2x^2 - 16x + 8$ trong $\mathbb{Q}[x]$.

4.9. $a = x^4 + x + 1, b = x^3 + x^2 + x$ trong $\mathbb{Z}_3[x]$.

4.10. $a = x^4 + 2, b = x^3 + 3$ trong $\mathbb{Z}_5[x]$.

4.11. $a = 4 - i, b = 1 + i$ trong $\mathbb{Z}[i]$.

4.12. $\mathbb{Z}[x]$ có phải là một vành $\mathcal{O}$ lit không khi $\delta(f(x)) = \deg f(x)$ với mỗi đa thức khác 0 hay không? $\mathbb{Z}[x]$ có phải là một vành $\mathcal{O}$ lit với một định nghĩa nào khác của $\delta(f(x))$ hay không?

4.13. Nếu R là một miền nguyên và $R[x]$ là vành $\mathcal{O}$ lit, chứng minh rằng R phải là một trường.

Với các bài tập từ 4.14, 4.15, xác định bằng cộng và nhân cho các vành đã cho. Tìm tất cả các ước của 0 trong mỗi vành. Vành nào trong các vành này là trường?

4.14. $\mathbb{Z}_2[x]/(x^3 + 1)$.

4.15. $\mathbb{Z}_3[x]/(x^2 + 2x + 2)$.

Các phần tử nào trong các bài tập từ 4.16 đến 4.21 là bất khả quy trong các vành đã cho? Nếu có phần tử bất khả quy, tìm trường các thương tương ứng theo môđun idêan sinh bởi phần tử đó.

4.16. $x^2 - 2$ trong $\mathbb{R}[x]$.

4.17. $x^3 + x^2 + 2$ trong $\mathbb{Z}_3[x]$.

4.18. $x^4 - 2$ trong $\mathbb{Q}[x]$.

4.19. $x^7 + 4x^3 - 3ix + 1$ trong $\mathbb{C}[x]$.

4.20. $x^2 - 3$ trong $\mathbb{Q}(\sqrt{2})[x]$.

4.21. $3x^5 - 4x^3 + 2$ trong $\mathbb{Q}[x]$.

4.22. Giả sử vành E với ánh xạ $\delta : E^* \rightarrow \mathbb{N}$ là một vành Oclit. Chứng minh tồn tại ánh xạ Oclit

$$\delta' : E^* \rightarrow \mathbb{N}$$

sao cho $\delta'(E^*) = \{0, 1, \dots, n\}$ với $n \geq 0$ hoặc $\delta'(E^*) = \mathbb{N}$.

4.23. Giả sử E là một vành Oclit với ánh xạ Oclit δ . Chứng minh $\delta(u)$ là phần tử bé nhất của $\delta(E^*)$ khi và chỉ khi u khả nghịch trong E .

4.24. Giả sử E là một miền nguyên nhưng không là trường. Chứng minh rằng điều kiện cần để E là vành Oclit là tồn tại một phần tử không khả nghịch $x \in E$ sao cho mọi lớp của $E/(x)$ có một đại diện hoặc khả nghịch hoặc bằng 0.

4.25. Chứng minh vành

$$A = \left\{ a + b \frac{1 + i\sqrt{19}}{2} \mid a, b \in \mathbb{Z} \right\}$$

không phải là một vành Oclit. (Người ta có thể chứng minh A là vành chính).

Chương VI

PHÂN TÍCH ĐA THỨC TRÊN CÁC TRƯỜNG SỐ

1. *Phân tích các đa thức thực và phức*
2. *Phân tích các đa thức nguyên và hữu tỷ*
3. *Phân tích các đa thức trên trường hữu hạn*

Trong chương trước chúng ta thấy rằng mỗi đa thức trên một trường F luôn có thể phân tích thành tích của những đa thức bất khả quy (Hệ quả 3.9 Chương IV), và chúng ta cũng đã thấy rằng nếu một đa thức phân tích được thành tích những đa thức bất khả quy thì ta có thể xây dựng được trường mới chứa nghiệm của đa thức này. Bây giờ chúng ta sẽ nghiên cứu các phương pháp phân tích các đa thức trên các trường hệ số khác nhau.

1. Phân tích các đa thức thực và phức

Ta nhắc lại rằng, một đa thức $f(x)$ có bậc dương được gọi là *khả quy trên trường F* nếu nó có thể phân tích được thành 2 đa thức có bậc dương trong $F[x]$. Nếu nó không thể phân tích như vậy, $f(x)$ được gọi là *bất khả quy trên F* , và $f(x)$ là một phần tử bất khả quy của vành $F[x]$.

Cần chú ý rằng tính khả quy phụ thuộc vào trường F .

Để xác định các đa thức nào là bất khả quy trong $\mathbb{C}[x]$ và trong $\mathbb{R}[x]$ chúng ta cần tới Định lý cơ bản sau đây, lần đầu tiên được chứng minh bởi Gauss trong luận án tiến sĩ của ông năm 1799.

Định lý 1.1 (Định lý cơ bản của Đại số). *Nếu $f(x)$ là một đa thức trong $\mathbb{C}[x]$ có bậc dương, thì $f(x)$ có nghiệm trong $\mathbb{C}$.*

Phép chứng minh của định lý này là không thuần túy đại số. Nó dựa trên một kết quả được chứng minh bằng giải tích, đó là một đa thức bậc lẻ thì có nghiệm thực.

Bây giờ chúng ta sẽ sử dụng Định lý cơ bản của đại số để xét tính bất khả quy của các đa thức trên các trường số thực và phức.

Định lý sau đây chứng tỏ rằng các nghiệm phức của các đa thức thực tồn tại theo từng cặp liên hợp.

Định lý 1.2. (i) Nếu $z = a + ib$ là một nghiệm phức của đa thức thực $f(x) \in \mathbb{R}[x]$, thì liên hợp của nó $\bar{z} = a - ib$ cũng là một nghiệm. Do đó đa thức thực

$$(x - z)(x - \bar{z}) = x^2 - 2ax + (a^2 + b^2)$$

là một nhân tử của $f(x)$.

