TRƯỜNG ĐẠI HỌC SÀI GÒN

TÔN THẤT TRÍ ĐỒNG THANH TRIẾT

Giáo trình

ĐẠI SỐ ĐẠI CƯƠNG

TP. HỒ CHÍ MINH - 2014

Lời nói đầu

Như chúng ta đã biết, các kết quả về nhóm, vành và trường nói riêng, về đại số nói chung đã được ứng dụng trong hầu hết các lĩnh vực toán học: từ tô-pô và hình học, lý thuyết hàm, lý thuyết mã đến cơ học lượng tử, vật lý lý thuyết và nhiều ngành khoa học cơ bản khác. Chính vì thế đại số đại cương trở thành môn học bắt buộc trong các trường giảng dạy toán và ứng dụng toán học.

Giáo trình "Đại số đại cương" được biên soạn dựa trên chương trình của môn học cùng tên do Khoa Toán - Ứng dụng thuộc Trường đại học Sài Gòn đề xuất. Nội dung giáo trình tương ứng với môn học bốn tín chỉ, vì thời lượng có hạn nên môn học chỉ trình bày các kết quả cơ bản về nhóm, vành và trường, một số cấu trúc khác như mô-đun hay đại số không được đề cập đến.

Giáo trình gồm có bảy chương. Chương 0 nhắc lại các kiến thức cơ bản để giúp sinh viên dễ theo dõi các chương sau. Nội dung giáo trình được trình bày trong sáu chương còn lại với các mục được đề cập đến như trong bảng mục lục của sách. Mỗi chương bao gồm nhiều mục, sau mỗi mục là phần bài tập. Bài tập được lựa chọn không quá khó, chủ yếu là tính toán trên những đối tượng quen thuộc của toán học và sinh viên nên làm hết các bài tập này để hiểu thêm lý thuyết và rèn luyện kỹ năng cho mình.

Mặc dù đã cố gắng rất nhiều nhưng chắc chắn vẫn không thể tránh khỏi những thiếu sót, vì vậy chúng tôi mong nhận được những ý kiến đóng góp của quý đồng nghiệp để giáo trình được hoàn thiện hơn.

Cuối cùng, chúng tôi chân thành cảm ơn Ban lãnh đạo Trường đại học Sài Gòn cũng như Khoa Toán - Ứng dụng của Trường đã tạo điều kiện thuận lợi để chúng tôi hoàn thành giáo trình này.

Tp. HCM, 2014

Các tác giả

Mục lục

0 KIẾN THỨC CHUẨN BỊ 1
0.1 Tập hợp 1
0.2 Ánh xạ 6
0.3 Đơn ánh - Toàn ánh - Song ánh 10
0.4 Ánh xạ ngược 13
0.5 Tập hợp đếm được 16
0.6 Quan hệ tương đương 19
0.7 Quan hệ thứ tự 22

1 NHÓM 27
1.1 Phép toán hai ngôi 27
1.2 Khái niệm về nhóm 31
1.3 Nhóm con 35
1.4 Nhóm cyclic 39
1.5 Nhóm đối xứng và nhóm thay phiên 45
1.6 Lớp kề 50
1.7 Nhóm con chuẩn tắc và nhóm thương 54
1.8 Đồng cấu 58

2 NHÓM ABEL HỮU HẠN SINH 67
2.1 Tích trực tiếp của các nhóm 67
2.2 Tổng trực tiếp của các nhóm Abel 74
2.3 Nhóm Abel hữu hạn 78
2.4 Nhóm Abel tự do 83
2.5 Nhóm Abel hữu hạn sinh 88

3 VÀNH 91
3.1 Vành và vành con 91
3.2 Miền nguyên và trường 96

3.3 Iđêan và vành thương ... 100
3.4 Đồng cấu vành ... 105
3.5 Trường các thương ... 113

4 VÀNH ĐA THỨC ... 117
4.1 Vành đa thức một biến ... 117
4.2 Phép chia Euclid ... 120
4.3 Hàm đa thức ... 124
4.4 Đa thức bất khả quy ... 125
4.5 Nhân tử hóa đa thức hệ số phức và thực ... 128
4.6 Nhân tử hóa đa thức hệ số hữu tỷ và hệ số nguyên ... 131
4.7 Phương trình bậc ba và bậc bốn ... 136
4.8 Đa thức nhiều biến ... 140
4.9 Đa thức đối xứng ... 141

5 MIỀN EUCLID - MIỀN IĐÊAN CHÍNH ... 149
5.1 Tính chất số học trong một miền nguyên ... 149
5.2 Miền Euclid ... 151
5.3 Miền iđêan chính ... 155

6 TRƯỜNG ... 161
6.1 Đặc số của một trường ... 161
6.2 Mở rộng đại số ... 163
6.3 Trường phân rã ... 171
6.4 Trường hữu hạn ... 176

Tài liệu tham khảo ... 183

Chỉ mục ... 185

Chương 0
KIẾN THỨC CHUẨN BỊ

Trong chương này chúng ta nhắc lại một số khái niệm cơ bản của toán học như tập hợp, ánh xạ, quan hệ tương đương và quan hệ thứ tự. Các khái niệm này được sử dụng trong suốt cuốn sách.

0.1 Tập hợp

Tập hợp là khái niệm nguyên thủy nên không có định nghĩa, ta thường nói tập hợp các đối tượng thỏa mãn một số tính chất nào đó. Tập hợp được ký hiệu bởi các chữ cái A,B,C,... Ta nói đối tượng x nằm trong tập hợp A là một *phần tử* của A và viết $x \in A$, ngược lại x không là phần tử của A và viết $x \notin A$.

Một tập hợp có hữu hạn phần tử gọi là tập hợp *hữu hạn*. Tập hợp *rỗng* là tập hợp không có phần tử nào và nó cũng được xem là tập hợp hữu hạn. Một tập hợp không là tập hợp hữu hạn gọi là tập hợp *vô hạn*.

Tập hợp được mô tả bằng cách liệt kê các phần tử của nó nằm giữa hai dấu $\{\ldots\}$ hoặc nêu lên tính chất đặc trưng của nó.

Ví dụ 0.1. (a) Tập hợp các số tự nhiên $\mathbb{N} = \{0, 1, 2, \ldots\}$.

(b) Tập hợp các số nguyên $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$.

(c) Tập hợp các số hữu tỷ $\mathbb{Q} = \{p/q \mid p, q \in \mathbb{Z}, q \neq 0\}$.

(d) Tập hợp các số thực

$$\mathbb{R} = \{\pm x_1 x_2 \ldots x_n, y_1 y_2 \ldots \mid n \in \mathbb{N}, n > 0, 0 \leq x_i, y_j \leq 9\}.$$

(e) Tập hợp các số phức $\mathbb{C} = \{x + iy \mid x, y \in \mathbb{R}, i^2 = -1\}$.

Định nghĩa 0.2. Cho hai tập hợp A và B. Ta nói A là một *tập con* của B, và viết $A \subset B$ nếu mọi phần tử của A đều là phần tử của B; A bằng B, $A = B$ nếu $B \subset A$ và $A \subset B$.

Ta quy ước tập hợp rỗng là tập con của mọi tập hợp.

Định nghĩa 0.3. Cho hai tập hợp A và B.

(a) *Giao* của A và B là tập hợp $A \cap B$ gồm các phần tử chung của A và B, tức là những phần tử vừa thuộc A vừa thuộc B.

(b) *Hợp* của A và B là tập hợp $A \cup B$ gồm các phần tử của A và các phần tử của B, tức là những phần tử thuộc A hoặc thuộc B.

Mệnh đề 0.4. *Cho ba tập hợp A, B, C tùy ý. Khi đó ta có:*

(a) $A \cap B = B \cap A$.

(b) $A \cup B = B \cup A$.

(c) $A \cap (B \cap C) = (A \cap B) \cap C$.

(d) $A \cup (B \cup C) = (A \cup B) \cup C$.

(e) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

(f) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Chứng minh. Từ (a) đến (d) là hiển nhiên.

(e) Nếu $x \in A \cap (B \cup C)$ thì x thuộc A và x thuộc một trong hai tập hợp B hoặc C, chẳng hạn $x \in B$. Khi đó $x \in A \cap B$, suy ra $x \in (A \cap B) \cup (A \cap C)$. Đảo lại, nếu $x \in (A \cap B) \cup (A \cap C)$ thì x thuộc một trong hai tập hợp $A \cap B$ hoặc $A \cap C$, chẳng hạn $x \in A \cap B$, và vì $A \cap B \subset A \cap (B \cup C)$ nên $x \in A \cap (B \cup C)$.Vậy ta có (e).

(f) Giả sử $x \in A \cup (B \cap C)$, khi đó $x \in A$ hoặc $x \in B \cap C$. Nếu $x \in A$ thì $x \in A \cup B$ và $x \in A \cup C$, suy ra $x \in (A \cup B) \cap (A \cup C)$. Nếu $x \in B \cap C$ thì $x \in B$ và $x \in C$, suy ra $x \in A \cup B$ và $x \in A \cup C$, do đó $x \in (A \cup B) \cap (A \cup C)$. Đảo lại, giả sử $x \in (A \cup B) \cap (A \cup C)$ thì x vừa thuộc $A \cup B$ vừa thuộc $A \cup C$. Nếu $x \in A$ thì $x \in A \cup (B \cap C)$. Nếu $x \notin A$ thì $x \in B$ và $x \in C$, suy ra $x \in B \cap C$, và vì vậy $x \in A \cup (B \cap C)$. Vậy (f) được chứng minh.

□

Định nghĩa 0.5. Cho hai tập hợp A và B. *Hiệu* của A và B là tập hợp $A \setminus B$ gồm các phần tử thuộc A nhưng không thuộc B. Nếu $B \subset A$, ta viết $C_A B$ thay cho $A \setminus B$ và gọi là *phần bù* của B trong A.

Mệnh đề 0.6. *Cho A, B là hai tập con của X. Khi đó ta có:*

(a) $C_X(A \cup B) = C_X A \cap C_X B$.

(b) $C_X(A \cap B) = C_X A \cup C_X B$.

Chứng minh. Xét x là phần tử tùy ý trong X.

(a) Nếu $x \in C_X(A \cup B)$ thì x không thuộc cả A lẫn B, suy ra $x \in C_X A$ và $x \in C_X B$, và do đó $x \in C_X A \cap C_X B$. Đảo lại, nếu $x \in C_X A \cap C_X B$ thì x vừa thuộc $C_X A$ vừa thuộc $C_X B$ nên x không thuộc cả A lẫn B, và do đó $x \in C_X(A \cup B)$. Vậy (a) được chứng minh.

(b) Giả sử $x \in C_X(A \cap B)$, tức là $x \notin A \cap B$. Khi đó x có các khả năng sau: nếu x không thuộc cả A lẫn B, tức là $x \in C_X A$ và $x \in C_X B$ nên $x \in C_X A \cap C_X B \subset$

$C_X A \cup C_X B$; nếu x thuộc A nhưng không thuộc B thì $x \in C_X B \subset C_X A \cup C_X B$; trường hợp còn lại x thuộc B nhưng không thuộc A thì $x \in C_X A \subset C_X A \cup C_X B$. Đảo lại, nếu $x \in C_X A \cup C_X B$ thì x thuộc một trong hai tập hợp $C_X A$, $C_X B$. Do đó $x \notin A \cap B$, tức là $x \in C_X(A \cap B)$. Vậy ta có điều phải chứng minh.

□

Với hai phần tử a và b ta có *cặp thứ tự* (a, b) được viết theo thứ tự trên. Hai cặp thứ tự (a, b) và (c, d) được xem là như nhau và viết $(a, b) = (c, d)$ nếu $a = b$ và $c = d$. Tích Descartes của hai tập hợp được định nghĩa như sau.

Định nghĩa 0.7. Cho hai tập hợp A và B. *Tích Descartes* của A và B là tập hợp $A \times B$ gồm các cặp thứ tự (a, b), trong đó a là phần tử tùy ý trong A và b tùy ý trong B.

Chú ý rằng nếu $A = \emptyset$ hay $B = \emptyset$ thì $A \times B = \emptyset$.

Ví dụ 0.8. Cho $A = \{1, 2, 3\}$ và $B = \{a, b\}$. Khi đó

$$A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}.$$

Mệnh đề 0.9. *Cho ba tập hợp A, B, C tùy ý. Khi đó ta có:*
(a) $(A \cap B) \times C = (A \times C) \cap (B \times C)$.
(b) $(A \cup B) \times C = (A \times C) \cup (B \times C)$.
(c) $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$.

Chứng minh. (a) Ta có

$$\begin{aligned}(x, y) \in (A \cap B) \times C &\Leftrightarrow x \in A \cap B \text{ và } y \in C \\ &\Leftrightarrow x \in A \text{ và } x \in B \text{ và } y \in C \\ &\Leftrightarrow (x, y) \in A \times C \text{ và } (x, y) \in B \times C \\ &\Leftrightarrow (x, y) \in (A \times C) \cap (B \times C).\end{aligned}$$

Do đó (a) được chứng minh.
(b) Ta có

$$\begin{aligned}(x, y) \in (A \cup B) \times C &\Leftrightarrow x \in A \cup B \text{ và } y \in C \\ &\Leftrightarrow (x \in A \text{ hoặc } x \in B) \text{ và } y \in C \\ &\Leftrightarrow (x \in A \text{ và } y \in C) \text{ hoặc } (x \in B \text{ và } y \in C) \\ &\Leftrightarrow (x, y) \in A \times C \text{ hoặc } (x, y) \in B \times C \\ &\Leftrightarrow (x, y) \in (A \times C) \cup (B \times C).\end{aligned}$$

Khi đó (b) được chứng minh.

(c) Ta có

$$\begin{aligned}(x,y) \in A \times (B \setminus C) &\Leftrightarrow x \in A \text{ và } y \in B \setminus C \\ &\Leftrightarrow x \in A \text{ và } y \in B \text{ và } y \notin C \\ &\Leftrightarrow (x,y) \in A \times B \text{ và } (x,y) \notin A \times C \\ &\Leftrightarrow (x,y) \in (A \times B) \setminus (A \times C).\end{aligned}$$

Vậy (c) được chứng minh.

□

Định nghĩa giao, hợp và tích Descartes cũng được mở rộng cho một số hữu hạn các tập hợp như sau.

Giao của n tập hợp $A_1, A_2, \ldots, A_n$ là tập hợp $\cap_{i=1}^n A_i$ gồm các phần tử chung của $A_1, A_2, \ldots, A_n$; *hợp* của n tập hợp $A_1, A_2, \ldots, A_n$ là tập hợp $\cup_{i=1}^n A_i$ gồm các phần tử x sao cho có chỉ số j nào đó để $x \in A_j$.

Ta nói một *bộ n-thứ tự* $(a_1, a_2, \ldots, a_n)$ là dãy các phần tử được viết theo thứ tự trên. Hai bộ n-thứ tự $(a_1, a_2, \ldots, a_n)$ và $(b_1, b_2, \ldots, b_n)$ được xem là như nhau và viết

$$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$$

nếu $a_1 = b_1, a_2 = b_2, \ldots, a_n = b_n$.

Tích Descartes của n tập hợp $A_1, A_2, \ldots, A_n$ là tập hợp

$$A_1 \times A_2 \times \cdots \times A_n$$

gồm các bộ n-thứ tự $(a_1, a_2, \ldots, a_n)$, trong đó $a_i \in A_i$ với mọi $i = 1, \ldots, n$. Đặc biệt, khi $A_1 = A_2 = \cdots = A_n = A$ ta viết A^n thay cho $A \times A \times \cdots \times A$ (n lần).

Bây giờ ta định nghĩa phép giao, hợp và tích Descartes của tùy ý các tập hợp. Xét tập hợp I khác rỗng. Nếu mỗi $i \in I$ tương ứng với một tập hợp A_i thì ta nói có một họ các tập hợp A_i với chỉ số trong I và viết $(A_i)_{i \in I}$. Đặc biệt, khi mỗi A_i chỉ có một phần tử a_i thì ta có một họ các phần tử lấy chỉ số trong I và viết $(a_i)_{i \in I}$. Hai họ $(a_i)_{i \in I}$, $(b_i)_{i \in I}$ được xem là như nhau và viết $(a_i)_{i \in I} = (b_i)_{i \in I}$ nếu $a_i = b_i$ với mọi chỉ số $i \in I$.

Định nghĩa 0.10. Cho một họ các tập hợp $(A_i)_{i \in I}$.

(a) *Giao* của $(A_i)_{i \in I}$ là tập hợp $\cap_{i \in I} A_i$ gồm các phần tử x sao cho $x \in A_i$ với mọi $i \in I$.

(b) *Hợp* của $(A_i)_{i \in I}$ là tập hợp $\cup_{i \in I} A_i$ gồm các phần tử x sao cho có $j \in I$ để $x \in A_j$.

(c) *Tích Descartes* của $(A_i)_{i\in I}$ là tập hợp $\Pi_{i\in I}A_i$ gồm các họ $(a_i)_{i\in I}$ trong đó a_i là phần tử tùy ý thuộc A_i với mỗi $i \in I$. Nếu các A_i đều bằng A ta viết A^I thay cho $\Pi_{i\in I}A_i$.

Ví dụ 0.11. (a) Với mỗi số nguyên i ta đặt $A_i = [\mathrm{i}, +\infty)$. Khi đó

$$\cap_{i\in\mathbb{Z}}A_i = \emptyset,\ \cup_{i\in\mathbb{Z}}A_i = \mathbb{R}.$$

Thật vậy, giả sử $\cap_{i\in\mathbb{Z}}A_i \neq \emptyset$, khi đó có $x \in A_i$ với mọi $i \in \mathbb{Z}$. Lấy số nguyên n lớn hơn x thì $x \notin A_n$. Mâu thuẫn này chứng tỏ $\cap_{i\in\mathbb{Z}}A_i = \emptyset$.

Ta có $\cup_{i\in\mathbb{Z}}A_i \subset \mathbb{R}$. Với mỗi $x \in \mathbb{R}$ lấy số nguyên n nhỏ hơn x thì $x \in A_n$, suy ra $x \in \cup_{i\in\mathbb{Z}}A_i$ và do đó $\mathbb{R} \subset \cup\, _{i\in\mathbb{Z}}A_i$. Vậy $\cup_{i\in\mathbb{Z}}A_i = \mathbb{R}$.

(b) $\mathbb{R}^{\mathbb{N}}$ là tập hợp các dãy số thực $(a_i)_{i\in\mathbb{N}}$.

Ta định nghĩa tập hợp *các phần* của tập hợp X là tập hợp $\mathcal{P}(X)$ gồm các tập con của X. Nói cách khác, A là một phần tử của $\mathcal{P}(X)$ nếu và chỉ nếu A là một tập con của X.

Ví dụ 0.12. $\mathcal{P}(\emptyset) = \{\emptyset\}$, $\mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$.

Chú ý rằng nếu I là tập hợp hữu hạn thì giao, hợp và tích Descartes của các tập hợp với chỉ số trong I chính là giao, hợp và tích Descartes của hữu hạn các tập hợp.

Vì không có tập hợp lớn nhất tức là tập hợp chứa mọi tập hợp, do đó khi bàn về tập hợp ta thường dùng từ *lớp* các tập hợp để chỉ các tập hợp mà ta đang khảo sát.

Bài tập

1. Hãy xác định $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$.
2. Cho tập hợp A có n phần tử, chứng tỏ $\mathcal{P}(A)$ có 2^n phần tử.
3. Cho hai tập hợp hữu hạn A và B. Chứng minh rằng

$$|A \cup B| = |A| + |B| - |A \cap B|,$$

trong đó $|X|$ là số phần tử của tập hợp X. Hãy mở rộng kết quả trên cho ba tập hợp hữu hạn.

4. Trong một kỳ thi học sinh giỏi, mỗi thí sinh có thể tham gia thi ba môn Toán, Văn và Ngoại ngữ. Biết rằng có 20 em thi Toán, 14 em thi Văn, 10 em thi Ngoại ngữ, 6 em thi vừa Toán vừa Ngoại ngữ, 5 em thi vừa Văn vừa Ngoại ngữ, 2 em thi vừa Văn vừa toán, 1 em thi cả ba môn. Hỏi có bao nhiêu thí sinh tham gia kỳ thi này.
5. Có bao nhiêu số tự nhiên nhỏ hơn 1000, không chia hết cho một trong ba số $2, 3, 5$?

6. Chứng tỏ rằng nếu $A \subset X$ và $B \subset Y$ thì $A \times B \subset X \times Y$. Điều ngược lại có đúng không?
7. Cho X, Y và Z là ba tập hợp tùy ý. Chứng tỏ $X \times Y = X \times Z$ khi và chỉ khi $Y = Z$ hoặc $X = \emptyset$.
8. Cho $(A_i)_{i\in I}$ là một họ gồm các tập con của tập hợp X với chỉ số trong tập hợp I. Chứng tỏ rằng
   (a) $C_X(\cap_{i\in I} A_i) = \cup_{i\in I}(C_X A_i)$.
   (b) $C_X(\cup_{i\in I} A_i) = \cap_{i\in I}(C_X A_i)$.

0.2 Ánh xạ

Định nghĩa 0.13. Một *ánh xạ* f từ tập hợp X đến tập hợp Y là một quy tắc: mỗi $x \in X$ tương ứng với một và chỉ một phần tử được ký hiệu $f(x) \in Y$. Ta viết

$$\begin{array}{rl} f : X \longrightarrow & Y \\ x \longmapsto & f(x) \end{array} \quad \text{hay} \quad x \in X \longmapsto f(x) \in Y$$

để chỉ ánh xạ từ X đến Y. Ta nói $f(x)$ là ảnh của x, còn x là một tạo ảnh của $f(x)$. X được gọi là miền xác định của ánh xạ f.

Ví dụ 0.14. (a) $f : \mathbb{N} \longrightarrow \{0, 1\}$ được định nghĩa bởi quy tắc

$$f(n) = \begin{cases} 0 & \text{nếu } n \text{ chẵn} \\ 1 & \text{nếu } n \text{ lẻ} \end{cases}$$

là một ánh xạ, nhưng $g : \mathbb{N} \longrightarrow \{0, 1\}$ được định nghĩa bởi quy tắc

$$g(n) = \begin{cases} 0 & \text{nếu } n \text{ chẵn} \\ 1 & \text{nếu } n \text{ là bội của } 3 \end{cases}$$

không phải ánh xạ vì quy tắc không nói cho chúng ta biết $g(1)$ bằng bao nhiêu, và $g(6)$ bằng 0 hay bằng 1.

(b) Quy tắc

$$(x, y) \in \mathbb{R}^2 \longmapsto x + y \in \mathbb{R}, \quad (x, y) \in \mathbb{R}^2 \longmapsto xy \in \mathbb{R}$$

là hai ánh xạ từ $\mathbb{R}^2$ đến $\mathbb{R}$ lần lượt gọi là phép cộng, nhân hai số thực.

(c) Với tập hợp X cho trước, quy tắc

$$(x, y) \in X^2 \longmapsto x \in X, \quad (x, y) \in X^2 \longmapsto y \in X$$

là hai ánh xạ từ X^2 đến X lần lượt gọi là phép chiếu xuống tọa độ thứ nhất, thứ hai.

(d) Với tập hợp X cho trước, quy tắc $x \in X \longmapsto x \in X$ là một ánh xạ, gọi là ánh xạ đồng nhất được ký hiệu bởi id_X.

Ta nói hai ánh xạ f, g từ tập hợp X đến tập hợp Y là như nhau, và viết $f = g$ nếu $f(x) = g(x)$ với mọi $x \in X$.

Xét ánh xạ $f : X \longrightarrow Y$ và A là một tập con của X. Ta gọi ánh xạ $f\mid_A : A \longrightarrow Y$ được xác định với mỗi $x \in A$, $f\mid_A (x) = f(x)$ là *thu hẹp* của f về A, còn f là một *mở rộng* của ánh xạ $g = f\mid_A$.

Chú ý rằng với ánh xạ f cho trước thì có duy nhất một thu hẹp của f về A, nhưng có nhiều mở rộng của ánh xạ g từ A lên X.

Định nghĩa 0.15. Xét ánh xạ $f : X \longrightarrow Y$.

(a) Cho A là một tập con của X. Ta gọi *ảnh* của A bởi f là tập con $f(A) \subset Y$ được xác định

$$f(A) = \{y \in Y \mid \exists x \in A, y = f(x)\}.$$

Ta còn viết $f(A) = \{f(x) \in Y \mid x \in A\}$. Đặc biệt ta ký hiệu $\operatorname{Im} f = f(X)$ và gọi $\operatorname{Im} f$ là ảnh của ánh xạ f.

(b) Cho B là một tập con của Y. Ta nói *tạo ảnh* của B bởi f là tập con $f^{-1}(B) \subset X$ được định nghĩa

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

Như vậy, với phần tử $y \in Y$ cho trước thì $y \in f(A)$ nếu y là ảnh của phần tử nào đó ở trong A. Với phần tử $x \in X$ thì $x \in f^{-1}(B)$ nếu và chỉ nếu $f(x) \in B$.

Ví dụ 0.16. Xét phép chiếu $p : \mathbb{R}^2 \longrightarrow \mathbb{R}$ được xác định bởi $p(x, y) = x$ với mỗi $(x, y) \in \mathbb{R}^2$. Nếu $A = \{(x, y) \in \mathbb{R}^2 / x^2 + y^2 = 1\}$ thì $p(A) =$ [-1,1] và p^{-1}([-1,1])=[-1,1] $\times \mathbb{R}$.

Mệnh đề 0.17. *Xét ánh xạ $f : X \longrightarrow Y$ và A, A' là hai tập con của X, B, B' hai tập con của Y. Khi đó ta có:*

(a) $f(f^{-1}(B)) \subset B$.
(b) $f(A \cup A') = f(A) \cup f(A')$.
(c)$f(A \cap A') \subset f(A) \cap f(A')$.
(d) $f^{-1}(f(A)) \supset A$.
(e) $f^{-1}(B \cup B') = f^{-1}(B) \cup f^{-1}(B')$.
(f) $f^{-1}(B \cap B') = f^{-1}(B) \cap f^{-1}(B')$.
(g) $f^{-1}(C_Y B) = C_X(f^{-1}(B))$.

Chứng minh. (a) Nếu $y \in f(f^{-1}(B))$ thì có $x \in f^{-1}(B)$ sao cho $y = f(x)$. Vì $x \in f^{-1}(B)$ nên $y = f(x) \in B$ và (a) được chứng minh.

(b) Nếu

$$\begin{aligned} y \in f(A \cup A') &\Rightarrow \exists x \in A \cup A' \text{ sao cho } y = f(x) \\ &\Rightarrow y = f(x),\ x \in A \text{ hoặc } x \in A' \\ &\Rightarrow y \in f(A) \text{ hoặc } y \in f(A') \\ &\Rightarrow y \in f(A) \cup f(A') \end{aligned}$$

và do đó $f(A \cup A') \subset f(A) \cup f(A')$. Đảo lại, vì $A, A' \subset A \cup A'$ nên $f(A), f(A') \subset f(A \cup A')$, và do đó $f(A) \cup f(A') \subset f(A \cup A')$. Vậy có (b).

(c) Nếu

$$\begin{aligned} y \in f(A \cap A') &\Rightarrow \exists x \in A \cap A' \text{ sao cho } \ y = f(x) \\ &\Rightarrow y = f(x),\ x \in A \text{ và } \ x \in A' \\ &\Rightarrow y \in f(A) \text{ và } y \in f(A') \\ &\Rightarrow y \in f(A) \cap f(A') \end{aligned}$$

và (c) được chứng minh.

(d) Nếu $x \in A$ thì $f(x) \in f(A)$, suy ra $x \in f^{-1}(f(A))$. Và (d) được chứng minh.

(e) Ta có

$$\begin{aligned} x \in f^{-1}(B \cup B') &\Leftrightarrow f(x) \in B \cup B' \\ &\Leftrightarrow f(x) \in B \text{ hoặc } f(x) \in B' \\ &\Leftrightarrow x \in f^{-1}(B) \text{ hoặc } x \in f^{-1}(B') \\ &\Leftrightarrow x \in f^{-1}(B) \cup f^{-1}(B'). \end{aligned}$$

Vậy (e) được chứng minh.

Chứng minh tương tự (e) ta có (f).

(g) Xét x là phần tử tùy ý trong X. Ta có

$$\begin{aligned} x \in f^{-1}(C_Y(B)) &\Leftrightarrow f(x) \in C_Y B \\ &\Leftrightarrow f(x) \notin B \\ &\Leftrightarrow x \notin f^{-1}(B) \\ &\Leftrightarrow x \in C_X(f^{-1}(B)) \end{aligned}$$

và (g) được chứng minh.

□

Trong mệnh đề trên, dấu "=" trong (a) và (d) nói chung không xảy ra. Để thấy điều đó ta xét ví dụ sau. Cho ánh xạ $f : \mathbb{R} \longrightarrow \mathbb{R}$ được xác định bởi $f(x) = x^2$ với mỗi $x \in \mathbb{R}$. Lấy $B = \{-2, 1\}$ và $A = \{-1\}$. Khi đó

$$f(f^{-1}(B)) = f(\{-1,1\}) = \{1\} \subsetneq B,$$

$$f^{-1}(f(A)) = f^{-1}(\{1\}) = \{-1,1\} \supsetneq A.$$

Cho trước ánh xạ f từ X dến Y, tạo ảnh của phần tử $y \in Y$ để cho tiện ta sẽ viết $f^{-1}(y)$ thay vì $f^{-1}(\{y\})$. Nếu $y \notin \operatorname{Im} f$ thì $f^{-1}(y) = \emptyset$.

Định nghĩa 0.18. Xét hai ánh xạ $f : X \longrightarrow Y$ và $g : Y \longrightarrow Z$. *Hợp thành* của f và g theo thứ tự đó là ánh xạ $g \circ f$ từ X đến Z được xác định bởi $(g \circ f)(x) = g(f(x))$ với mỗi $x \in X$.

Ví dụ 0.19. Cho hai ánh xạ từ $\mathbb{R}$ vào chính nó được xác định bởi $f(x) = x^2$ và $g(x) = \sin x$. Khi đó $(g \circ f)(x) = \sin x^2$ và $(f \circ g)(x) = \sin^2 x$. Ta có $g \circ f \neq f \circ g$, do đó phép hợp thành không có tính giao hoán.

Mệnh đề 0.20. *Cho ba ánh xạ $f : X \longrightarrow Y$, $g : Y \longrightarrow Z$ và $h : Z \longrightarrow W$. Khi đó ta có:*

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

(b) $id_Y \circ f = f \circ id_X = f$.

Chứng minh. Cho phần tử x tùy ý trong X. Khi đó

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

và ta có (a).

(b) là hiển nhiên.

□

Bài tập

1. Giả sử $f : X \longrightarrow Y$ là một ánh xạ. Ký hiệu

$$G_f = \{(x, f(x)) \in X \times Y | x \in X\},$$

G_f gọi là đồ thị của f. Cho A là một tập con của $U \times V$ sao cho với mỗi $x \in U$ có duy nhất một $y \in V$ để $(x, y) \in A$, chứng tỏ có duy nhất một ánh xạ từ U đến V có đồ thị là A.

2. Hãy xác định một ánh xạ f từ mặt phẳng $\mathbb{R}^2$ đến chính nó sao cho

(a) Ảnh của hình vuông $\{(x, y) \in \mathbb{R}^2 | \, 0 \leq x, y \leq 1\}$ bởi f là hình chữ nhật $\{(x, y) \in \mathbb{R}^2 | \, 2 \leq x \leq 4, \, 3 \leq y \leq 9\}$.

(b) Ảnh của hình vuông $\{(x, y) \in \mathbb{R}^2 | \, 0 \leq x, y \leq 1\}$ bởi f là hình tròn tâm $I(2, 3)$ bán kính bằng 2.

3. Cho tập hợp $A \neq \emptyset$ và $f : \mathcal{P}(A) \longrightarrow \mathcal{P}(A)$ là một ánh xạ đơn điệu tăng, tức là

$$\forall X, Y \in \mathcal{P}(A), X \subset Y \Longrightarrow f(X) \subset f(Y).$$

Chứng minh rằng f có điểm bất động, tức là có $U \in \mathcal{P}(A)$ sao cho $f(U) = U$.

0.3 Đơn ánh - Toàn ánh - Song ánh

Định nghĩa 0.21. Xét ánh xạ $f : X \longrightarrow Y$.

(a) f là một *đơn ánh* nếu với mọi $x, x' \in X$ mà $x \neq x'$ thì $f(x) \neq f(x')$. Nói cách khác, f là một đơn ánh nếu $f(x) = f(x')$ thì $x = x'$.

(b) f là một *toàn ánh* nếu với mọi $y \in Y$ thì có $x \in X$ sao cho $y = f(x)$. Vậy f là một toàn ánh nếu $\operatorname{Im} f = Y$.

(c) f là một *song ánh* nếu f vừa đơn ánh vừa toàn ánh. Điều này tương đương với bất kỳ $y \in Y$ có duy nhất $x \in X$ sao cho $y = f(x)$.

Định nghĩa trên được phát biểu lại như sau. Với phần tử $y \in Y$ tùy ý cho trước ta có các khẳng định sau.

f là một đơn ánh nếu y không phải ảnh của bất kỳ phần tử nào trong X hoặc y là ảnh của duy nhất một phần tử x trong X, tức là phương trình $f(x) = y$ có nhiều nhất một nghiệm trong X.

f là một toàn ánh nếu y luôn là ảnh của ít nhất một phần tử trong X, nói cách khác phương trình $f(x) = y$ luôn có nghiệm trong X.

f là một song ánh nếu y luôn là ảnh của duy nhất một phần tử trong X, tức là phương trình $f(x) = y$ có đúng một nghiệm trong X.

Ví dụ 0.22. (a) Ánh xạ $n \in \mathbb{N} \mapsto n^2 \in \mathbb{N}$ là một đơn ánh vì nếu với mọi $m, m' \in \mathbb{N}$, $m \neq m'$ thì ta luôn có $m^2 \neq m'^2$. Tuy nhiên ánh xạ $n \in \mathbb{Z} \mapsto n^2 \in \mathbb{N}$ không phải đơn ánh vì 1 và -1 là hai phần tử khác nhau nhưng có cùng một ảnh 1.

(b) Ánh xạ $n \in \mathbb{Z} \mapsto n^3 \in \mathbb{Z}$ không phải toàn ánh vì phần tử $2 \in \mathbb{Z}$ không là ảnh của bất kỳ phần tử nào trong $\mathbb{Z}$. Nhưng ánh xạ $x \in \mathbb{R} \mapsto x^3 \in \mathbb{R}$ là một toàn ánh, hơn nữa nó là một song ánh vì với mỗi $y \in \mathbb{R}$ có duy nhất một tạo ảnh $x = \sqrt[3]{y}$.

(c) Cho A là một tập con của tập hợp X. Khi đó ánh xạ $x \in A \mapsto x \in X$ là một đơn ánh, gọi là ánh xạ nhúng A vào X.

(d) Với mỗi tập con A của tập hợp X ta tương ứng với tập hợp $C_X A$. Đây là một song ánh từ tập hợp các phần $\mathcal{P}(X)$ của X đến chính nó.

Mệnh đề 0.23. *Cho ánh xạ $f : X \longrightarrow Y$, trong đó X, Y là hai tập hợp hữu hạn có cùng số phần tử. Khi đó ba điều sau tương đương.*

(a) *f là một đơn ánh.*

(b) *f là một toàn ánh.*

(c) *f là một song ánh.*

Chứng minh. (a)⇒(b) f là một đơn ánh nên X và $\operatorname{Im} f$ có cùng số phần tử. Vì $\operatorname{Im} f$ là một tập con của Y nên $\operatorname{Im} f = Y$. Vậy f là một toàn ánh.

(b)⇒(c) f là một toàn ánh nên $\operatorname{Im} f = Y$. Nếu f không phải đơn ánh thì có $a, b \in X$, $a \neq b$ sao cho $f(a) = f(b)$. Khi đó $\operatorname{Im} f$ có số phần tử nhỏ hơn số phần tử của X nên $\operatorname{Im} f \neq Y$, điều này mâu thuẫn với $\operatorname{Im} f = Y$. Do đó f là một đơn ánh, và như vậy f là một song ánh.

(c)⇒(a) là hiển nhiên.

□

Mệnh đề 0.24. *Giả sử phép hợp thành của hai ánh xạ thực hiện được. Khi đó ta có:*

(a) *Hợp thành của hai đơn ánh là một đơn ánh.*

(b) *Hợp thành của hai toàn ánh là một toàn ánh.*

(c) *Hợp thành của hai song ánh là một song ánh.*

Chứng minh. Xét hai ánh xạ $f : X \longrightarrow Y$ và $g : Y \longrightarrow Z$.

(a) Giả sử f và g là hai đơn ánh. Khi đó với $x, x' \in X$ mà $x \neq x'$ thì $f(x) \neq f(x')$, và do đó $g(f(x)) \neq g(f(x'))$. Vậy $g \circ f$ là một đơn ánh.

(b) Giả sử f và g là hai toàn ánh, khi đó $f(X) = Y$ và $g(Y) = Z$. Từ đây suy ra $g \circ f(X) = g(f(X)) = g(Y) = Z$. Vậy $g \circ f$ là một toàn ánh.

(c) được suy từ (a) và (b).

□

Một câu hỏi tự nhiên là nếu hợp thành của hai ánh xạ lần lượt là đơn ánh, toàn ánh thì các ánh xạ trong hợp thành đó có là đơn ánh, toàn ánh không? Ta có câu trả lời như sau.

Mệnh đề 0.25. *Cho hai ánh xạ $f : X \longrightarrow Y$ và $g : Y \longrightarrow Z$.*

(a) *Nếu $g \circ f$ là một đơn ánh thì f là một đơn ánh.*

(b) *Nếu $g \circ f$ là một toàn ánh thì g là một toàn ánh.*

Chứng minh. (a) Giả sử $g \circ f$ là một đơn ánh. Với $x, x' \in X$ mà $x \neq x'$ thì $g(f(x)) \neq g(f(x'))$, và do đó $f(x) \neq f(x')$. Vậy f là một đơn ánh.

(b) Giả sử $g \circ f$ là một toàn ánh. Vì $Z = g(f(X)) \subset g(Y) \subset Z$ ta suy ra $g(Y) = Z$. Vậy g là một toàn ánh.

□

Với hai tập hợp hữu hạn thì ta luôn có thể so sánh số phần tử của chúng. Ta thường nói số phần tử của tập hợp này không nhiều hơn số phần tử của tập hợp kia hoặc ngược lại, nghĩa là giữa chúng luôn có một đơn ánh. Đối với hai tập hợp bất

kỳ thì điều trên còn đúng không? Định lý sau trả lời câu hỏi trên mà chứng minh của nó được trình bày ở phần tiếp theo vì cần đến Bổ đề Zorn.

Định lý 0.26. *Giả sử X, Y là hai tập hợp không rỗng, khi đó luôn có một đơn ánh từ X đến Y hoặc ngược lại.*

Chú ý rằng nếu có một họ $(a_i)_{i\in I}$ trong X^I thì ta có một ánh xạ $f : I \longrightarrow X$ được xác định bởi: với mỗi $i \in I$ thì $f(i) = a_i$. Đảo lại, với mỗi $f : I \longrightarrow X$ ta đặt $a_i = f(i) \in X$ thì f xác định một họ $(a_i)_{i\in I}$ trong X^I. Tương ứng này là một song ánh. Ta đồng nhất một họ $(a_i)_{i\in I}$ trong X^I với một ánh xạ $f : I \longrightarrow X$ và do đó tập hợp X^I được đồng nhất với tập hợp các ánh xạ $f : I \longrightarrow X$.

Một cách tổng quát, giả sử $(A_i)_{i\in I}$ là một họ tùy ý các tập hợp lấy chỉ số trong tập hợp I. Khi đó phần tử $(a_i)_{i\in I} \in \Pi_{i\in I}A_i$ xác định một ánh xạ $f : I \longrightarrow \cup_{i\in I}A_i$ sao cho với mỗi $i \in I$ thì $f(i) = a_i \in A_i$. Ngược lại, với ánh xạ như trên sẽ xác định duy nhất một phần tử trong $\Pi_{i\in I}A_i$. Do đó ta có thể xem $\Pi_{i\in I}A_i$ như là tập hợp các ánh xạ $f : I \longrightarrow \cup_{i\in I}A_i$ sao cho với mỗi $i \in I$ thì $f(i) \in A_i$.

Bài tập

1. Cho tập hợp X gồm 29 ký tự. Hỏi có bao nhiêu đơn ánh từ X đến tập hợp các dãy $(a_1, a_2, \ldots, a_{16})$, trong đó a_i nhận các giá trị 0 hoặc 1?
2. Cho ánh xạ $f : X \longrightarrow Y$. Chứng minh rằng
   (a) f là một đơn ánh khi và chỉ khi với mọi tập con A, B của X thì $f(A \cap B) = f(A) \cap f(B)$.
   (b) f là một đơn ánh khi và chỉ khi với mọi tập con $A \subset X$ thì $f^{-1}(f(A)) = A$.
   (c) f là một toàn ánh khi và chỉ khi với mọi tập con $B \subset Y$ thì $f(f^{-1}(B)) = B$.
   (d) f là một song ánh khi và chỉ khi với mọi tập con $A \subset X$ thì $f(C_X A) = C_Y f(A)$.
3. Cho ánh xạ $f : X \longrightarrow Y$. Chứng minh rằng
   (a) f là một đơn ánh khi và chỉ khi với mọi tập hợp A và mọi ánh xạ $g, g' : A \longrightarrow X$, $f \circ g = f \circ g'$ kéo theo $g = g'$.
   (b) f là một toàn ánh khi và chỉ khi với mọi tập hợp B và mọi ánh xạ $h, h' : Y \longrightarrow B$, $h \circ f = h' \circ f$ kéo theo $h = h'$.
4. Chứng tỏ không tồn tại một đơn ánh từ tập hợp các phần $\mathcal{P}(X)$ của tập hợp X đến X.

0.4 Ánh xạ ngược

Định nghĩa 0.27. Xét ánh xạ $f : X \longrightarrow Y$. Ta nói ánh xạ $k : Y \longrightarrow X$ là một ánh xạ *ngược* của f nếu $k \circ f = id_X$ và $f \circ k = id_Y$. Ánh xạ ngược của f được ký hiệu bởi f^{-1}.

Do tính đối xứng, nếu f^{-1} là ánh xạ ngược của f thì f cũng là ánh xạ ngược của f^{-1}. Ánh xạ ngược được xác định bởi công thức

$$x = f^{-1}(y) \Longleftrightarrow y = f(x).$$

Ví dụ 0.28. (a) Ánh xạ $x \in \mathbb{R} \longmapsto e^x \in \mathbb{R}^+$ với $\mathbb{R}^+$ tập hợp các số thực dương có ánh xạ ngược là $y \in \mathbb{R}^+ \longmapsto \ln y \in \mathbb{R}$.

(b) Trong mặt phẳng phép tịnh tiến véc-tơ $\overrightarrow{V}$ có ánh xạ ngược là phép tịnh tiến véc-tơ $-\overrightarrow{V}$, phép quay quanh gốc tọa độ một góc θ có ánh xạ ngược là phép quay quanh gốc tọa độ một góc $-\theta$.

Định nghĩa 0.29. Xét ánh xạ $f : X \longrightarrow Y$. Ta nói ánh xạ $g : Y \longrightarrow X$ là một ánh xạ ngược *bên trái* của f nếu $g \circ f = id_X$; là một ánh xạ ngược *bên phải* của f nếu $f \circ g = id_Y$.

Một ánh xạ có ánh xạ ngược thì có ánh xạ ngược bên trái và bên phải. Tuy nhiên điều ngược lại không đúng, tức là nếu một ánh xạ có ánh xạ ngược một bên thì chưa chắc đã có ánh xạ ngược. Một ánh xạ có thể có nhiều ánh xạ ngược một bên. Mệnh đề sau thiết lập mối quan hệ giữa ánh xạ ngược hai bên.

Mệnh đề 0.30. *Cho ánh xạ $f : X \longrightarrow Y$. Nếu $g, h : Y \longrightarrow X$ lần lượt là hai ánh xạ ngược bên trái và bên phải của f thì $g = h$.*

Chứng minh. Bởi giả thiết ta có $g \circ f = id_X$ và $f \circ h = id_Y$. Khi đó

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

Ta có điều phải chứng minh.

□

Một hệ quả hiển nhiên từ mệnh đề trên là

Hệ quả 0.31. *Cho ánh xạ $f : X \longrightarrow Y$. Nếu f có ánh xạ ngược thì f^{-1} là duy nhất. Khi đó f^{-1} cũng có ánh xạ ngược và $(f^{-1})^{-1} = f$.*

Bây giờ ta thiết lập điều kiện cần và đủ để một ánh xạ có ánh xạ ngược một bên.

Mệnh đề 0.32. *Cho ánh xạ $f : X \longrightarrow Y$. Khi đó ta có:*

(a) *f có ánh xạ ngược bên trái khi và chỉ khi f là một đơn ánh.*

(b) *f có ánh xạ ngược bên phải khi và chỉ khi f là một toàn ánh.*

Chứng minh. (a) Giả sử $g : Y \longrightarrow X$ là một ánh xạ ngược bên trái của f. Nếu $f(x) = f(x')$ thì $g \circ f(x) = g \circ f(x')$, suy ra $x = x'$. Vậy f là một đơn ánh. Đảo lại, giả sử f là một đơn ánh. Lấy $x_0 \in X$ và cố định x_0, ta định nghĩa ánh xạ $g : Y \longrightarrow X$ như sau: với mỗi $y \in Y$, nếu $y \notin f(X)$ ta tương ứng $g(y) = x_0$, ngược lại do f là một đơn ánh nên có duy nhất $x \in X$ sao cho $f(x) = y$, ta tương ứng $g(y) = x$. Khi đó $g \circ f = id_X$. Vậy f có ánh xạ ngược bên trái.

(b) Giả sử $h : Y \longrightarrow X$ là một ánh xạ ngược bên phải của f. Vì $f(X) \supset f(h(Y)) = id_Y(Y) = Y$ ta suy ra $f(X) = Y$. Vậy f là một toàn ánh. Đảo lại, giả sử f là một toàn ánh. Ta định nghĩa ánh xạ $h : Y \longrightarrow X$ như sau: với mỗi $y \in Y$, chọn một phần tử cố định $x \in f^{-1}(y)$ và ta tương ứng $h(y) = x$. Khi đó $f \circ h = id_Y$. Vậy f có ánh xạ ngược bên phải.

□

Hệ quả 0.33. *Ánh xạ $f : X \longrightarrow Y$ có ánh xạ ngược khi và chỉ khi f là một song ánh.*

Chứng minh. Suy ra trực tiếp từ các Mệnh đề 0.32 và 0.30.

□

Ví dụ 0.34. (a) Xét ánh xạ $f : \mathbb{R}\setminus\{1\} \longrightarrow \mathbb{R} \setminus \{2\}$ được cho bởi $f(x) = \frac{2x}{x-1}$. Với phần tử tùy ý $y \in \mathbb{R} \setminus \{2\}$ ta xét phương trình $f(x) = y$. Phương trình này có nghiệm duy nhất $x = \frac{y}{y-2} \in \mathbb{R} \setminus \{1\}$, do đó f là một song ánh. Ánh xạ ngược của f được xác định bởi $f^{-1}(x) = \frac{x}{x-2}$.

(b) sin : [-$\frac{\pi}{2}$, $\frac{\pi}{2}$] $\longrightarrow$ [-1,1] là một song ánh, có ánh xạ ngược là arcsin : [-1,1] $\longrightarrow$ $[-\frac{\pi}{2}, \frac{\pi}{2}]$.

(c) cos : $[0, \pi] \longrightarrow$ [-1,1] là một song ánh, có ánh xạ ngược là arccos : [-1,1] $\longrightarrow$ $[0, \pi]$.

(d) tan : (-$\frac{\pi}{2}$, $\frac{\pi}{2}$) $\longrightarrow$ (-∞,+∞) là một song ánh, có ánh xạ ngược là arctan : (-∞,+∞) $\longrightarrow$ $(-\frac{\pi}{2}, \frac{\pi}{2})$.

Mệnh đề sau là hiển nhiên.

Mệnh đề 0.35. *Giả sử hai ánh xạ $f : X \longrightarrow Y$ và $g : Y \longrightarrow Z$ có ánh xạ ngược. Khi đó $g \circ f$ có ánh xạ ngược và $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Định lý 0.36. (Cantor - Bernstein hay Schroder - Bernstein) *Cho hai tập hợp X, Y tùy ý. Nếu có một đơn ánh từ X đến Y và một đơn ánh từ Y đến X thì sẽ có một song ánh giữa chúng.*

Chứng minh. Giả sử f là một song ánh từ X đến tập con $Y' \subset Y$ và g là một song ánh từ Y đến tập con $X' \subset X$. Khi đó $h = g \circ f$ là một song ánh từ X đến $h(X) \subset X'$. Đặt $Z = X' \setminus h(X)$. Nếu $Z = \emptyset$ thì h là một song ánh từ X đến X'. Khi đó $g^{-1} \circ h$ là một song ánh từ X đến Y. Nếu $Z \neq \emptyset$ thì ta đặt

$$W = Z \cup h(Z) \cup h^2(Z) \cup h^3(Z) \cup \cdots$$

với h^i là hợp thành của h i lần. Ta thấy

$$X' = Z \cup h(X) = Z \cup h(W \cup (X \setminus W)) = Z \cup h(W) \cup h(X \setminus W).$$

Vì $h(W) = h(Z) \cup h^2(Z) \cup h^3(Z) \cup \cdots$ nên

$$X' = W \cup h(X \setminus W).$$

Bây giờ ta chứng tỏ ánh xạ $k : X \longrightarrow X'$ được xác định bởi

$$k(x) = \begin{cases} x & \text{nếu } x \in W \\ h(x) & \text{nếu } x \in X \setminus W \end{cases}$$

là một song ánh. Hiển nhiên k là một toàn ánh. Để chứng tỏ k là một đơn ánh ta chỉ cần chứng tỏ $k(W) \cap k(X \setminus W) = \emptyset$ là đủ. Thật vậy, từ định nghĩa của k ta có

$$k(X \setminus W) = h(X \setminus W) = h(X) \setminus h(W) = h(X) \setminus W.$$

Do đó

$$k(W) \cap k(X \setminus W) = W \cap (h(X) \setminus W) = \emptyset.$$

Vậy k là một đơn ánh nên là một song ánh. Khi đó $g^{-1} \circ k$ là một song ánh từ X đến Y.

□

Bài tập

1. Ánh xạ nào sau đây là một đơn ánh, toàn ánh, song ánh? Nếu là một song ánh hãy xác định ánh xạ ngược.
   (a) $f : \mathbb{R} \setminus \{1\} \longrightarrow \mathbb{R}$ được cho bởi $f(x) = x + \frac{1}{x-1}$.
   (b) $f : \mathbb{R} \longrightarrow \mathbb{R}$ được cho bởi $f(x) = x^3 + 3x^2 + 3x$.
   (c) $f : \mathbb{R} \longrightarrow \mathbb{R}$ được cho bởi $f(x) = \frac{1}{2}(e^x - e^{-x})$.
2. Ánh xạ nào sau đây là một đơn ánh, toàn ánh, song ánh? Nếu là một song ánh hãy xác định ánh xạ ngược.
   (a) $f : \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2$ với $f(x, y) = (2x - y, x + y)$.
   (b) $f : \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2$ với $f(x, y) = (2x + y, x + y)$.

0.5 Tập hợp đếm được

Định nghĩa 0.37. Ta nói hai tập hợp có *cùng lực lượng* nếu có một song ánh giữa chúng.

Định nghĩa 0.38. Một tập hợp gọi là *đếm được* nếu nó có cùng lực lượng với tập hợp các số tự nhiên.

Ví dụ 0.39. Tập hợp $\mathbb{Z}$ các số nguyên là một tập hợp đếm được. Thật vậy, ánh xạ từ $\mathbb{Z}$ đến $\mathbb{N}$ được xác định bởi: số nguyên không âm n tương ứng với $2n$, số nguyên âm n tương ứng với $-2n-1$ là một song ánh.

Mệnh đề 0.40. *Cho N là một tập hợp đếm được. Nếu X là một tập con vô hạn của N thì X là tập hợp đếm được.*

Chứng minh. Giả sử X là một tập con vô hạn của N. Vì N là đếm được nên có song ánh f từ N đến $\mathbb{N}$ và thu hẹp của f về X là một song ánh từ X đến $Y = f(X) \subset \mathbb{N}$. Mệnh đề sẽ được chứng minh nếu ta chứng tỏ Y là đếm được. Gọi a_0 là số nhỏ nhất của Y. Giả sử quy nạp a_k được định nghĩa với $k \geq 0$, thì a_{k+1} được xác định là số nhỏ nhất của tập hợp $Y \setminus \{a_0, \ldots, a_k\}$. Khi đó ánh xạ mỗi $n \in \mathbb{N}$ tương ứng với $a_n \in Y$ là một song ánh và Y là đếm được.

□

Mệnh đề 0.41. (a) *Nếu X là một tập hợp vô hạn và có một đơn ánh từ X đến tập hợp đếm được N thì X là một tập hợp đếm được.*

(b) *Nếu X là một tập hợp vô hạn và có một toàn ánh từ tập hợp đếm được N đến X thì X là một tập hợp đếm được.*

Chứng minh. (a) Giả sử có một đơn ánh f từ X đến N. Khi đó f là một song ánh từ X đến $f(X)$. Vì X là một tập hợp vô hạn nên $f(X)$ cũng vậy. Theo Mệnh đề 0.40 thì $f(X)$ là một tập hợp đếm được và (a) được chứng minh.

(b) Giả sử có một toàn ánh g từ N đến X. Khi đó theo Mệnh đề 0.32 thì g có một ánh xạ ngược bên phải h. Bởi Mệnh đề 0.25, h là một đơn ánh. Theo (a) thì X là một tập hợp đếm được và (b) được chứng minh.

□

Hệ quả 0.42. *Nếu X, Y là hai tập hợp đếm được thì tích $X \times Y$ cũng là một tập hợp đếm được.*

Chứng minh. Nếu X, Y là hai tập hợp đếm được thì có các song ánh f, g lần lượt từ X, Y đến tập hợp $\mathbb{N}$ các số tự nhiên. Khi đó ánh xạ

$$(x, y) \in X \times Y \longmapsto (f(x), g(y)) \in \mathbb{N} \times \mathbb{N}$$

là một song ánh. Hệ quả sẽ được chứng minh nếu ta chứng tỏ $\mathbb{N} \times \mathbb{N}$ là đếm được. Xét ánh xạ h được xác định bởi

$$(m, n) \in \mathbb{N} \times \mathbb{N} \longmapsto h(m, n) = 2^m 3^n \in \mathbb{N},$$

ta chứng tỏ h là một đơn ánh. Thật vậy, nếu $h(m, n) = h(m', n')$ thì $2^m 3^n = 2^{m'} 3^{n'}$, suy ra $m = m'$ và $n = n'$. Do đó theo Mệnh đề 0.41 thì $\mathbb{N} \times \mathbb{N}$ là đếm được và hệ quả được chứng minh.

□

Hệ quả 0.43. *Hợp của một họ đếm được gồm các tập hợp đếm được cũng là một tập hợp đếm được.*

Chứng minh. Giả sử I là một tập hợp đếm được và $(A_i)_{i \in I}$ là một họ các tập hợp trong đó A_i đếm được với mỗi $i \in I$. Không mất tính tổng quát ta có thể xem I là tập hợp $\mathbb{N}$ các số tự nhiên. Với mỗi $i \in \mathbb{N}$ thì $\mathbb{N} \times \{i\}$ là một tập hợp đếm được, do đó có song ánh f_i từ $\mathbb{N} \times \{i\}$ đến A_i. Khi đó ánh xạ

$$(m, n) \in \mathbb{N} \times \mathbb{N} \longmapsto f_n(m, n) \in \cup_{k \in \mathbb{N}} A_k$$

là một toàn ánh. Bởi Hệ quả 0.42, $\mathbb{N} \times \mathbb{N}$ đếm được và theo Mệnh đề 0.41 thì $\cup_{k \in \mathbb{N}} A_k$ là một tập hợp đếm được.

□

Mệnh đề 0.44. *Tập hợp các số hữu tỷ là đếm được.*

Chứng minh. Đặt $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$. Xét ánh xạ $f : \mathbb{Z} \times \mathbb{N}^* \longrightarrow \mathbb{Q}$ được định nghĩa bởi $f(m, n) = \frac{m}{n}$ với mỗi cặp $(m, n) \in \mathbb{Z} \times \mathbb{N}^*$. Bởi Hệ quả 0.42 thì $\mathbb{Z} \times \mathbb{N}^*$ đếm được. Vì f là một toàn ánh nên theo Mệnh đề 0.41 ta có $\mathbb{Q}$ đếm được.

□

Định lý 0.45. *Tập hợp các số thực là vô hạn, không đếm được.*

Chứng minh. Ánh xạ $x \in (0, 1) \longmapsto \cot(\pi x) \in \mathbb{R}$ là một song ánh nên tập hợp $(0, 1)$ có cùng lực lượng với tập hợp $\mathbb{R}$ các số thực, do đó ta chỉ cần chứng tỏ tập hợp $(0, 1)$ không đếm được là đủ. Các số thực trong $(0, 1)$ đều được biểu diễn ở dạng số thập phân. Nếu tập hợp $(0, 1)$ đếm được thì ta có thể liệt kê các phần tử của nó như sau:

$$\begin{aligned}
a_0 &= 0, a_{00} a_{01} \dots a_{0n} \dots \\
a_1 &= 0, a_{10} a_{11} \dots a_{1n} \dots \\
\dots &= \dots \\
a_n &= 0, a_{n0} a_{n1} \dots a_{nn} \dots \\
\dots &= \dots
\end{aligned}$$

trong đó a_{ij} là các số nguyên nhận giá trị từ 0 đến 9. Khi đó phần tử $a = 0, b_0 b_1 \dots b_n \dots$, trong đó $b_n \neq a_{nn}$ với mọi n, thuộc $(0,1)$ nhưng không là một trong các phần tử được liệt kê ở trên. Điều này vô lý. Vậy tập hợp $(0,1)$ không đếm được.

□

Xét hai tập hợp X, Y tùy ý. Nếu có một đơn ánh từ X đến Y và không có song ánh giữa chúng thì ta nói lực lượng của X nhỏ hơn lực lượng của Y và viết card$X$ <card$Y$. Ta cũng nói tập hợp có n phần tử có lực lượng bằng n, tập hợp $\mathbb{N}$ các số tự nhiên có lực lượng đếm được hay lực lượng $\mathcal{N}_0$, tập hợp $\mathbb{R}$ các số thực có lực lượng continum hay lực lượng $\mathcal{N}$. Vì có một đơn ánh từ $\mathbb{N}$ đến $\mathbb{R}$ và không có song ánh giữa chúng nên $\mathcal{N}_0 < \mathcal{N}$. Một câu hỏi tự nhiên là liệu có tập hợp X sao cho $\mathcal{N}_0$ <card$X$< $\mathcal{N}$ không? Và người ta chứng tỏ được rằng câu hỏi trên độc lập với tiên đề chọn tức là không thể chứng minh điều trên bằng tiên đề chọn.

Tiên đề chọn. Cho một họ các tập hợp không rỗng $(A_i)_{i\in I}$ với chỉ số trong một tập hợp I tùy ý không rỗng. Khi đó $\Pi_{i\in I} A_i$ là một tập hợp không rỗng.

Bài tập

1. Chứng tỏ tập hợp các số 8 trong mặt phẳng không chứa lẫn nhau, không cắt nhau là một tập hợp đếm được.
2. Cho X là một tập hợp. Với mỗi $A \subset X$ ta định nghĩa ánh xạ $\varphi_A : X \longrightarrow \{0,1\}$ được cho bởi
$$\varphi_A(x) = \begin{cases} 1 & \text{nếu } x \in A; \\ 0 & \text{nếu } x \in X \setminus A. \end{cases}$$
Đặt M là tập hợp các ánh xạ từ X đến $\{0,1\}$. Chứng tỏ ánh xạ $\varphi : \mathcal{P}(X) \longrightarrow M$ được xác định bởi $\varphi(A) = \varphi_A$ với mỗi $A \in \mathcal{P}(X)$ là một song ánh. Từ đây suy ra $\mathcal{P}(X)$ có cùng lực lượng với M.
3. Chứng tỏ rằng
(a) Tập hợp gồm các dãy $(a_1, \dots, a_n, \dots)$ với hữu hạn các a_n nhận giá trị 1 còn các phần tử khác nhận giá trị 0 là một tập hợp đếm được.
(b) Tập hợp gồm các dãy $(a_1, \dots, a_n, \dots)$ với các a_n nhận giá trị 0 hay 1 là một tập hợp vô hạn, không đếm được. Tập hợp này có cùng lực lượng với tập hợp các số thực.
4. (a) Hãy xây dựng một song ánh từ tập hợp đếm được X đến $X \cup Y$ với tập hợp Y hữu hạn hay đếm được.
(b) Hãy xây dựng một song ánh từ tập hợp [0,1) đến tập hợp $(0,1)$.

5. Một số thực a gọi là số đại số nếu nó là nghiệm của một đa thức khác không với hệ số nguyên, ngược lại gọi là số siêu việt. Chứng tỏ tập hợp các số đại số là đếm được. Từ đây suy ra rằng tập hợp các số siêu việt có cùng lực lượng với tập hợp các số thực.

0.6 Quan hệ tương đương

Quan hệ tương đương đóng một vai trò quan trọng trong nhiều cấu trúc đại số. Như chúng ta sẽ thấy trong mục này, quan hệ tương đương trên một tập hợp sẽ xác định một phân hoạch, phân lớp các phần tử của một tập hợp thành các tập con không rỗng rời nhau, và đảo lại, một phân hoạch như thế sẽ xác định một quan hệ tương đương trên tập hợp đó.

Định nghĩa 0.46. Một *quan hệ tương đương* trên tập hợp E không rỗng là một mối liên hệ $x \sim y$ giữa các phần tử $x, y \in E$ thỏa mãn các điều kiện sau:

(a) $x \sim x$ với mọi $x \in E$ (tính phản xạ).

(b) Nếu $x \sim y$ thì $y \sim x$ (tính đối xứng).

(c) Nếu $x \sim y$ và $y \sim z$ thì $x \sim z$ (tính bắc cầu).

Nếu $\sim$ là một quan hệ tương đương trên E, khi đó với bất kỳ $x \in E$, *lớp tương đương* của x là tập hợp

$$\overline{x} = \{y \in E / y \sim x\}.$$

Phần tử bất kỳ $y \in \overline{x}$ được gọi là một đại diện của lớp tương đương $\overline{x}$.

Mệnh đề 0.47. *Cho $\sim$ là một quan hệ tương đương trên tập hợp E và $x, y \in E$. Khi đó ta có:*

(a) *$x \in \overline{x}$, tức là mỗi lớp tương đương đều không rỗng.*

(b) *Nếu $y \in \overline{x}$ thì $\overline{y} = \overline{x}$.*

(c) *$\overline{y} = \overline{x}$ nếu và chỉ nếu $y \sim x$.*

(d) *Hoặc $\overline{x} = \overline{y}$ hoặc $\overline{x} \cap \overline{y} = \emptyset$.*

(e) *E là hợp rời các lớp tương đương.*

Chứng minh. (a) Tính phản xạ cho ta $x \sim x$ và do đó $x \in \overline{x}$.

(b) Giả sử $y \in \overline{x}$, khi đó $y \sim x$. Bây giờ nếu $z \in \overline{y}$ thì $z \sim y$, tính bắc cầu cho ta $z \sim x$ và suy ra $z \in \overline{x}$. Vậy $\overline{y} \subset \overline{x}$. Tương tự nếu $z \in \overline{x}$ thì $z \sim x$, bởi tính đối xứng và bắc cầu ta có $z \sim y$ và do đó $z \in \overline{y}$. Vậy $\overline{x} \subset \overline{y}$ và ta có (b).

(c) Giả sử $\overline{y} = \overline{x}$. Theo (a) ta có $y \in \overline{y}$ nên $y \in \overline{x}$, bởi định nghĩa ta có $y \sim x$. Đảo lại, nếu $y \sim x$ thì $y \in \overline{x}$, và theo (b) ta có $\overline{y} = \overline{x}$.

(d) Giả sử $\overline{x} \cap \overline{y} \neq \emptyset$. Khi đó có $z \in \overline{x}$ và $z \in \overline{y}$. Theo (b) thì $\overline{z} = \overline{x}$, $\overline{z} = \overline{y}$, và do đó $\overline{x} = \overline{y}$.

(e) được suy ra từ (a) và (d).

□

Ta ký hiệu $E/\sim = \{\overline{x}/x \in E\}$ và gọi $E/\sim$ là tập hợp *thương* của E theo quan hệ tương đương $\sim$.

Ví dụ 0.48. (a) Cho trước số tự nhiên $n \geq 2$. Trên tập hợp $\mathbb{Z}$ các số nguyên ta xét quan hệ đồng dư:

$$x \equiv y \,(\text{mod } n)$$

nếu có $k \in \mathbb{Z}$ sao cho $x = y + kn$. Quan hệ $\equiv$ có những tính chất sau:

Với mỗi $x \in \mathbb{Z}$ ta có $x = x + 0 \cdot n$, do đó $x \equiv x \,(\text{mod } n)$.

Nếu $x \equiv y \,(\text{mod } n)$ thì có $k \in \mathbb{Z}$ sao cho $x = y + kn$. Khi đó $y = x - kn$ và $y \equiv x \,(\text{mod } n)$.

Nếu $x \equiv y \,(\text{mod } n)$ và $y \equiv z \,(\text{mod } n)$ thì có $k, l \in \mathbb{Z}$ sao cho $x = y + kn$ và $y = z + ln$. Từ đây suy ra $x = z + (k + l)n$ và $x \equiv z \,(\text{mod } n)$.

Vậy $\equiv$ là một quan hệ tương đương. Lớp tương đương của x gồm các số nguyên y sao cho có số nguyên k để $y = x + kn$. Do đó

$$\overline{x} = \{x + kn/k \in \mathbb{Z}\}\,.$$

Nếu $x \in \mathbb{Z}$ thì x có quan hệ với phần dư khi chia x cho n và các phần dư không quan hệ với nhau, do đó theo Mệnh đề 0.47 trong $\mathbb{Z}$ chỉ có các lớp tương đương $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. Đặt $\mathbb{Z}_n = \mathbb{Z}/\equiv$,

$$\mathbb{Z}_n = \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}$$

được gọi là tập hợp các số nguyên modulo n. Chẳng hạn: $\mathbb{Z}_2$ có hai lớp tương đương, đó là lớp các số chẵn và lớp các số lẻ; $\mathbb{Z}_{10}$ có mười lớp tương đương từ lớp $\overline{0}$ đến lớp $\overline{9}$.

(b) Trên tập hợp $\mathbb{N} \times \mathbb{N}$, ta xét quan hệ $(m, n) \sim (m', n')$ nếu $m + n' = m' + n$. Khi đó $\sim$ là một quan hệ tương đương. Với mỗi cặp $(m, n) \in \mathbb{N} \times \mathbb{N}$ lớp tương đương của nó được xác định như sau: nếu $m \geq n$ thì có duy nhất $r \in \mathbb{N}$ sao cho $m + 0 = r + n$, do đó $(m, n) \sim (r, 0)$ và $\overline{(m, n)} = \overline{(r, 0)}$; nếu $m < n$ thì có duy nhất $s \in \mathbb{N}, s > 0$ sao cho $m + s = 0 + n$, do đó $(m, n) \sim (0, s)$ và $\overline{(m, n)} = \overline{(0, s)}$. Đặt $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim$,

$$\mathbb{Z} = \left\{\overline{(r, 0)}/r \in \mathbb{N}\right\} \cup \left\{\overline{(0, s)}/s \in \mathbb{N}, s > 0\right\}.$$

Ta gọi $\mathbb{Z}$ là tập hợp các số nguyên và mỗi lớp tương đương $\overline{(m, n)}$ là một số nguyên.

(c) Trên lớp các tập hợp ta xét quan hệ "cùng lực lượng". Rõ ràng rằng với tập hợp A tùy ý thì $id_A : A \longrightarrow A$ là một song ánh nên A có cùng lực lượng với chính nó. Nếu A có cùng lực lượng với B thì có một song ánh f từ A đến B, khi đó f^{-1} là

một song ánh từ B đến A và do đó B có cùng lực lượng với A. Nếu A có cùng lực lượng với B và B có cùng lực lượng với C thì có các song ánh f từ A đến B, g từ B đến C và hiển nhiên $g \circ f$ là một song ánh từ A đến C nên A có cùng lực lượng với C. Vậy "cùng lực lượng" là một quan hệ tương đương trên lớp các tập hợp. Với quan hệ này, lớp các tập hợp đang xét được chia thành các lớp tương đương có lực lượng khác nhau, mỗi lớp tương đương gồm các tập hợp có cùng lực lượng. Chẳng hạn lớp tương đương của tập hợp $\mathbb{N}$ các số tự nhiên là lớp các tập hợp đếm được. Với tập hợp X có n phần tử thì lớp tương đương của X là lớp các tập hợp có n phần tử. Đặc biệt, lớp tương đương của tập hợp rỗng chỉ có một phần tử là tập hợp rỗng.

Định nghĩa 0.49. Một *phân hoạch* của tập hợp E là một họ $(A_i)_{i\in I}$ các tập con không rỗng của E có tính chất $A_i \cap A_j = \emptyset$ với mọi $i \neq j$, và $E = \cup_{i\in I} A_i$.

Rõ ràng rằng nếu $\sim$ là một quan hệ tương đương trên E thì họ các lớp tương đương khác nhau là một phân hoạch của E. Ngược lại, ta có

Mệnh đề 0.50. *Giả sử $(A_i)_{i\in I}$ là một phân hoạch của tập hợp E. Khi đó có một quan hệ tương đương trên E sao cho mỗi tập con A_i của E là một lớp tương đương.*

Chứng minh. Trên E ta định nghĩa quan hệ $x \sim y$ nếu có $i \in I$ sao cho $x, y \in A_i$. Khi đó $\sim$ là một quan hệ tương đương và mỗi $A_i, i \in I$ là một lớp tương đương. □

Ví dụ 0.51. Cho $E = \{a, b\}$. Khi đó họ gồm hai tập hợp $\{a\}, \{b\}$ là một phân hoạch của E và phân hoạch khác là chính E. Vậy chỉ có hai quan hệ tương đương trên E.

Chú ý rằng với một tập hợp E cho trước, mỗi quan hệ tương đương xác định một phân hoạch và ngược lại. Do đó có một song ánh giữa tập hợp các quan hệ tương đương và tập hợp các phân hoạch của E.

Bài tập

1. Trong mặt phẳng (P) cho trước điểm O. Ta xét quan hệ $M \sim M'$ nếu có một góc θ sao cho M' là ảnh của M bởi phép quay tâm O, góc quay θ. Chứng tỏ $\sim$ là một quan hệ tương đương. Xác định lớp tương đương của điểm M và tập hợp thương $(P)/\sim$.
2. Cho trước điểm O trong mặt phẳng (P), đặt $E = (P) \setminus \{O\}$. Trên E ta xét quan hệ $M \sim M'$ nếu O, M, M' thẳng hàng. Chứng tỏ $\sim$ là một quan hệ tương đương. Xác định lớp tương đương của điểm M và tập hợp thương $E/\sim$.
3. Đặt $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$. Trên tập hợp $\mathbb{Z} \times \mathbb{N}^*$ ta xét quan hệ

$$(p, q) \sim (p', q') \text{ nếu } pq' = p'q.$$

Chứng tỏ $\sim$ là một quan hệ tương đương. Xác định lớp tương đương của (p, q).