(ii) Nếu $a, b, c \in \mathbb{Q}$ và $a + b\sqrt{c}$ là một nghiệm vô tỷ của đa thức hữu tỷ $f(x) \in \mathbb{Q}[x]$, thì $a - b\sqrt{c}$ cũng là một nghiệm, và đa thức hữu tỷ

$$x^2 - 2ax + (a^2 - b^2c)$$

là một nhân tử của $f(x)$.

Chứng minh. (i) Xét đa thức

$$g(x) = x^2 - 2ax + a^2 + b^2 = (x - z)(x - \bar{z}).$$

Theo thuật toán chia trong $\mathbb{R}[x]$, tồn tại các đa thức thực $q(x)$ và $r(x)$ sao cho

$$f(x) = q(x)g(x) + r(x), \text{ trong đó } r(x) = 0 \text{ hoặc } \deg r(x) < 2.$$

Do đó $r(x) = r_0 + r_1x$ trong đó $r_0, r_1 \in \mathbb{R}$. Bây giờ $z = a + ib$ là một nghiệm của $f(x)$ và của $g(x)$; do đó, nó cũng là một nghiệm của $r(x)$, do đó $0 = r_0 + r_1(a + ib)$. Cho phần thực và phần ảo bằng nhau, chúng ta có $r_0 + r_1a = 0$ và $r_1b = 0$. Nhưng khi đó

$$r(\bar{z}) = r(a - ib) = r_0 + r_1(a - ib) = r_0 + r_1a - ir_1b = 0.$$

Do $\bar{z}$ là một nghiệm của $r(x)$ và $g(x)$, nó phải là nghiệm của $f(x)$.

Nếu z là số phức và không phải là số thực, thì $b \neq 0$. Trong trường hợp này $r_1 = 0$ và $r_0 = 0$; do đó $g(x) | f(x)$.

(ii) Được chứng minh tương tự như phần (i). □

Các đa thức bất khả quy trên các trường số thực và phức được cho bởi định lý sau.

Định lý 1.3. (i) Các đa thức bất khả quy trong vành $\mathbb{C}[x]$ là các đa thức bậc 1.

(ii) Các đa thức bất khả quy trong vành $\mathbb{R}[x]$ là các đa thức bậc 1 cùng với các đa thức bậc 2 có dạng $ax^2 + bx + c$, trong đó $b^2 < 4ac$.

Chứng minh. (i) Các đa thức bậc 0 là các phân tử khả nghịch trong $\mathbb{C}[x]$. Theo định lý cơ bản của Đại số, mỗi đa thức có bậc dương có một nghiệm trong $\mathbb{C}$ và do đó là nhân tử tuyến tính. Do đó tất cả các đa thức có bậc lớn hơn 1 khả quy và các đa thức bậc 1 là các đa thức bất khả quy.

(ii) Các đa thức bậc 0 là các phân tử khả nghịch của $\mathbb{R}[x]$. Theo phần (i) và theo định lý nhân tử duy nhất, mọi đa thức thực có bậc dương có thể phân tích được thành tích các nhân tử tuyến tính trong $\mathbb{C}[x]$. Theo Định lý 1.2(i), các nghiệm không thực của nó tạo thành các cặp liên hợp, mà tích các nhân tử tương ứng cho ta nhân tử bậc 2 trong $\mathbb{R}[x]$ có dạng $ax^2 + bx + c$, trong đó $b^2 < 4ac$. Do đó mỗi đa thức thực có thể được phân tích thành tích các nhân tử tuyến tính thực và các nhân tử bậc 2 thực có dạng trên. $\square$

Ví dụ. Tìm hạt nhân và ảnh của cầu xạ vành $\psi : \mathbb{Q}[x] \rightarrow \mathbb{R}$ được cho bởi $\psi(f(x)) = f(\sqrt{2})$.

Lời giải. Nếu $p(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Q}[x]$, thì

$$\begin{aligned}\psi(p(x)) &= a_0 + a_1\sqrt{2} + \cdots + a_n(\sqrt{2})^n \\ &= (a_0 + 2a_2 + 4a_4 + \cdots) + \sqrt{2}(a_1 + 2a_3 + 4a_5 + \cdots),\end{aligned}$$

do đó

$$\psi(p(x)) \in \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

Vì vậy $\text{Im}\psi \subseteq \mathbb{Q}(\sqrt{2})$ và $\text{Im}\psi = \mathbb{Q}(\sqrt{2})$ bởi vì $\psi(a + bx) = a + b\sqrt{2}$.

Nếu $p(x) \in \text{Ker}\psi$, thì $p(\sqrt{2}) = 0$; do đó, theo Định lý 1.2(ii), $p(-\sqrt{2}) = 0$, và $p(x)$ chứa một nhân tử $(x^2 - 2)$. Ngược lại, nếu $p(x)$ chứa một nhân tử $(x^2 - 2)$, thì $p(\sqrt{2}) = 0$ và $p(x) \in \text{Ker}\psi$. Từ đó

$$\text{Ker}\psi = \{(x^2 - 2)q(x) \mid q(x) \in \mathbb{Q}[x]\},$$

tức là, tập tất cả các đa thức trong $\mathbb{Q}[x]$ có $(x^2 - 2)$ là một nhân tử.

2. Phân tích các đa thức nguyên và các đa thức hữu tỷ

Một đa thức hữu tỷ luôn luôn có thể đưa được về một đa thức nguyên bằng cách nhân nó với bội chung nhỏ nhất (BCNN) của các mẫu số của các hệ số của nó. Bây giờ chúng ta đưa ra các phương pháp khác nhau để xác định xem một đa thức nguyên có nghiệm hữu tỷ hay bất khả quy trên $\mathbb{Q}$.

Định lý 2.1 (Định lý nghiệm hữu tỷ). Cho đa thức với hệ số nguyên

$$p(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x].$$

Nếu r/s là nghiệm hữu tỷ của $p(x)$ và $\text{UCLN}(r, s) = 1$, thì:

- (i) $r|a_0$.
- (ii) $s|a_n$.