4. Có bao nhiêu quan hệ tương đương trên một tập hợp có ba phần tử?
5. Cho f là một toàn ánh từ tập hợp X đến tập hợp Y. Trên X ta xét quan hệ $x \sim y$ nếu $f(x) = f(y)$. Chứng tỏ $\sim$ là một quan hệ tương đương và tập hợp thương $X/\sim$ có cùng lực lượng với Y.

0.7 Quan hệ thứ tự

Quan hệ thứ tự trên một tập hợp giúp ta sắp xếp các phần tử của tập hợp đó theo một trật tự nhất định.

Định nghĩa 0.52. Một *quan hệ thứ tự* (ngắn gọn là thứ tự) trên tập hợp E không rỗng là một mối liên hệ $x \preceq y$ giữa các phần tử $x, y \in E$ thỏa mãn các điều kiện sau:

(a) $x \preceq x$ với mọi $x \in E$ (tính phản xạ).

(b) Nếu $x \preceq y$ và $y \preceq x$ thì $x = y$ (tính phản đối xứng).

(c) Nếu $x \preceq y$ và $y \preceq z$ thì $x \preceq z$ (tính bắc cầu).

Khi E có một thứ tự $\preceq$ ta nói E là tập hợp *được sắp*. Với $x, y \in E$ mà $x \preceq y$ hay $y \preceq x$ thì ta nói x, y so sánh được với nhau, trong trường hợp ngược lại ta nói x, y không so sánh được.

Một thứ tự trên E mà mọi cặp phần tử đều so sánh được với nhau được gọi là thứ tự *toàn phần*, ngược lại là thứ tự *bộ phận.* Ta nói tập hợp có một thứ tự toàn phần là tập hợp *được sắp thẳng*.

Nếu $x \preceq y$ ta còn viết $y \succeq x$. Ta ký hiệu $x \prec y$ (đọc là x nhỏ hơn y) hay $y \succ x$ (y lớn hơn x) nếu $x \preceq y$ và $x \neq y$.

Định nghĩa 0.53. Xét tập hợp E có thứ tự $\preceq$ và $A \subset E$.

(a) Phần tử $a \in A$ là *tối đại* trong A nếu với mọi $x \in A$ mà $a \preceq x$ thì $x = a$, tức là trong các phần tử của A mà so sánh được với a thì không có phần tử nào lớn hơn a.

(b) Phần tử $b \in A$ là *tối tiểu* trong A nếu với mọi $x \in A$ mà $x \preceq b$ thì $x = b$, tức là trong các phần tử của A mà so sánh được với b thì không có phần tử nào nhỏ hơn b.

(c) Phần tử $c \in A$ là *lớn nhất* trong A nếu $x \preceq c$ với mọi $x \in A$, tức là mọi phần tử của A đều so sánh được với c và không có phần tử nào lớn hơn c.

(d) Phần tử $d \in A$ là *nhỏ nhất* trong A nếu $d \preceq x$ với mọi $x \in A$, tức là mọi phần tử của A đều so sánh được với d và không có phần tử nào nhỏ hơn d.

Chú ý rằng phần tử lớn nhất (tương ứng nhỏ nhất) trong A nếu tồn tại thì duy nhất. Thật vậy, giả sử a, a' là hai phần tử lớn nhất (t.ư. nhỏ nhất) trong A, khi đó $a \preceq a'$ và $a' \preceq a$ nên $a = a'$.

Nếu phần tử lớn nhất (t.ư. nhỏ nhất) trong A tồn tại thì nó là phần tử tối đại (t.ư. tối tiểu) duy nhất. Tuy nhiên điều ngược lại không đúng, trong A có thể có nhiều phần tử tối đại, tối tiểu.

Định nghĩa 0.54. Xét tập hợp E có thứ tự $\preceq$ và $A \subset E$.

(a) Phần tử $a \in E$ là một *chặn trên* của A nếu $x \preceq a$ với mọi $x \in A$. Phần tử nhỏ nhất trong tập hợp các chặn trên của A, nếu có, được gọi là *supremum* của A và ký hiệu là $\sup A$.

(b) Phần tử $b \in E$ là một *chặn dưới* của A nếu $b \preceq x$ với mọi $x \in A$. Phần tử lớn nhất trong tập hợp các chặn dưới của A, nếu có, được gọi là *infimum* của A và ký hiệu là $\inf A$.

Nhận xét rằng nếu a là phần tử lớn nhất (t.ư. nhỏ nhất) trong A thì $a = \sup A$ (t.ư. $a = \inf A$).

Ví dụ 0.55. (a) Trên tập hợp $\mathbb{R}$ các số thực thì quan hệ $\leq$ thông thường là một thứ tự toàn phần. Với $A = [0,1)$ thì 0 là phần tử nhỏ nhất, trong A không có phần tử tối đại nên không có phần tử lớn nhất, $\inf A = 0$, $\sup A = 1$.

(b) Trên tập hợp $\mathbb{N}$ các số tự nhiên ta xét quan hệ chia hết "$|$", tức là với mỗi $a, b \in \mathbb{N}$ ta nói $a|b$ nếu có $k \in \mathbb{N}$ sao cho $b = ka$. Quan hệ chia hết có những tính chất sau:

Rõ ràng $a|a$ với mọi $a \in \mathbb{N}$.

Giả sử $a|b$ và $b|a$, khi đó có $k, l \in \mathbb{N}$ sao cho $b = ka$ và $a = lb$. Nếu $a = 0$ thì $b = 0$, suy ra $a = b$. Nếu $a \neq 0$, ta có $a = (lk)a$, suy ra $lk = 1$, do đó $l = k = 1$ và $a = b$.

Nếu $a|b$ và $b|c$ thì có $k, l \in \mathbb{N}$ sao cho $b = ka$ và $c = lb$. Khi đó $c = (lk)a$ và $a|c$.

Vậy quan hệ chia hết là một thứ tự trên $\mathbb{N}$. Vì 2 và 3 không chia hết cho nhau nên quan hệ chia hết là thứ tự bộ phận. Trong $\mathbb{N}$ ta có 1 chia hết mọi số tự nhiên nên 1 là phần tử nhỏ nhất; mọi số tự nhiên đều chia hết 0 nên 0 là phần tử lớn nhất. Với $A = \{1, 2, 3, 4, 5, 6\}$ thì trong A, 1 là phần tử tối tiểu và cũng là phần tử nhỏ nhất; $4, 5, 6$ là các phần tử tối đại nên không có phần tử lớn nhất; $\inf A = 1$; các chặn trên của A là các bội số của 60, do đó $\sup A = 60$.

Chú ý rằng quan hệ chia hết không là một thứ tự trên $\mathbb{Z}$ vì nó không có tính phản đối xứng.

Nếu trên $\mathbb{N}$ ta xét thứ tự $\leq$ thông thường thì phần tử nhỏ nhất là 0 và không có phần tử lớn nhất.

(c) Xét tập hợp E có hơn một phần tử. Trên tập hợp $\mathcal{P}(E)$ thì quan hệ chứa trong "$\subset$" là một thứ tự bộ phận. $\emptyset$ là phần tử nhỏ nhất, E là phần tử lớn nhất.

Nếu chỉ xét quan hệ chứa trong nói trên trên tập hợp $X = \mathcal{P}(E)\backslash\emptyset$ thì trong X không có phần tử nhỏ nhất, mỗi tập con của E chỉ có một phần tử là những phần tử tối tiểu.

(d) Giả sử tập hợp E được sắp thẳng bởi thứ tự $\leq_E$. Trên E^n ta định nghĩa quan hệ

$$(x_1, \ldots, x_n) \preceq (y_1, \ldots, y_n)$$

nếu $(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$ hoặc có một chỉ số i sao cho $x_1 = y_1, \ldots, x_{i-1} = y_{i-1}, x_i <_E y_i$. Khi đó quan hệ có những tính chất sau:

Với mọi $(x_1, \ldots, x_n) \in E^n$ ta có $(x_1, \ldots, x_n) \preceq (x_1, \ldots, x_n)$.

Giả sử $(x_1, \ldots, x_n) \preceq (y_1, \ldots, y_n)$ và $(y_1, \ldots, y_n) \preceq (x_1, \ldots, x_n)$. Nếu $(x_1, \ldots, x_n) \neq (y_1, \ldots, y_n)$ thì có chỉ số i sao cho $x_i \neq y_i$. Gọi j là chỉ số nhỏ nhất sao cho $x_j \neq y_j$, nếu $x_j <_E y_j$ thì mâu thuẫn với $(y_1, \ldots, y_n) \preceq (x_1, \ldots, x_n)$ hoặc ngược lại thì mâu thuẫn với $(x_1, \ldots, x_n) \preceq (y_1, \ldots, y_n)$. Vậy $(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$.

Giả sử $(x_1, \ldots, x_n) \preceq (y_1, \ldots, y_n)$ và $(y_1, \ldots, y_n) \preceq (z_1, \ldots, z_n)$. Nếu $(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$ hoặc $(y_1, \ldots, y_n) = (z_1, \ldots, z_n)$ thì ta có

$$(x, \ldots, x_n) \preceq (z_1, \ldots, z_n).$$

Trong trường hợp ngược lại, gọi j là chỉ số nhỏ nhất sao cho $x_j <_E y_j$ và k chỉ số nhỏ nhất sao cho $y_k <_E z_k$, nếu $k \leq j$ thì $x_1 = z_1, \ldots, x_{k-1} = z_{k-1}$, $x_k \leq_E y_k <_E z_k$ nên

$$(x_1, \ldots, x_n) \preceq (z_1, \ldots, z_n),$$

nếu $k > j$ thì $x_1 = z_1, \ldots, x_{j-1} = z_{j-1}, x_j <_E y_j = z_j$ nên

$$(x_1, \ldots, x_n) \preceq (z_1, \ldots, z_n).$$

Vậy $\preceq$ là một thứ tự trên E^n. Hơn nữa, nó là thứ tự toàn phần. Thứ tự này còn được gọi là thứ tự *từ điển*.

Định nghĩa 0.56. Một tập hợp E gọi là sắp *thứ tự tốt* nếu nó là tập hợp được sắp và mọi tập con khác rỗng của E đều có phần tử nhỏ nhất.

Ví dụ 0.57. Tập hợp $\mathbb{N}$ các số tự nhiên với thứ tự $\leq$ thông thường là tập hợp sắp thứ tự tốt.

Trong toán học, để chứng minh sự tồn tại một đối tượng (thường là bài toán khó) ta hay sử dụng bổ đề sau (Bổ đề Zorn).

Bổ đề 0.58. *Cho E là một tập hợp được sắp. Nếu mọi tập con không rỗng được sắp thẳng của E đều có chặn trên thì trong E có phần tử tối đại.*

Bây giờ ta sử dụng Bổ đề Zorn để chứng minh Định lý 0.26.

Chứng minh. Đặt $\mathcal{U}$ là tập hợp tất cả các bộ ba (A, B, f), trong đó A là tập con của X, B tập con của Y và $f : A \longrightarrow B$ là một song ánh. Vì X, Y không rỗng nên $\mathcal{U}$ không rỗng. Trên $\mathcal{U}$ ta xét quan hệ

$$(A, B, f) \preceq (A', B', f') \quad \text{nếu} \quad A \subset A', B \subset B' \text{ và } f'|_A = f.$$

Quan hệ trên là một thứ tự. Giả sử $\mathcal{V}= \{(A_i, B_i, f_i)|i \in I\}$ là một tập con tùy ý không rỗng của $\mathcal{U}$ được sắp thẳng. Đặt $\overline{A} = \cup_{i\in I} A_i$, $\overline{B} = \cup_{i\in I} B_i$ và $\overline{f} : \overline{A} \longrightarrow \overline{B}$ được định nghĩa: với mỗi $x \in A$ có $j \in I$ sao cho $x \in A_j$, ta đặt $\overline{f}(x) = f_j(x)$. Giả sử có $k \in I$ sao cho $x \in A_k$, bởi tính sắp thẳng của $\mathcal{V}$ ta có $A_j \subset A_k$ hoặc ngược lại và khi đó $f_j(x) = f_k(x)$. Do đó $\overline{f}$ được định nghĩa như trên hoàn toàn đúng đắn, nói cách khác $\overline{f}$ là một ánh xạ. Khi đó bộ ba $(\overline{A}, \overline{B}, \overline{f}) \in \mathcal{U}$ là một chặn trên của $\mathcal{V}$. Theo Bổ đề Zorn trong $\mathcal{U}$ có phần tử tối đại (C, D, g).

Nếu $C = X$ thì hợp thành của g và ánh xạ nhúng D vào Y là một đơn ánh từ X đến Y. Nếu $D = Y$ thì tương tự như trên ta có một đơn ánh từ Y đến X. Xét trường hợp $C \subsetneq X$ và $D \subsetneq Y$, khi đó có $c \in C_X(C)$ và $d \in C_Y(D)$. Ta đặt $C' = C \cup \{c\}$, $D' = D \cup \{d\}$ và $g' : C' \longrightarrow D'$ được xác định $g'(c) = d$, $g'(x) = g(x)$ với mọi $x \in C$ thì $(C, D, g) \prec (C', D', g')$. Điều này mâu thuẫn với tính tối đại của (C, D, g). Vậy định lý được chứng minh.

□

Chú ý rằng người ta chứng minh được "việc chứng minh Bổ đề Zorn tương đương với việc chứng minh tiên đề chọn".

Bài tập

1. Giả sử có một đơn ánh từ tập hợp X đến tập hợp $\mathbb{N}$ các số tự nhiên. Chứng tỏ có một thứ tự trên X sao cho X được sắp thẳng bởi thứ tự đó.
2. Giả sử E là một tập hợp không rỗng, đặt M là tập hợp các ánh xạ từ E đến $\{0, 1\}$. Trên M ta xét quan hệ

   $$f \preceq g \text{ nếu } \forall x \in E, f(x)g(x) = f(x).$$

   Chứng tỏ $\preceq$ là một thứ tự, nó có phải là thứ tự toàn phần không? Xác định các phần tử lớn nhất, nhỏ nhất.
3. Với hai tập hợp X, Y cho trước, đặt M là tập hợp các ánh xạ từ các tập con của X đến Y. Trên M ta xét quan hệ

   $$f \preceq g \text{ nếu } g \text{ là một mở rộng của } f.$$

Chứng tỏ $\preceq$ là một thứ tự, và nếu Y có hơn một phần tử thì thứ tự trên là bộ phận. Tìm các phần tử tối đại, tối tiểu, lớn nhất, nhỏ nhất.

4. Chứng minh rằng nếu một tập hợp sắp thứ tự tốt thì nó được sắp thẳng.

Chương 1

NHÓM

Từ mong muốn tìm hiểu những tính chất của số nguyên, từ việc tìm lời giải của những phương trình đại số cũng như việc nghiên cứu các phép biến đổi trên những đối tượng hình học, trong nhiều thế kỷ đã hình thành và phát triển khái niệm mà toán học hiện đại gọi là nhóm. Cấu trúc nhóm là một cấu trúc đại số đẹp và phong phú, nó là cơ sở cho nhiều lý thuyết hiện đại và có ứng dụng trong nhiều lĩnh vực khác nhau. Trong chương này chúng ta sẽ tìm hiểu về nó.

1.1 Phép toán hai ngôi

Định nghĩa 1.1. Một *phép toán hai ngôi* (ngắn gọn hơn là phép toán) trên tập hợp X là một ánh xạ $* : X \times X \longrightarrow X$, mỗi cặp $(x, y) \in X \times X$ tương ứng với một phần tử được ký hiệu $x * y \in X$.

Định nghĩa 1.2. Ta nói phép toán $*$ trên tập hợp X có *tính kết hợp* nếu

$$x * (y * z) = (x * y) * z$$

với mọi x, y, z thuộc X; có *tính giao hoán* nếu

$$x * y = y * x$$

với mọi x, y thuộc X.

Lưu ý rằng khi phép toán $*$ trên X có tính kết hợp ta sẽ viết $x*y*z$ với $x, y, z \in X$ mà không cần đến các dấu ngoặc.

Định nghĩa 1.3. Giả sử $*$ là một phép toán trên tập hợp X. Ta nói phần tử $e \in X$ là *trung lập* nếu

$$e * x = x * e = x$$

với mọi $x \in X$.

Ví dụ 1.4. (a) Phép cộng và phép nhân thông thường trên các tập hợp $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ và $\mathbb{C}$ là những phép toán có tính kết hợp, có tính giao hoán, phần tử trung lập của phép cộng là số 0 và của phép nhân là số 1.

(b) Cho trước số tự nhiên $n \geq 2$. Trên tập hợp $\mathbb{Z}_n$ các số nguyên mod n, phép cộng được định nghĩa như sau:

$$\overline{x} + \overline{y} = \overline{x+y}$$

với mọi $\overline{x}, \overline{y} \in \mathbb{Z}_n$. Ta chứng tỏ định nghĩa trên là đúng đắn, tức là nếu $\overline{x} = \overline{x'}, \overline{y} = \overline{y'}$ thì phải có

$$\overline{x+y} = \overline{x'+y'}.$$

Thật vậy, từ giả thiết $\overline{x} = \overline{x'}$, $\overline{y} = \overline{y'}$ suy ra có $h, k \in \mathbb{Z}$ sao cho $x = x' + hn$ và $y = y' + kn$. Cộng hai vế của hai phương trình trên ta có

$$x + y = x' + y' + (h+k)n.$$

Do đó $\overline{x+y} = \overline{x'+y'}$.

Phép nhân trên $\mathbb{Z}_n$ được định nghĩa

$$\overline{x} \cdot \overline{y} = \overline{xy}$$

với mọi $\overline{x}, \overline{y} \in \mathbb{Z}_n$. Tương tự như phép cộng, phép nhân được định nghĩa như trên là đúng đắn. Dễ thấy phép cộng và phép nhân có tính kết hợp, có tính giao hoán, với phép cộng phần tử trung lập là $\overline{0}$ và với phép nhân phần tử trung lập là $\overline{1}$.

(c) Phép cộng và phép nhân hai ma trận trên tập hợp $M_n(\mathbb{R})$ gồm các ma trận vuông cấp n hệ số thực là các phép toán. Phép cộng có tính kết hợp, có tính giao hoán, phần tử trung lập là ma trận không. Phép nhân có tính kết hợp, không có tính giao hoán nếu $n \geq 2$, phần tử trung lập là ma trận đơn vị.

(d) Đặt M_X là tập hợp các ánh xạ từ tập hợp X đến chính nó. Phép hợp thành hai ánh xạ là một phép toán trên M_X. Phép toán này có tính kết hợp, không có tính giao hoán nếu X có hơn một phần tử, phần tử trung lập là ánh xạ đồng nhất.

Định nghĩa 1.5. Giả sử $*$ là một phép toán trên tập hợp X. Ta nói phần tử $e \in X$ là trung lập *trái* nếu

$$e * x = x$$

với mọi $x \in X$; là trung lập *phải* nếu

$$x * e = x$$

với mọi $x \in X$.

Rõ ràng rằng nếu phần tử e là trung lập thì nó là trung lập trái và phải. Mệnh đề sau nói về quan hệ giữa các phần tử trung lập trái và phải.

Mệnh đề 1.6. *Giả sử $*$ là một phép toán trên tập hợp X. Nếu e là trung lập trái và e' là trung lập phải thì $e = e'$.*

Chứng minh. Ta có $e * e' = e$ vì e' là trung lập phải. Mặt khác, $e * e' = e'$ do e là trung lập trái. Vậy $e = e'$.

□

Hệ quả 1.7. *Trong một tập hợp với phép toán cho trước thì có nhiều nhất một phần tử trung lập.*

Chứng minh. Giả sử e, e' là hai phần tử trung lập của phép toán. Khi đó e là trung lập trái và e' là trung lập phải. Theo Mệnh đề 1.6 thì $e = e'$.

□

Định nghĩa 1.8. Giả sử $*$ là một phép toán trên tập hợp X với phần tử trung lập e và $x \in X$. Ta nói $x' \in X$ là một phần tử *đối xứng* của x nếu

$$x' * x = x * x' = e.$$

Nhận xét rằng vì $e * e = e$ nên phần tử đối xứng của e là chính nó.

Do tính đối xứng, nếu x' là phần tử đối xứng của x thì x cũng là phần tử đối xứng của x'.

Định nghĩa 1.9. Giả sử $*$ là một phép toán trên tập hợp X với phần tử trung lập e và $x \in X$. Ta nói $x' \in X$ là một phần tử đối xứng *trái* của x nếu

$$x' * x = e;$$

là một phần tử đối xứng *phải* của x nếu

$$x * x' = e.$$

Nhận xét rằng nếu x có phần tử đối xứng thì nó có phần tử đối xứng trái và phải. Nhưng điều ngược lại nói chung không đúng. Để thấy điều này ta xem ví dụ sau. Xét M_X như trong Ví dụ 1.4 với X có vô hạn phần tử. Lấy $f \in M_X$ và f là một đơn ánh nhưng không phải toàn ánh. Khi đó theo Mệnh đề 0.32 thì f có ánh xạ ngược bên trái nhưng không có ánh xạ ngược bên phải, tức là f có phần tử đối xứng trái nhưng không có phần tử đối xứng phải. Tương tự, nếu $g \in M_X$ và g là một toàn ánh nhưng không phải đơn ánh, cũng theo Mệnh đề 0.32 thì g có ánh xạ ngược bên phải nhưng không có ánh xạ ngược bên trái, tức là g có phần tử đối xứng phải nhưng không có phần tử đối xứng trái.

Định nghĩa 1.10. Giả sử X là một tập hợp với phép toán trên nó. Ta nói X là một *nửa nhóm* nếu phép toán có tính kết hợp ; là một *vị nhóm* nếu nó là một nửa nhóm có phần tử trung lập.

Mệnh đề 1.11. *Trong một vị nhóm, nếu phần tử x có phần tử đối xứng trái x' và phần tử đối xứng phải x'' thì $x' = x''$.*

Chứng minh. Giả sử vị nhóm với phép toán $*$ có phần tử trung lập e. Ta có

$$\begin{aligned} x' &= x' * e = x' * (x * x'') \\ &= (x' * x) * x'' \text{ (do tính kết hợp của phép toán)} \\ &= e * x'' = x''. \end{aligned}$$

Vậy mệnh đề được chứng minh.

□

Hệ quả 1.12. *Trong một vị nhóm, mỗi phần tử có nhiều nhất một phần tử đối xứng.*

Chứng minh. Xét vị nhóm X tùy ý. Nếu x', x'' là hai phần tử đối xứng của $x \in X$ thì x' là phần tử đối xứng trái, x'' phần tử đối xứng phải của x. Theo Mệnh đề 1.11 thì $x' = x''$.

□

Trong phần còn lại của chương này, nếu không nói gì thêm thì ta hiểu phép toán được ký hiệu theo lối nhân.

Bài tập

1. Với mỗi phép toán $*$ được cho trên $\mathbb{Q}$, hãy xác định phép toán nào có tính kết hợp, có tính giao hoán.
   (a) $x * y = x - y + xy$ (b) $x * y = \frac{x+y+xy}{2}$ (c) $x * y = \frac{x+y}{3}$.
2. Đặt X là tập hợp các số thực không âm.
   (a) Trên X ta xét phép toán $x * y = \sqrt{x^2 + y^2}$. Tìm phần tử trung lập và các phần tử có đối xứng.
   (b) Trên X ta xét phép toán $x * y = \max\{x, y\}$. Tìm phần tử trung lập và các phần tử có đối xứng.
3. Chứng tỏ $\mathbb{R}^2$ là một vị nhóm với phép toán $*$ trong các trường hợp sau.
   (a) $(x, y) * (u, v) = (xu - yv, xv + yu)$ với mọi $(x, y), (u, v) \in \mathbb{R}^2$.
   (b) $(x, y) * (u, v) = (xu, yu + v)$ với mọi $(x, y), (u, v) \in \mathbb{R}^2$.

1.2 Khái niệm về nhóm

Định nghĩa 1.13. Một tập hợp G với phép toán trên nó được gọi là một *nhóm* nếu thỏa mãn các điều kiện sau:

(a) Phép toán có tính kết hợp.

(b) Trong G có phần tử trung lập.

(c) Với mọi $x \in G$ thì x luôn có phần tử đối xứng.

Giả sử G là một nhóm. Ta nói G là một nhóm *giao hoán* hay một nhóm *Abel* nếu phép toán trên G có tính giao hoán; là một nhóm *hữu hạn* nếu G có hữu hạn phần tử. Khi đó ta ký hiệu $|G|$ để chỉ số phần tử của tập hợp G và gọi là *cấp* của nhóm G. Một nhóm không là nhóm hữu hạn thì gọi là nhóm vô hạn.

Lưu ý rằng phần tử trung lập còn gọi là đơn vị; phần tử đối xứng của x còn gọi là nghịch đảo của x và được ký hiệu x^{-1}. Nếu phép toán được viết theo lối cộng thì phần tử trung lập còn được gọi là phần tử không; phần tử đối xứng của x là đối của x và được ký hiệu $-x$.

Ví dụ 1.14. (a) Tập hợp $\mathbb{Z}$ các số nguyên với phép cộng thông thường là một nhóm Abel, phần tử không là số 0, và mỗi $x \in \mathbb{Z}$ thì đối của nó là $-x$. Tương tự, tập hợp $\mathbb{Q}$ các số hữu tỷ, $\mathbb{R}$ các số thực, $\mathbb{C}$ các số phức với phép cộng thông thường lần lượt là các nhóm Abel.

(b) Tập hợp $\mathbb{Q}$ các số hữu tỷ với phép nhân thông thường không phải một nhóm. Mặc dù phép nhân có tính kết hợp, trong $\mathbb{Q}$ có đơn vị là số 1, và mọi số hữu tỷ x khác không đều có nghịch đảo là $1/x$ nhưng vẫn còn số 0 không có nghịch đảo.

(c) Các tập hợp $\{\pm 1\}$, $\mathbb{Q}^* = \mathbb{Q}\setminus\{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ là các nhóm với phép toán nhân. Đây là các nhóm Abel.

(d) Tập hợp các căn bậc n ($n \geq 2$) của đơn vị trong tập hợp các số phức, cụ thể là tập hợp

$$\left\{1, a, a^2, \ldots, a^{n-1}\right\},$$

ở đây a=$\cos(2\pi/n) + i\sin(2\pi/n)$, với phép nhân hai số phức là một nhóm Abel.

(e) Cho trước số nguyên $n \geq 2$. Tập hợp $\mathbb{Z}_n = \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}$ với phép toán cộng là một nhóm Abel, phần tử không là $\overline{0}$, và với mỗi $\overline{x} \in \mathbb{Z}_n$ thì đối của nó là $\overline{n-x}$.

(f) Xét tập hợp $\mathbb{Z}_n$ ($n \geq 2$). Ta chứng tỏ $\overline{a} \in \mathbb{Z}_n$ là khả nghịch khi và chỉ khi a và n nguyên tố cùng nhau. Thật vậy, nếu $\overline{a}$ là khả nghịch thì có $\overline{b} \in \mathbb{Z}_n$ sao cho $\overline{ba} = \overline{b}\overline{a} = \overline{1}$, và do đó có số nguyên k để $ba + kn = 1$. Từ đây ta thấy mọi ước số chung của a và n đều là ước số của 1 nên a và n nguyên tố cùng nhau. Đảo lại, nếu a và n nguyên tố cùng nhau thì có hai số nguyên r và s sao cho $ra + sn = 1$. Khi đó $\overline{r} \cdot \overline{a} = \overline{ra} = \overline{ra + sn} = \overline{1}$ và vì thế $\overline{a}$ là khả nghịch.

Đặt $U(n)$ là tập hợp gồm các phần tử khả nghịch trong $\mathbb{Z}_n$. Nếu $\overline{x}, \overline{y} \in U(n)$ thì x, y nguyên tố cùng nhau với n nên tích xy cũng nguyên tố cùng nhau với n, và vì thế $\overline{x} \cdot \overline{y} = \overline{xy} \in U(n)$. $U(n)$ với phép nhân mod n là một nhóm Abel, đơn vị là $\overline{1}$. Cấp của $U(n)$ bằng $\varphi(n)$, trong đó φ là hàm Euler. Đặc biệt, khi $n = p$ là một số nguyên tố thì $U(p) = \mathbb{Z}_p \setminus \{\overline{0}\}$ là một nhóm có cấp $p - 1$.

(g) Đặt $M(n, R)$ là tập hợp các ma trận vuông cấp n hệ số trong R, ở đây R có thể là $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ hay $\mathbb{Z}_n$. Khi đó $M(n, R)$ với phép cộng hai ma trận là một nhóm Abel.

(h) Đặt S_n là tập hợp gồm các song ánh từ $\{1, 2, \ldots n\}$ đến chính nó. Vì hợp thành hai song ánh cũng là một song ánh nên phép hợp thành là một phép toán trên S_n. Phép toán này có tính kết hợp, phần tử trung lập là ánh xạ đồng nhất, và vì ánh xạ ngược của một song ánh cũng là một song ánh nên mọi phần tử trong S_n đều có đối xứng. Vậy S_n là một nhóm, tuy nhiên nhóm này không phải nhóm Abel khi $n \geq 3$.

Ta có mệnh đề sau là hiển nhiên.

Mệnh đề 1.15. *Trong một nhóm G thì*

(a) *Phần tử đơn vị là duy nhất.*

(b) *Với mỗi $x \in G$ thì nghịch đảo x^{-1} là duy nhất.*

(c) *Với bất kỳ $x \in G$ thì $(x^{-1})^{-1} = x$.*

(d) *Với bất kỳ $x, y \in G$ thì $(xy)^{-1} = y^{-1}x^{-1}$.*

Mệnh đề 1.16. *Trong một nhóm G ta có*

(a) *Phép giản ước có hiệu lực, tức là với mọi $x, y, z \in G$, nếu có $xy = xz$ hay $yx = zx$ thì ta luôn có $y = z$.*

(b) *Với mọi $a, b \in G$ cho trước thì phương trình $ax = b$ ($xa = b$) có nghiệm duy nhất $x = a^{-1}b$ ($x = ba^{-1}$).*

Chứng minh. (a) Giả sử $xy = xz$. Nhân bên trái hai vế của đẳng thức với x^{-1}, và bởi tính kết hợp của phép toán ta có $(x^{-1}x)y = (x^{-1}x)z$, suy ra $y = z$. Chứng minh tương tự đối với trường hợp còn lại.

(b) Xét phương trình $ax = b$. Ta thấy ngay $x_0 = a^{-1}b$ là một nghiệm của phương trình vì

$$ax_0 = a\left(a^{-1}b\right) = \left(aa^{-1}\right)b = eb = b.$$

Ta chứng minh đây là nghiệm duy nhất của phương trình. Giả sử x_1 là một nghiệm khác của phương trình. Khi đó $ax_1 = ax_0 = b$, giản ước hai vế cho a ta có $x_1 = x_0$. Vậy $x_0 = a^{-1}b$ là nghiệm duy nhất của phương trình $ax = b$. Chứng minh tương tự cho phương trình còn lại.

□

Ta nhận thấy một nhóm là một nửa nhóm, trong một nhóm thì phương trình bậc nhất luôn có nghiệm. Thật ra đây cũng là điều kiện đủ để một nửa nhóm không rỗng là một nhóm. Ta có mệnh đề sau.

Định lý 1.17. *Cho G là một nửa nhóm không rỗng. Nếu với mọi $a, b \in G$ cho trước, các phương trình $ax = b$ và $xa = b$ đều có nghiệm thì G là một nhóm.*

Chứng minh. Trước hết ta chứng tỏ trong G có đơn vị. Vì G không rỗng nên có phần tử $a \in G$. Xét phương trình $ax = a$, theo giả thiết phương trình có nghiệm e, tức là $ae = a$. Ta sẽ chứng tỏ với mọi $b \in G$ thì $be = b$. Thật vậy, bởi giả thiết phương trình $xa = b$ luôn có nghiệm nên nếu gọi d là một nghiệm của phương trình này thì $da = b$. Ta có

$$be = (da)\, e = d\,(ae) = da = b.$$

Do đó e là đơn vị phải. Tương tự, nếu e' là một nghiệm của phương trình $xa = a$ thì e' là đơn vị trái. Bởi Mệnh đề 1.6 thì $e = e'$ và do đó e là đơn vị.

Tiếp theo ta chứng tỏ mọi phần tử trong G đều có nghịch đảo. Với mọi $b \in G$ thì phương trình $bx = e$ và $xb = e$ luôn có nghiệm. Gọi b', b'' lần lượt là các nghiệm của hai phương trình trên, tức là

$$bb' = b''b = e.$$

Khi đó theo Mệnh đề 1.11 thì $b' = b''$ và như vậy b' chính là nghịch đảo của b. Vậy G là một nhóm.

□

Một chú ý về ký hiệu mà ta sẽ dùng: với số nguyên dương n cho trước ta viết a^n thay cho tích $aa \cdots a$ (n lần) và a^{-n} thay cho $a^{-1}a^{-1} \cdots a^{-1}$($n$ lần). Ta cũng quy ước $a^0 = e$. Khi phép toán ký hiệu theo lối cộng, ta viết na thay vì a^n với $n \in \mathbb{Z}$.

Bài tập

1. Trên tập hợp $G = \{1, 2, 3, 4, 6, 12\}$ ta xét phép toán $x * y = \gcd(x, y)$, ở đây $\gcd(x, y)$ là ước chung lớn nhất của x và y. Cặp $(G, *)$ có phải một nhóm không?
2. Trên tập hợp $\mathbb{Z}$ các số nguyên ta xét phép toán $x * y$ là $x + y$ nếu x chẵn, và $x - y$ nếu x lẻ. Cặp $(\mathbb{Z}, *)$ có phải một nhóm không?
3. Trên tập hợp $\mathbb{Q}$ các số hữu tỷ ta xét phép toán

$$x * y = x + y + xy.$$

   (a) Cặp $(\mathbb{Q}, *)$ có phải một nhóm không?
   (b) Chứng tỏ $\mathbb{Q} \setminus \{-1\}$ với $*$ là một nhóm.

4. Định nghĩa phép toán trên $G = \mathbb{Z} \times \mathbb{Z}$ bởi

$$(a, b) * (c, d) = (a + c, (-1)^c b + d).$$

Chứng tỏ G là một nhóm, nhưng không phải một nhóm Abel.

5. Đặt K là tập hợp gồm bốn ma trận hệ số thực

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Lập bảng nhân các phần tử của K, từ đây suy ra nó là một nhóm Abel. K được gọi là *4-nhóm Klein*.

6. Đặt $Q_8 = \{\pm a, \pm b, \pm c, \pm d\}$, ở đây

$$a = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ b = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \ c = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ d = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

là các ma trận hệ số phức. Lập bảng nhân các phần tử của Q_8, từ đây suy ra nó là một nhóm nhưng không phải nhóm Abel. Q_8 được gọi là nhóm *quaternion*.

7. Trong một nhóm Abel G, chứng tỏ với mọi $a, b \in G$ và $n \in \mathbb{Z}$ ta luôn có $(ab)^n = a^n b^n$.

8. Cho G là một nhóm. Chứng tỏ G là Abel nếu và chỉ nếu $(ab)^2 = a^2 b^2$ với mọi $a, b \in G$.

9. Trong nhóm S_3 tìm hai phần tử a, b sao cho $(ab)^2 \neq a^2 b^2$.

10. Cho G là nhóm nhân gồm các căn bậc n ($n \geq 2$) của đơn vị trong tập hợp các số phức. Nếu $x \in G$, hãy xác định x^{-1}.

11. Cho G là một nhóm. Chứng tỏ rằng nếu với mọi $a \in G$ mà $a^2 = e$ thì G là một nhóm Abel.

12. Giả sử G là một nhóm. Cho $a \in G$ và m, n là hai số nguyên nguyên tố cùng nhau. Chứng tỏ rằng nếu $a^n = e$ thì có $b \in G$ sao cho $a = b^m$.

13. Cho $G = \{a_1, a_2, \ldots, a_n\}$ là một nhóm Abel có tính chất với mọi $a \in G$, $a \neq e$ thì $a^2 \neq e$. Hãy xác định $a_1 a_2 \cdots a_n$.

14. Trên tập hợp $Z = (\mathbb{N} \times \mathbb{N})/\sim$ như trong Ví dụ 0.48, chứng tỏ phép cộng được định nghĩa $\overline{(a, b)} + \overline{(c, d)} = \overline{(a + c, b + d)}$ với mọi $\overline{(a, b)}, \overline{(c, d)} \in Z$ là đúng đắn và Z với phép toán trên là một nhóm Abel. Phép cộng trên Z gọi là phép cộng các số nguyên và nhóm cộng Z gọi là nhóm cộng các số nguyên.

15. Cho R có thể là $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ hay $\mathbb{Z}_p$ với p nguyên tố. Chứng tỏ tập hợp $GL(n, R)$ gồm các ma trận vuông cấp n, hệ số thuộc R, khả nghịch tạo thành một nhóm với phép nhân ma trận. Nhóm này được gọi là nhóm tuyến tính tổng quát. Hãy xác định cấp của $GL(n, \mathbb{Z}_p)$.

16. Cho E là một hình n-giác đều ($n \geq 3$). Ta nói ánh xạ $\sigma : E \to E$ là một đẳng cự nếu nó bảo toàn khoảng cách giữa hai điểm tùy ý trong E, tức là với $A, B \in E$ thì $d(\sigma(A), \sigma(B)) = d(A, B)$, trong đó $d(M, N)$ là khoảng cách thông thường giữa hai điểm M và N. Ký hiệu D_n là tập hợp gồm tất cả các đẳng cự của E.
(a) Chứng tỏ D_n là một nhóm với phép hợp thành các ánh xạ, D_n được gọi là nhóm *dihedral bậc n*.
(b) Gọi O là tâm của E và A một đỉnh của E. Đặt ρ là phép quay hình E quanh O theo chiều kim đồng hồ một góc $2\pi/n$ radian và τ phép đối xứng qua đường thẳng AO. Chứng tỏ

$$D_n = \left\{id_E, \rho, \rho^2, \ldots, \rho^{n-1}, \tau, \tau\rho, \tau\rho^2, \ldots, \tau\rho^{n-1}\right\}$$

gồm $2n$ phần tử.

1.3 Nhóm con

Định nghĩa 1.18. Xét nhóm G và $H \subset G$ *ổn định* đối với phép toán trên G, tức là với mọi $x, y \in H$ thì $xy \in H$. Ta nói H là một *nhóm con* của G nếu H là một nhóm với cùng phép toán trên G.

Ví dụ 1.19. (a) $\mathbb{Z}$ là một nhóm con của nhóm cộng $\mathbb{Q}$, $\mathbb{Q}$ là một nhóm con của nhóm cộng $\mathbb{R}$, $\mathbb{R}$ là một nhóm con của nhóm cộng $\mathbb{C}$.

(b) $\mathbb{Q}^*$ là một nhóm con của nhóm nhân $\mathbb{R}^*$, $\mathbb{R}^*$ là một nhóm con của nhóm nhân $\mathbb{C}^*$.

(c) Cho G là một nhóm với đơn vị e. Khi đó $\{e\}$ là một nhóm con của G và gọi là nhóm con *tầm thường* của G; G là một nhóm con của chính nó và gọi là nhóm con *không thật sự* của G. Các nhóm con khác, trừ hai nhóm con ở trên, gọi là các nhóm con thật sự không tầm thường của G.

Định lý 1.20. *Cho nhóm G và một tập con H không rỗng của G. Khi đó ba điều sau tương đương.*

(a) *H là một nhóm con của G.*
(b) *Với mọi $x, y \in H$ thì $xy \in H$ và $y^{-1} \in H$.*
(c) *Với mọi $x, y \in H$ thì $xy^{-1} \in H$.*

Chứng minh. (a)⇒(b) và (b)⇒(c) là hiển nhiên. Ta chứng minh (c) ⇒(a). Do H không rỗng nên có $a \in H$, theo (c) thì $e = aa^{-1} \in H$. Với mọi $y \in H$ ta có $y^{-1} = ey^{-1} \in H$. Vì $y^{-1} \in H$ nên với mọi $x \in H$ thì $xy = x(y^{-1})^{-1} \in H$. Với mọi $x, y, z \in H$ thì $x, y, z \in G$ nên ta có $(xy)z = x(yz)$. Vậy H là một nhóm và do đó là một nhóm con của G.

□

Ví dụ 1.21. (a) Với số nguyên $n \geq 0$ cho trước thì tập hợp $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ là một nhóm con của nhóm cộng $\mathbb{Z}$. Thật vậy, $n\mathbb{Z}$ không rỗng. Nếu $x, y \in n\mathbb{Z}$ thì có các số nguyên r, s sao cho $x = nr$ và $y = ns$, khi đó $x - y = n(r - s) \in n\mathbb{Z}$. Bởi Định lý 1.20, $n\mathbb{Z}$ là một nhóm con của $\mathbb{Z}$.

(b) Tập hợp H gồm các số nguyên lẻ không phải nhóm con của nhóm cộng $\mathbb{Z}$ vì $3, 5 \in H$ nhưng $3 + 5 \notin H$.

Ta nhận thấy rằng để tập hợp H là một nhóm con của nhóm G thì trước hết H phải ổn định đối với phép toán trên G. Đây chỉ là điều kiện cần, không là điều kiện đủ. Chẳng hạn $\mathbb{N}$ là một tập con của nhóm cộng $\mathbb{Z}$, ổn định đối với phép toán cộng nhưng không phải nhóm con vì phép lấy đối của phần tử trong $\mathbb{N}$ không thuộc $\mathbb{N}$. Tuy nhiên đối với tập hợp hữu hạn lại là điều kiện đủ như trong định lý dưới đây.

Định lý 1.22. *Cho G là một nhóm. Một tập con hữu hạn H không rỗng của G là một nhóm con của G khi và chỉ khi với mọi $x, y \in H$ thì $xy \in H$.*

Chứng minh. Xét phần tử tùy ý $x \in H$. Nếu $x = e$ thì $x^{-1} = e = x \in H$. Nếu $x \neq e$, ta xét các lũy thừa $x^1, x^2, x^3 \ldots$ các lũy thừa này thuộc H và không thể khác nhau vì H là một tập hợp hữu hạn. Do đó có i, j với $i < j$ sao cho $x^i = x^j$. Khi đó

$$x^{j-i} = x^j x^{-i} = x^j (x^i)^{-1} = e,$$

và vì thế $xx^{j-i-1} = e$, do đó $x^{-1} = x^{j-i-1} \in H$. Theo Định lý 1.20 thì H là một nhóm con của G.

□

Mệnh đề 1.23. *Giao của một họ tùy ý các nhóm con của một nhóm cũng là một nhóm con của nhóm đó.*

Chứng minh. Giả sử $(H_i)_{i \in I}$ là một họ các nhóm con của nhóm G. Đặt $H = \cap_{i \in I} H_i$. Ta thấy phần tử đơn vị $e \in H_i$ với mọi $i \in I$ nên $e \in H$ và do đó H không rỗng. Nếu $x, y \in H$ thì $x, y \in H_i$ với mọi $i \in I$, và vì H_i là nhóm con của G nên $xy^{-1} \in H_i$, do đó $xy^{-1} \in H$. Theo Định lý 1.20 thì H là một nhóm con của G.

□

Chú ý rằng hợp của hai nhóm con của một nhóm không hẳn là một nhóm con của nhóm đó. Để thấy điều đó ta xét ví dụ sau. Lấy $2\mathbb{Z}, 3\mathbb{Z}$ lần lượt là các tập hợp gồm các bội số của 2, bội số của 3, đây là hai nhóm con của nhóm cộng $\mathbb{Z}$. Ta có $2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ nhưng $2 + 3 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$. Vậy $2\mathbb{Z} \cup 3\mathbb{Z}$ không phải nhóm con của nhóm cộng $\mathbb{Z}$.

Bây giờ giả sử S là một tập con của nhóm G, thế thì S được chứa trong ít nhất một nhóm con của G, chẳng hạn đó là nhóm G. Xét họ các nhóm con của G chứa S và gọi $\langle S \rangle$ là giao của tất cả các nhóm con trong họ đó

$$\langle S\rangle = \cap_{H \text{ là nhóm con của } G \text{chứa } S} H.$$

Theo Mệnh đề 1.23 thì $\langle S\rangle$ là một nhóm con của G và là nhóm con nhỏ nhất của G chứa S. Ta gọi $\langle S\rangle$ là nhóm con của G *được sinh ra bởi* S. Đặc biệt, nếu $G = \langle S\rangle$ thì ta nói G được sinh ra bởi S hay S là một *tập sinh* của G.

Chú ý rằng $\langle\emptyset\rangle = \{e\}$ và $\langle S\rangle = S$ nếu S là một nhóm con của G.

Mệnh đề sau mô tả cụ thể các phần tử của nhóm $\langle S\rangle$.

Mệnh đề 1.24. *Cho S là một tập con không rỗng của nhóm G. Khi đó với x tùy ý thuộc $\langle S\rangle$ thì có số nguyên $n > 0$ và $s_1, s_2, \ldots, s_n \in S \cup S^{-1}$ sao cho $x = s_1 s_2 \cdots s_n$, ở đây $S^{-1} = \{s^{-1} \mid s \in S\}$.*

Chứng minh. Đặt

$$H = \left\{s_1 s_2 \cdots s_n \mid n \in \mathbb{N}, n > 0, s_1, s_2, \ldots, s_n \in S \cup S^{-1}\right\}.$$

Với mọi $s \in S$ ta luôn có $s \in H$, do đó $S \subset H$. Nếu $x, y \in H$ thì có $s_1, s_2, \ldots, s_n, t_1, t_2, \ldots, t_m \in S \cup S^{-1}$ sao cho $x = s_1 s_2 \cdots s_n$, $y = t_1 t_2 \cdots t_m$. Khi đó $xy^{-1} = s_1 s_2 \cdots s_n t_m^{-1} \cdots t_2^{-1} t_1^{-1} \in H$. Vậy H là một nhóm con của G chứa S nên $\langle S\rangle \subset H$. Mặt khác, $S \subset \langle S\rangle$ nên $S^{-1} \subset \langle S\rangle$. Vì phần tử trong H là tích hữu hạn các phần tử trong $S \cup S^{-1}$ nên cũng là phần tử trong nhóm con $\langle S\rangle$ và do đó $H \subset \langle S\rangle$. Vậy $\langle S\rangle = H$ và ta có điều phải chứng minh.

□

Ta xét trường hợp đặc biệt khi S chỉ có một phần tử a. Khi đó nếu x là một phần tử tùy ý trong $\langle a\rangle$ thì $x = s_1 s_2 \cdots s_n$ với $s_i \in \{a, a^{-1}\}$ hay $x = a^m$, trong đó m là số nguyên nào đó trong $\mathbb{Z}$. Từ đây ta có định nghĩa.

Định nghĩa 1.25. Cho a là một phần tử của nhóm G. Ta nói nhóm con được sinh ra bởi a là

$$\langle a\rangle = \{a^m \mid m \in \mathbb{Z}\}$$

(nếu phép toán viết theo lối cộng, $\langle a\rangle = \{ma \mid m \in \mathbb{Z}\}$), và gọi là nhóm con *cyclic* của G.

Ví dụ 1.26. (a) Cho $n \in \mathbb{N}$, nhóm con của nhóm cộng $\mathbb{Z}$ được sinh ra bởi n là $\langle n\rangle = n\mathbb{Z}$.

(b) Nhóm con của nhóm nhân $\mathbb{C}^*$ được sinh ra bởi i là

$$\langle i\rangle = \{i^m \mid m \in \mathbb{Z}\} = \{1, -1, i, -i\}.$$

(c) Xét nhóm S_3. S_3 có sáu phần tử, nếu $\sigma \in S_3$ biểu diễn ở dạng $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ \sigma(1) & \sigma(2) & \sigma(3) \end{pmatrix}$ thì sáu phần tử đó là:

$$e = \begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix}, \rho = \begin{pmatrix} 1\,2\,3 \\ 3\,1\,2 \end{pmatrix}, \rho^2 = \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix},$$

$$\rho_1 = \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix}, \rho_2 = \begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix}, \rho_3 = \begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix}.$$

Ta tìm nhóm con được sinh ra bởi ρ. Ta có $\rho^3 = \begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix} = e$. Với m là số nguyên tùy ý, chia m cho 3 ta được $m = 3q + r$ với $0 \leq r < 3$. Khi đó

$$\rho^m = \rho^{3q+r} = (\rho^3)^q \rho^r = e^q \rho^r = \rho^r$$

là một trong ba phần tử e, ρ, ρ^2. Vậy $\langle \rho \rangle = \{e, \rho, \rho^2\}$.

Mệnh đề 1.27. *Giả sử G là một nhóm. Đặt*

$$Z(G) = \{x \in G \mid xa = ax \text{ với mọi } a \in G\}.$$

Khi đó $Z(G)$ là một nhóm con giao hoán của G. $Z(G)$ được gọi là tâm của G.

Chứng minh. Ta có $ea = e = ae$ với mọi $a \in G$, vì thế $e \in Z(G)$ và $Z(G)$ không rỗng. Cho $x, y \in Z(G)$, bởi định nghĩa ta có $xa = ax$ và $ya = ay$ với mọi $a \in G$. Khi đó

$$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy),$$

suy ra $xy \in Z(G)$. Ta cũng có

$$y^{-1}a = y^{-1}(a^{-1})^{-1} = (a^{-1}y)^{-1} = (ya^{-1})^{-1} = (a^{-1})^{-1}y^{-1} = ay^{-1},$$

suy ra $y^{-1} \in Z(G)$. Hơn nữa, phép toán trên $Z(G)$ luôn giao hoán. Vậy $Z(G)$ là một nhóm con giao hoán của G.

□

Chú ý rằng nếu G là một nhóm Abel thì $Z(G) = G$.

Ví dụ 1.28. Tìm tâm của nhóm S_3. Ta có

$$\rho_i \circ \rho = \rho^2 \circ \rho_i$$

với $i = 1, 2, 3$, suy ra trong S_3 không có phần tử nào giao hoán với mọi phần tử khác ngoại trừ e nên $Z(S_3) = \{e\}$.

Bài tập

1. Đặt $G = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$. Chứng tỏ G là một nhóm con của nhóm cộng $\mathbb{R}$.
2. Đặt $G = \{m + ni \mid m, n \in \mathbb{Z},\ i^2 = -1\}$. Chứng tỏ G là một nhóm con của nhóm cộng $\mathbb{C}$.
3. Đặt $G = \{\cos(2k\pi/11) + i\sin(2k\pi/11) \mid k \in \mathbb{Z}\}$. Chứng tỏ G là một nhóm con của nhóm nhân $\mathbb{C}^*$. Tìm cấp của G.
4. Đặt
$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}.$$
Chứng tỏ G là một nhóm con của nhóm tuyến tính tổng quát $GL(3, \mathbb{R})$.
5. Trong mỗi nhóm sau, hãy tìm ít nhất hai nhóm con thật sự không tầm thường.
(a) $\mathbb{Z}$ (b) $\mathbb{R}$ (c) $\mathbb{C}^*$ (d) $16\mathbb{Z}$ (e) $\mathbb{Z}_{27}$ (f) Q_8 (g) $GL(2, \mathbb{R})$
6. Cho G là nhóm con của nhóm tuyến tính tổng quát $GL(2, \mathbb{R})$ được sinh ra bởi hai ma trận $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ và $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Chứng tỏ G là một nhóm không giao hoán có cấp 8.
7. Tìm một nhóm con của S_5 có cấp 3.
8. Tìm một nhóm con của S_7 có cấp 10.
9. Tìm tâm của D_4.
10. Cho G là một nhóm và $a \in G$. Tâm hóa của a trong G, được ký hiệu $C_G(a)$, là tập hợp gồm các phần tử trong G giao hoán với a.
(a) Chứng tỏ $C_G(a)$ là một nhóm con của G.
(b) Chứng tỏ $C_G(a) = G$ khi và chỉ khi $a \in Z(G)$.
11. Tìm tâm hóa $C_{S_3}(\rho)$ trong S_3.
12. Giả sử H và K là hai nhóm con của nhóm G, ta đặt
$$HK = \{hk/h \in H, k \in K\}.$$
Chứng tỏ HK là một nhóm con của G khi và chỉ khi $HK = KH$.
13. Chứng minh rằng mọi nhóm có cấp vô hạn đều có vô hạn nhóm con.

1.4 Nhóm cyclic

Trong mục này ta sẽ nghiên cứu những nhóm được sinh ra bởi một phần tử mà ta gọi là nhóm cyclic.

Định nghĩa 1.29. Cho nhóm G, nếu có phần tử $a \in G$ sao cho

$$G = \langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$$

thì ta nói G là nhóm *cyclic* được sinh ra bởi a hay a là một *phần tử sinh* của G.

Khi phép toán viết theo lối cộng thì nhóm cyclic được sinh ra bởi phần tử a là $G = \langle a \rangle = \{ma \mid m \in \mathbb{Z}\}$.

Ví dụ 1.30. (a) Nhóm cộng $\mathbb{Z}$ là cyclic vì $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. Nhóm cộng $2\mathbb{Z}$ là cyclic được sinh ra bởi 2. Tổng quát với số tự nhiên $n \geq 1$, nhóm cộng $n\mathbb{Z}$ được sinh ra bởi n. Đây là những nhóm cyclic vô hạn.

(b) Nhóm cộng $\mathbb{Z}_{10} = \langle \overline{1} \rangle = \langle \overline{3} \rangle = \langle \overline{7} \rangle = \langle \overline{9} \rangle$. $\overline{1}$,$\overline{3}, \overline{7}, \overline{9}$ là các phần tử sinh của nhóm $\mathbb{Z}_{10}$. Ta kiểm tra điều này cho phần tử $\overline{3}$ bằng cách cộng liên tiếp các phần tử $\overline{3}$. Ta có $2\overline{3} = \overline{3} + \overline{3} = \overline{6}$, $3\overline{3} = \overline{3} + \overline{3} + \overline{3} = \overline{9}$, $4\overline{3} = \overline{3} + \overline{3} + \overline{3} + \overline{3} = \overline{12} = \overline{2}$. Tương tự, $5\overline{3} = \overline{5}$, $6\overline{3} = \overline{8}$, $7\overline{3} = \overline{1}$, $8\overline{3} = \overline{4}$, $9\overline{3} = \overline{7}$, $10\overline{3} = \overline{0}$.

(c) Nhóm nhân $G = \{1. - 1, i, -i\} = \{i^0, i^1, i^2, i^3\} = \langle i \rangle$. Vậy G là cyclic được sinh ra bởi i.

(d) Xét nhóm $\mathbb{S}_3$. Như trong Ví dụ 1.26 ta có $\langle \rho \rangle = \{e, \rho, \rho^2\}$. Tương tự, ta cũng có $\langle \rho^2 \rangle = \{e, \rho, \rho^2\}$, $\langle \rho_i \rangle = \{e, \rho_i\}$ với $i = 1, 2, 3$. Vì không có phần tử nào trong S_3 sinh ra toàn nhóm S_3 nên S_3 không phải nhóm cyclic.

Định nghĩa 1.31. Xét phần tử a thuộc nhóm G.

(a) Nếu có $m \in \mathbb{N} \setminus \{0\}$ sao cho $a^m = e$ thì ta nói a có *cấp hữu hạn.* Ký hiệu $|a|$ là số nguyên dương nhỏ nhất sao cho $a^{|a|} = e$, $|a|$ được gọi là *cấp* của a.

(b) Ngược lại, tức là với mọi $m \in \mathbb{N} \setminus \{0\}$ thì $a^m \neq e$, khi đó ta nói a có *cấp vô hạn* và viết $|a|{=}\infty$.

Chú ý rằng phần tử đơn vị của một nhóm luôn có cấp bằng 1.

Ví dụ 1.32. (a) Xét nhóm cộng $\mathbb{Z}$. Phần tử 0 có cấp 1; a có cấp ∞ với mọi $a \in \mathbb{Z}$, $a \neq 0$.

(b) Trong nhóm cộng $\mathbb{Z}_6$ các phần tử $\overline{1}, \overline{5}$ có cấp 6; $\overline{2}, \overline{4}$ có cấp 3; $\overline{3}$ có cấp 2.

(c) Trong nhóm nhân $\mathbb{C}^*$ phần tử i có cấp 4; 2 có cấp vô hạn.

(d) Trong nhóm S_3 các phần tử ρ, ρ^2 có cấp 3; ρ_1, ρ_2, ρ_3 có cấp 2.

Mệnh đề 1.33. *Cho nhóm G và $a \in G$. Khi đó với mọi $i, j \in \mathbb{Z}$ ta có:*

(a) *Nếu a có cấp vô hạn, thì $a^i = a^j$ khi và chỉ khi $i = j$.*

(b) *Nếu a có cấp hữu hạn $|a| = n$, thì $a^i = a^j$ khi và chỉ khi $i - j$ chia hết cho n.*

Chứng minh. (a) Giả sử $|a| = \infty$. Nếu $a^i = a^j$ $(i \geq j)$ thì $a^{i-j} = a^i a^{-j} = e$. Do đó $i - j = 0$ và $i = j$. Đảo lại là hiển nhiên.

(b) Giả sử $|a| = n$. Nếu $a^i = a^j$ thì $a^{i-j} = a^i a^{-j} = e$. Chia $i - j$ cho n ta được $i - j = qn + r$ với $0 \leq r < n$. Khi đó

$$e = a^{i-j} = a^{qn+r} = a^{nq}a^r = (a^n)^q a^r = e^q a^r = ea^r = a^r.$$

Vì $0 \leq r < n$ và n là số nguyên dương nhỏ nhất sao cho $a^n = e$ nên $r = 0$, suy ra $i - j = qn$ và $i - j$ chia hết cho n. Đảo lại, nếu $i - j$ chia hết cho n thì có $k \in \mathbb{Z}$ sao cho $i = nk + j$. Khi đó ta có

$$a^i = a^{nk+j} = a^{nk}a^j = (a^n)^k a^j = e^k a^j = ea^j = a^j.$$

Vậy mệnh đề được chứng minh.

□

Hệ quả 1.34. *Cho nhóm G và $a \in G$ với $|a| = n$. Khi đó với bất kỳ $k \in \mathbb{Z}$, $a^k = e$ nếu và chỉ nếu k chia hết cho n.*

Chứng minh. Giả sử k là số nguyên sao cho $a^k = e$. Vì $a^k = e = a^0$ nên theo (b) của Mệnh đề 1.33 thì $k = k - 0$ chia hết cho n. Đảo lại, nếu $k = nq$ thì $a^k = (a^n)^q = e^q = e$.

□

Hệ quả 1.35. *Cho nhóm G và $a \in G$ với $|a| = n$. Khi đó*

$$\langle a \rangle = \left\{e, a, a^2, \ldots, a^{n-1}\right\}$$

và c*ấp của $\langle a \rangle$ bằng n.*

Chứng minh. Theo Mệnh đề 1.33 thì các phần tử $e, a, a^2, \ldots, a^{n-1}$ đôi một khác nhau. Cho x là phần tử tùy ý trong $\langle a \rangle$, khi đó có số nguyên m sao cho $x = a^m$. Chia m cho n ta được $m = qn + r$ với $0 \leq r < n$. Ta có

$$x = a^m = a^{qn+r} = (a^n)^q a^r = ea^r = a^r,$$

do đó x là một trong các phần tử $e, a, a^2, \ldots, a^{n-1}$ và hệ quả được chứng minh.

□

Ví dụ 1.36. Cho G là một nhóm cyclic có cấp 6 được sinh ra bởi a,

$$G = \langle a \rangle = \left\{e,\, a,\, a^2,\, a^3,\, a^4,\, a^5\right\}.$$

Ta tìm $|a^4|$. Ta có $(a^4)^2 = a^8 = a^{6+2} = a^6a^2 = ea^2 = a^2 \neq e$, trong khi $(a^4)^3 = a^{12} = a^{6\cdot 2} = (a^6)^2 = e^2 = e$. Do đó $|a^4| = 3$.

Mệnh đề sau cho ta công thức tìm cấp của phần tử trong một nhóm cyclic dễ dàng hơn.

Mệnh đề 1.37. *Cho $G = \langle a \rangle$ là một nhóm cyclic có cấp n. Khi đó với phần tử bất kỳ $a^s \in G$ ta có $|a^s| = n/\gcd(n, s)$, ở đây $\gcd(n, s)$ là ước số chung lớn nhất của n và s.*

Chứng minh. Bởi Hệ quả 1.34, $(a^s)^k = a^{sk} = e$ khi và chỉ khi sk là bội số của n. Theo định nghĩa của cấp thì $|a^s|$ là số k nguyên dương nhỏ nhất sao cho $(a^s)^k = e$, từ đây suy ra $|a^s|$ là số k nhỏ nhất sao cho sk là bội số của s và cũng là bội số của n. Điều này có nghĩa sk là bội chung nhỏ nhất của s và k, ta ký hiệu $sk = \text{lcm}(n, s)$ và khi đó $k = \text{lcm}(n, s)/s$. Vì $\text{lcm}(b, c) = bc/\text{gcd}(b, c)$ nên ta có $k = sn/s\text{gcd}(n, s) = n/\text{gcd}(n, s)$.

□

Hệ quả 1.38. *Cho $G = \langle a \rangle$ là một nhóm cyclic có cấp n. Khi đó với phần tử bất kỳ $a^s \in G$, ta có a^s là phần tử sinh của G khi và chỉ khi* $\text{gcd}(n, s) = 1$.

Chứng minh. Theo định nghĩa, a^s là phần tử sinh của G khi và chỉ khi $G = \langle a^s \rangle$, và do đó khi và chỉ khi $|\langle a^s \rangle| = n$. Theo Hệ quả 1.35 thì $|\langle a^s \rangle| = |a^s|$, và theo Mệnh đề 1.37 thì $|a^s| = n/\text{gcd}(n, s)$. Vì vậy a^s là phần tử sinh của G khi và chỉ khi $n/\text{gcd}(n, s) = n$, tức là $\text{gcd}(n, s) = 1$.

□

Hệ quả 1.39. *Cho $G = \langle a \rangle$ là một nhóm cyclic có cấp n. Khi đó số phần tử sinh của G là $\varphi(n)$, ở đây φ là hàm Euler.*

Chứng minh. Theo Hệ quả 1.38, a^s là phần tử sinh của G nếu và chỉ nếu $\text{gcd}(n, s) = 1$. Số các số nguyên s sao cho $1 \leq s < n$ và $\text{gcd}(n, s) = 1$ chính là $\varphi(n)$. Vậy hệ quả được chứng minh.

□

Định lý 1.40. *Mọi nhóm con của một nhóm cyclic là cyclic.*

Chứng minh. Cho $G = \langle a \rangle$ là một nhóm cyclic và H một nhóm con của G. Nếu $H = \{e\}$ thì H là cyclic được sinh ra bởi e. Giả sử $H \neq \{e\}$, khi đó có phần tử $b \in H$ với $b \neq e$. Vì $b \in G$ nên có $s \in \mathbb{Z}$, $s \neq 0$ sao cho $b = a^s$. Khi đó $a^{-s} = (a^s)^{-1} = b^{-1} \in H$. Suy ra trong H chứa phần tử a^t với $t \in \mathbb{Z}$, $t > 0$. Gọi m là số nguyên dương nhỏ nhất sao cho $a^m \in H$. Với phần tử bất kỳ $y \in H$ thì $y = a^k$ với số nguyên k nào đó. Chia k cho m ta được $k = qm + r$, $0 \leq r < m$. Khi đó

$$y = a^k = a^{qm+r} = a^{mq}a^r = (a^m)^q a^r$$

và $a^r = (a^m)^{-q} y$. Vì $a^m, y \in H$ suy ra $a^r \in H$. Nhưng vì $0 \leq r < m$ và m là số nguyên dương nhỏ nhất sao cho $a^m \in H$ ta suy ra $r = 0$ và $y = (a^m)^q$. Vậy mỗi phần tử của H là một lũy thừa của a^m và do đó H là một nhóm cyclic được sinh ra bởi a^m.

□

Ví dụ 1.41. Xác định các nhóm con của nhóm cộng $\mathbb{Z}$. Cho H là một nhóm con của $\mathbb{Z}$, nếu $H = \{0\}$ là nhóm con tầm thường thì $H = 0\mathbb{Z}$. Nếu $H \neq \{0\}$, vì $\mathbb{Z}$ là một

nhóm cyclic được sinh ra bởi 1, như trong chứng minh của Định lý 1.40 thì H là một nhóm cyclic được sinh ra bởi phần tử $m = m1 \in H$ với m là số nguyên dương nhỏ nhất thuộc H và $H = m\mathbb{Z}$.

Định lý 1.42. *Cho $G = \langle a \rangle$ là một nhóm cyclic có cấp n. Khi đó*

(a) *Cấp $|H|$ của nhóm con H của G là một ước của n.*

(b) *Với mỗi số nguyên dương d là ước của n thì có duy nhất một nhóm con của G có cấp d, đó là nhóm con $H = \left\langle a^{n/d} \right\rangle$.*

Chứng minh. (a) Giả sử H là một nhóm con của nhóm $G = \langle a \rangle$. Theo Định lý 1.40 thì H là một nhóm cyclic được sinh ra bởi phần tử a^m với số nguyên m không âm nào đó, và bởi Mệnh đề 1.33 $|H| = |a^m| = n/\gcd(n, m)$ là một ước số của n.

(b) Với $d = 1$ thì có duy nhất nhóm con tầm thường $\{e\} = \langle e \rangle$. Lấy d là một ước của n và $d > 1$. Khi đó theo Mệnh đề 1.33 ta có $\left|a^{n/d}\right| = n/\gcd(n, n/d) = d$. Do đó $\left\langle a^{n/d} \right\rangle$ là một nhóm con của G có cấp d. Định lý sẽ được chứng minh nếu ta chứng tỏ đây là nhóm con duy nhất của G có cấp d. Giả sử H là một nhóm con của G có cấp d. Như trong chứng minh Định lý 1.40 ta có $H = \langle a^s \rangle$ với s là số nguyên dương nhỏ nhất sao cho $a^s \in H$. Như đã biết có các số nguyên u, v sao cho $\gcd(n, s) = un + vs$ và

$$a^{\gcd(n,s)} = a^{un+vs} = (a^n)^u (a^s)^v = e(a^s)^v \in H.$$

Vì $1 \leq \gcd(n, s) \leq s$ và s là số nguyên dương nhỏ nhất sao cho $a^s \in H$, do đó ta phải có $\gcd(n, s) = s$. Khi đó theo Mệnh đề 1.33 thì $d = |H| = |a^s| = n/\gcd(n, s) = n/s$. Vì vậy $s = n/d$ và $H = \langle a^s \rangle = \left\langle a^{n/d} \right\rangle$ và định lý được chứng minh.

□

Ví dụ 1.43. Xác định các nhóm con của nhóm cộng $\mathbb{Z}_{10}$. Ta biết $\mathbb{Z}_{10}$ là một nhóm cyclic được sinh ra bởi $\overline{1}$. Theo Định lý 1.42 thì các nhóm con của $\mathbb{Z}_{10}$ có cấp là các ước số của 10, do đó $\mathbb{Z}_{10}$ có đúng bốn nhóm con có số phần tử lần lượt là 1, 10, 2, 5 gồm: nhóm con tầm thường $\left\{\overline{0}\right\}$, nhóm con không thật sự $\mathbb{Z}_{10}$, hai nhóm con thật sự không tầm thường đó là nhóm con được sinh ra bởi $\overline{5}$ có cấp 2, $\left\langle \overline{5} \right\rangle = \left\{\overline{0}, \overline{5}\right\}$ và nhóm con được sinh ra bởi $\overline{2}$ có cấp 5, $\left\langle \overline{2} \right\rangle = \left\{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\right\}$.

Bài tập

1. Trong nhóm nhân $\mathbb{C}^*$, hãy xác định cấp của những phần tử sau:
   (a) $\left(1 - \sqrt{3}i\right)/2$ (b) $-1 + \sqrt{3}i$ (c) $\cos(2\pi/9) + i\sin(2\pi/9)$

2. Tìm cấp của các phần tử $\overline{45}, \overline{70}, \overline{77} \in \mathbb{Z}_{210}$.

3. Cho $\theta \in \mathbb{R}$, đặt $X(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \in GL(2,\mathbb{R})$.
   (a) Chứng tỏ $H = \{X(\theta) \mid \theta \in \mathbb{R}\}$ là một nhóm con của nhóm tuyến tính tổng quát $GL(2,\mathbb{R})$.
   (b) Tìm cấp của $X(2\pi/3)$ và nghịch đảo của nó.

4. Tìm tất cả các phần tử sinh của các nhóm $\mathbb{Z}_{15}$, $\mathbb{Z}_{20}$.
5. Cho $G = \langle a \rangle$ là một nhóm cyclic có cấp 30. Hãy tìm tất cả phần tử sinh của G.
6. Cho G là một nhóm cylic có cấp 20. Tìm các phần tử trong G có cấp 10.
7. Cho G là một nhóm và $a, b \in G$. Chứng tỏ
   (a) a và a^{-1} có cùng cấp.
   (b) $b^{-1}ab$ và a có cùng cấp.
   (c) ab và ba có cùng cấp.

8. Cho G là một nhóm và $a, b \in G$ sao cho $ab = ba$. Chứng tỏ rằng nếu a có cấp m, b có cấp n và m, n nguyên tố cùng nhau thì ab có cấp mn.
9. Cho G là một nhóm Abel. Chứng tỏ tập hợp gồm các phần tử của G có cấp hữu hạn là một nhóm con của G.
10. Cho G là một nhóm hữu hạn có cấp chẵn. Chứng tỏ trong G có phần tử có cấp hai.
11. Cho G là một nhóm Abel và H, K hai nhóm con cyclic của G, trong đó H có cấp 10 và K có cấp 14. Chứng tỏ G chứa một nhóm con cyclic có cấp 70.
12. Chứng minh rằng nhóm G không có nhóm con thật sự không tầm thường là một nhóm cyclic. Khi đó có thể nói gì về cấp của G.
13. Cho m, n là các số nguyên. Đặt

$$m\mathbb{Z} + n\mathbb{Z} = \{a + b \mid a \in m\mathbb{Z},\ b \in n\mathbb{Z}\}.$$

   (a) Chứng tỏ $m\mathbb{Z} + n\mathbb{Z}$ là một nhóm con của $\mathbb{Z}$.
   (b) Tìm một phần tử sinh của $12\mathbb{Z} + 15\mathbb{Z}$.
   (c) Tìm một phần tử sinh của $m\mathbb{Z} + n\mathbb{Z}$.

14. Tìm một phần tử sinh của nhóm con $6\mathbb{Z} \cap 15\mathbb{Z}$ của $\mathbb{Z}$.
15. Cho m, n là các số nguyên. Tìm một phần tử sinh của nhóm con $m\mathbb{Z} \cap n\mathbb{Z}$ của $\mathbb{Z}$.
16. Các nhóm sau nhóm nào là cyclic: $U(20)$, $U(22)$, $U(24)$.
17. Cho G là một nhóm và a, b hai phần tử của G có cấp lần lượt là 14, 15. Hãy mô tả nhóm con $\langle a \rangle \cap \langle b \rangle$.
18. Cho $G = \langle a \rangle$ là một nhóm cyclic có cấp 45 và H, K hai nhóm con thật sự không tầm thường của G sao cho H là một nhóm con của K, và $a^9 \notin K$. Mô tả H và K.

19. Các nhóm nhân $\mathbb{Q}^*$, $\mathbb{R}^*$ có phải là các nhóm cyclic không?
20. Cho $H_1, H_2, \ldots$ là một dãy các nhóm con cyclic của nhóm G. Chứng tỏ rằng nếu $H_i \subsetneq H_{i+1}$ với mọi $i = 1, 2, \ldots$ thì $H_1 \cup H_2 \cup \cdots$ là một nhóm nhưng không phải nhóm cyclic.