Chứng minh. Nếu $p(r/s) = 0$, thì

$$a_0 + a_1(r/s) + \cdots + a_{n-1}(r/s)^{n-1} + a_n(r/s)^n = 0,$$

từ đó

$$a_0s^n + a_1rs^{n-1} + \cdots + a_{n-1}r^{n-1}s + a_nr^n = 0.$$

Bởi vậy,

$$a_0s^n = -r(a_1s^{n-1} + \cdots + a_{n-1}r^{n-2}s + a_nr^{n-1}),$$

vì vậy $r|a_0s^n$. Do $\text{UCLN}(r, s) = 1$, từ Mệnh đề 4.9 Chương I ta suy ra rằng $r|a_0$.

Bây giờ ta lại có

$$a_nr^n = -s(a_0s^{n-1} + a_1rs^{n-2} + \cdots + a_{n-1}r^{n-1}).$$

Lập luận tương tự ta có $s|a_n$. □

Ví dụ. Phân tích $p(x) = 2x^3 + 3x^2 - 1$ trong $\mathbb{Q}[x]$.

Lời giải. Nếu $p(r/s) = 0$, thì theo Định lý 2.1, $r|(-1)$, và $s|2$. Do đó $r = \pm 1$ và $s = \pm 1$ hoặc ± 2 , và các giá trị của r/s chỉ có thể là $\pm 1, \pm 1/2$. Do $p(1) = 4, p(-1) = 0$ nên $p(x)$ chia hết cho $x + 1$. Thực

hiện phép chia ta được $p(x) = (x+1)(2x^2+x-1)$. Tam thức bậc hai $2x^2+x-1$ có hai nghiệm là $x = -1$ và $x = \frac{1}{2}$ nên ta có

$$p(x) = (x+1)^2(2x-1).$$

Trong định lý trên nếu $a_n = 1$ ta có hệ quả sau:

Hệ quả 2.2. Cho đa thức $p(x) \in \mathbb{Z}[x]$ với hệ tử cao nhất bằng 1. Khi đó nghiệm hữu tỷ (nếu có) của $f(x)$ là nghiệm nguyên, và số nguyên này là ước của số hạng tự do.

Ví dụ. Chứng minh rằng $\sqrt[5]{2}$ là số vô tỷ.

Lời giải. Trước hết ta thấy $\sqrt[5]{2}$ là một nghiệm của $x^5 - 2$. Nếu đa thức này có một nghiệm hữu tỷ c thì theo Hệ quả 2.2, c là một số nguyên ước của 2. Do đó các nghiệm hữu tỷ chỉ có thể là $\pm 1, \pm 2$. Từ bảng dưới đây chúng ta thấy rằng không có số nào trong chúng là nghiệm, nên tất cả các nghiệm của đa thức $x^5 - 2$ phải là các số vô tỷ.

Bảng giá trị

x	-2	-1	1	2
$x^5 - 2$	-34	-3	-1	30

Nghiệm hữu tỷ của đa thức $p(x) \in \mathbb{Z}[x]$ cũng có thể được tính theo phương pháp sau.

Nhân hai vế của phương trình $p(x) = 0$ với a_n^{n-1} và đặt $y = a_n x$ ta được phương trình

$$q(y) = b_0 + b_1 y + \dots + b_{n-1} y^{n-1} + y^n = 0,$$

ở đó hệ số của y^n bằng 1. Khi đó theo Hệ quả 2.2 nghiệm hữu tỷ của phương trình $q(y) = 0$ nếu có phải là số nguyên và là ước của b_0 . Trong trường hợp đơn giản ta có thể kiểm tra trực tiếp những ước này có là nghiệm của phương trình hay không. Đối với trường hợp chung ta có thể làm giảm số phép thử nhờ một kỹ thuật đơn giản được trình bày dưới đây.

Giả sử $q(1) \neq 0$ và $q(-1) \neq 0$. Nếu c là một nghiệm nguyên của $q(y)$ thì $q(y)$ chia hết cho $y - c$:

$$q(y) = (y - c)h(y).$$

Theo định lý về phép chia với dư ta có $h(y) \in \mathbb{Z}[y]$, nghĩa là các hệ số của $h(y)$ đều là số nguyên. Từ đó

$$h(1) = \frac{q(1)}{1-c}, -h(-1) = \frac{q(-1)}{1+c}$$

là những số nguyên. Điều này cho phép chúng ta chỉ cần kiểm tra đối với những ước c của b_0 mà

$$\frac{q(1)}{1-c}, \frac{q(-1)}{1+c}$$

đều là những số nguyên.

Nếu $q(1) = 0$ hoặc $q(-1) = 0$ thì ta chia $q(y)$ cho $y - 1$ (tương ứng cho $y + 1$) và tiếp tục làm như trên với đa thức thương.

Ví dụ. Tìm nghiệm hữu tỷ của phương trình

$$4x^3 + 6x^2 + 12x - 5 = 0.$$

Lời giải. Nhân hai vế của phương trình với 2 ta được

$$8x^3 + 12x^2 + 24x - 10 = 0.$$

Đặt $y = 2x$ phương trình được đưa về dạng

$$f(y) = y^3 + 3y^2 + 12y - 10 = 0.$$

Các ước của 10 là $\pm 1, \pm 2, \pm 5$. Trước hết, ta thấy $f(1) = 6, f(-1) = -20$. Từ đó có thể thấy các phân số

$$\frac{f(1)}{1-c}, \frac{f(-1)}{1+c}$$

cùng là số nguyên chỉ với $c = -2$. Thử lại ta thấy rằng $f(-2) \neq 0$. Vậy phương trình không có nghiệm hữu tỷ.