1.5 Nhóm đối xứng và nhóm thay phiên

Cho X là một tập hợp không rỗng. Đặt S_X là tập hợp tất cả song ánh từ X đến chính nó, một phần tử của S_X được gọi là một *hoán vị* của X, ngắn gọn hơn là hoán vị. Vì hợp thành hai song ánh là một song ánh nên phép hợp thành là phép toán trên S_X. Phép hợp thành ở trên còn gọi là *phép nhân các hoán vị*.

Mệnh đề 1.44. *S_X với phép nhân các hoán vị là một nhóm. Ta gọi S_X là* nhóm đối xứng *của tập hợp X, nhóm này không giao hoán nếu X có hơn hai phần tử.*

Chứng minh. Phép nhân các hoán vị có tính kết hợp vì phép hợp thành các ánh xạ có tính kết hợp. Rõ ràng hoán vị đồng nhất id_X từ X đến chính nó là phần tử trung lập của phép toán. Với $\sigma \in S_X$ thì σ là một song ánh, khi đó tồn tại σ^{-1}, nó cũng là một song ánh nên là một phần tử trong S_X và là nghịch đảo của σ. Vậy S_X là một nhóm.

Nếu X có hơn hai phần tử, gọi a, b, c là ba phần tử khác nhau của X. Lấy $\rho, \tau \in S_X$ được xác định bởi

$$\rho(a) = b,\ \rho(b) = a,\ \rho(x) = x$$

với mọi $x \neq a$, $x \neq b$ và

$$\tau(a) = c,\ \tau(c) = a,\ \rho(y) = y$$

với mọi $y \neq a$, $y \neq c$. Ta có $\rho\tau(a) = \rho(c) = c$, trong khi đó $\tau\rho(a) = \tau(b) = b$. Từ đây suy ra $\rho\tau \neq \tau\rho$ và do đó S_X là nhóm không giao hoán.

□

Trong trường hợp đặc biệt khi $X = \{1, 2, \ldots, n\}$ thì ta viết S_n thay cho S_X. Mỗi phần tử $\sigma \in S_n$ được biểu diễn ở dạng

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n-1) & \sigma(n) \end{pmatrix}.$$

Ta gọi S_n là nhóm đối xứng bậc n, bây giờ ta tính bậc của nhóm này. Cho phần tử tùy ý $\sigma \in S_n$ thì $\sigma(1)$ có n cách lựa chọn tùy ý trong $X = \{1, 2, \ldots, n\}$, khi $\sigma(1)$

đã chọn, do σ là một song ánh nên $\sigma(2)$ chỉ được quyền chọn trong $X \setminus \{\sigma(1)\}$, và cứ thế $\ldots$, $\sigma(n-1)$ chỉ được quyền chọn trong $X \setminus \{\sigma(1), \ldots, \sigma(n-2)\}$ và $\sigma(n)$ chỉ được quyền chọn trong $X \setminus \{\sigma(1), \ldots, \sigma(n-2), \sigma(n-1)\}$. Vậy S_n có tất cả là $n(n-1)\cdots 2 \cdot 1 = n!$ phần tử.

Định nghĩa 1.45. Cho $a_1, a_2, \ldots, a_k$ là các phần tử trong tập hợp $\{1, 2, \ldots, n\}$ và từng đôi một khác nhau. Ta nói $\sigma \in S_n$ là một *chu trình* và viết $\sigma = (a_1 a_2 \ldots a_k)$ nếu

$$\sigma(a_1) = a_2,\ \sigma(a_2) = a_3, \ldots, \sigma(a_{k-1}) = a_k,\ \sigma(a_k) = a_1$$

và σ giữ nguyên những phần tử khác. Số k được gọi là *độ dài* của chu trình và một chu trình có độ dài k được gọi là k-chu trình, đặc biệt 2-chu trình còn được gọi là *chuyển vị*. Hai chu trình $(a_1 a_2 \ldots a_k)$ và $(b_1 b_2 \ldots b_l)$ gọi là rời nhau nếu $\{a_1, a_2, \ldots, a_k\} \cap \{b_1, b_2, \ldots, b_l\} = \emptyset$.

Ví dụ 1.46. Ta tìm tất cả 3-chu trình trong S_4. Chúng gồm

$$(123) \quad (132) \quad (124) \quad (142)$$

$$(134) \quad (143) \quad (234) \quad (243).$$

Chú ý rằng một chu trình có thể viết ở nhiều dạng khác nhau. Chẳng hạn $(123) = (231) = (312)$.

Mệnh đề 1.47. *Giả sử σ và τ là hai chu trình rời nhau trong S_n. Khi đó $\sigma\tau = \tau\sigma$.*

Chứng minh. Giả sử $\sigma = (a_1 a_2 \ldots a_k)$ và $\tau = (b_1 b_2 \ldots b_l)$ là hai chu trình rời nhau. Ta có $\sigma(x) \in \{a_1, a_2, \ldots, a_k\}$ với mọi $x \in \{a_1, a_2, \ldots, a_k\}$ và $\tau(y) \in \{b_1, b_2, \ldots, b_l\}$ với mọi $y \in \{b_1, b_2, \ldots, b_l\}$. Nếu $z \in \{a_1, a_2, \ldots, a_k\}$ thì

$$\sigma\tau(z) = \sigma(z) = \tau\sigma(z).$$

Nếu $z \notin \{a_1, a_2, \ldots, a_k\}$ thì

$$\sigma\tau(z) = \sigma(\tau(z)) = \tau(z) = \tau\sigma(z).$$

Vậy ta có $\sigma\tau = \tau\sigma$.

□

Định lý 1.48. *Mọi hoán vị $\sigma \in S_n$ luôn có thể phân tích được thành tích của những chu trình rời nhau.*

Chứng minh. Cho trước $\sigma \in S_n$. Trên $X = \{1, 2, \ldots, n\}$ ta xét quan hệ: $x \sim y$ nếu có $i \in \mathbb{Z}$ sao cho $y = \sigma^i(x)$. Ta chứng tỏ quan hệ là tương đương. Thật vậy, $x = \sigma^0(x)$ nên $x \sim x$ với mọi $x \in X$. Nếu $x \sim y$ thì có $i \in \mathbb{Z}$ sao cho $y = \sigma^i(x)$. Khi

đó $x = \sigma^{-i}(y)$ và vì vậy $y \sim x$. Nếu $x \sim y$ và $y \sim z$ thì có $i, j \in \mathbb{Z}$ sao cho $y = \sigma^i(x)$ và $z = \sigma^j(y)$. Khi đó $z = \sigma^{i+j}(x)$ và do đó $x \sim z$.

Gọi $O_1, O_2, \ldots, O_l$ là các lớp tương đương. Với mỗi lớp tương đương O_k ta định nghĩa chu trình σ_k tương ứng như sau:

$$\sigma_k(x) = \begin{cases} \sigma(x) & \text{nếu } x \in O_k \\ x & \text{nếu } x \notin O_k \end{cases}$$

Các chu trình σ_k là rời nhau vì các O_k là các lớp tương đương khác nhau. Khi đó dễ thấy rằng $\sigma = \sigma_1\sigma_2 \cdots \sigma_l$ và định lý được chứng minh.

□

Bổ đề 1.49. *Mọi chu trình đều phân tích được thành tích của các chuyển vị.*

Chứng minh. Giả sử $\sigma = (a_1 a_2 \ldots a_k)$. Khi đó

$$\sigma = (a_1 a_k) \cdots (a_1 a_3)(a_1 a_2)$$

và bổ đề được chứng minh.

□

Kết hợp Định lý 1.48 và Bổ đề 1.49 ta có

Mệnh đề 1.50. *Mọi hoán vị đều phân tích được thành tích của các chuyển vị.*

Định nghĩa 1.51. Cho $\sigma \in S_n$. Ta nói *dấu* của σ, ký hiệu $\operatorname{sgn}(\sigma)$, là số

$$\operatorname{sgn}(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

Chú ý rằng vì σ là một song ánh nên các nhân tử $\sigma(i) - \sigma(j)$ xuất hiện ở tử cũng xuất hiện ở mẫu sai khác dấu ± 1, do đó $\operatorname{sgn}(\sigma) \in \{\pm 1\}$. Với hai phần tử $i < j$ nếu $\sigma(i) > \sigma(j)$ ta nói có một nghịch thế, như vậy nếu số nghịch thế là chẵn thì $\operatorname{sgn}(\sigma) = 1$, ngược lại $\operatorname{sgn}(\sigma) = -1$.

Mệnh đề 1.52. *Cho $\sigma, \tau \in S_n$. Khi đó* $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$.

Chứng minh. Ta có

$$\begin{aligned} \operatorname{sgn}(\sigma\tau) &= \prod_{1 \le i < j \le n} \frac{\sigma\tau(i) - \sigma\tau(j)}{i - j} \\ &= \prod_{1 \le i < j \le n} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \prod_{1 \le i < j \le n} \frac{\tau(i) - \tau(j)}{i - j} \\ &= \prod_{1 \le \tau(k) < \tau(l) \le n} \frac{\sigma(\tau(k)) - \sigma(\tau(l))}{\tau(k) - \tau(l)} \prod_{1 \le i < j \le n} \frac{\tau(i) - \tau(j)}{i - j} \\ &= \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau). \end{aligned}$$

Vậy mệnh đề được chứng minh.

□

Hệ quả 1.53. (a) $\text{sgn}(id) = 1$.

(b) $\text{sgn}(\sigma^{-1}) = \text{sgn}(\sigma)$ *với mọi* $\sigma \in S_n$.

Chứng minh. (a) là hiển nhiên.

(b) Ta có $1 = \text{sgn}(id) = \text{sgn}(\sigma^{-1}\sigma) = \text{sgn}(\sigma^{-1})\text{sgn}(\sigma)$ với mọi $\sigma \in S_n$. Từ đây ta có (b).

□

Theo Mệnh đề 1.50 thì mọi hoán vị đều phân tích được thành tích của các chuyển vị. Khi đó áp dụng Mệnh đề 1.52 dấu của hoán vị được tính thông qua dấu của chuyển vị, do đó ta cần xác định dấu của chuyển vị.

Mệnh đề 1.54. *Dấu của chuyển vị tùy ý* $(kl) \in S_n$ *luôn bằng* -1.

Chứng minh. Cho chuyển vị $\sigma = (kl)$ với $k < l$, ta tính số các nghịch thế của σ. Xét cặp (i, j) với $i < j$.

Nếu $i < k$, ta có $\sigma(i) = i < \sigma(j)$ nên cặp (i, j) không là một nghịch thế.

Nếu $l < j$, ta có $\sigma(i) < j = \sigma(j)$ nên cặp (i, j) không là một nghịch thế.

Nếu $i = k$, khi đó với mọi j mà $k < j < l$, ta có $\sigma(i) = l > j = \sigma(j)$ nên cặp (i, j) là một nghịch thế. Số các nghịch thế như thế bằng $l - k - 1$.

Nếu $j = l$, khi đó với mọi i mà $k < i < l$, ta có $\sigma(i) = i > k = \sigma(j)$ nên cặp (i, j) là một nghịch thế. Và một lần nữa số các nghịch thế như thế bằng $l - k - 1$.

Cuối cùng $i = k$ và $j = l$ ta có cặp (i, j) là một nghịch thế.

Vì vậy tổng cộng có tất cả là $2(l - k - 1) + 1$ là số lẻ nghịch thế nên dấu của σ bằng -1.

□

Định lý 1.55. *Mọi hoán vị của* S_n *luôn phân tích được thành tích của các chuyển vị. Số các chuyển vị trong phân tích luôn là một số chẵn hoặc luôn là một số lẻ.*

Chứng minh. Theo Mệnh đề 1.50 ta có phần đầu của định lý. Giả sử hoán vị có hai cách phân tích với số chuyển vị trong phân tích lần lượt là k và k'. Khi đó theo các Mệnh đề 1.52 và 1.54 thì dấu của hoán vị bằng $(-1)^k = (-1)^{k'}$. Từ đây ta suy ra k và k' luôn cùng chẵn hoặc cùng lẻ và định lý được chứng minh.

□

Định nghĩa 1.56. Ta nói một hoán vị trong S_n là hoán vị *chẵn* nếu nó có dấu bằng 1; là hoán vị *lẻ* nếu nó có dấu bằng -1.

Ví dụ 1.57. Trong S_9 xét hoán vị

$$\sigma = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 8\,6\,9\,7\,2\,5\,1\,3\,4 \end{pmatrix}.$$

Trước hết ta phân tích σ thành tích các chu trình rời nhau. Ta có $\sigma = (183947)(265)$ và do đó $\sigma = (17)(14)(19)(13)(18)(25)(26)$. Vì dấu của chuyển vị bằng -1 nên dấu của σ là $(-1)^7 = -1$. Vậy σ là một hoán vị lẻ.

Định lý 1.58. *Đặt A_n là tập hợp tất cả các hoán vị chẵn trong S_n. Khi đó A_n là một nhóm con của S_n được gọi là nhóm* thay phiên *bậc n, nhóm này có $n!/2$ phần tử.*

Chứng minh. Hoán vị đồng nhất là hoán vị chẵn nên thuộc A_n, do đó A_n không rỗng. Nếu $\sigma, \tau \in A_n$ thì

$$\operatorname{sgn}(\sigma\tau^{-1}) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau^{-1}) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau) = 1 \cdot 1 = 1$$

nên $\sigma\tau^{-1} \in A_n$. Vậy A_n là một nhóm con của S_n. Gọi O_n là tập hợp tất cả hoán vị lẻ của S_n. Vì mỗi hoán vị hoặc là hoán vị chẵn hoặc là hoán vị lẻ và không thể đồng thời là cả hai nên $|S_n| = |A_n| + |O_n|$. Định lý sẽ được chứng minh nếu ta chứng tỏ $|A_n| = |O_n|$. Để chứng tỏ hai tập hợp có cùng số phần tử ta cần xây dựng một song ánh giữa chúng. Ta định nghĩa ánh xạ $f : A_n \longrightarrow O_n$ như sau: với mỗi hoán vị chẵn $\sigma \in A_n$ tương ứng với hoán vị lẻ $(12)\sigma$. Ta chứng tỏ f là một song ánh. Thật vậy, f là một đơn ánh vì nếu $f(\sigma) = f(\tau)$ suy ra $(12)\sigma = (12)\tau$, giản ước hai vế cho (12) ta có $\sigma = \tau$. Hơn nữa, f là một toàn ánh vì nếu $\mu \in O_n$ hoán vị lẻ thì $(12)\mu \in A_n$ là hoán vị chẵn và $f((12)\mu) = (12)(12)\mu = \mu$.

□

Ví dụ 1.59. (a) S_3 có $3! = 6$ phần tử, do đó nhóm A_3 có ba phần tử ứng với ba hoán vị chẵn, đó là: hoán vị đồng nhất e, $\rho = (123)$, $\rho^2 = (132)$.

(b) S_4 có $4! = 24$ phần tử, do đó nhóm A_4 có 12 phần tử, ta hãy xác định A_4.. Trước hết ta có ba hoán vị chẵn sau không giữ cố định phần tử nào, đó là:

$$\sigma_1 = (12)(34) \qquad \sigma_2 = (13)(24) \qquad \sigma_3 = (14)(23).$$

Tiếp theo ta xét các hoán vị chẵn không tầm thường giữ cố định một phần tử i với $1 \leq i \leq 4$. Với $i = 1$ ta có hai hoán vị chẵn trong các hoán vị của các phần tử còn lại, cho i thay đổi ta nhận được tám hoán vị chẵn trong A_4 như sau:

$$\rho_1 = (234) \qquad \rho_1^2 = (243) \qquad \text{(giữ cố định 1)}$$

$$\rho_2 = (134) \qquad \rho_2^2 = (143) \qquad \text{(giữ cố định 2)}$$

$$\rho_3 = (124) \qquad \rho_3^2 = (142) \qquad \text{(giữ cố định 3)}$$

$$\rho_4 = (123) \qquad \rho_4^2 = (132) \qquad \text{(giữ cố định 4)}.$$

Ngoài ra còn có phần tử đơn vị e giữ cố định mọi phần tử. Vậy

$$A_4 = \left\{e, \sigma_1, \sigma_2, \sigma_3, \rho_1, \rho_1^2, \rho_2, \rho_2^2, \rho_3, \rho_3^2, \rho_4, \rho_4^2\right\}.$$

Bài tập

1. Tính các hoán vị sau.
   (a) $\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$ (b) $\begin{pmatrix}1&2&3&4&5&6\\4&5&2&3&6&1\end{pmatrix}^3$ (c) $\begin{pmatrix}1&2&3&4&5\end{pmatrix}\begin{pmatrix}2&3&4\end{pmatrix}$.
2. Biểu diễn mỗi hoán vị sau thành tích của những chu trình rời nhau và tính cấp của nó.
   (a) $\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\1&8&2&9&7&5&4&3&10&6\end{pmatrix}$ (b) $\begin{pmatrix}1&2&3&4&5&6&7\\5&6&2&4&3&7&1\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7\\7&6&4&5&1&3&2\end{pmatrix}$
3. Tìm cấp của các phần tử trong nhóm A_4.
4. Chứng tỏ một k-chu trình có cấp bằng k.
5. Giả sử σ và τ trong S_n là hai chu trình rời nhau và $\rho = \sigma \cdot \tau$. Chứng tỏ cấp của ρ bằng bội số chung nhỏ nhất của cấp của σ và cấp của τ.
6. Chứng tỏ với bất kỳ nhóm con H của S_n thì mọi phần tử của H đều là hoán vị chẵn hoặc có đúng một nửa các phần tử của H là hoán vị chẵn.
7. Đặt $H = \{\sigma \in S_4 \mid \sigma(3) = 3\}$.
   (a) Chứng tỏ H là một nhóm con của S_4 và tìm cấp của H.
   (b) Tìm tất cả hoán vị chẵn trong H.
8. Cho $n \geq 3$, $i \leq n$ và đặt $H = \{\sigma \in S_n \mid \sigma(i) = i\}$.
   (a) Chứng tỏ H là một nhóm con của S_n và tìm cấp của H.
   (b) Tìm tất cả hoán vị chẵn trong H.
9. Chứng minh rằng nhóm S_n được sinh ra bởi các phần tử (12), $(23), \ldots, (n-1\,n)$.
10. Chứng tỏ nhóm S_n được sinh ra bởi phần tử $(123\cdots n)$ và (12).
11. Chứng tỏ nhóm A_n được sinh ra bởi tập hợp $\{(12r) \mid r = 3, 4, \ldots, n\}$.

1.6 Lớp kề

Mệnh đề 1.60. *Cho G là một nhóm và H một nhóm con của G. Trên G ta xét quan hệ $\sim$ được xác định như sau: với $x, y \in G$, $x \sim y$ nếu $x^{-1}y \in H$. Khi đó*

(a) *Quan hệ $\sim$ là một quan hệ tương đương.*

(b) *Lớp tương đương của $x \in G$ là tập hợp $xH = \{xh \mid h \in H\}$, xH được gọi là một lớp kề trái của H trong G.*

Chứng minh. (a) Với mỗi $x \in G$ ta luôn có $x^{-1}x = e \in H$, do đó $x \sim x$. Nếu $x, y \in G$ và $x \sim y$ thì $x^{-1}y \in H$. Vì H là một nhóm nên phần tử nghịch đảo của $x^{-1}y$ cũng là phần tử trong H, do đó $y^{-1}x = (x^{-1}y)^{-1} \in H$. Vậy $y \sim x$. Nếu $x, y, z \in G$ và $x \sim y, y \sim z$ thì $x^{-1}y, y^{-1}z \in H$. Khi đó $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$ vì H là một nhóm, và vì thế $x \sim z$. Vậy quan hệ là tương đương.

(b) Lớp tương đương $\overline{x}$ của $x \in G$ gồm các phần tử $y \in G$ sao cho $x^{-1}y = h \in H$, do đó $y = xh$. Vậy $\overline{x} = xH = \{xh \mid h \in H\}$.

□

Từ Mệnh đề 0.47 ta suy ra các lớp kề trái có những tính chất sau.

Mệnh đề 1.61. *Giả sử H là một nhóm con của nhóm G và x, y là hai phần tử tùy ý của G. Khi đó*

(a) *$x \in H$ nếu và chỉ nếu $xH = H$.*

(b) *Hoặc $xH = yH$ hoặc $xH \cap yH = \emptyset$.*

(c) *$xH = yH$ nếu và chỉ nếu $x^{-1}y \in H$.*

Chú ý rằng nếu quan hệ giữa các phần tử trong G là $x \sim y$ khi $xy^{-1} \in H$, thì tương tự như trên ta cũng chứng tỏ được quan hệ là tương đương và lớp tương đương của x theo quan hệ này là $Hx = \{hx \mid h \in H\}$, và được gọi là một lớp kề phải của H trong G. Các lớp kề phải cũng có những tính chất tương tự như các lớp kề trái.

Khi G là một nhóm giao hoán thì lớp kề trái xH và lớp kề phải Hx luôn bằng nhau.

Ví dụ 1.62. Ta xét nhóm $\mathbb{S}_3$ trong Ví dụ 1.26 và nhóm con H được sinh ra bởi ρ_1 có cấp hai. Ta có $H = \{e, \rho_1\}$, ta lập các lớp kề trái của H trong $\mathbb{S}_3$. Ta có

$$\begin{aligned}
eH &= \{ee, e\rho_1\} = \{e, \rho_1\} \\
\rho H &= \{\rho e, \rho\rho_1\} = \{\rho, \rho_3\} \\
\rho^2 H &= \{\rho^2 e, \rho^2\rho_1\} = \{\rho^2, \rho_2\} \\
\rho_1 H &= eH \text{ vì } \rho_1 \in H \\
\rho_2 H &= \rho^2 H \text{ vì } \rho_2^{-1}\rho^2 \in H \\
\rho_3 H &= \rho H \text{ vì } \rho_3^{-1}\rho \in H.
\end{aligned}$$

Tương tự ta có các lớp kề phải của H là:

$$\begin{aligned}
He &= \{e, \rho_1\} = H\rho_1 \\
H\rho &= \{\rho, \rho_2\} = H\rho_2 \\
H\rho^2 &= \{\rho^2, \rho_3\} = H\rho_3.
\end{aligned}$$

Ta thấy $\rho H \neq H\rho$, $\rho^2 H \neq H\rho^2$.

Chú ý rằng tương ứng $xH \longmapsto Hx^{-1}$ là một song ánh từ tập hợp các lớp kề trái đến tập hợp các lớp kề phải. Trước hết ta chứng tỏ định nghĩa trên là đúng đắn, tức là nếu $xH = yH$ thì $Hx^{-1} = Hy^{-1}$. Thật vậy, giả sử $xH = yH$ suy ra $x^{-1}y \in H$. Ta có $x^{-1}(y^{-1})^{-1} = x^{-1}y \in H$ và do đó $Hx^{-1} = Hy^{-1}$. Vậy tương ứng ở trên là một ánh xạ. Khi đó dễ thấy rằng tương ứng là một song ánh, do đó tập hợp các lớp kề trái và các lớp kề phải có cùng lực lượng. Đặt $G/H = \{xH \mid x \in G\}$ là tập hợp gồm tất cả các lớp kề trái của H trong G. Ta ký hiệu $[G : H]$ là lực lượng của G/H và gọi là chỉ số của H trong G.

Bây giờ ta tìm hiểu mối quan hệ giữa cấp của một nhóm hữu hạn và cấp của nhóm con của nó.

Định lý 1.63. (Lagrange) *Cho G là một nhóm hữu hạn và H một nhóm con của G. Khi đó*

$$|G| = [G : H]\,|H|\,.$$

Chứng minh. Vì các lớp kề trái của H là các lớp tương đương, do đó chúng tạo thành một phân hoạch của G. Giả sử G có các lớp kề trái khác nhau là $x_1H, x_2H, x_3H, \ldots, x_nH$. Ta có

$$G = x_1H \sqcup x_2H \sqcup x_3H \sqcup \cdots \sqcup x_nH$$

là hợp rời các lớp kề trái và do đó

$$|G| = |x_1H| + |x_2H| + |x_3H| + \cdots + |x_nH|\,.$$

Với mỗi i mà $1 \leq i \leq n$, ta xét ánh xạ

$$h \in H \mapsto f(h) = x_ih \in x_iH.$$

Ta chứng tỏ f là một song ánh. Giả sử với $h, h' \in H$ mà $f(h) = f(h')$, khi đó $x_ih = x_ih'$, giản ước x_i bên trái của đẳng thức ta có $h = h'$ nên f là một đơn ánh. Dễ thấy f là một toàn ánh và do đó là một song ánh, suy ra $|H| = |x_iH|$. Và vì vậy $|G| = [G : H]\,|H|$, trong đó $[G : H] = n$.

□

Chú ý rằng cho trước nhóm hữu hạn G, nếu H là một nhóm con tùy ý của G thì theo Định lý Lagrange $|H|$ là một ước số của $|G|$. Tuy nhiên điều ngược lại nói chung không đúng, tức là nếu cho d là một ước tùy ý của $|G|$ thì không hẳn có nhóm con của G có cấp bằng d.

Hệ quả 1.64. *Cấp của mỗi phần tử của một nhóm hữu hạn G đều là một ước số của $|G|$.*

Chứng minh. Ta biết mỗi phần tử $a \in G$ sinh ra một nhóm cyclic $\langle a \rangle$ và $|\langle a \rangle| = |a|$. Vì $\langle a \rangle$ là một nhóm con của G nên $|\langle a \rangle| \mid |G|$, và do đó $|a| \mid |G|$.

□

Hệ quả 1.65. *Cho G là một nhóm hữu hạn. Khi đó với mọi phần tử $a \in G$ thì $a^{|G|} = e$.*

Chứng minh. Với mỗi $a \in G$, gọi m là cấp của a thì $m \mid |G|$. Khi đó có $q \in \mathbb{N}$ sao cho $|G| = mq$. Ta có $a^{|G|} = a^{mq} = (a^m)^q = e$.

□

Hệ quả 1.66. *Một nhóm có cấp là số nguyên tố là nhóm cyclic.*

Chứng minh. Cho nhóm G với cấp $|G| = p$, ở đây p là số nguyên tố. Lấy $a \in G$, $a \neq e$. Khi đó nhóm con của G được sinh ra bởi a là một nhóm không tầm thường có cấp là ước số của p nên phải bằng p. Vậy G là nhóm cyclic được sinh ra bởi a.

□

Ví dụ 1.67. Tìm các nhóm con của nhóm S_3 trong Ví dụ 1.26. Giả sử H là một nhóm con của nhóm S_3. Vì S_3 có sáu phần tử nên theo Định lý Lagrange cấp của H chỉ có thể là $1, 2, 3$ hoặc 6. Nếu $|H| = 1$ thì H là nhóm tầm thường, nếu $|H| = 6$ thì H là nhóm S_3. Xét $|H| = 2$, vì 2 là số nguyên tố nên theo Hệ quả 1.66 thì H là nhóm cyclic được sinh ra bởi phần tử có cấp hai. Trong S_3 chỉ có ba phần tử có cấp hai, đó là ρ_1, ρ_2, ρ_3 và do đó có ba nhóm con có cấp hai: $\langle \rho_1 \rangle = \{e, \rho_1\}$, $\langle \rho_2 \rangle = \{e, \rho_2\}$, $\langle \rho_3 \rangle = \{e, \rho_3\}$. Xét $|H| = 3$, tương tự như trên H là nhóm cyclic được sinh ra bởi phần tử có cấp ba. Trong S_3 chỉ có ρ, ρ^2 có cấp ba và nhóm con $\langle \rho \rangle = \{e, \rho, \rho^2\} = \langle \rho^2 \rangle$. Vậy S_3 có sáu nhóm con khác nhau.

Hệ quả 1.68. (Định lý Euler) *Cho trước số nguyên n ($n \geq 2$), khi đó với mọi số nguyên a nguyên tố cùng nhau với n thì $a^{\varphi(n)} \equiv 1$ mod n.*

Chứng minh. Vì $\gcd(a, n) = 1$ nên $\overline{a} \in U(n)$. Như đã biết $|U(n)| = \varphi(n)$, theo Hệ quả 1.65 ta có $\overline{a^{\varphi(n)}} = \overline{a}^{\varphi(n)} = \overline{1}$. Do đó $a^{\varphi(n)} \equiv 1 \bmod n$.

□

Hệ quả 1.69. (Định lý Fermat nhỏ) *Cho trước số nguyên tố p, khi đó với mọi số nguyên a ta có $a^p \equiv a \bmod p$.*

Chứng minh. Nếu p chia hết a thì $a \equiv 0 \bmod p$. Khi đó hiển nhiên $a^p \equiv 0 \bmod p$. Nếu p không chia hết a, khi đó $\gcd(a, p) = 1$ vì p là số nguyên tố. Theo Hệ quả 1.68 thì $a^{\varphi(p)} \equiv 1 \bmod p$. Nhưng $\varphi(p) = p - 1$, do đó $a^{p-1} \equiv 1 \bmod p$ và $a^p \equiv a \bmod p$.

□

Bài tập

1. Tìm các lớp kề của nhóm con $25\mathbb{Z}$ trong $\mathbb{Z}$ và $25\mathbb{Z}$ trong $5\mathbb{Z}$.
2. Tìm các lớp kề của nhóm con $\langle\overline{6}\rangle$ trong $\mathbb{Z}_{18}$ và $\langle\overline{6}\rangle$ trong nhóm con $\langle\overline{2}\rangle$ của $\mathbb{Z}_{18}$.
3. Cho nhóm cyclic $G = \langle a\rangle$ có cấp 50 và $H = \langle a^{35}\rangle$. Liệt kê tất cả lớp kề của H trong G.
4. Cho $H = \{(1), (12), (34), (12)(34)\}$ là một tập con của nhóm S_4.. Chứng tỏ H là một nhóm con của S_4, tìm các lớp kề trái của H trong S_4.
5. Cho H là một nhóm con của A_4 giữ cố định phần tử 1. Tìm các lớp kề trái và phải của H trong A_4.
6. Cho nhóm G có cấp pq với p, q hai số nguyên tố. Chứng tỏ mọi nhóm con thật sự của G đều là cyclic.
7. Cho H và K là hai nhóm con của nhóm G với cấp của H và K nguyên tố cùng nhau. Chứng tỏ $H \cap K = \{e\}$.
8. Chứng tỏ $n^{19} - n$ chia hết cho 21 với mọi số nguyên n.
9. Tìm phần dư của 9^{1572} khi chia cho 11.
10. Tìm phần dư của 5^{1259} khi chia cho 12.
11. Tìm phần dư của 3^{153} khi chia cho 75.
12. Chứng tỏ nhóm thay phiên A_4 không có nhóm con có cấp 6. Từ đây suy ra điều ngược lại của Định lý Lagrange là sai.

1.7 Nhóm con chuẩn tắc và nhóm thương

Định nghĩa 1.70. Giả sử G là một nhóm và H một nhóm con của G. Ta nói H là một nhóm con *chuẩn tắc* của G, ký hiệu $H \triangleleft G$, nếu $xH = Hx$ với mọi $x \in G$.

Ví dụ 1.71. (a) Trong một nhóm G, nhóm con tầm thường $\{e\}$, nhóm con không thật sự G là các nhóm con chuẩn tắc của G.

(b) G là một nhóm giao hoán thì mọi nhóm con của G đều chuẩn tắc.

(c) $Z(G)$, tâm của nhóm G, là một nhóm con chuẩn tắc của G vì mọi phần tử của $Z(G)$ đều giao hoán với các phần tử của G.

Do định nghĩa trên, từ giờ trở đi nếu H là một nhóm con chuẩn tắc của G thì ta không phân biệt lớp kề trái, lớp kề phải của H và gọi là một *lớp kề* của H trong G.

Mệnh đề 1.72. *Cho G là một nhóm và H một nhóm con của G với chỉ số $[G : H]$=2. Khi đó H là một nhóm con chuẩn tắc của G.*

Chứng minh. Vì $[G : H]$=2, H chỉ có hai lớp kề trái và hai lớp kề phải. $eH = H = He$ là một lớp kề trái cũng như lớp kề phải. Vì tập hợp các lớp kề trái cũng như tập

hợp các lớp kề phải tạo thành phân hoạch của G. Do đó với $g \notin H$ thì lớp kề trái còn lại là $gH = \{k \in G \mid k \notin H\}$ bằng với lớp kề phải Hg, và vì vậy $H \triangleleft G$.

□

Ví dụ 1.73. (a) Xét nhóm S_3 trong Ví dụ 1.26. Nhóm con $\langle \rho \rangle$ có chỉ số $[S_3 : \langle \rho \rangle]$=2 và do đó $\langle \rho \rangle$ là một nhóm con chuẩn tắc của S_3.

(b) Một cách tổng quát xét nhóm đối xứng S_n. Nhóm con A_n gồm các hoán vị chẵn trong S_n có chỉ số $[S_n : A_n] = 2$ và do đó A_n là một nhóm con chuẩn tắc của S_n.

Mệnh đề 1.74. *Cho G là một nhóm và H một nhóm con của G. Khi đó các điều sau tương đương.*

(a) $H \lhd G$.

(b) $x^{-1}Hx = \{x^{-1}hx \mid h \in H\} \subset H$ *với mọi* $x \in G$.

(c) $x^{-1}Hx = H$ *với mọi* $x \in G$.

Chứng minh. (a)⇒(b) Với mọi $x \in G$, $h \in H$ ta có $hx \in Hx$. Vì $H \lhd G$ nên $Hx = xH$ và do đó $hx \in xH$, khi đó có $h' \in H$ sao cho $hx = xh'$. Từ đây suy ra $x^{-1}hx = h' \in H$, và vì vậy $x^{-1}Hx \subset H$.

(b)⇒(c) Với mọi $x \in G$, ta có $(x^{-1})^{-1}H(x^{-1}) \subset H$ và do đó $H \subset x^{-1}Hx$. Mặt khác, ta cũng có $x^{-1}Hx \subset H$, suy ra $x^{-1}Hx = H$.

(c)⇒(a) Với mọi $x \in G$, $h \in H$ ta có $x^{-1}hx = h' \in H$, do đó $hx = xh'$. Vậy $Hx \subset xH$. Tương tự, nếu ta bắt đầu từ $x^{-1} \in G$ thì ta có $xH \subset Hx$. Vậy $xH = Hx$.

□

Mệnh đề 1.75. *Cho H và K là hai nhóm con của nhóm G. Nếu $H \triangleleft G$ thì $HK = \{hk \mid h \in H, k \in K\}$ là một nhóm con của G.*

Chứng minh. Giả sử $H \triangleleft G$. Ta có HK không rỗng vì có $e = e.e \in HK$. Cho $x, y \in HK$, khi đó có $h_1, h_2 \in H$, $k_1, k_2 \in K$ sao cho $x = h_1k_1$, $y = h_2k_2$. Ta có

$$xy^{-1} = h_1k_1\,(h_2k_2)^{-1} = (h_1k_1)(k_2^{-1}h_2^{-1}) = h_1kh_2^{-1}$$

với $k = k_1k_2^{-1} \in K$ vì K là một nhóm con. $kh_2^{-1} \in kH$, vì $H \triangleleft G$ nên $kH = Hk$, suy ra $kh_2^{-1} \in Hk$. Do đó có $h \in H$ sao cho $kh_2^{-1} = hk$ và

$$xy^{-1} = h_1kh_2^{-1} = h_1hk = h'k$$

với $h' = h_1h \in H$. Vì vậy $xy^{-1} \in HK$ và HK là một nhóm con của G.

□

Một hệ quả hiển nhiên là

Hệ quả 1.76. *Cho H và K là hai nhóm con của nhóm Abel G. Khi đó HK là một nhóm con của G.*

Mệnh đề 1.77. *Cho G là một nhóm và H một nhóm con chuẩn tắc của G. Trên tập hợp thương G/H ta định nghĩa phép toán như sau:*

$$xH \cdot yH = (xy)H$$

với mọi $xH, yH \in G/H$. Khi đó G/H là một nhóm.