Ví dụ. Tìm nghiệm hữu tỷ của đa thức

$$f(x) = x^5 - 2x^4 - 4x^3 + 4x^2 - 5x + 6.$$

Lời giải. Trước hết ta thấy $f(1) = 0$, bởi vậy chia $f(x)$ cho $x - 1$ ta được

$$f(x) = (x - 1)g(x), \quad g(x) = x^4 - x^3 - 5x^2 - x - 6.$$

Ta có $g(1) = -12$, $g(-1) = -8$ và các ước của 6 là $\pm 2, \pm 3, \pm 6$. Lần lượt thay các giá trị $c = \pm 2$ vào các biểu thức

$$\frac{g(1)}{1-c}, \frac{g(-1)}{1+c}$$

ta thấy chúng là số nguyên chỉ với $c = -2$. Khi đó $g(-2) = 0$. Chia $g(x)$ cho $x + 2$ ta được

$$g(x) = (x + 2)h(x), h(x) = x^3 - 3x^2 + x - 3.$$

Tiếp tục làm như trên với đa thức $h(x)$ ta được các nghiệm của $f(x)$ là 1, -2 và 3.

Việc tính các hệ số của đa thức thương $h(x)$ và dư trong phép chia $f(x)$ cho $x - c$ có thể được thực hiện nhờ sơ đồ Hoocne. Giả sử

$$f(x) = (x - c)h(x) + r$$

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$$

$$h(x) = b_0x^{n-1} + b_1x^{n-2} + \dots + b_{n-2}x + b_{n-1}$$

So sánh hệ số của các đa thức ở hai vế ta có

$$\begin{aligned} a_0 &= b_0, & a_1 &= b_1 - b_0c \\ a_{n-1} &= b_{n-1} - b_{n-2}c \\ a_n &= -b_{n-1}c + r \end{aligned}$$

Từ đó ta có

$$b_0 = a_0, b_1 = a_1 + b_0c, \dots, b_{n-1} = a_{n-1} + b_{n-2}c, r = a_n + b_{n-1}c$$

Nghĩa là các hệ số b_i ($i > 0$) và r có được bằng cách lấy hệ số a_i tương ứng cộng với $b_{i-1}c$.

Kết quả này có thể viết dưới dạng thuận lợi sau:

	a_0	a_1	$\dots$	a_{n-1}	a_n
c	b_0	$a_1 + b_0c$	$\dots$	$a_{n-1} + b_{n-2}c$	$r = a_n + b_{n-1}c$

Định lý 2.3 (Bổ đề Gauss). Cho đa thức với hệ số nguyên

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x].$$

Nếu $f(x)$ có thể phân tích được trong $\mathbb{Q}[x]$ thành $f(x) = g(x)h(x)$ với $g(x), h(x) \in \mathbb{Q}[x]$, thì $f(x)$ cũng phân tích được trong $\mathbb{Z}[x]$.

Một cách tương đương, nếu đa thức $f(x) \in \mathbb{Z}[x]$, bậc $n > 1$, bất khả quy trên $\mathbb{Z}$ thì cũng bất khả quy trên $\mathbb{Q}$.

Chứng minh. Trước hết ta có nhận xét rằng: Một đa thức $f(x) \in \mathbb{Q}[x]$ luôn luôn viết được dưới dạng tích của một phân số tối giản và một đa thức có các hệ số nguyên tố cùng nhau. Một đa thức như vậy được gọi là đa thức nguyên bản. Thật vậy, giả sử

$$f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \cdots + \frac{a_n}{b_n}x^n, \quad a_i, b_i \in \mathbb{Z}$$

trong đó các hệ số hữu tỷ của $f(x)$ ở dạng phân số tối giản. Đặt $q = b_0b_1 \cdots b_n$ ta có

$$f(x) = \frac{1}{q}g(x), \quad g(x) \in \mathbb{Z}[x].$$

Gọi p là ước chung lớn nhất của các hệ tử của $g(x)$ ta được $g(x) = pf^*(x)$, với $f^*(x)$ là đa thức nguyên bản. Từ đó

$$f(x) = \frac{p}{q}f^*(x).$$

Tính duy nhất của biểu diễn này có thể chứng minh dễ dàng, dành cho bạn đọc như một bài tập.

Bây giờ ta chứng minh định lý. Giả sử $f(x) = g(x)h(x)$ là sự phân tích trong $\mathbb{Q}[x]$. Theo nhận xét trên ta có,

$$f = \frac{s}{u}g^*(x)\frac{t}{v}h^*(x) = \frac{st}{uv}g^*(x)h^*(x),$$

trong đó $g^*(x), h^*(x)$ là những đa thức nguyên bản. Từ đó

$$uvf(x) = stg^*(x)h^*(x).$$

Để chứng minh định lý, chúng ta chứng minh rằng $uv|st$ bằng cách chứng minh rằng không có ước nguyên tố p của uv có thể chia hết mọi hệ số của $g^*(x)h^*(x)$. Thật vậy, giả sử

$$\begin{aligned}g^*(x) &= b_0 + \cdots + b_k x^k, \\h^*(x) &= c_0 + \cdots + c_l x^l.\end{aligned}$$

Chọn một ước nguyên tố p của uv . Do $g^*(x), h^*(x)$ là nguyên bản nên phải có những hệ số đầu tiên b_r, c_s không chia hết cho p . Hệ số của x^{r+s} của tích $g^*(x)h^*(x)$ là

$$(b_0 c_{r+s} + \cdots + b_{r-1} c_{s+1}) + b_r c_s + (b_{r+1} c_{s-1} + \cdots + b_{r+s} c_0).$$

Các tổng ở hai đầu ngoặc đều chia hết cho p , nhưng $b_r c_s$ không chia hết cho p nên hệ số của x^{r+s} không chia hết cho p . Điều này chứng tỏ p không là ước chung của các hệ số của tích $g^*(x)h^*(x)$. Bởi vậy, p phải là ước của st . Từ đó suy ra rằng $uv|st$, và do đó $f(x)$ phân tích được trong $\mathbb{Z}[x]$. $\square$

Ví dụ. Phân tích $p(x) = x^4 - 3x^2 + 2x + 1$ thành các nhân tử bất khả quy trong $\mathbb{Q}[x]$.

Lời giải. Theo Hệ quả 2.2, các nghiệm hữu tỷ của $p(x)$ chỉ có thể là ± 1 . Tuy nhiên dễ thử lại rằng các số này không phải là nghiệm, do đó $p(x)$ không có nhân tử tuyến tính.

Bởi vậy, nếu $p(x)$ phân tích được thì nó phải phân tích thành tích của hai đa thức bậc 2, và theo Bổ đề Gauss các nhân tử này có thể chọn được sao cho các hệ số là nguyên. Giả sử rằng

$$\begin{aligned}x^4 - 3x^2 + 2x + 1 &= (x^2 + ax + b)(x^2 + cx + d) \\&= x^4 + (a + c)x^3 + (b + d + ac)x^2 + (bc + ad)x + bd\end{aligned}$$

Do đó chúng ta phải giải các hệ sau để tìm nghiệm nguyên:

$$\begin{aligned}a + c &= 0, \\b + d + ac &= -3, \\bc + ad &= 2, \\bd &= 1.\end{aligned}$$

Từ đẳng thức cuối cùng ta có

$$b = d = \pm 1 \quad \text{và} \quad b(a + c) = 2.$$

Từ đó $a + c = \pm 2$, và chúng ta gặp mâu thuẫn. Đa thức đã cho không thể phân tích thành tích của hai đa thức bậc 2 và do đó nó bất khả quy trong $\mathbb{Q}[x]$.

Định lý sau cho ta một điều kiện đủ khá thuận tiện để xác định một đa thức với hệ số nguyên là bất khả quy trên $\mathbb{Q}$.

Định lý 2.4 (Tiêu chuẩn Eisenstein). Cho đa thức với các hệ số nguyên

$$f(x) = a_0 + a_1x + \dots + a_nx^n, \quad (n > 1)$$

và giả sử tồn tại số nguyên tố p sao cho p không chia hết a_n nhưng chia hết các hệ số còn lại và p^2 không chia hết a_0 . Khi đó $f(x)$ là bất khả quy trong $\mathbb{Q}[x]$.

Chứng minh. Giả sử $f(x)$ khả quy trên $\mathbb{Q}$. Khi đó theo Định lý 2.3 nó cũng khả quy trên $\mathbb{Z}$,

$$f(x) = g(x)h(x)$$

$$g(x) = b_0 + b_1x + \dots + b_rx^r, \quad 0 < r < n, \quad b_i \in \mathbb{Z}$$

$$h(x) = c_0 + c_1x + \dots + c_sx^s, \quad 0 < s < n, \quad c_i \in \mathbb{Z}.$$

Theo giả thiết p chia hết $a_0 = b_0c_0$. Nhưng vì p^2 không chia hết a_0 nên chỉ có một trong hai số b_0, c_0 chia hết cho p , chẳng hạn b_0 chia hết cho p . Do p không chia hết $a_n = b_rc_s$ nên p không chia hết b_r . Giả sử b_k là hệ số đầu tiên của $g(x)$ không chia hết cho p . Khi đó từ đẳng thức

$$a_k = (b_0c_k + b_1c_{k-1} + \dots + b_{k-1}c_1) + b_kc_0$$

ta suy ra b_kc_0 chia hết cho p vì a_k và tổng trong dấu ngoặc chia hết cho p . Vì c_0 không chia hết cho p nên b_k chia hết cho p , điều này trái với giả thiết về b_k . $\square$

Mệnh đề 2.5 (Tiêu chuẩn bất khả quy thu gọn). Cho p là một số nguyên tố và đa thức

$$f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{Z}[x],$$

có đa thức $\bar{f}(x)$ tương ứng

$$\bar{f}(x) = \bar{a}_0 + \bar{a}_1x + \dots + \bar{a}_nx^n \in \mathbb{Z}_p[x]$$

sao cho $\bar{f}(x) \neq 0$ và bậc của $\bar{f}(x)$ bằng bậc của $f(x)$. Khi đó, nếu $\bar{f}(x)$ là đa thức bất khả quy trong $\mathbb{Z}_p[x]$ thì $f(x)$ bất khả quy trong $\mathbb{Q}[x]$.

Chứng minh. Giả sử

$$f(x) = u(x)v(x), \quad u(x), v(x) \in \mathbb{Z}[x].$$

Khi đó

$$\bar{f}(x) = \bar{u}(x)\bar{v}(x), \quad \bar{u}(x), \bar{v}(x) \in \mathbb{Z}_p[x].$$

Do $\deg f = \deg \bar{f}$ nên $\deg u = \deg \bar{u}$ và $\deg v = \deg \bar{v}$.

Nếu $\bar{f}(x)$ bất khả quy trong $\mathbb{Z}_p[x]$ thì $\bar{u}(x)$ hoặc $\bar{v}(x)$ là phần tử khả nghịch trong $\mathbb{Z}_p[x]$, chẳng hạn $\bar{u}(x) \in \mathbb{Z}_p[x]$, $\bar{u}(x) \neq 0$. Thế thì $\deg \bar{u}(x) = \deg u(x) = 0$, nghĩa là $u(x) \in \mathbb{Z}^*$, và do đó khả nghịch trong $\mathbb{Q}$. Vậy $f(x)$ bất khả quy trên $\mathbb{Q}$. $\square$

Ví dụ. Xét tính khả quy của đa thức

$$f(x) = x^4 - x^3 + 2x + 1.$$

Thay $x = y + 1$ ta được đa thức

$$g(y) = y^4 + 3y^3 + 3y^2 + 3y + 3.$$

Sử dụng tiêu chuẩn Eisenstein với $p = 3$ ta được $g(y)$ là bất khả quy, và do đó $f(x)$ bất khả quy.

Chú ý. Tiêu chuẩn Eisenstein vẫn đúng nếu thay $\mathbb{Z}$ bởi vành A và $\mathbb{Q}$ bởi trường các thương của A .

Ví dụ. Chứng minh rằng đa thức

$$\phi(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

bất khả quy trên $\mathbb{Q}$ với mỗi số nguyên tố p .