Chứng minh. Trước hết ta chứng tỏ phép toán trên được định nghĩa đúng đắn, tức là nếu $xH = x'H$, $yH = y'H$ thì ta phải có

$$(xy)H = (x'y')H.$$

Thật vậy, vì $xH = x'H$, $yH = y'H$ nên có $h, k \in H$ sao cho $x = x'h$, $y = y'k$. Ta có

$$xy = (x'h)(y'k) = x'(hy')k.$$

Bởi tính chuẩn tắc của H, $hy' = y'h'$ với h' là phần tử nào đó trong H và do đó

$$xy = x'(hy')k = (x'y')k'$$

với $k' = h'k \in H$. Vậy hai lớp kề trái của xy và $x'y'$ là bằng nhau. Phép nhân trên G/H có tính kết hợp vì với mọi $xH, yH, zH \in G/H$ ta có

$$(xH \cdot yH) \cdot zH = (xy)H \cdot zH = (xy)zH = x(yz)H = xH \cdot (yH \cdot zH).$$

Phần tử trung lập là $eH = H \in G/H$ vì với mọi $xH \in G/H$ thì

$$xH \cdot eH = xeH = xH = exH = eH \cdot xH.$$

Với mọi $xH \in G/H$ ta có $x^{-1}H \in G/H$ thỏa

$$xH \cdot x^{-1}H = (xx^{-1})H = eH = (x^{-1}x)H = x^{-1}H \cdot xH.$$

Vậy G/H là một nhóm.

□

Ví dụ 1.78. (a) Cho nhóm G. Ta có $\{e\}$ là nhóm con chuẩn tắc tầm thường của G và $G/\{e\} = G$; G là nhóm con chuẩn tắc không thật sự của chính nó và G/G là nhóm chỉ có một phần tử.

(b) Xét nhóm cộng $\mathbb{Z}$. Với $n \in \mathbb{N}$, $n \geq 2$ cho trước thì $n\mathbb{Z}$ là nhóm con chuẩn tắc của $\mathbb{Z}$ và $\mathbb{Z}/n\mathbb{Z}$ chính là nhóm cộng $\mathbb{Z}_n$ các số nguyên mod n.

Định nghĩa 1.79. Giả sử G *là một nhóm và* H một nhóm con chuẩn tắc của G. Khi đó nhóm G/H được gọi là *nhóm thương* của G theo H.

Bài tập

1. Nhóm con cyclic $\{(1), (123), (132)\}$ có chuẩn tắc trong S_4 không?
2. Nhóm con cyclic $\{(1), (123), (132)\}$ có chuẩn tắc trong A_4 không?
3. Tìm tất cả nhóm con chuẩn tắc trong D_4.
4. Cho một ví dụ về một dãy các nhóm con $H \subset K \subset G$ sao cho $H \lhd K$ và $K \lhd G$ nhưng $H \not\lhd G$.
5. Chứng tỏ nếu $H \lhd G$ và $K \lhd G$ thì $H \cap K \lhd G$, $HK \lhd G$.
6. Cho $K \lhd G$ và H là một nhóm con của G. Chứng tỏ $K \cap H \lhd H$.
7. Giả sử H là nhóm con duy nhất với cấp cho trước trong một nhóm G, chứng tỏ H chuẩn tắc trong G.
8. Cho nhóm G có cấp pq, ở đây p và q là hai số nguyên tố khác nhau. Giả sử G có duy nhất một nhóm con có cấp p và duy nhất một nhóm con có cấp q. Chứng tỏ G là một nhóm cyclic.
9. Cho nhóm G có duy nhất một nhóm con có cấp m và duy nhất một nhóm con có cấp n, ở đây m và n nguyên tố cùng nhau. Chứng tỏ G có một nhóm con chuẩn tắc có cấp mn.
10. Nếu G là một nhóm con của S_n và G chứa một hoán vị lẻ, chứng tỏ G chứa một nhóm con chuẩn tắc có chỉ số 2.
11. Tìm cấp của mỗi phần tử trong các nhóm thương sau:
    (a) $\overline{5} + \langle \overline{8} \rangle$ trong $\mathbb{Z}_{10}/\langle \overline{8} \rangle$.
    (b) $\overline{2} + \langle \overline{6} \rangle$ trong $\mathbb{Z}_{15}/\langle \overline{6} \rangle$.
12. Chứng tỏ $\mathbb{Q}/\mathbb{Z}$ là một nhóm có cấp vô hạn nhưng mỗi phần tử có cấp hữu hạn.
13. Cho G là một nhóm. Chứng tỏ
    (a) $Z(G) \lhd G$.
    (b) Nếu $G/Z(G)$ là một nhóm cyclic thì G là một nhóm giao hoán.
14. Cho H là một nhóm con của nhóm G. Đặt

$$N_G(H) = \{x \in G \mid x^{-1}Hx = H\}$$

    gọi là chuẩn tắc hóa của H trong G. Chứng tỏ
    (a) $N_G(H)$ là một nhóm con của G.
    (b) $H \lhd N_G H$.
    (c) Nếu K là một nhóm con của G sao cho $H \lhd K$ thì $K \subset N_G H$.
    (d) $H \lhd G$ khi và chỉ khi $N_G H = G$.
15. Cho G là một nhóm và đặt $[x, y]{=}x^{-1}y^{-1}xy$ với $x, y \in G$. Ký hiệu $[G, G]$ là nhóm con của G được sinh ra bởi các $[x, y]$ với mọi $x, y \in G$, ta nói $[G, G]$ là nhóm con giao hoán tử của G. Chứng tỏ rằng
    (a) $[G, G] \lhd G$ và $G/[G, G]$ là một nhóm giao hoán.

(b) Nếu H là một nhóm con chuẩn tắc của G và G/H là một nhóm giao hoán thì $[G,G] \subset H$.

(c) Nếu H là một nhóm con của G với $[G,G] \subset H$ thì $H \triangleleft G$.

16. Tìm nhóm con giao hoán tử của S_3.
17. Tìm nhóm con giao hoán tử của D_4.

1.8 Đồng cấu

Để nghiên cứu một nhóm, thường người ta khảo sát nó trong mối quan hệ với những nhóm khác thông qua công cụ gọi là đồng cấu. Ta có định nghĩa đồng cấu như sau.

Định nghĩa 1.80. Ánh xạ f từ nhóm G đến nhóm H được gọi là một *đồng cấu* (*nhóm*) nếu

$$f(xy) = f(x)f(y)$$

với mọi $x, y \in G$.

Định nghĩa 1.81. Giả sử f là một đồng cấu từ nhóm G đến nhóm H. Ta nói f là một *đơn cấu* nếu f là một đơn ánh; là một *toàn cấu* nếu f là một toàn ánh; là một *đẳng cấu* nếu f là một song ánh. Một đẳng cấu từ nhóm G đến chính nó còn được gọi là một *tự đẳng cấu*.

Ví dụ 1.82. (a) Cho G và H là hai nhóm. Khi đó ánh xạ $x \in G \longmapsto e \in H$ với mọi $x \in G$ là một đồng cấu được gọi là đồng cấu *tầm thường*.

(b) Đặt $\mathbb{R}^+$ là nhóm nhân các số thực dương. Khi đó các ánh xạ $x \in \mathbb{R} \longmapsto 2^x \in \mathbb{R}^+$, $x \in \mathbb{R}^+ \longmapsto \log x \in \mathbb{R}$ là các đồng cấu. Hơn nữa, các đồng cấu trên đều là đẳng cấu.

(c) Ánh xạ $\sigma \in S_n \longmapsto \text{sgn}(\sigma) \in \{1, -1\}$ là một toàn cấu.

(d) Cho H là một nhóm con của nhóm G. Khi đó ánh xạ $x \in H \longmapsto x \in G$ với mọi $x \in H$ là một đơn cấu.

(e) Cho G là một nhóm. Khi đó ánh xạ đồng nhất $x \in G \longmapsto x \in G$ là một tự đẳng cấu.

(f) Giả sử H là một nhóm con chuẩn tắc của nhóm G. Khi đó ánh xạ

$$\begin{aligned} \text{Pr} : G &\longrightarrow G/H \\ x &\mapsto \text{Pr}(x) = xH \end{aligned}$$

là một toàn cấu và được gọi là phép chiếu chính tắc.

Sau đây là một số tính chất đơn giản của đồng cấu.

Mệnh đề 1.83. *Cho $f : G \longrightarrow H$ là một đồng cấu. Khi đó*

(a) $f(e_G) = e_H$.

(b) $f(x^{-1}) = f(x)^{-1}$ *với mọi* $x \in G$.

(c) $f(x^n) = f(x)^n$ *với mọi* $n \in \mathbb{Z}$.

Chứng minh. (a) Ta có

$$f(e_G)f(e_G) = f(e_G e_G) = f(e_G) = e_H f(e_G).$$

Giản ước bên phải hai vế cho $f(e_G)$ ta có $f(e_G) = e_H$.

(b) Với x tùy ý thuộc G, theo (a) ta có

$$e_H = f(e_G) = f(x^{-1}x) = f(x^{-1})f(x)$$

và do đó $f(x^{-1}) = f(x)^{-1}$.

(c) Ta chứng minh bằng quy nạp theo n. Bởi (a), mệnh đề đúng khi $n = 0$. Giả sử mệnh đề đúng với $n = k \geq 0$. Ta có

$$f(x^{k+1}) = f(x^k x) = f(x^k)f(x),$$

bởi giả thiết quy nạp

$$f(x^{k+1}) = f(x^k)f(x) = f(x)^k f(x) = f(x)^{k+1}.$$

Do đó mệnh đề đúng với mọi số tự nhiên n. Bây giờ xét n là số nguyên âm, bởi (b),

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

Theo trên ta vừa chứng tỏ $f(x^{-n}) = f(x)^{-n}$, vì vậy

$$f(x^n) = (f(x)^{-n})^{-1} = f(x)^n$$

và ta có (c).

□

Mệnh đề 1.84. *Cho $f : G \longrightarrow H$ là một đồng cấu. Khi đó*

(a) *Nếu A là một nhóm con của G thì $f(A)$ là một nhóm con của H.*

(b) *Nếu B là một nhóm con của H thì $f^{-1}(B)$ là một nhóm con của G. Hơn nữa, nếu $B \triangleleft H$ thì $f^{-1}(B) \triangleleft G$.*

Chứng minh. (a) Ta có $e_G \in A$ vì A là một nhóm con, suy ra $e_H = f(e_G) \in f(A)$ và do đó $f(A)$ không rỗng. Xét hai phần tử tùy ý $y, y' \in f(A)$, khi đó có $x, x' \in A$ sao cho $y = f(x)$, $y' = f(x')$. Bởi Mệnh đề 1.83,

$$yy'^{-1} = f(x)f(x')^{-1} = f(x)f(x'^{-1}) = f(xx'^{-1})$$

và do đó $yy'^{-1} \in f(A)$ vì $xx'^{-1} \in A$. Vậy ta có (a).

(b) Ta có $f(e_G) = e_H \in B$ do B là một nhóm con, suy ra $e_G \in f^{-1}(B)$ và $f^{-1}(B)$ không rỗng. Xét hai phần tử tùy ý $x, x' \in f^{-1}(B)$, suy ra $f(x), f(x') \in B$. Ta có

$$f(xx'^{-1}) = f(x)f(x'^{-1}) = f(x)f(x')^{-1} \in B$$

vì B là một nhóm con, và do đó $xx'^{-1} \in f^{-1}(B)$. Vậy $f^{-1}(B)$ là một nhóm con của G. Giả sử $B \triangleleft H$, khi đó với bất kỳ $g \in G$, $x \in f^{-1}(B)$ thì

$$f(g^{-1}xg) = f(g^{-1})f(x)f(g) = f(g)^{-1}f(x)f(g) \in B$$

vì $B \triangleleft H$. Do đó $g^{-1}xg \in f^{-1}(B)$ và $f^{-1}(B) \triangleleft G$.

□

Một hệ quả hiển nhiên là

Hệ quả 1.85. *Cho $f : G \longrightarrow H$ là một đồng cấu. Khi đó*
(a) $\mathrm{Im}f = f(G)$ *là một nhóm con của* H.
(b) $\ker f = f^{-1}(e_H)$ *là một nhóm con chuẩn tắc của* G.

Mệnh đề 1.86. *Cho $f : G \longrightarrow H$ là một đồng cấu. Khi đó*
(a) f *là một toàn ánh khi và chỉ khi* $\mathrm{Im}f = H$.
(b) f *là một đơn ánh khi và chỉ khi* $\ker f = \{e_G\}$.

Chứng minh. (a) là hiển nhiên.

(b) Giả sử f là một đơn ánh và $x \in \ker f$. Khi đó $f(x) = e_H = f(e_G)$, suy ra $x = e_G$ và $\ker f = \{e_G\}$. Đảo lại, giả sử $\ker f = \{e_G\}$ và với $x, x' \in G$ mà $f(x) = f(x')$. Khi đó

$$f(xx'^{-1}) = f(x)f(x'^{-1}) = f(x)f(x')^{-1} = f(x')f(x')^{-1} = e_H$$

nên $xx'^{-1} \in \ker f = \{e_G\}$, vì thế $xx'^{-1} = e_G$ và $x = x'$. Vậy f là một đơn ánh.

□

Mệnh đề 1.87. *Cho $f : G \longrightarrow H$ và $g : H \longrightarrow K$ là hai đồng cấu. Khi đó $g \circ f$ cũng là một đồng cấu. Hơn nữa, nếu f, g lần lượt là các đơn cấu, toàn cấu, đẳng cấu thì $g \circ f$ cũng lần lượt là đơn cấu, toàn cấu, đẳng cấu.*

Chứng minh. Với mọi $x, x' \in G$ ta có

$$\begin{aligned} g \circ f(xx') &= g(f(xx')) \\ &= g(f(x)f(x')) \\ &= g(f(x))g(f(x')) \\ &= (g \circ f(x))(g \circ f(x')). \end{aligned}$$

Vậy $g \circ f$ là một đồng cấu. Các khẳng định còn lại là hiển nhiên.

□

Mệnh đề 1.88. *Nếu $f : G \longrightarrow H$ là một đẳng cấu thì f^{-1}cũng là một đẳng cấu.*

Chứng minh. Giả sử $f : G \longrightarrow H$ là một đẳng cấu. Khi đó f là một song ánh nên tồn tại ánh xạ ngược f^{-1} và f^{-1}cũng là một song ánh. Mệnh đề sẽ được chứng minh nếu ta chứng tỏ f^{-1}là một đồng cấu. Với bất kỳ $y, y' \in H$, do f là một song ánh nên tồn tại duy nhất $x, x' \in G$ sao cho $f(x) = y$, $f(x') = y'$. Vì $f(xx') = f(x)f(x') = yy'$ nên

$$f^{-1}(yy') = xx' = f^{-1}(y)f^{-1}(y')$$

và mệnh đề được chứng minh.

□

Định nghĩa 1.89. Ta nói hai nhóm G và H là *đẳng cấu*, ký hiệu $G \cong H$, nếu có một đẳng cấu f từ G đến H.

Mệnh đề 1.90. *Quan hệ đẳng cấu là một quan hệ tương đương trên lớp các nhóm.*

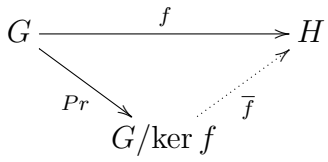
Chứng minh. Với bất kỳ nhóm G cho trước thì $id : G \longrightarrow G$ là một đẳng cấu, do đó $G \cong G$. Giả sử G, H là hai nhóm và $G \cong H$, khi đó có $f : G \longrightarrow H$ là một đẳng cấu. Theo Mệnh đề 1.88 thì $f^{-1} : H \longrightarrow G$ là một đẳng cấu nên $H \cong G$. Nếu G, H, K là ba nhóm và $G \cong H$, $H \cong K$ thì có các đẳng cấu $f : G \longrightarrow H$ và $g : H \longrightarrow K$. Bởi Mệnh đề 1.87, $g \circ f : G \longrightarrow K$ là một đẳng cấu và $G \cong K$. Vậy quan hệ đẳng cấu là một quan hệ tương đương.

□

Từ giờ trở đi ta sẽ không phân biệt hai nhóm nếu như chúng đẳng cấu với nhau. Bài toán phân loại lớp các nhóm sai khác một đẳng cấu là bài toán khó và quan trọng trong lý thuyết nhóm.

Định lý 1.91. *Giả sử $f : G \longrightarrow H$ là một đồng cấu và $\mathrm{Pr} : G \longrightarrow G/\ker f$ là phép chiếu chính tắc. Khi đó*

(a) *Có duy nhất một đồng cấu $\overline{f} : G/\ker f \longrightarrow H$ sao cho biểu đồ*



giao hoán, tức là $\overline{f} \circ Pr = f$.

(b) $\overline{f}$ *là một đơn cấu và* $\operatorname{Im}\overline{f} = \operatorname{Im} f$.

Chứng minh. (a) Trước hết ta chứng tỏ sự tồn tại của $\overline{f}$. Định nghĩa

$$\begin{aligned} \overline{f} : G/\ker f &\longrightarrow H, \\ x\ker f &\longmapsto f(x) \end{aligned}$$

ta chứng minh định nghĩa trên là đúng đắn, tức là nếu $x\ker f = x'\ker f$ thì $f(x) = f(x')$. Thật vậy, từ $x\ker f = x'\ker f$ suy ra có $a \in \ker f$ sao cho $x = x'a$, và do đó

$$f(x) = f(x'a) = f(x')\, f(a) = f(x')\, e_H = f(x').$$

Tiếp theo ta chứng tỏ $\overline{f}$ là một đồng cấu. Với bất kỳ $x\ker f, x'\ker f \in G/\ker f$ thì

$$\begin{aligned} \overline{f}(x\ker f \cdot x'\ker f) &= \overline{f}(xx'\ker f) \\ &= f(xx') \\ &= f(x)\, f(x') \\ &= \overline{f}(x\ker f)\overline{f}(x'\ker f). \end{aligned}$$

Hơn nữa, với mọi $x \in G$ ta có

$$\overline{f} \circ \operatorname{Pr}(x) = \overline{f}(\operatorname{Pr}(x)) = \overline{f}(x\ker f) = f(x),$$

suy ra $\overline{f} \circ \operatorname{Pr} = f$. Cuối cùng, ta chứng minh tính duy nhất của đồng cấu $\overline{f}$. Giả sử có đồng cấu $g : G/\ker f \to H$ sao cho $g \circ \operatorname{Pr} = f$, ta chứng tỏ $g = \overline{f}$. Với mọi $x\ker f \in G/\ker f$ thì

$$g(x\ker f) = g(\operatorname{Pr}(x)) = g \circ \operatorname{Pr}(x) = f(x) = \overline{f}(x\ker f)$$

và $g = \overline{f}$.

(b) Với mỗi $x\ker f \in \ker\overline{f}$ thì $\overline{f}(x\ker f) = f(x) = e_H$, suy ra $x \in \ker f$ và $x\ker f = \ker f$. Vậy $\ker\overline{f} = \{\ker f\}$, theo Mệnh đề 1.86 thì $\overline{f}$ là một đơn cấu. Vì Pr là một toàn cấu nên ta có $\operatorname{Im}\operatorname{Pr} = G/\ker f$. Mặt khác, $\overline{f} \circ \operatorname{Pr} = f$ suy ra

$$\operatorname{Im} f = f(G) = \overline{f} \circ \operatorname{Pr}(G) = \overline{f}(\operatorname{Pr}(G)) = \overline{f}(G/\ker f) = \operatorname{Im}\overline{f}.$$

Vậy ta có điều phải chứng minh.

□

Hệ quả 1.92. (Định lý đẳng cấu thứ nhất) *Giả sử* $f : G \to H$ *là một đồng cấu. Khi đó*

$$G/\ker f \cong \operatorname{Im} f.$$

Ví dụ 1.93. (a) Xét ánh xạ $x \in \mathbb{R}^* \longmapsto f(x) \in \{\pm 1\}$ từ nhóm nhân các số thực khác không đến nhóm nhân $\{\pm 1\}$ với

$$f(x) = \begin{cases} 1 & \text{nếu } x > 0 \\ -1 & \text{nếu } x < 0. \end{cases}$$

Hiển nhiên f là một đồng cấu, hơn nữa nó là một toàn cấu có $\ker f = \mathbb{R}^+$. Khi đó theo Hệ quả 1.92 thì $\mathbb{R}^*/\mathbb{R}^+ \cong \{\pm 1\}$.

(b) Cho trước số tự nhiên n ($n \geq 2$). Xét ánh xạ f từ nhóm cộng $\mathbb{Z}$ các số nguyên đến nhóm nhân $\mathbb{C}^*$ các số phức khác không được xác định như sau:

$$f(h) = \cos\frac{2h\pi}{n} + i\sin\frac{2h\pi}{n}$$

với mọi $h \in \mathbb{Z}$. Cho $h, k \in \mathbb{Z}$ ta có

$$\begin{aligned} f(h+k) &= \cos\frac{2(h+k)\pi}{n} + i\sin\frac{2(h+k)\pi}{n} \\ &= (\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n})^{h+k} \quad \text{(bởi công thức Moirve)} \\ &= (\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n})^{h}(\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n})^{k} \\ &= (\cos\frac{2h\pi}{n} + i\sin\frac{2h\pi}{n})(\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}) \\ &= f(h)f(k), \end{aligned}$$

do đó f là một đồng cấu. $f(\mathbb{Z})$ là các căn bậc n của đơn vị và $\ker f = n\mathbb{Z}$. Khi đó $f(\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$, tức là nhóm nhân các căn bậc n của đơn vị đẳng cấu với nhóm cộng các số nguyên mod n.

Mệnh đề 1.94. *Cho G là một nhóm cyclic. Khi đó*

(a) *Nếu $|G| = \infty$ thì $G \cong \mathbb{Z}$.*

(b) *Nếu $|G| = n$ thì $G \cong \mathbb{Z}_n$.*

Chứng minh. Giả sử $G = \langle a \rangle$ là nhóm cyclic được sinh ra bởi phần tử a. Xét ánh xạ

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow G. \\ m &\longmapsto a^m \end{aligned}$$

f là một đồng cấu vì với $m, m' \in \mathbb{Z}$ ta có

$$f(m+m') = a^{m+m'} = a^m a^{m'} = f(m)\, f(m').$$

Hơn nữa, f là một toàn cấu và theo Hệ quả 1.92 thì $\mathbb{Z}/\ker f \cong G$.

(a) Nếu $|G| = \infty$ thì $|a| = \infty$. Ta có $m \in \ker f$ khi và chỉ khi $a^m = e$. Bởi định nghĩa cấp của a thì $m = 0$. Vậy $\ker f = \{0\}$ và $\mathbb{Z} = \mathbb{Z}/\ker f \cong G$.

(b) Nếu $|G| = n$ thì $|a| = n$. Ta có $m \in \ker f$ khi và chỉ khi $a^m = e$. Theo Hệ quả 1.34 thì m là một bội số của n. Do đó $\ker f = n\mathbb{Z}$ và $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\ker f \cong G$.

□

Định lý 1.95. (Cayley) *Cho G là một nhóm. Khi đó có một đơn cấu từ G đến S_G. Nói cách khác, G đẳng cấu với một nhóm con của nhóm đối xứng S_G.*

Chứng minh. Với mỗi $a \in G$ ta định nghĩa ánh xạ $l_a : G \longrightarrow G$ như sau: $l_a(x) = ax$ với mọi $x \in G$, l_a gọi là phép tịnh tiến trái. Ta chứng tỏ l_a là một song ánh. Thật vậy, với $y \in G$ tùy ý cho trước thì phương trình $ax = y$ có nghiệm duy nhất $x = a^{-1}y$. Như vậy l_a là một hoán vị của các phần tử trong G nên là phần tử trong S_G. Bây giờ ta chứng tỏ ánh xạ $l : G \longrightarrow S_G$ được xác định bởi $l(a) = l_a$ với mọi $a \in G$ là một đồng cấu. Thật vậy, với $a, a' \in G$ tùy ý ta có

$$l(aa')(x) = l_{aa'}(x) = (aa')x = a(a'x) = l_a \circ l_{a'}(x)$$

với mọi $x \in G$, và do đó $l(aa') = l_a \circ l_{a'}$. Hơn nữa, l là một đơn ánh vì $a \in \ker l$ khi và chỉ khi l_a là hoán vị đồng nhất, điều này có nghĩa là $a = e$, tức là $\ker l = \{e\}$. Định lý được chứng minh.

□

Ta xét trường hợp đặc biệt khi G là một nhóm hữu hạn có n phần tử. Vì S_G đẳng cấu với S_n nên ta có

Hệ quả 1.96. *Cho G là một nhóm hữu hạn có n phần tử. Khi đó G đẳng cấu với một nhóm con của nhóm đối xứng S_n.*

Bài tập

1. Giả sử $f : G \longrightarrow H$ là một đồng cấu từ nhóm hữu hạn G đến nhóm H. Chứng tỏ
   (a) Với mọi $a \in G$ thì cấp của $f(a)$ chia hết cấp của a.
   (b) Cấp của $f(G)$ chia hết cấp của G.
2. Ánh xạ f nào dưới đây là một đồng cấu, trong trường hợp f là một đồng cấu hãy xác định $\ker f$.
   (a) $f : GL(2, \mathbb{R}) \longrightarrow \mathbb{R}^*$, ở đây $f(A) = \det A$.
   (b) $f : S_4 \longrightarrow \mathbb{Z}_2$, ở đây

$$f(\sigma) = \begin{cases} 0 & \text{nếu } \sigma \text{ là hoán vị chẵn} \\ 1 & \text{nếu } \sigma \text{ là hoán vị lẻ} \end{cases}$$

(c) $f : G \longrightarrow G$, ở đây G là một nhóm tùy ý, và $f(x) = x^{-1}$.

(d) $f : \mathbb{Z}_6 \longrightarrow \mathbb{Z}_3$, ở đây $f(\overline{x}) = \overline{x}$.

3. Tìm một đồng cấu không tầm thường (nếu có) trong các trường hợp sau.

(a) $f : \mathbb{Z}_9 \longrightarrow \mathbb{Z}_{20}$ (b) $f : \mathbb{Z}_{10} \longrightarrow \mathbb{Z}_8$

(c) $f : \mathbb{Z} \longrightarrow \mathbb{Z}_6$ (d) $f : D_4 \longrightarrow S_5$

4. Xác định đồng cấu f trong mỗi trường hợp sau:

(a) $f : \mathbb{Q} \longrightarrow \mathbb{Z}$ (b) $f : \mathbb{Z} \longrightarrow \mathbb{Z}$

5. Xác định đồng cấu f trong mỗi trường hợp sau:

(a) $f : \mathbb{Z}_5 \longrightarrow \mathbb{Z}_{10}$ (b) $f : S_3 \longrightarrow \mathbb{Z}_6$

6. Chứng minh rằng ảnh của một nhóm cyclic bởi một đồng cấu là cyclic.

7. Cho G là một nhóm và H là một tập hợp có phép toán. Giả sử có một song ánh $f : G \longrightarrow H$ thỏa mãn $f(ab) = f(a)f(b)$ với mọi $a, b \in G$. Chứng minh rằng H cũng là một nhóm với phép toán đã cho; hơn nữa nếu G giao hoán thì H là giao hoán, G cyclic thì H là cyclic.

8. Chứng tỏ các nhóm thương sau đều là cyclic và do đó đẳng cấu với nhóm $\mathbb{Z}_n$ với số nguyên n nào đó. Trong mỗi trường hợp hãy tìm số n này.

(a) $\mathbb{Z}_6/\left\langle\overline{3}\right\rangle$ (b) $\mathbb{Z}_{12}/\left\langle\overline{8}\right\rangle$ (c) $\mathbb{Z}_{15}/\left\langle\overline{10}\right\rangle$ (d) S_5/A_5

9. Đặt S^1 là tập hợp các số phức có mô-đun bằng 1. Chứng tỏ

(a) S^1 là một nhóm con của nhóm $\mathbb{C}^*$.

(b) Nhóm thương $\mathbb{R}/\mathbb{Z}$ đẳng cấu với nhóm S^1.

10. Chứng tỏ $H = \{(1), (12)(34), (13)(24), (14)(23)\}$là nhóm con chuẩn tắc trong A_4 và nhóm thương A_4/H đẳng cấu với $\mathbb{Z}_3$.

11. Đặt R có thể là $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Chứng tỏ $SL(n, R)$ tập hợp gồm các ma trận trong $GL(n, R)$ có định thức bằng 1 là một nhóm con chuẩn tắc của $GL(n, R)$ và nhóm thương $GL(n, R)/SL(n, R)$ đẳng cấu với R^* nhóm nhân các phần tử khác không trong R.

12. Chứng tỏ $\mathbb{Z}_4$ và 4-nhóm Klein là không đẳng cấu.

13. Chứng tỏ nhóm thay phiên A_4 chứa một nhóm con đẳng cấu với 4-nhóm Klein.

14. Chứng tỏ $U(14)$ và $U(18)$ là đẳng cấu.

15. Chứng tỏ D_3 đẳng cấu với S_3.

16. Chứng tỏ $GL(2, \mathbb{Z}_2)$ đẳng cấu với S_3.

17. Chứng tỏ D_4 và Q_8 là không đẳng cấu.

18. Ký hiệu Aut (G) là tập hợp tất cả các tự đẳng cấu của nhóm G. Chứng tỏ Aut(G) là một nhóm với phép hợp thành các ánh xạ.

19. Cho G là một nhóm cyclic có cấp n. Chứng tỏ Aut(G) đẳng cấu với $U(n)$.

20. Xác định Aut$(\mathbb{Z})$, Aut$(\mathbb{Z}_{10})$.

21. Chứng tỏ Aut$(\mathbb{Z}_p)$ đẳng cấu với $\mathbb{Z}_{p-1}$, ở đây p là số nguyên tố.

22. Cho V là 4-nhóm Klein. Chứng tỏ Aut(V) đẳng cấu với $GL(2, \mathbb{Z}_2)$.

23. Chứng tỏ $\mathrm{Aut}(S_3)$ đẳng cấu với S_3.
24. Chứng tỏ $\mathrm{Aut}(D_4)$ đẳng cấu với D_4.
25. Chứng tỏ $\mathrm{Aut}(Q_8)$ đẳng cấu với S_4.
26. Cho nhóm G và $a \in G$, ký hiệu C_a là ánh xạ từ G đến chính nó được xác định bởi $C_a(x) = a^{-1}xa$ với mọi $x \in G$.
    (a) Chứng tỏ C_a là một tự đẳng cấu, gọi là tự đẳng cấu trong.
    (b) Ký hiệu $\mathrm{Inn}(G)$ là tập hợp tất cả các tự đẳng cấu trong của G. Chứng tỏ $\mathrm{Inn}(G)$là một nhóm con chuẩn tắc của $\mathrm{Aut}(G)$.
    (c) Chứng tỏ $\mathrm{Inn}(G)$ đẳng cấu với $G/Z(G)$.
27. Chứng tỏ $\mathrm{Inn}(S_3)$ đẳng cấu với S_3.
28. Chứng tỏ $\mathrm{Inn}(Q_8)$ đẳng cấu với 4-nhóm Klein.
29. (Định lý đẳng cấu thứ hai) Cho N là một nhóm con chuẩn tắc của nhóm G và H là nhóm con tùy ý của G. Chứng tỏ HN là một nhóm con của G và $H \cap N$ là một nhóm con chuẩn tắc của H. Khi đó hãy chứng minh

$$H/(H \cap N) \cong HN/N.$$

30. (Định lý đẳng cấu thứ ba) Cho M và N là hai nhóm con chuẩn tắc của nhóm G và N là một nhóm con của M. Chứng tỏ

$$(G/N)/(M/N) \cong G/M.$$

Chương 2

NHÓM ABEL HỮU HẠN SINH

Trong chương này chúng ta sẽ tìm hiểu nhóm Abel hữu hạn sinh, tức là nhóm Abel được sinh ra bởi một tập hợp hữu hạn. Kết quả chính ở đây là chứng tỏ một nhóm Abel hữu hạn sinh đẳng cấu với tích trực tiếp của hữu hạn các nhóm cyclic.

2.1 Tích trực tiếp của các nhóm

Mệnh đề 2.1. *Cho H và K là hai nhóm. Trên tích Descartes $H \times K$ ta định nghĩa phép toán theo từng thành phần*

$$(h,k)(h',k') = (hh',kk')$$

với mọi $(h,k),(h',k') \in H \times K$. Khi đó $H \times K$ là một nhóm.

Chứng minh. Cho $(h,k),(h',k'),(h'',k'') \in H \times K$, sử dụng tính kết hợp trong H và K ta có

$$\begin{aligned}
[(h,k)(h',k')](h'',k'') &= (hh',kk')\,(h'',k'') \\
&= ((hh')h'',(kk')k'') \\
&= (h(h'h''),k(k'k'')) \\
&= (h,k)\,(h'h'',k'k'') \\
&= (h,k)\,[(h',k')(h'',k'')].
\end{aligned}$$

Lấy e_H và e_K lần lượt là các đơn vị trong H và K. Với bất kỳ $(h,k) \in H \times K$ hiển nhiên ta có

$$(h,k)(e_H,e_K) = (h,k) = (e_H,e_K)(h,k),$$

do đó (e_H,e_K) là đơn vị trong $H \times K$.

Với bất kỳ $(h,k) \in H \times K$, lấy h^{-1} là nghịch đảo của h trong H và k^{-1} nghịch đảo của k trong K. Ta có

$$(h,k)(h^{-1},k^{-1}) = (e_H, e_K) = (h^{-1},k^{-1})(h,k),$$

do đó (h^{-1}, k^{-1}) là nghịch đảo của (h,k). Vậy $H \times K$ là một nhóm.

□

Định nghĩa 2.2. Giả sử H và K là hai nhóm. Khi đó nhóm $H \times K$ với phép toán được định nghĩa như trong mệnh đề trên gọi là *tích trực tiếp* của H và K.

Khi H và K là hai nhóm hữu hạn, rõ ràng rằng $|H \times K| = |H|\,|K|$. Nếu H và K là những nhóm không tầm thường thì cấp của $H \times K$ khác với cấp của H và cấp của K, do đó không đẳng cấu với nhóm H cũng như nhóm K. Vậy tích trực tiếp là cách để cấu tạo những nhóm mới.

Một cách tổng quát ta có thể cấu tạo tích trực tiếp cho tùy ý các nhóm. Tuy nhiên ở đây ta chỉ trình bày cho tích trực tiếp hữu hạn các nhóm. Mệnh đề sau được chứng minh tương tự như Mệnh đề 2.1.

Mệnh đề 2.3. *Cho $G_1, G_2, ..., G_n$ là các nhóm. Khi đó $G_1 \times G_2 \times \cdots \times G_n$ là một nhóm với phép toán theo từng thành phần*

$$(x_1, x_2, \ldots, x_n)(y_1, y_2, \ldots, y_n) = (x_1y_1, x_2y_2, \ldots, x_ny_n),$$

trong đó tích x_iy_i là phép toán trong G_i. Nhóm $G_1 \times G_2 \times \cdots \times G_n$ được gọi là tích trực tiếp *của n nhóm.*

Mệnh đề 2.4. *Cho H và K là hai nhóm. Khi đó $H \times K \cong K \times H$.*

Chứng minh. Xét ánh xạ $f : H \times K \longrightarrow K \times H$ được định nghĩa bởi $f(h,k) = (k,h)$ với mọi $(h,k) \in H \times K$. Khi đó dễ thấy rằng f là một song ánh và đồng cấu nên là một đẳng cấu.

□

Từ mệnh đề trên ta có hệ quả sau mà chứng minh của nó dành cho bạn đọc.

Mệnh đề 2.5. *Cho $G_1, G_2, ..., G_n$ là các nhóm và σ một hoán vị của tập hợp $\{1, 2, \ldots, n\}$. Khi đó*

$$G_{\sigma(1)} \times G_{\sigma(2)} \times \cdots \times G_{\sigma(n)} \cong G_1 \times G_2 \times \cdots \times G_n.$$

Mệnh đề 2.6. *Cho H và K là hai nhóm. Khi đó $H \times K$ là một nhóm giao hoán khi và chỉ khi H và K đều giao hoán.*

Chứng minh. Lấy $(h,k), (h',k') \in H \times K$, ta có

$$(h,k)(h',k') = (hh', kk') \text{ và } (h',k')(h,k) = (h'h, k'k).$$

Vì vậy

$$(h,k)(h',k') = (h',k')(h,k)$$

nếu và chỉ nếu $hh' = h'h$ đối với các phần tử trong H và $kk' = k'k$ đối với các phần tử trong K.