Đa thức này được gọi là *đa thức chia đường tròn* và có thể viết được dưới dạng $\phi(x) = (x^p - 1)/(x - 1)$.

Lời giải. Chúng ta chưa thể áp dụng ngay tiêu chuẩn Eisenstein cho $\phi(x)$ ở dạng trên. Tuy nhiên, nếu chúng ta đặt $x = y + 1$, chúng ta nhận được

$$\begin{aligned} \phi(y+1) &= \frac{1}{y}[(y+1)^p - 1] \\ &= y^{p-1} + \binom{p}{p-1} y^{p-2} + \binom{p}{p-2} y^{p-3} + \cdots + \binom{p}{2} y + p \end{aligned}$$

trong đó $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ là các hệ số trong khai triển nhị thức Newton (Niutơn). Do đó p chia hết $k!(p-k)!$ $\binom{p}{k}$. Nếu $1 \leq k \leq p-1$, thì số nguyên tố p không chia hết $k!(p-k)!$, do đó nó phải chia hết $\binom{p}{k}$. Từ đó $\phi(y+1)$ bất khả quy theo tiêu chuẩn Eisenstein, bởi vậy $\phi(x)$ bất khả quy.

3. Phân tích các đa thức trên trường hữu hạn

Trước hết ta thấy rằng, các nghiệm của đa thức trong $\mathbb{Z}_p[x]$ có thể tìm được bằng cách thử tất cả p giá trị có thể của $\mathbb{Z}_p$. Bây giờ ta sẽ áp dụng điều đó để giải ví dụ dưới đây.

Ví dụ. Đa thức $x^4 + 4 \in \mathbb{Z}_7[x]$ có nghiệm trong $\mathbb{Z}_7$ hay không?

Lời giải. Từ bảng dưới đây chúng ta thấy rằng $x^4 + 4$ không thể bằng 0 và do đó không có nghiệm trong $\mathbb{Z}_7$.

Bảng giá trị

x	0	1	2	3	4	5	6
x^4	0	1	2	4	4	2	1
$x^4 + 4$	4	5	6	1	1	6	5

Mệnh đề 3.1. Một đa thức trong $\mathbb{Z}_2[x]$ có một nhân tử $x+1$ nếu và chỉ nếu nó có một số chẵn các hệ số khác 0.

Chứng minh. Xét đa thức với các hệ tử thuộc trường hữu hạn $\mathbb{Z}_2[x]$

$$p(x) = a_0 + a_1x + \cdots + a_nx^n.$$

Theo định lý nhân tử, $(x+1)$ là một nhân tử của $p(x)$ nếu và chỉ nếu $p(1) = 0$. (Nhớ rằng $x-1 = x+1$ trong $\mathbb{Z}_2[x]$). Bây giờ

$$p(1) = a_0 + a_1 + \cdots + a_n$$

bằng 0 trong $\mathbb{Z}_2$ nếu và chỉ nếu $p(x)$ có một số chẵn các hệ số khác 0. $\square$

Ví dụ. Tìm tất cả các đa thức bất khả quy có bậc nhỏ hơn hoặc bằng 4 trên $\mathbb{Z}_2$.

Lời giải. Các đa thức bậc 1 là các đa thức bất khả quy; trong $\mathbb{Z}_2[x]$ những đa thức đó gồm có x và $x + 1$.

Bây giờ chúng ta xác định các đa thức bất khả quy có bậc $n > 1$. Xét

$$p(x) = a_0 + \cdots + a_n x^n \in \mathbb{Z}_2[x].$$

Nếu $p(x)$ có bậc n , thì $a_n \neq 0$, và 1 là một nghiệm nếu và chỉ nếu $p(x)$ có một số chẵn các số hạng khác 0. Do đó sau đây là các đa thức bậc 2, 3 và 4 trong $\mathbb{Z}_2[x]$ không có nhân tử tuyến tính:

$$x^2 + x + 1 \quad (\text{bậc } 2)$$

$$x^3 + x + 1,$$

$$x^3 + x^2 + 1 \quad (\text{bậc } 3)$$

$$x^4 + x + 1,$$

$$x^4 + x^2 + 1,$$

$$x^4 + x^3 + 1,$$

$$x^4 + x^3 + x^2 + x + 1 \quad (\text{bậc } 4).$$

Nếu một đa thức bậc 2 hoặc 3 là khả quy, nó phải có một nhân tử tuyến tính; do đó các đa thức bậc 2 và 3 ở trên là bất khả quy.

Nếu một đa thức bậc 4 là khả quy, thì hoặc nó có nhân tử tuyến tính hoặc nó là tích của 2 nhân tử bậc 2 bất khả quy. Bây giờ chỉ có 1 đa thức bậc 2 bất khả quy trong $\mathbb{Z}_2[x]$, và bình phương của nó $(x^2 + x + 1)^2 = x^4 + x^2 + 1$ là khả quy.

Do đó các đa thức bất khả quy bậc nhỏ hơn hoặc bằng 4 trên $\mathbb{Z}_2$ là

$$x, x + 1, x^2 + x + 1,$$

$$x^3 + x + 1, x^3 + x^2 + 1,$$

$$x^4 + x + 1, x^4 + x^3 + 1,$$

$$\text{và} \quad x^4 + x^3 + x^2 + x + 1.$$

Như vậy các đa thức bậc 4 trong $\mathbb{Z}_2[x]$ phân tích thành các nhân tử

như sau:

$$\begin{array}{ll}
 x^4 & = x^4 \\
 x^4 + 1 & = (x + 1)^4 \\
 x^4 + x & = x(x + 1)(x^2 + x + 1) \\
 x^4 + x + 1 & \text{bất khả quy} \\
 x^4 + x^2 & = x^2(x + 1)^2 \\
 x^4 + x^2 + 1 & = (x^2 + x + 1)^2 \\
 x^4 + x^2 + x & = x(x^3 + x + 1) \\
 x^4 + x^2 + x + 1 & = (x + 1)(x^3 + x^2 + 1) \\
 x^4 + x^3 & = x^3(x + 1) \\
 x^4 + x^3 + 1 & \text{bất khả quy} \\
 x^4 + x^3 + x & = x(x^3 + x^2 + 1) \\
 x^4 + x^3 + x + 1 & = (x + 1)^2(x^2 + x + 1) \\
 x^4 + x^3 + x^2 & = x^2(x^2 + x + 1) \\
 x^4 + x^3 + x^2 + 1 & = (x + 1)(x^3 + x + 1) \\
 x^4 + x^3 + x^2 + x & = x(x + 1)^3 \\
 x^4 + x^3 + x^2 + x + 1 & \text{bất khả quy}
 \end{array}$$

Bài tập

- 6.1. Tìm tất cả các đa thức bất khả quy bậc 2 trên Z_2 .
- 6.2. Tìm tất cả các đa thức bất khả quy bậc 2 trên Z_5 .
- 6.3. Tìm tất cả các đa thức bất khả quy bậc 2 trên Z_7 .
- 6.4. Hãy định nghĩa một thuật toán chia trong $\mathbb{R}[x, y]$? Chia $x^3 + 3xy + y + 4$ cho $xy + y^3 + 2$?
- 6.5. Cho L_p là tập tất cả các hàm tuyến tính $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ có dạng $f(x) = ax + b$, trong đó $a \neq 0$ trong $\mathbb{Z}_p$. Chứng minh rằng $(L_p, \circ)$ là một nhóm có cấp $p(p - 1)$ với phép toán hợp thành.
- 6.6. Nếu p là một số nguyên tố, chứng minh rằng $(x - a) \mid (x^{p-1} - 1)$ trong $\mathbb{Z}_p[x]$ với mọi số $a \neq 0$ trong $\mathbb{Z}_p$. Từ đó chứng minh rằng

$$x^{p-1} - 1 = (x - 1)(x - 2) \dots (x - p + 1) \text{ trong } \mathbb{Z}_p[x].$$

- 6.7. (Định lý Wilson). Chứng minh rằng $(n - 1)! \equiv -1 \pmod n$ nếu và chỉ nếu n là số nguyên tố.

- 6.8. Nếu r/s là một nghiệm hữu tỷ, ở dạng tối giản, của một đa thức $p(x)$ với hệ số nguyên, chứng minh rằng $p(x) = (sx - r)g(x)$ với một đa thức $g(x)$ nào đó với hệ số nguyên.
- 6.9. Chứng minh rằng r/s , ở dạng tối giản, không thể là một nghiệm của đa thức nguyên $p(x)$ trừ khi $(s - r) \mid p(1)$. Điều này có thể được sử dụng để rút ngắn danh sách các nghiệm hữu tỷ có thể có của một đa thức nguyên.

Bảng thuật ngữ

A

ánh xạ, 15
ánh xạ ngược, 18
ánh xạ Öclit, 182
ảnh, 16
ảnh đồng cấu, 78

B

biểu diễn thặng dư, 138
bổ đề Gauss, 199
bổ đề Zorn, 27
bội, 31, 168
bội chung, 37
bội chung nhỏ nhất, 37

C

cái ổn định, 105
cảm sinh, 50
cận dưới, 27
cận dưới đúng, 27
cận trên, 27
cận trên đúng, 27
cấp, 62
cấu trúc đại số, 47
chỉ số, 70
chia hết, 31, 168
chia hết cho, 31, 168
chuyển trí, 97

D

dãy chuyển, 26
dãy chuyển dừng, 173
dãy chuyển tăng, 173

Đ

đa thức, 155
đa thức bất khả quy, 160
đa thức chia đường tròn, 202
đa thức nguyên bản, 199
đại số hai ngôi, 46
đặc số, 147
đẳng cấu, 51, 77
định lý Cayley, 100
định lý đồng cấu, 79
định lý Lagrange, 69
định lý nhân tử hoá, 176
đơn ánh, 16
đơn cấu, 51, 77
đơn cấu chính tắc, 77
đồng cấu, 51, 76
đồng cấu vành, 132

G

giao của hai tập hợp, 10
giá trị tuyệt đối, 31
G-tập, 104

H

hạng tử trực tiếp, 90
hạt nhân đồng cấu, 78
hiệu của hai tập hợp, 11
hợp của hai tập hợp, 11
hợp thành ánh xạ, 17

I

idêan, 120
idêan chính, 122
idêan hữu hạn sinh, 122

idêan nguyên tố, 127
idêan tối đại, 127

L

liên kết, 169
liên hợp, 70
lớp ghép, 67
lớp tương đương, 23

M

miền nguyên, 115

N

nhóm, 54
nhóm con, 61
nhóm con chuẩn tắc, 70
nhóm con liên hợp, 65, 106
nhóm D_n , 64
nhóm đối xứng, 55, 97
nhóm đơn, 71
nhóm Klein, 57
nhóm phép thế, 55
nhóm quaternion, 65
nhóm thay phiên, 99
nhóm thương, 72
nguyên tố cùng nhau, 34, 171
nửa nhóm, 47
nửa nhóm con, 50

P

phân hoạch, 24
phần bù, 12
phần tử âm, 150
phần tử bất khả quy, 170
phần tử dương, 150
phần tử đại số, 162
phần tử đơn vị, 47

phần tử nghịch đảo, 55
phần tử liên kết, 169
phần tử nguyên tố, 170
phần tử sinh, 64
phần tử siêu việt, 162
phần tử trung hoà, 47
phần tử tối đại, 27
phần tử tối tiểu, 27
phép chiếu, 77, 89, 132
phép toán cảm sinh, 50
phép toán hai ngôi, 46
phép thế, 55
phép nhúng, 77, 89, 132
phép thế chẵn, 99
phép thế lẻ, 99

Q

quan hệ hai ngôi, 22
quan hệ tương đương, 23
quan hệ thứ tự, 25
quan hệ thứ tự toàn phần, 26
quỹ đạo, 106