□

Mệnh đề 2.7. *Cho $G = H \times K$ là tích trực tiếp của hai nhóm H và K. Khi đó*
(a) *$\hat{H} = \{(h, e_K) \mid h \in H\}$ và $\hat{K} = \{(e_H, k) \mid k \in K\}$ là hai nhóm con của G.*
(b) *$G = \hat{H}\hat{K}$, $\hat{H} \cap \hat{K} = \{(e_H, e_K)\}$ và bất kỳ $\hat{x} \in \hat{H}$, $\hat{y} \in \hat{K}$ thì $\hat{x}\hat{y} = \hat{y}\hat{x}$.*
(c) *$H \cong \hat{H}$, $K \cong \hat{K}$.*

Chứng minh. (a) Rõ ràng $\hat{H}$ không rỗng. Nếu (h, e_K), $(h', e_K) \in \hat{H}$ thì

$$(h, e_K)(h', e_K)^{-1} = (h, e_K)(h'^{-1}, e_K) = (hh'^{-1}, e_K) \in \hat{H}.$$

Do đó $\hat{H}$ là một nhóm con của G. Tương tự $\hat{K}$ cũng là một nhóm con của G.

(b) Một phần tử bất kỳ (h, k) của G luôn được viết ở dạng $(h, e_K)(e_{H,}k)$, vì thế $G = \hat{H}\hat{K}$. Hiển nhiên $\hat{H} \cap \hat{K} = \{(e_H, e_K)\}$. Bây giờ cho $\hat{h} = (h, e_K) \in \hat{H}$ và $\hat{k} = (e_H, k) \in \hat{K}$, khi đó

$$\hat{h}\hat{k} = (h, e_K)(e_H, k) = (h, k) = (e_H, k)(h, e_K) = \hat{k}\hat{h}.$$

(c) Ánh xạ $f : H \longrightarrow \hat{H}$ được định nghĩa bởi $f(h) = (h, e_K)$ với mọi $h \in H$ rõ ràng là một đẳng cấu. Tương tự ta cũng có K đẳng cấu với $\hat{K}$.

□

Như chiều ngược lại ta có

Định lý 2.8. *Cho G là một nhóm với hai nhóm con H và K sao cho $G = HK$, $H \cap K = \{e\}$, và mỗi phần tử của H giao hoán với các phần tử của K. Khi đó $G \cong H \times K$.*

Chứng minh. Trước hết ta chứng tỏ với bất kỳ $g \in G$ thì có duy nhất $h \in H$, $k \in K$ sao cho $g = hk$. Vì $G = HK$ nên có $h \in H$, $k \in K$ để $g = hk$. Nếu có $h' \in H$, $k' \in K$ sao cho $g = h'k'$ thì từ $hk = h'k'$ ta suy ra $h'^{-1}h = k'k^{-1} \in H \cap K$. Do $H \cap K = \{e\}$ nên $h'^{-1}h = k'k^{-1} = e$, và vì thế $h = h'$, $k = k'$.

Bây giờ xét ánh xạ $f : G \longrightarrow H \times K$ được định nghĩa bởi $f(g) = (h, k)$, ở đây $g = hk \in G$. Vì với mỗi cặp $(h, k) \in H \times K$ xác định duy nhất một phần tử $g = hk \in G$ nên f là một song ánh. Tiếp theo ta chứng tỏ f là một đồng cấu. Bất kỳ $g = hk$ và $g' = h'k'$ là hai phần tử tùy ý trong G, khi đó

$$\begin{aligned} f(gg') &= f(hkh'k') = f(hh'kk') \\ &= (hh', kk') = (h, k)(h'k') \\ &= f(g)f(g'). \end{aligned}$$

Vậy f là một đẳng cấu và ta có điều phải chứng minh.

□

Chú ý rằng nếu $G = HK$ và mỗi phần tử của H giao hoán với các phần tử của K thì rõ ràng H và K là hai nhóm con chuẩn tắc của G. Ngược lại, nếu H và K là hai nhóm con chuẩn tắc của G và $H \cap K = \{e\}$ thì mỗi phần tử của H giao hoán với các phần tử của K. Thật vậy, nếu $h \in H$ và $k \in K$ thì

$$h^{-1}k^{-1}hk = h^{-1}(k^{-1}hk) = (h^{-1}k^{-1}h)k \in H \cap K.$$

Do $H \cap K = \{e\}$ nên $h^{-1}k^{-1}hk = e$, suy ra $hk = kh$. Vì vậy ta có thể phát biểu lại Định lý 2.8 như sau.

Hệ quả 2.9. *Cho G là một nhóm với hai nhóm con chuẩn tắc H và K sao cho $G = HK$, $H \cap K = \{e\}$. Khi đó $G \cong H \times K$.*

Giả thiết của Định lý 2.8 nói rằng $G = HK$. Khi G là một nhóm hữu hạn, nếu có $|G| = |HK|$ thì ta suy ra $G = HK$. Do đó việc đếm số phần tử của tập hợp HK là cần thiết.

Mệnh đề 2.10. *Nếu H và K là hai nhóm con hữu hạn của nhóm G thì $|HK| = |H|\,|K| \,/\, |H \cap K|$.*

Chứng minh. Đặt $s = [H : H \cap K]$ và s lớp kề trái khác nhau của $H \cap K$ trong H là $h_1 (H \cap K), \ldots, h_s (H \cap K)$. Theo Định lý Lagrange ta có

$$s = [H : H \cap K] = |H| \,/\, |H \cap K|.$$

Mệnh đề sẽ được chứng minh nếu ta chứng tỏ $|HK| = s\,|K|$. Thật vậy, ta thấy rằng các lớp kề trái $h_1K, \ldots, h_sK$ là khác nhau vì nếu $h_iK = h_jK$ với $i \neq j$ thì $h_i^{-1}h_j \in K$, và do đó thuộc $H \cap K$, điều này mâu thuẫn với cách chọn $h_1, \ldots, h_s$. Với bất kỳ $hk \in HK$ thì có $1 \leq i \leq s$ sao cho $h \in h_i (H \cap K)$, và $hk \in h_iK$. Vậy các h_iK, $1 \leq i \leq s$ là một phân hoạch của HK, mỗi h_iK có đúng $|K|$ phần tử, do đó $|HK| = s\,|K|$ và ta có điều cần chứng minh.

□

Bây giờ ta sẽ tính cấp của một phần tử trong tích trực tiếp của hữu hạn các nhóm.

Mệnh đề 2.11. *Cho H, K là hai nhóm và $(h, k) \in H \times K$. Nếu h, k có cấp hữu hạn thì (h, k) cũng có cấp hữu hạn và*

$$|(h, k)| = \operatorname{lcm}(|h|, |k|)$$

là bội số chung nhỏ nhất của $|h|$ và $|k|$.

Chứng minh. Đặt $r = \text{lcm}(|h|,|k|)$. Khi đó

$$(h,k)^r = (h^r, k^r) = (e_H, e_K)$$

vì $|h| \mid r$ và $|k| \mid r$. Do đó (h,k) có cấp hữu hạn, đặt $n = |(h,k)|$ ta suy ra $n \mid r$. Mặt khác, vì

$$(h^n, k^n) = (h,k)^n = (e_H, e_K)$$

ta suy ra $h^n = e_H$ và $k^n = e_K$, do đó n là bội số chung của $|h|$ và $|k|$ nên $r \mid n$. Vậy $r = n$ và mệnh đề được chứng minh.

□

Hệ quả 2.12. *Cho $G = G_1 \times \cdots \times G_n$ là tích trực tiếp của hữu hạn các nhóm và $(a_1, a_2, \ldots, a_n) \in G$. Nếu $a_1, a_2, \ldots, a_n$ có cấp hữu hạn thì $(a_1, a_2, \ldots, a_n)$ cũng có cấp hữu hạn và*

$$|(a_1, a_2, \ldots, a_n)| = \text{lcm}(|a_1|, |a_2|, \ldots, |a_n|).$$

Chứng minh. Chứng minh quy nạp theo n. Trong trường hợp $n = 2$, theo Mệnh đề 2.11 thì hệ quả đúng. Giả sử hệ quả đúng đối với tích trực tiếp của $n = k$ nhóm. Ta chứng minh hệ quả đúng đối với tích trực tiếp

$$G_1 \times \cdots \times G_k \times G_{k+1} = (G_1 \times \cdots \times G_k) \times G_{k+1}$$

của $n = k + 1$ nhóm. Thật vậy, theo Mệnh đề 2.11 ta có

$$\begin{aligned} |(a_1, a_2, \ldots, a_k, a_{k+1})| &= \text{lcm}(|(a_1, a_2, \ldots, a_k)|, |a_{k+1}|) \\ &= \text{lcm}(\text{lcm}(|a_1|, |a_2|, \ldots, |a_k|), |a_{k+1}|) \\ &= \text{lcm}(|a_1|, |a_2|, \ldots, |a_k|, |a_{k+1}|). \end{aligned}$$

Vậy hệ quả được chứng minh.

□

Ví dụ 2.13. Ta tìm cấp của phần tử $(\overline{10}, \overline{4})$ trong $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$. Trong $\mathbb{Z}_{12}$ ta có $\overline{10} = 10\overline{1}$ và do đó $\left|\overline{10}\right| = 12/\gcd(12,10) = 6$. Trong $\mathbb{Z}_{18}$ ta có $\overline{4} = 4\overline{1}$ và do đó $\left|\overline{4}\right| = 18/\gcd(18,4) = 9$. Vậy theo Mệnh đề 2.11 thì $\left|(\overline{10}, \overline{4})\right| = \text{lcm}(6,9) = 18$.

Định lý 2.14. *Nhóm $\mathbb{Z}_m \times \mathbb{Z}_n$ đẳng cấu với nhóm cyclic $\mathbb{Z}_{mn}$ khi và chỉ khi m và n nguyên tố cùng nhau.*

Chứng minh. Nhận xét rằng nếu $(\overline{r}, \overline{s})$ là phần tử trong $\mathbb{Z}_m \times \mathbb{Z}_n$ thì $|\overline{r}| \mid m$ và $|\overline{s}| \mid n$. Do đó

$$|(\overline{r}, \overline{s})| = \text{lcm}(|\overline{r}|, |\overline{s}|) \leq \text{lcm}(m,n).$$

Mặt khác, trong $\mathbb{Z}_m$ ta có $\left|\overline{1}\right| = m$ và trong $\mathbb{Z}_n$ thì $\left|\overline{1}\right| = n$, vì thế $\left|(\overline{1}, \overline{1})\right| = \text{lcm}(m,n)$. Vậy $(\overline{1}, \overline{1})$ là phần tử có cấp lớn nhất trong $\mathbb{Z}_m \times \mathbb{Z}_n$.

Giả sử $\mathbb{Z}_{\mathrm{m}} \times \mathbb{Z}_{\mathrm{n}}$ đẳng cấu với $\mathbb{Z}_{mn}$ và do nó cyclic thì theo nhận xét trên $(\overline{1}, \overline{1})$ phải là một phần tử sinh, và ta có $\left|(\overline{1}, \overline{1})\right| = mn$. Mặt khác, từ Mệnh đề 2.11 ta có

$$\left|(\overline{1}, \overline{1})\right| = \operatorname{lcm}(m, n) = mn/\gcd(m, n)$$

và do đó $\gcd(m, n) = 1$, tức là m và n nguyên tố cùng nhau.

Đảo lại, nếu $\gcd(m, n) = 1$ thì

$$\left|(\overline{1}, \overline{1})\right| = \operatorname{lcm}(m, n) = mn/\gcd(m, n) = mn,$$

và $(\overline{1}, \overline{1})$ là phần tử sinh của $\mathbb{Z}_{\mathrm{m}} \times \mathbb{Z}_{\mathrm{n}}$. Vậy nó là cyclic và do đó đẳng cấu với $\mathbb{Z}_{\mathrm{mn}}$. □

Hệ quả 2.15. $\mathbb{Z}_{\mathrm{n_1}} \times \mathbb{Z}_{\mathrm{n_2}} \times \cdots \times \mathbb{Z}_{\mathrm{n_s}} \cong \mathbb{Z}_{\mathrm{n_1 n_2 \cdots n_s}}$ *khi và chỉ khi* $\gcd(n_i, n_j) = 1$ *với mọi* $1 \leq i < j \leq s$.

Chứng minh. Chứng minh quy nạp theo s. Với $s = 2$ thì hệ quả hiển nhiên đúng theo Định lý 2.14. Giả sử hệ quả đúng với $s = k$, nghĩa là

$$\mathbb{Z}_{\mathrm{n_1}} \times \mathbb{Z}_{\mathrm{n_2}} \times \cdots \times \mathbb{Z}_{\mathrm{n_k}} \cong \mathbb{Z}_{\mathrm{n_1 n_2 \cdots n_k}}$$

khi và chỉ khi $\gcd(n_i, n_j) = 1$ với mọi $1 \leq i < j \leq k$. Ta chứng minh hệ quả đúng với $s = k + 1$. Ta có

$$\mathbb{Z}_{\mathrm{n_1}} \times \cdots \times \mathbb{Z}_{\mathrm{n_k}} \times \mathbb{Z}_{\mathrm{n_{k+1}}} \cong \mathbb{Z}_{\mathrm{n_1 \cdots n_k}} \times \mathbb{Z}_{n_{k+1}}$$

bởi giả thiết quy nạp. Khi đó theo Định lý 2.14 ta có $\mathbb{Z}_{n_1 \cdots n_k} \times \mathbb{Z}_{n_{k+1}} \cong \mathbb{Z}_{n_1 \cdots n_k n_{k+1}}$ khi và chỉ khi $\gcd(n_1 \cdots n_k, n_{k+1}) = 1$. Vậy

$$\mathbb{Z}_{\mathrm{n_1}} \times \mathbb{Z}_{\mathrm{n_2}} \times \cdots \times \mathbb{Z}_{\mathrm{n_{k+1}}} \cong \mathbb{Z}_{\mathrm{n_1 n_2 \cdots n_{k+1}}}$$

khi và chỉ khi $\gcd(n_i, n_j) = 1$ với mọi $1 \leq i < j \leq k+1$ và hệ quả được chứng minh. □

Ví dụ 2.16. (a) Cho nhóm G có cấp bốn. Ta chứng tỏ G đẳng cấu với $\mathbb{Z}_4$ hoặc $\mathbb{Z}_2 \times \mathbb{Z}_2$. Nếu trong G có phần tử có cấp bốn thì G là cyclic nên đẳng cấu với $\mathbb{Z}_4$. Ngược lại, trong G không có phần tử có cấp bốn thì theo Định lý Lagrange các phần tử khác đơn vị đều có cấp hai. Lấy $a, b \in G$ khác đơn vị và $a \neq b$. Đặt $H = \langle a \rangle$ và $K = \langle b \rangle$ là hai nhóm con của G có cấp hai nên đẳng cấu với $\mathbb{Z}_2$ và vì có chỉ số hai nên là hai nhóm con chuẩn tắc trong G. Hơn nữa, $H \cap K = \{e\}$ và $G = HK$ vì $|HK| = |H|\,|K| \,/\, |H \cap K| = 2 \cdot 2/1 = 4 = |G|$, theo Hệ quả 2.9 ta có $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(b) Xét $(\mathbb{Z}_4 \times \mathbb{Z}_4)/\left\langle (\overline{1}, \overline{1}) \right\rangle$. Vì $|\mathbb{Z}_4 \times \mathbb{Z}_4| = 4 \cdot 4 = 16$ và $\left|\left\langle (\overline{1}, \overline{1}) \right\rangle\right| = \left|(\overline{1}, \overline{1})\right| = \operatorname{lcm}(4, 4) = 4$ nên

$$\left|(\mathbb{Z}_4 \times \mathbb{Z}_4)/\left\langle (\overline{1}, \overline{1}) \right\rangle\right| = 16/4 = 4,$$

và nó đẳng cấu với $\mathbb{Z}_4$ hoặc $\mathbb{Z}_2 \times \mathbb{Z}_2$. Nhưng vì phần tử $(\overline{1}, \overline{0}) + \langle(\overline{1}, \overline{1})\rangle$ có cấp 4, do đó nhóm là cyclic nên đẳng cấu với $\mathbb{Z}_4$.

(c) Xét hai nhóm nhân $U(8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ và $U(10) = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$. $U(8) \times U(10)$ là nhóm có cấp 16. Lấy H là một nhóm con của $U(8) \times U(10)$ được sinh ra bởi $(\overline{7}, \overline{3})$, ta có

$$H = \{(\overline{1}, \overline{1}), (\overline{7}, \overline{3}), (\overline{1}, \overline{9}), (\overline{7}, \overline{7})\},$$

và do đó $(U(8) \times U(10))/H$ là nhóm có cấp 4. Ta thấy rằng H, $(\overline{1}, \overline{3})H$, $(\overline{3}, \overline{3})H$, $(\overline{5}, \overline{3})H$ là 4 lớp kề khác nhau của H, do đó là tất cả các phần tử của nhóm thương, và vì

$$(\overline{1}, \overline{3})(\overline{1}, \overline{3}) = (\overline{3}, \overline{3})(\overline{3}, \overline{3}) = (\overline{5}, \overline{3})(\overline{5}, \overline{3}) = (\overline{1}, \overline{9}) \in H$$

nên

$$\left|(\overline{1}, \overline{3})H\right| = \left|(\overline{3}, \overline{3})H\right| = \left|(\overline{5}, \overline{3})H\right| = 2.$$

Theo (a) ta có $(U(8) \times U(10)/\langle(\overline{7}, \overline{3})\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Bài tập

1. Tìm cấp của mỗi phần tử trong nhóm được cho trước trong các trường hợp sau.
   (a) $(\overline{15}, \overline{14}) \in \mathbb{Z}_{20} \times \mathbb{Z}_{27}$.
   (b) $(\overline{12}, \overline{5}) \in \mathbb{Z}_{20} \times U(12)$.
   (c) $((2, 3, 4), \overline{7}) \in A_4 \times U(12)$.
2. Xác định các lớp kề khác nhau của nhóm con trong nhóm được cho trước trong các trường hợp sau.
   (a) $\langle(\overline{4}, \overline{2})\rangle$ trong $\mathbb{Z}_{10} \times \mathbb{Z}_4$.
   (b) $\langle(9, 4)\rangle$ trong $3\mathbb{Z} \times 2\mathbb{Z}$.
   (c) $\langle(\overline{5}, \overline{5})\rangle$ trong $U(8) \times U(12)$.
3. Tìm cấp của mỗi phần tử trong nhóm thương được cho trước trong các trường hợp sau.
   (a) $(\overline{1}, \overline{1}) + \langle(\overline{4}, \overline{2})\rangle \in (\mathbb{Z}_{10} \times \mathbb{Z}_4)/\langle(\overline{4}, \overline{2})\rangle$.
   (b) $(3, 2) + \langle(6, 4)\rangle \in (3\mathbb{Z} \times 2\mathbb{Z})/\langle(6, 4)\rangle$.
   (c) $(\overline{7}, \overline{5})\langle(\overline{3}, \overline{5})\rangle \in (U(8) \times U(12))/\langle(\overline{3}, \overline{5})\rangle$.
4. Cho H và K là hai nhóm. Chứng tỏ $Z(H \times K) \cong Z(H) \times Z(K)$.
5. Tìm tâm và nhóm con giao hoán tử của $\mathbb{Z}_2 \times S_3$ và $S_3 \times D_4$.
6. Cho K là 4-nhóm Klein. Chứng tỏ $K \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
7. Chứng tỏ $(\mathbb{Z} \times \mathbb{Z})/\langle(1, 3)\rangle$ đẳng cấu với $\mathbb{Z}$.
8. Trong $\mathbb{Z}_2 \times \mathbb{Z}_4$ tìm một nhóm con đẳng cấu với $\mathbb{Z}_2 \times \mathbb{Z}_2$.
9. Trong D_4 tìm một nhóm con đẳng cấu với $\mathbb{Z}_2 \times \mathbb{Z}_2$.
10. Chứng tỏ $U(8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

11. Chứng tỏ $\mathbb{Z}_{n^2}$ không đẳng cấu với $\mathbb{Z}_n \times \mathbb{Z}_n$.
12. Cho G là một nhóm Abel có cấp p^2, ở đây p là số nguyên tố. Chứng tỏ G đẳng cấu với $\mathbb{Z}_{p^2}$ hoặc $\mathbb{Z}_p \times \mathbb{Z}_p$.
13. Cho m và n là hai số nguyên dương nguyên tố cùng nhau. Chứng tỏ $U(mn) \cong U(m) \times U(n)$.
14. Chứng tỏ $U(105) \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_6$.
15. Chứng tỏ hai trong các nhóm D_4, Q_8, $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ là không đẳng cấu.
16. Chứng tỏ A_4 và $\mathbb{Z}_2 \times S_3$ là không đẳng cấu.
17. (a) Xác định các đồng cấu từ $\mathbb{Z}_4$ đến $\mathbb{Z}_2 \times \mathbb{Z}_2$.
    (b) Xác định các đồng cấu từ $\mathbb{Z}_6$ đến $\mathbb{Z}_2 \times \mathbb{Z}_3$.

2.2 Tổng trực tiếp của các nhóm Abel

Trong phần còn lại của chương này ta luôn giả thiết G là một nhóm Abel với phép toán được viết theo lối cộng. Cho H và K là hai nhóm con của G, vì nhóm G là Abel nên H, K là hai nhóm con chuẩn tắc, và do đó $H + K$ là một nhóm con của G. Mỗi phần tử trong $H + K$ được biểu diễn ở dạng tổng $h + k$ với $h \in H$ và $k \in K$.

Định nghĩa 2.17. Giả sử G là một nhóm Abel và H, K hai nhóm con của G. Ta nói tổng $H + K$ là trực tiếp, ký hiệu $H \oplus K$, nếu mọi phần tử $x \in H + K$ đều có biểu diễn duy nhất ở dạng $x = h + k$, trong đó $h \in H$ và $k \in K$.

Mệnh đề 2.18. *Cho H và K là hai nhóm con của nhóm Abel G. Khi đó tổng $H+K$ là trực tiếp khi và chỉ khi $H \cap K = \{0\}$.*

Chứng minh. Giả sử tổng $H + K$ là trực tiếp. Với mỗi $x \in H \cap K$ ta có $x = x + 0 = 0 + x$, bởi tính duy nhất của biểu diễn ta suy ra $x = 0$ và do đó $H \cap K = \{0\}$. Đảo lại, giả sử $H \cap K = \{0\}$. Nếu $x \in H + K$ và x có hai biểu diễn $x = h + k = h' + k'$ với $h, h' \in H$, $k, k' \in K$, khi đó $h - h' = k' - k \in H \cap K$ nên $h - h' = k' - k = 0$, và do đó $h = h'$, $k = k'$. Mệnh đề được chứng minh.

□

Ví dụ 2.19. Trong $\mathbb{Z}_{12}$ lấy $H = \langle \overline{3} \rangle = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$ là nhóm con có cấp 4 và $K = \langle \overline{4} \rangle = \{\overline{0}, \overline{4}, \overline{8}\}$ là nhóm con có cấp 3. Chú ý rằng $H \cap K = \{\overline{0}\}$ và $H + K$ có cấp

$$|H + K| = |H|\,|K| \,/\, |H \cap K| = 4 \cdot 3/1 = 12,$$

do đó $\mathbb{Z}_{12} = \mathrm{H} + \mathrm{K}$. Vì $H \cap K = \{\overline{0}\}$ nên tổng là trực tiếp và ta có $\mathbb{Z}_{12} = H \oplus K$.

Khái niệm tổng trực tiếp cũng được mở rộng cho tùy ý các nhóm. Tuy nhiên ở đây ta chỉ trình bày cho hữu hạn các nhóm. Giả sử $H_1, H_2, \ldots, H_n$ là các nhóm con của

nhóm Abel G, khi đó các nhóm H_i đều là chuẩn tắc, và do đó tổng $H_1+H_2+\cdots+H_n$ gồm các phần tử có dạng $h_1+h_2+\cdots+h_n$ với $h_i \in H_i$ là một nhóm con của G.

Định nghĩa 2.20. Giả sử $H_1, H_2, \ldots, H_n$ là các nhóm con của một nhóm Abel G. Ta nói tổng $H_1+H_2+\cdots+H_n$ là trực tiếp, ký hiệu $H_1 \oplus H_2 \oplus \cdots \oplus H_n$, nếu mọi phần tử $x \in H_1+H_2+\cdots+H_n$ đều có biểu diễn duy nhất ở dạng $x = h_1+h_2+\cdots+h_n$, trong đó $h_i \in H_i$ với mọi $i = 1, \ldots, n$.

Mệnh đề 2.21. *Cho $H_1, H_2, \ldots, H_n$ là các nhóm con của một nhóm Abel G. Khi đó các khẳng định sau tương đương.*

(a) *Tổng $H_1+\cdots+H_n$ là trực tiếp.*

(b) $(H_1+H_2+\cdots+H_{i-1}) \cap H_i = \{0\}$ *với mọi* $i = 2, \ldots, n$.

(c) *Nếu $h_1+\cdots+h_n = 0$, trong đó $h_i \in H_i$ thì suy ra $h_i = 0$ với mọi $i = 1, \ldots, n$.*

Chứng minh. (a)⇒(b) Với mỗi $i = 2, \ldots, n$, lấy $x \in (H_1+H_2+\cdots+H_{i-1}) \cap H_i$, khi đó

$$x = h_1+h_2+\cdots+h_{i-1}$$

với $h_j \in H_j$, $1 \le j \le i-1$. Và vì $x \in H_i$, ta có 2 cách biểu diễn của $0 \in H_1+\cdots+H_n$ là

$$\begin{aligned} 0 &= h_1+h_2+\cdots+h_{i-1}+(-x)+0+\cdots+0 \\ &= 0+0+\cdots+0+0+0+\cdots+0. \end{aligned}$$

Từ định nghĩa về tổng trực tiếp ta suy ra rằng mỗi số hạng trong biểu diễn đầu tiên đều bằng 0 và do đó $x = 0$. Vậy ta có (b).

(b)⇒(c) Nếu $h_1+\cdots+h_n = 0$ với $h_i \in H_i$, ta cần chứng tỏ $h_i = 0$ với mọi i. Giả sử ngược lại, có chỉ số j sao cho $h_j \neq 0$. Gọi k là số nguyên lớn nhất, $1 \le k \le n$ sao cho $h_k \neq 0$. Vì vậy $h_{k+1} = \cdots = h_n = 0$, và $0 = h_1+\cdots+h_k$. Ta có

$$h_k = -h_1-\cdots-h_{k-1} \in (H_1+H_2+\cdots+H_{k-1}) \cap H_k = \{0\},$$

do đó $h_k = 0$. Mâu thuẫn này chứng tỏ không tồn tại k và vì thế $h_i = 0$ với mọi $i = 1, \ldots, n$.

(c)⇒(a) Nếu $x \in H_1+\cdots+H_n$ và x có hai cách biểu diễn $x = h_1+\cdots+h_n = h'_1+\cdots+h'_n$, trong đó $h_i, h'_i \in H_i$. Khi đó ta có

$$(h_i-h'_1)+\cdots+(h_n-h'_n) = 0$$

với $h_i-h'_i \in H_i$, do đó $h_i-h'_i = 0$ và suy ra $h_i = h'_i$ với mọi $i = 1, \ldots, n$.

□

Bây giờ ta chỉ ra rằng tổng trực tiếp và tích trực tiếp của một số hữu hạn các nhóm là đẳng cấu.

Mệnh đề 2.22. *Cho G là một nhóm Abel sao cho $G = H_1 \oplus \cdots \oplus H_n$. Khi đó*

$$G \cong H_1 \times \cdots \times H_n.$$

Chứng minh. Xét ánh xạ $f : H_1 \times \cdots \times H_n \longrightarrow G$ được xác định bởi

$$f(h_1, \ldots, h_n) = h_1 + \cdots + h_n$$

với mọi $(h_1, \ldots, h_n) \in H_1 \times \cdots \times H_n$. f là một đồng cấu vì

$$\begin{aligned} f((h_1, \ldots, h_n) + (h'_1, \ldots, h'_n)) &= f(h_1 + h'_1, \ldots, h_n + h'_n) \\ &= (h_1 + h'_1) + \cdots + (h_n + h'_n) \\ &= (h_1 + \cdots + h_n) + (h'_1 + \cdots + h'_n) \\ &= f(h_1, \ldots, h_n) + f(h'_1, \ldots, h'_n). \end{aligned}$$

Cho $y \in G$, khi đó có duy nhất các $h_i \in H_i$, $1 \leq i \leq n$ sao cho $y = h_1 + \cdots + h_n$ và $f(h_1, \ldots, h_n) = h_1 + \cdots + h_n = y$. Vậy f là một song ánh nên là một đẳng cấu.

□

Hệ quả 2.23. *Cho G là một nhóm Abel hữu hạn sao cho $G = H_1 \oplus \cdots \oplus H_n$ và $x = h_1 + \cdots + h_n \in G$, ở đây $h_i \in H_i$ với mọi $i = 1, \ldots, n$. Khi đó $|x| = \operatorname{lcm}(|h_1|, \ldots, |h_n|)$.*

Chứng minh. Bởi Mệnh đề 2.22, tương ứng

$$(h_1, \ldots, h_n) \in H_1 \times \cdots \times H_n \longmapsto x = h_1 + \cdots + h_n \in G$$

là một đẳng cấu. Do đó theo Hệ quả 2.12 thì

$$|x| = |(h_1, \ldots, h_n)| = \operatorname{lcm}(|h_1|, \ldots, |h_n|)$$

và hệ quả được chứng minh.

□

Bổ đề 2.24. *Cho G là một nhóm Abel sao cho $G = H_1 \oplus \cdots \oplus H_n$ và K_i là một nhóm con của H_i với mỗi $i = 1, \ldots, n$. Khi đó tổng $K_1 + \cdots + K_n$ là trực tiếp.*

Chứng minh. Xét $x \in K_1 + \cdots + K_n$ và giả sử x có hai biểu diễn $x = k_1 + \cdots + k_n = k'_1 + \cdots + k'_n$, $k_i, k'_i \in K_i$ với mọi $i = 1, \ldots, n$. Vì K_i là một nhóm con của H_i và $G = H_1 \oplus \cdots \oplus H_n$ nên $k_i = k'_i$ với mọi $i = 1, \ldots, n$.

□

Mệnh đề 2.25. *Cho G là một nhóm Abel sao cho $G = H_1 \oplus \cdots \oplus H_n$ và K_i là một nhóm con của H_i với mỗi $i = 1, \ldots, n$. Đặt $K = K_1 + \cdots + K_n$, khi đó*

$$G/K = G/(K_1 \oplus \cdots \oplus K_n) \cong H_1/K_1 \times \cdots \times H_n/K_n.$$

Chứng minh. Theo Bổ đề 2.24 thì $K = K_1 \oplus \cdots \oplus K_n$. Ta định nghĩa ánh xạ

$$f : G \longrightarrow H_1/K_1 \times \cdots \times H_n/K_n$$

được xác định bởi $f(x) = f(h_1 + \cdots + h_n) = (h_1 + K_1, \ldots, h_n + K_n)$ với $x = h_1 + \cdots + h_n$, $h_i \in H_i$, $i = 1, \ldots, n$. Vì phép biểu diễn của $x \in G$ theo các phần tử trong H_i là duy nhất nên ánh xạ trên được định nghĩa đúng đắn.

f là một đồng cấu vì với mọi $x = h_1 + \cdots + h_n$ và $x' = h'_1 + \cdots + h'_n \in G$ ta có

$$\begin{aligned} f(x + x') &= f((h_1 + h'_1) + \cdots + (h_n + h'_n)) \\ &= ((h_1 + h'_1) + K_1, \ldots, (h_n + h'_n) + K_n) \\ &= (h_1 + K_1, \ldots, h_n + K_n) + (h'_1 + K_1, \ldots, h'_n + K_n) \\ &= f(x) + f(x'). \end{aligned}$$

Chú ý rằng đơn vị của $H_1/K_1 \times \cdots \times H_n/K_n$ là $(K_1, \ldots, K_n)$. Vì vậy, $x = h_1 + \cdots + h_n \in \ker f$ khi và chỉ khi $h_i + K_i = K_i$, suy ra $h_i \in K_i$ với mọi $i = 1, \ldots, n$. Điều này tương đương với $x \in K_1 \oplus \cdots \oplus K_n$. Vậy $\ker f = K_1 \oplus \cdots \oplus K_n = K$. Hơn nữa, f là một toàn ánh và vì thế theo Hệ quả 1.92 ta có

$$G/K \cong H_1/K_1 \times \cdots \times H_n/K_n.$$

Vậy mệnh đề được chứng minh.

□

Bài tập

1. Tìm hai nhóm con thực sự không tầm thường H và K của nhóm G cho trước sao cho $G = H \oplus K$ trong các trường hợp sau.

   (a) $G = \mathbb{Z}_{15}$ (b) $G = \mathbb{Z}_{20}$ (c) $G = \mathbb{Z}_{36}$

2. Chứng tỏ không tồn tại hai nhóm con thực sự không tầm thường H và K của $\mathbb{Z}_{25}$ sao cho $\mathbb{Z}_{25} = H \oplus K$.
3. Tìm hai nhóm con thực sự không tầm thường H và K của nhóm G cho trước sao cho $G = HK$ trong các trường hợp sau.

   (a) $G = U(12)$ (b) $G = U(15)$

4. Chứng tỏ không tồn tại hai nhóm con thực sự không tầm thường H và K của $U(10)$ sao cho $U(10) = HK$.
5. Cho H và K là hai nhóm con của nhóm Abel G. Chứng tỏ $G = H \oplus K$ khi và chỉ khi có một đồng cấu $\varphi : G \longrightarrow H$ sao cho $\varphi(h) = h$ với mọi $h \in H$ và $\ker \varphi = K$.

6. Cho một nhóm Abel G và đồng cấu $\varphi : G \longrightarrow G$ sao cho $\varphi \circ \varphi = id_G$. Chứng tỏ $G \cong \mathrm{Im}\varphi \times \ker \varphi$.
7. Cho một nhóm G có cấp mn với m và n nguyên tố cùng nhau. Giả sử G có đúng một nhóm con H có cấp m và có đúng một nhóm con K có cấp n. Chứng tỏ $G \cong H \times K$.
8. Cho nhóm Abel $G = H \oplus K$ và A là một nhóm con của G chứa H. Chứng tỏ $A = H \oplus (K \cap A)$.
9. Cho nhóm Abel $G = H \oplus K$. Chứng tỏ $G/H \cong K$.

2.3 Nhóm Abel hữu hạn

Trong phần này chúng ta sẽ chỉ ra rằng một nhóm Abel hữu hạn đẳng cấu với tích trực tiếp của các nhóm cyclic có cấp là lũy thừa của các số nguyên tố. Trước hết ta cần bổ đề sau.

Bổ đề 2.26. *Cho G là một nhóm Abel hữu hạn và số nguyên tố p là một ước số của $|G|$. Khi đó trong G tồn tại phần tử có cấp p.*

Chứng minh. Ta chứng minh bổ đề bằng quy nạp theo $n = |G|$. Nếu $n = 2$ thì bổ đề hiển nhiên đúng. Xét $n > 2$ và giả sử bổ đề đúng với mọi nhóm Abel có cấp nhỏ hơn n. Nếu mọi nhóm con thật sự của G đều tầm thường thì G là cyclic, khi đó vì p là một ước số của $|G|$ nên trong G có phần tử có cấp p và bổ đề đúng. Ngược lại, gọi H là một nhóm con thật sự không tầm thường của G.

Nếu p chia hết $|H|$, vì H là một nhóm Abel và $|H| < |G|$ nên theo giả thiết quy nạp tồn tại $a \in H \subset G$ có cấp p.