S

song ánh, 17
sắp thứ tự, 26
sắp thứ tự Acsmet, 153
sắp thứ tự tuyến tính, 26
sắp thứ tự tốt, 26
số nguyên tố, 39
sự chia lớp, 24
sự phân tích tiêu chuẩn, 41

T

tác động, 104
tác động trung thành, 105
tạo ảnh, 15
tạo ảnh toàn phần, 16

tập con, 10
 tập con ổn định, 50, 61
 tập hợp sinh, 64
 tập rỗng, 10
 tập thương, 24
 thuật toán Oclit, 36
 thứ tự bộ phận, 25
 tích của hai idêan, 124
 tích Đề-các, 22
 tích trực tiếp, 89, 139
 tích trực tiếp yếu, 91
 tiên đề sắp thứ tự tốt, 31
 tiên đề tách, 10
 tiên đề quy nạp, 31
 tiêu chuẩn Eisenstein, 201
 toàn ánh, 16
 toàn cầu, 51, 77, 132
 toàn cầu chính tắc, 77
 tổng của hai idêan, 127
 tổng trực tiếp, 89, 137
 trừ mất hữu tỷ, 153
 trường, 115
 trường các thương, 144
 trường con, 117

trường sắp thứ tự, 149
 tự đồng cấu, 51, 132

Ư

ước, 31, 168
 ước chung, 33
 ước chung lớn nhất, 33, 171
 ước của không, 114
 ước thực sự, 170

V

vành, 110
 vành các tự đồng cấu, 111
 vành chính, 173
 vành con, 117
 vành Oclit, 182
 vành sắp thứ tự Acsimet, 153
 vành thương, 126
 vành (trường) sắp thứ tự, 149
 vị nhóm, 47
 vị nhóm xyclic, 49
 vòng xích, 97

Tài liệu tham khảo

1. M. F. Atiyah - I. G. Macdonald. *Introduction to Commutative Algebra*, Massachusetts, 1969.
2. G. Birkhoff - S. MacLane. *A Survey of Modern Algebra* (Bản dịch tiếng Việt, NXB Đại học và Trung học chuyên nghiệp, 1979).
3. G. Birkhoff - S. MacLane. *Algebra*, 1967.
4. G. Birkhoff - T. Bartee. *Modern applied algebra*, 1976.
5. W. J. Gilbert - W. K. Nicholson. *Modern algebra with applications*, Wiley-Interscience, 1976.
6. T. W. Hungerford. *Algebra*, Springer, 1974.
7. Ngô Thúc Lanh. *Đại số và số học* tập I, II, NXB Giáo dục, 1986, 1987.
8. S. Lang. *Algebra*, Columbia University, New York (Phần I bản dịch tiếng Việt, NXB Đại học và Trung học chuyên nghiệp, 1974).
9. Hoàng Xuân Sính. *Đại số cao cấp* tập I, NXB Giáo dục, 1995.

Chịu trách nhiệm xuất bản :

Chủ tịch HĐQT kiêm Tổng Giám đốc NGÔ TRẦN ÁI
Phó Tổng Giám đốc kiêm Tổng biên tập NGUYỄN QUÝ THAO

Tổ chức bản thảo và chịu trách nhiệm nội dung :

Chủ tịch HĐQT kiêm Giám đốc Công ty CP Sách ĐH – DN
TRẦN NHẬT TÂN

Biên tập nội dung và sửa bản in :

ĐỖ HỮU PHÚ

Biên tập mỹ thuật và trình bày bìa :

ĐINH XUÂN DŨNG

Thiết kế sách và chế bản :

NGUYỄN TIẾN QUANG

ĐẠI SỐ ĐẠI CƯƠNG

Mã số : 7B706Y8 – DAI

In 1.000 cuốn (QĐ : 20), khổ 16 x 24cm. In tại Công ty CP In Anh Việt.

Địa chỉ : Số 74, ngõ 310, đường Nghi Tàm, Tây Hồ, Hà Nội.

Số ĐKKH xuất bản : 113 – 2008/CXB/60 – 175/GD.

In xong và nộp lưu chiểu tháng 5 năm 2008.



CÔNG TY CỔ PHẦN SÁCH ĐẠI HỌC - DẠY NGHỀ
HEVOBCO
25 HÀN THUYỀN - HÀ NỘI
Website : www.hevobco.com.vn

**TÌM ĐỌC SÁCH THAM KHẢO VỀ TOÁN – TIN
CỦA NHÀ XUẤT BẢN GIÁO DỤC**

1. Toán học cao cấp (tập 1, 2, 3)	Nguyễn Đình Trí (Chủ biên)
2. Bài tập Toán học cao cấp (tập 1, 2, 3)	Nguyễn Đình Trí (Chủ biên)
3. Đại số tuyến tính và hình học giải tích	PGS. TS. Trần Trọng Huệ
4. Đồ thị và các thuật toán	PGS. TS. Hoàng Chí Thành
5. Hướng dẫn giải Bài tập Toán rời rạc	PGS. TS. Đỗ Đức Giáo
6. Phương pháp tính	Tạ Văn Đình
7. Toán học tính toán	Doãn Tam Hoè
8. Cấu trúc máy tính	TS. Trần Quang Vinh
9. Lập trình bằng ngôn ngữ Assembly cho máy tính	TS. Nguyễn Mạnh Giang

*Bạn đọc có thể mua tại các Công ty Sách - Thiết bị trường học ở các địa phương
hoặc các Cửa hàng sách của Nhà xuất bản Giáo dục :*

Tại Hà Nội : 25 Hàn Thuyên ; 187B Giảng Võ ; 232 Tây Sơn ; 23 Tràng Tiền ;

Tại Đà Nẵng : Số 15 Nguyễn Chí Thanh ; Số 62 Nguyễn Chí Thanh ;

Tại Thành phố Hồ Chí Minh : Cửa hàng 451B - 453, Hai Bà Trưng, Quận 3 ;
240 Trần Bình Trọng – Quận 5 ;

Tại Thành phố Cần Thơ : Số 5/5, đường 30/4 ;

Website : www.nxbgd.com.vn



Giá: 26.000 đ