Nếu p không chia hết $|H|$, vì G Abel và $H \lhd G$ nên G/H là một nhóm Abel với $|G/H| = |G|/|H|$. Ta có $|G/H| < |G|$ vì H là một nhóm không tầm thường và $p \mid |G|$ nhưng không phải ước số của $|H|$ nên $p \mid |G/H|$. Khi đó theo giả thiết quy nạp trong G/H có phần tử $b + H$ có cấp p. Ta có $b \notin H$, vì nếu $b \in H$ thì phần tử $b + H = H \in G/H$ có cấp 1. Đặt $c = |H| b \in G$, khi đó

$$pc = p(|H| b) = |H| (pb) = 0$$

vì $pb \in H$. Ta chứng tỏ $c \neq 0$. Nếu $c = 0$, vì

$$|H| (b + H) = |H| b + H = c + H = H$$

do đó cấp của phần tử $b + H$ là một ước số của $|H|$, tức là $p \mid |H|$, điều này mâu thuẫn với giả sử p không chia hết $|H|$. Vậy $c \neq 0$ và $|c| = p$ và bổ đề được chứng minh.

□

Định lý 2.27. *Cho G là một nhóm Abel hữu hạn có cấp $p^k m$, trong đó p là số nguyên tố và không chia hết m. Đặt H là tập hợp gồm các phần tử của G có cấp là ước số của p^k và K là tập hợp gồm các phần tử của G có cấp là ước số của m. Khi đó*

(a) *H, K là hai nhóm con của G và $G = H \oplus K$.*

(b) *$|H| = p^k$, $|K| = m$.*

Chứng minh. (a) Trước hết ta chứng tỏ H, K là hai nhóm con của G. Ta có $0 \in H$. Nếu $x, y \in H$, vì p^k là một bội số của cấp của x và y nên

$$p^k(x - y) = p^k x - p^k y = 0,$$

do đó $x - y \in H$. Vậy H là một nhóm con của G. Tương tự ta cũng có K là một nhóm con của G. Kế đến ta chứng tỏ $G = H + K$. Vì p^k và m nguyên tố cùng nhau nên có các số nguyên u và v sao cho

$$vm + up^k = 1.$$

Khi đó với mỗi $g \in G$ ta có

$$g = 1g = (vm + up^k)g = (vm)g + (up^k)g.$$

Vì $|G| = p^k m$ nên $p^k(vmg) = p^k m(vg) = 0$, suy ra $(vm)g \in H$. Tương tự $(up^k)g \in K$. Do đó g được biểu diễn dưới dạng tổng của một phần tử của H và một phần tử của K. Cuối cùng, nếu $x \in H \cap K$ thì cấp của x chia hết cả p^k và m, vì vậy nó chia hết $\gcd(p^r, m) = 1$, do đó $x = 0$.Vậy $H \cap K = \{0\}$. Bởi Mệnh đề 2.18, (a) được chứng minh.

(b) H là một nhóm con của nhóm Abel nên H Abel. Nếu có số nguyên tố q khác p sao cho $q \mid |H|$ thì theo Bổ đề 2.26 H chứa một phần tử có cấp q. Điều này không thể được nên không có số nguyên tố nào khác p chia hết $|H|$. Tương tự p không chia hết $|K|$. Vì $|G| = |H|\,|K|$ nên $|H| = p^k$ và $|K| = m$.

□

Hệ quả 2.28. *Cho G là một nhóm Abel hữu hạn có cấp $p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, trong đó $p_1, \ldots, p_r$ là các số nguyên tố đôi một khác nhau. Đặt G_i là nhóm con của G gồm các phần tử có cấp là ước số của $p_i^{k_i}$. Khi đó*

(a) *$G = G_1 \oplus G_2 \oplus \cdots \oplus G_r$.*

(b) *$|G_i| = p_i^{k_i}$ với mỗi $i = 1, \ldots, r$.*

Chứng minh. Ta chứng minh hệ quả bằng quy nạp theo r. Với $r = 2$, theo Định lý 2.27 thì hệ quả đúng . Giả sử hệ quả đúng với r. Ta chứng minh hệ quả đúng với $r + 1$. Thật vậy, giả sử $|G| = p_1^{k_1} \cdots p_r^{k_r} p_{r+1}^{k_{r+1}}$ với $p_1, \ldots, p_{r+1}$ các số nguyên tố

đôi một khác nhau. Đặt $m = p_1^{k_1} \cdots p_r^{k_r}$, K là tập hợp gồm các phần tử của G có cấp là ước số của m. Khi đó theo Định lý 2.27 thì K là một nhóm con của G và $G = K \oplus G_{r+1}$ với $|K| = m$, $|G_{r+1}| = p_{r+1}^{k_{r+1}}$. Áp dụng giả thiết quy nạp cho K ta có $G = G_1 \oplus \cdots \oplus G_r \oplus G_{r+1}$, $|G_i| = p_i^{k_i}$ với mỗi $i = 1, \ldots, r+1$ và hệ quả được chứng minh.

□

Định nghĩa 2.29. Giả sử G là một nhóm hữu hạn. Nếu cấp của G là một lũy thừa của số nguyên tố p thì G được gọi là một *p-nhóm*.

Hệ quả 2.28 nói rằng bất kì nhóm Abel hữu hạn nào cũng có thể phân tích thành tổng trực tiếp của các p-nhóm. Tiếp theo ta sẽ chỉ ra rằng mỗi p-nhóm giao hoán lại là một tổng trực tiếp của các nhóm cyclic.

Định lý 2.30. *Cho G là một p-nhóm giao hoán. Giả sử $a \in G$ là phần tử có cấp lớn nhất, khi đó tồn tại một nhóm con H của G sao cho $G = \langle a \rangle \oplus H$.*

Chứng minh. Giả sử $|G| = p^k$, ta chứng minh định lý bằng quy nạp theo k. Nếu $k = 1$ thì G là một nhóm cyclic và $G = \langle a \rangle \oplus \langle 0 \rangle$. Giả sử định lý đúng đối với các p-nhóm giao hoán có cấp nhỏ hơn p^k.

Nếu $|a| = p^k$ thì $G = \langle a \rangle \oplus \langle 0 \rangle$.

Nếu $|a| = p^r$ với $r < k$, ta lấy $b \in G$ có cấp nhỏ nhất và $b \notin \langle a \rangle$. Ta chứng minh $\langle a \rangle \cap \langle b \rangle = \{0\}$. Thật vậy, ta chỉ cần chỉ ra $|b| = p$ là đủ. Ta có cấp của pb là $|b|/p$ nhỏ hơn cấp của b nên $pb \in \langle a \rangle$, suy ra $pb = ma$ với số nguyên m nào đó. Vì p^r là cấp của a và là cấp lớn nhất nên

$$0 = p^r b = p^{r-1}(pb) = p^{r-1}(ma) = (p^{r-1}m)a,$$

suy ra p^r chia hết $p^{r-1}m$ và vì thế $p \mid m$. Đặt $m = ps$, khi đó $pb = ma = psa$. Ta có $p(b - sa) = 0$, hơn nữa $b - sa \notin \langle a \rangle$ vì $b \notin \langle a \rangle$, do đó $b - sa$ là phần tử của G không thuộc $\langle a \rangle$ có cấp p. Do cách chọn b là phần tử của G không thuộc $\langle a \rangle$ có cấp nhỏ nhất nên $|b| = p$.

Trở lại chứng minh định lý, ta xét nhóm thương $\overline{G} = G/\langle b \rangle$ có $\left|\overline{G}\right| = p^{k-1}$. Đặt $\overline{a} = a + \langle b \rangle \in G$, cấp của $\overline{a}$ là số nguyên dương n nhỏ nhất sao cho $na \in \langle b \rangle$. Vì $\langle a \rangle \cap \langle b \rangle = \{0\}$ nên

$$|\overline{a}| = |a| = p^r.$$

Khi đó $\overline{a}$ là phần tử có cấp lớn nhất trong $\overline{G}$ nên theo giả thiết quy nạp có $\overline{H}$ nhóm con của $\overline{G}$ sao cho $\overline{G} = \langle \overline{a} \rangle \oplus \overline{H}$. Xét phép chiếu chính tắc

$$f : G \longrightarrow G/\langle b \rangle = \overline{G}$$

và $H = f^{-1}(\overline{H})$, khi đó H là một nhóm con của G với $H/\langle b \rangle \cong \overline{H}$, $|H| = p\left|\overline{H}\right|$ và

$$\begin{aligned}|G| &= \left|\overline{G}\right| |\langle b\rangle| = p\left|\overline{G}\right| = p\,|\langle \overline{a}\rangle|\left|\overline{H}\right| \\ &= pp^r\left|\overline{H}\right| = p^r\,|H| = |\langle a\rangle|\,|H|\,.\end{aligned}$$

Cuối cùng, để chứng tỏ $G = \langle a\rangle \oplus H$, theo Mệnh đề 2.18 ta chỉ còn chứng minh $\langle a\rangle \cap H = \{0\}$. Lấy $x \in \langle a\rangle \cap H$ thì $x + \langle b\rangle \in \langle \overline{a}\rangle \cap \overline{H} = \{0 + \langle b\rangle\}$ vì $\overline{G} = \langle \overline{a}\rangle \oplus \overline{H}$. Do đó $x \in \langle b\rangle$, vì $\langle a\rangle \cap \langle b\rangle = \{0\}$ nên $x = 0$ và vì vậy $\langle a\rangle \cap H = \{0\}$. Vậy định lý được chứng minh.

□

Khẳng định sau là hệ quả được suy ra trực tiếp từ định lý trên.

Hệ quả 2.31. *Cho G là một p-nhóm giao hoán. Khi đó tồn tại các nhóm con cyclic $C_1, C_2, \ldots, C_r$ của G sao cho*

$$G = C_1 \oplus C_2 \oplus \cdots \oplus C_r$$

với $|C_1| \geq |C_2| \geq \cdots \geq |C_r|$.

Mệnh đề 2.32. *Cho G là một p-nhóm giao hoán. Nếu $G = C_1 \oplus C_2 \oplus \cdots \oplus C_r$ và $G = D_1 \oplus D_2 \oplus \cdots \oplus D_s$, trong đó C_i, D_j với $1 \leq i \leq r$, $1 \leq j \leq s$ là các nhóm cyclic, và $|C_1| \geq |C_2| \geq \cdots \geq |C_r|$, $|D_1| \geq |D_2| \geq \cdots \geq |D_s|$ thì*

(a) $r = s$.

(b) $C_i \cong D_i$ *với mọi* $i = 1, \ldots, r$.

Chứng minh. (a) Đặt $G(p) = \{x \in G \mid |x| = 1, p\}$ thì $G(p)$ là một nhóm con của G. Nếu H là một nhóm con của G thì $H(p) = \{x \in H \mid |x| = 1, p\} = H \cap G(p)$ là một nhóm con của H.

Xét $x \in G(p)$ và $x = c_1 + \cdots + c_r$ với $c_i \in C_i$, theo Hệ quả 2.23 thì $|c_i| \mid p$, tức là

$$G(p) = C_1(p) + \cdots + C_r(p).$$

Bởi Bổ đề 2.24 thì tổng ở trên là trực tiếp, do đó theo Mệnh đề 2.22 ta có

$$|G(p)| = |C_1(p)| \cdots |C_r(p)|\,.$$

Nhưng tập hợp các phần tử có cấp 1 hoặc p trong một nhóm cyclic có cấp chia hết cho p là nhóm con cyclic duy nhất có cấp p. Vì vậy $|C_i(p)| = p$ và $|G(p)| = p^r$. Tương tự cho D_j, ta có $|G(p)| = p^s$. Vậy $r = s$.

(b) Ta chứng minh bằng quy nạp theo k với $|G| = p^k$. Nếu $k = 1$ thì G là cyclic, mệnh đề hiển nhiên đúng. Giả sử mệnh đề đúng với p-nhóm giao hoán có cấp nhỏ hơn p^k. Xét nhóm thương $G/G(p)$. Theo Mệnh đề 2.25 thì

$$G/G(p) \cong C_1/C_1(p) \oplus \cdots \oplus C_r/C_r(p),$$

$$G/G(p) \cong D_1/D_1(p) \oplus \cdots \oplus D_r/D_r(p).$$

Đây là hai cách phân tích của p-nhóm giao hoán $G/G(p)$ mà nó có cấp nhỏ hơn p^k, do đó theo giả thiết quy nạp thì $C_i/C_i(p) \cong D_i/D_i(p)$ với mọi $i = 1, \ldots, r$. Trong chứng minh (a) ta có $|C_i(p)| = |D_i(p)| = p$, suy ra

$$|C_i| = |D_i|.$$

Vì C_i và D_i là cyclic nên $C_i \cong D_i$ với mọi $i = 1, \ldots, r$.

□

Định lý 2.33. *Cho G là một nhóm giao hoán hữu hạn có cấp $p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, trong đó $p_1, p_2, \ldots, p_r$ là các số nguyên tố đôi một khác nhau. Khi đó*

$$G \cong \mathbb{Z}_{p_1^{a_1}} \times \cdots \times \mathbb{Z}_{p_1^{a_t}} \times \mathbb{Z}_{p_2^{b_1}} \times \cdots \times \mathbb{Z}_{p_2^{b_u}} \times \cdots \times \mathbb{Z}_{p_r^{c_1}} \times \cdots \times \mathbb{Z}_{p_r^{c_v}},$$

trong đó $a_1 \geq \cdots \geq a_t$, $b_1 \geq \cdots \geq b_u$, ... , $c_1 \geq \cdots \geq c_v$. Các nhân tử trong tích trực tiếp được xác định duy nhất bởi G.

Chứng minh. Theo Hệ quả 2.28 thì

$$G = G_1 \oplus G_2 \oplus \cdots \oplus G_r$$

với $|G_i| = p_i^{k_i}$ là sự phân tích duy nhất thành các p_i-nhóm. Bởi Hệ quả 2.31 thì

$$G_i \cong \mathbb{Z}_{p_i^{u_1}} \times \cdots \times \mathbb{Z}_{p_i^{u_i}}$$

với $u_1 \geq \cdots \geq u_i$ và ta có khẳng định đầu của định lý. Khẳng định còn lại của định lý được suy từ Mệnh đề 2.32.

□

Ví dụ 2.34. Tìm tất cả những nhóm Abel G sai khác một đẳng cấu có cấp 72. Ta có $72 = 2^3 3^2$, do đó theo Định lý 2.33 thì G đẳng cấu với một trong những nhóm sau:

$$\mathbb{Z}_8 \times \mathbb{Z}_9; \quad \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_9; \quad \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3;$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9; \quad \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3; \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3.$$

Bài tập

1. Xác định các nhóm Abel sai khác một đẳng cấu có cấp n cho trước trong các trường hợp sau.

   (a) $n = 80$ (b) $n = 108$ (c) $n = 120$ (d) $n = 160$

2. Cho nhóm Abel G có cấp n và hai số nguyên tố p, q khác nhau cùng chia hết n. Chứng tỏ G chứa một nhóm con cyclic có cấp pq.
3. Cho G là một p-nhóm giao hoán và H là một nhóm con cyclic không tầm thường của G. Đặt $G(p) = \{x \in G \mid |x| = 1, p\}$. Chứng tỏ $|G(p) \cap H| = p$.
4. Cho nhóm giao hoán G có cấp 81. Trong mỗi trường hợp hãy xác định $G(3) = \{x \in G \mid |x| = 1, 3\}$ và tìm $G/G(3)$.
5. Cho G là một p-nhóm giao hoán. Đặt $pG = \{px \mid x \in G\}$ và $G(p) = \{x \in G \mid |x| = 1, p\}$. Chứng tỏ $G/G(p) \cong pG$.
6. Cho G là một nhóm hữu hạn sao cho với mọi $x \in G$ thì $x^2 = e$. Chứng tỏ có số nguyên dương n sao cho $G \cong \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ (n lần).
7. Nếu G là một nhóm Abel hữu hạn và p là số nguyên tố sao cho $a^p = e$ với mọi $a \in G$, chứng tỏ G đẳng cấu với $\mathbb{Z}_p^n$ với số tự nhiên n nào đó.
8. Chứng minh rằng một nhóm cyclic có cấp p^n, ở đây p là số nguyên tố, không là tổng trực tiếp của hai nhóm con không tầm thường.

2.4 Nhóm Abel tự do

Trong phần này để đơn giản chúng ta sẽ tìm hiểu nhóm Abel tự do có cơ sở hữu hạn. Sau đó ta sẽ chứng tỏ một nhóm Abel không xoắn hữu hạn sinh là một nhóm Abel tự do.

Định nghĩa 2.35. Giả sử F là một nhóm Abel và $A = \{a_1, \ldots, a_r\} \subset F$. Ta nói A là một *cơ sở* của F nếu mỗi phần tử $x \in F$ đều có biểu diễn duy nhất

$$x = m_1 a_1 + \cdots + m_r a_r,$$

trong đó $m_1, \ldots, m_r \in \mathbb{Z}$.

Chú ý rằng không phải nhóm Abel nào cũng có cơ sở. Nhóm Abel có một cơ sở được gọi là nhóm Abel *tự do*. Ta quy ước nhóm chỉ có một phần tử cũng là nhóm Abel tự do.

Ví dụ 2.36. (a) $\mathbb{Z}_n$ ($n \geq 2$) không phải nhóm Abel tự do. Thật vậy, giả sử $\mathbb{Z}_n$ có một cơ sở $\{a_1, \ldots, a_r\}$. Khi đó $x_k = ka_1 + 0a_2 + \cdots + 0a_r$ với k tùy ý trong $\mathbb{Z}$ là vô hạn các phần tử khác nhau trong $\mathbb{Z}_n$, mâu thuẫn với $\mathbb{Z}_n$ là một tập hợp hữu hạn.

(b) Nhóm cộng $\mathbb{Z}$ các số nguyên là một nhóm Abel tự do với cơ sở $\{1\}$hoặc $\{-1\}$. Mọi nhóm con khác không của $\mathbb{Z}$ đều có dạng $n\mathbb{Z}$ với $n \in \mathbb{N} \setminus \{0\}$ cũng là một nhóm Abel tự do với cơ sở $\{n\}$ hoặc $\{-n\}$.

Định nghĩa 2.37. Giả sử F là một nhóm Abel và $B = \{b_1, \ldots, b_r\} \subset F$. Ta nói B là *độc lập* nếu $\sum_{i=1}^{r} m_i b_i = 0$ với $m_1, \ldots, m_r \in \mathbb{Z}$ thì luôn có $m_1 = m_2 = \cdots = m_r = 0$.

Mệnh đề 2.38. *Cho F là một nhóm Abel và A một tập con của F có hữu hạn phần tử. Khi đó A là một cơ sở của F khi và chỉ khi A là độc lập và là một tập sinh của F.*

Chứng minh. Đặt $A = \{a_1, \ldots, a_r\}$. Giả sử A là một cơ sở của F thì hiển nhiên A là một tập sinh của F. Hơn nữa, nếu $m_1a_1 + \cdots + m_ra_r = 0$ thì

$$m_1a_1 + \cdots + m_ra_r = 0 = 0a_1 + \cdots + 0a_r,$$

bởi tính duy nhất của biểu diễn ta có $m_1 = m_2 = \cdots = m_r = 0$. Vậy A là độc lập.

Đảo lại, giả sử $x \in F$ thì x luôn có biểu diễn $x = m_1a_1 + \cdots + m_ra_r$ với $m_i \in \mathbb{Z}$ vì A là một tập sinh của F. Nếu $x = n_1a_1 + \cdots + n_ra_r$ với $n_i \in \mathbb{Z}$ là một biểu diễn khác của x thì

$$(m_1 - n_1)a_1 + \cdots + (m_r - n_r)a_r = 0,$$

vì A là độc lập ta suy ra $m_i - n_i = 0$, và $m_i = n_i$ với mọi $i = 1, \ldots, r$. Vậy A là một cơ sở của F.

□

Mệnh đề 2.39. *Cho F là một nhóm Abel tự do với cơ sở A. Nếu g là ánh xạ tùy ý cho trước từ A đến nhóm Abel G thì có duy nhất một đồng cấu từ F đến G là mở rộng của g.*

Chứng minh. Giả sử $A = \{a_1, \ldots, a_r\}$ là một cơ sở của F và g là ánh xạ tùy ý từ A đến nhóm Abel G. Mỗi $x \in F$ có biểu diễn duy nhất $x = \sum_{i=1}^{r} m_ia_i$ với $m_1, \ldots, m_r \in \mathbb{Z}$, ta định nghĩa $\varphi : F \longrightarrow G$ bởi $\varphi(x) = \sum_{i=1}^{r} m_ig(a_i)$. φ là đồng cấu vì nếu $x = \sum_{i=1}^{r} m_ia_i$, $x' = \sum_{i=1}^{r} m'_ia_i \in F$ thì

$$\begin{aligned}
\varphi(x + x') &= \varphi(\sum_{i=1}^{r}(m_i + m'_i)a_i) \\
&= \sum_{i=1}^{r}(m_i + m'_i)g(a_i) \\
&= \sum_{i=1}^{r} m_ig(a_i) + \sum_{i=1}^{r} m'_ig(a_i) \\
&= \varphi(x) + \varphi(x').
\end{aligned}$$

Hiển nhiên $\varphi \mid_A = g$. Ta chứng tỏ φ là duy nhất. Giả sử $\psi : F \longrightarrow G$ là một đồng cấu sao cho $\psi \mid_A = g$, khi đó với bất kỳ $x = \sum_{i=1}^{r} m_ia_i \in F$, vì ψ là đồng cấu nên ta có

$$\begin{aligned}\psi(x) &= \psi(\sum_{i=1}^{r} m_i a_i) \\ &= \sum_{i=1}^{r} m_i \psi(a_i) \\ &= \sum_{i=1}^{r} m_i g(a_i) \\ &= \varphi(x).\end{aligned}$$

Vậy $\psi = \varphi$ và mệnh đề được chứng minh.

□

Ta nhận thấy rằng một đồng cấu từ nhóm Abel tự do đến nhóm Abel hoàn toàn được xác định bởi các giá trị của nó trên một cơ sở.

Hệ quả 2.40. *Mỗi nhóm Abel hữu hạn sinh đều đẳng cấu với một nhóm thương của nhóm Abel tự do.*

Chứng minh. Giả sử G là một nhóm Abel được sinh ra bởi tập hợp $S = \{s_1, \ldots, s_r\}$. Gọi F là nhóm Abel tự do với cơ sở $A = \{a_1, \ldots, a_r\}$ và ánh xạ $g : A \longrightarrow G$ được xác định bởi $g(a_i) = s_i$. Theo Mệnh đề 2.39 thì có đồng cấu $\varphi : F \longrightarrow G$ là mở rộng của g. $\mathrm{Im}\varphi$ là một nhóm con của G chứa S nên $\mathrm{Im}\varphi = G$ và do đó φ là một toàn cấu. Bởi Hệ quả 1.92 thì $G \cong F/\ker\varphi$ và hệ quả được chứng minh.

□

Định lý 2.41. *F là một nhóm Abel tự do với cơ sở gồm r phần tử khi và chỉ khi F đẳng cấu với tích trực tiếp $\mathbb{Z}^r$.*

Chứng minh. Giả sử F là một nhóm Abel tự do với cơ sở $\{a_1, \ldots, a_r\}$. $\mathbb{Z}^r$ có tập sinh $\{e_1, \ldots, e_r\}$ với $e_i = (0, \ldots, 0, \underset{i}{1}, 0, \ldots, 0)$, $i = 1, \ldots, r$. Như trong Hệ quả 2.40, tồn tại toàn cấu $\varphi : F \longrightarrow \mathbb{Z}^r$ được xác định bởi $\varphi(a_i) = e_i$ với $i = 1, \ldots, r$. Định lý sẽ được chứng minh nếu ta chứng tỏ φ là một đơn ánh. Thật vậy, $x = \sum_{i=1}^{r} m_i a_i \in \ker\varphi$ khi và chỉ khi

$$\varphi(x) = \sum_{i=1}^{r} m_i \varphi(a_i) = \sum_{i=1}^{r} m_i e_i = (m_1, \ldots, m_r) = (0, \ldots, 0).$$

Ta suy ra $m_1 = \cdots = m_r = 0$ và $x = 0$. Vậy $\ker\varphi = \{0\}$, do đó φ là một đơn ánh.

Đảo lại, giả sử F đẳng cấu với $\mathbb{Z}^r$, khi đó có đẳng cấu $\varphi : F \longrightarrow \mathbb{Z}^r$. Vì $\mathbb{Z}^r$ là một nhóm Abel tự do với cơ sở $\{e_1, \ldots, e_r\}$ nên $\{\varphi^{-1}(e_1), \ldots, \varphi^{-1}(e_r)\}$ là một cơ sở của F, và do đó F là một nhóm Abel tự do với một cơ sở gồm r phần tử.

□

Định lý này mô tả dầy đủ lớp nhóm Abel tự do có cơ sở hữu hạn. Hơn nữa, hai nhóm Abel tự do với hai cơ sở có số phần tử bằng nhau thì đẳng cấu.

Bây giờ ta sẽ chứng tỏ mọi cơ sở của một nhóm Abel tự do đều có cùng số phần tử.

Mệnh đề 2.42. *Nếu F là nhóm Abel tự do với một cơ sở gồm r phần tử thì mọi cơ sở khác của F cũng đều có đúng r phần tử.*

Chứng minh. Cho A là một cơ sở gồm r phần tử của nhóm Abel tự do F và $S \subset F$ là một tập độc lập ta chứng tỏ $|S| \leq r$. Thật vậy, như trong chứng minh của Định lý 2.41 tồn tại một đơn cấu $\varphi : F \longrightarrow \mathbb{Q}^r$ sao cho $\text{Im}\varphi = \mathbb{Z}^r$. Vì A độc lập trong F nên $\varphi(A)$ độc lập trong $\mathbb{Z}^r$. Nhận xét rằng một tập độc lập trong $\mathbb{Z}^r$ thì độc lập tuyến tính trong $\mathbb{Q}$-không gian véc-tơ $\mathbb{Q}^r$. Vì vậy $\varphi(A)$ độc lập tuyến tính trong $\mathbb{Q}^r$ và có đúng r phần tử nên là một cơ sở của $\mathbb{Q}$-không gian véc-tơ $\mathbb{Q}^r$. Tương tự ta cũng có $\varphi(S)$ độc lập tuyến tính trong $\mathbb{Q}$-không gian véc-tơ $\mathbb{Q}^r$. Vì r là chiều của $\mathbb{Q}$-không gian véc-tơ $\mathbb{Q}^r$ nên ta có

$$|S| = |\varphi(S)| \leq r = |\varphi(A)| = |A|\,.$$

Nếu B là một cơ sở khác của F, khi đó B là một tập độc lập và theo chứng minh trên thì $|B| \leq |A|$. Do vai trò của A và B như nhau nên ta cũng có bất đẳng thức ngược lại và mệnh đề được chứng minh.

□

Định nghĩa 2.43. Số phần tử trong một cơ sở của nhóm Abel tự do F gọi là *hạng* của F và được ký hiệu là rank$F$.

Ta quy ước hạng của nhóm chỉ có một phần tử bằng không.

Để chứng tỏ một nhóm con của nhóm Abel tự do cũng là một nhóm Abel tự do ta cần bổ đề

Bổ đề 2.44. *Giả sử $\varphi : G \longrightarrow F$ là một toàn cấu từ nhóm Abel G đến nhóm Abel tự do F. Khi đó có một nhóm con Abel tự do K của G đẳng cấu với F sao cho $G = \ker\varphi \oplus K$.*

Chứng minh. Giả sử $\{a_1, \ldots, a_r\}$ là một cơ sở của F. Vì φ là một toàn ánh nên với mỗi a_i có $b_i \in G$ sao cho $\varphi(b_i) = a_i$. Gọi K là nhóm con của G được sinh ra bởi $\{b_1, \ldots, b_r\}$. Ta chứng tỏ K là một nhóm Abel tự do. Thật vậy, nếu $\sum_{i=1}^{r} m_i b_i = 0$ thì

$$0 = \varphi(0) = \sum_{i=1}^{r} m_i \varphi(b_i) = \sum_{i=1}^{r} m_i a_i.$$

Vì $\{a_1, \ldots, a_r\}$ là một cơ sở của F nên $m_i = 0$ với mọi $i = 1, \ldots r$, và do đó $\{b_1, \ldots, b_r\}$ độc lập. Vậy K là nhóm Abel tự do với cơ sở $\{b_1, \ldots, b_r\}$, và vì có cùng hạng với F nên đẳng cấu với F.

Nếu $x \in \ker\varphi \cap K$ thì x có dạng $x = \sum_{i=1}^{r} n_i b_i$ và $\varphi(x) = 0$. Ta suy ra

$$0 = \sum_{i=1}^{r} n_i \varphi(b_i) = \sum_{i=1}^{r} n_i a_i,$$

do đó $n_i = 0$ với mọi $i = 1, \ldots, r$ và $x = 0$. Vậy $\ker\varphi \cap K = \{0\}$, suy ra $\ker\varphi + K = \ker\varphi \oplus K$. Tiếp theo ta chứng tỏ $G = \ker\varphi + K$. Thật vậy, với mỗi $x \in G$ thì $\varphi(x) \in F$ nên có thể viết dưới dạng $\varphi(x) = \sum_{i=1}^{r} m_i a_i$. Từ đây ta có $\varphi(x - \sum_{i=1}^{r} m_i b_i) = 0$ và $h = x - \sum_{i=1}^{r} m_i b_i \in \ker\varphi$. Vậy ta có $x = h + k \in \ker\varphi + K$ với $k = \sum_{i=1}^{r} m_i b_i$ và bổ đề được chứng minh.

□

Mệnh đề 2.45. *Giả sử F là một nhóm Abel tự do và H một nhóm con bất kỳ của F. Khi đó H cũng là một nhóm Abel tự do và* $\text{rank}H \leq \text{rank}F$.

Chứng minh. Mệnh đề được chứng minh bằng quy nạp theo $r = \text{rank } F$. Khi $r = 0$ thì mệnh đề hiển nhiên đúng. Khi $r = 1$ ta có F đẳng cấu với $\mathbb{Z}$, khi đó nhóm con H của F đẳng cấu với nhóm con của $\mathbb{Z}$ có dạng $n\mathbb{Z}$ với số tự nhiên n nào đó với hạng nhỏ hơn hoặc bằng 1, và do đó mệnh đề đúng. Giả sử mệnh đề đúng với các nhóm Abel tự do có hạng nhỏ hơn r. Xét F là nhóm Abel tự do với cơ sở $\{a_1, \ldots, a_r\}$. Khi đó phép chiếu $\varphi : F \longrightarrow \langle a_r \rangle$ cho bởi

$$\varphi(m_1 a_1 + \cdots + m_r a_r) = m_r a_r$$

với mọi $m_i \in \mathbb{Z}$ là một đồng cấu. $\ker\varphi$ được sinh ra bởi $\{a_1, \ldots, a_{r-1}\}$ là nhóm Abel tự do hạng $r - 1$. Đặt $\varphi_1 = \varphi\,|_H$ và $K = \ker\varphi_1 = \ker\varphi \cap H$ là nhóm con của $\ker\varphi$. Theo giả thiết quy nạp, K là nhóm Abel tự do với hạng nhỏ hơn hoặc bằng $r - 1$. Mặt khác, vì $\langle a_r \rangle$ đẳng cấu với $\mathbb{Z}$ nên là một nhóm Abel tự do và do đó nhóm con của nó $\text{Im}\varphi_1$ cũng là một nhóm Abel tự do với hạng nhỏ hơn hoặc bằng 1. Theo Bổ đề 2.44 có một nhóm con L của H đẳng cấu với $\text{Im}\varphi_1$ sao cho $H = L \oplus K$. Vì vậy H là nhóm Abel tự do với $\text{rank}H = \text{rank}L + \text{rank}K \leq 1 + (r - 1) = \text{rank}F$.

□

Định nghĩa 2.46. Ta nói nhóm Abel G là *không xoắn* nếu phần tử không của G là phần tử duy nhất có cấp hữu hạn.

Ví dụ 2.47. (a) Nhóm cộng $\mathbb{Z}$ các số nguyên, $\mathbb{Q}$ các số hữu tỷ, $\mathbb{R}$ các số thực là các nhóm không xoắn.

(b) Nhóm Abel tự do là nhóm không xoắn. Thật vậy, cho G là nhóm Abel tự do không tầm thường, nếu G không phải là nhóm không xoắn thì có $a \in G$, $a \neq 0$ có cấp n. Gọi $\{a_1, \ldots, a_r\}$ là một cơ sở của G và a có biểu diễn $a = m_1 a_1 + \cdots + m_r a_r$ với $m_1, \ldots, m_r \in \mathbb{Z}$. Khi đó $na = 0$ có hai biểu diễn

$$\begin{aligned} 0 &= nm_1a_1 + \cdots + nm_ra_r \\ &= 0a_1 + \cdots + 0a_r. \end{aligned}$$

Bởi tính duy nhất của biểu diễn ta suy ra $nm_1 = \cdots = nm_r = 0$ và do đó $m_1 = \cdots = m_r = 0$. Vậy $a = 0$, mâu thuẫn này chứng tỏ G là không xoắn.

Định lý 2.48. *Mọi nhóm Abel hữu hạn sinh và không xoắn đều là nhóm Abel tự do.*

Chứng minh. Xét nhóm Abel F hữu hạn sinh và không xoắn. Nếu $F = \{0\}$ thì định lý hiển nhiên đúng. Giả sử $F \neq \{0\}$ và S là một tập sinh hữu hạn của F. Gọi $\{a_1, \ldots, a_r\}$ là một tập con độc lập tối đại trong S, tức là không có tập con nào độc lập nào trong S thực sự chứa nó. Đặt H là nhóm con của F được sinh ra bởi $\{a_1, \ldots, a_r\}$, khi đó H là một nhóm Abel tự do. Do tính tối đại của $\{a_1, \ldots, a_r\}$ nên với mỗi $s \in S$ có các số nguyên $m_1, \ldots, m_r, m_s$ không đồng thời bằng không sao cho

$$m_1a_1 + \cdots + m_ra_r + m_ss = 0.$$

Khi đó $m_s \neq 0$, vì nếu trái lại thì $m_i = 0$ với mọi i, mâu thuẫn với các $m_1, \ldots, m_r, m_s$ không đồng thời bằng không. Từ điều trên ta suy ra $m_ss = -(m_1a_1 + \cdots + m_ra_r) \in H$. Đặt $m = \prod_{s\in S} m_s \neq 0$ thì $ms \in H$ với mọi $s \in S$. Vì S là một tập sinh của F nên $mF \subset H$. Theo Mệnh đề 2.45 thì mF là một nhóm Abel tự do. Mặt khác, vì F không xoắn nên đồng cấu $x \in F \longmapsto mx \in F$ là một đơn cấu. Vì vậy $F \cong mF$ là một nhóm Abel tự do.

□

2.5 Nhóm Abel hữu hạn sinh

Mệnh đề 2.49. *Đặt $T(G)$ gồm tất cả các phần tử có cấp hữu hạn của một nhóm Abel G. Khi đó $T(G)$ là một nhóm con của G và nhóm thương $G/T(G)$ là* không xoắn.

Chứng minh. Phần tử $0 \in G$ có cấp 1 nên $0 \in T(G)$. Nếu $x, y \in T(G)$ có cấp lần lượt là m và n thì

$$nm(x - y) = n(mx) - m(ny) = 0,$$

do đó $x - y$ có cấp hữu hạn và $x - y \in T(G)$. Vậy $T(G)$ là một nhóm con của G.

Xét nhóm thương $G/T(G)$. Nếu $x + T(G)$ có cấp n, tức là $nx + T(G) = n(x + T(G)) = T(G)$. Ta suy ra $nx \in T(G)$. Vì $T(G)$ gồm tất cả những phần tử có cấp hữu hạn nên có số nguyên dương m sao cho $m(nx) = 0$. Khi đó x có cấp hữu hạn và $x \in T(G)$, do đó $x + T(G) = T(G)$. Vậy chỉ có $0 + T(G)$ trong $G/T(G)$ có cấp hữu hạn nên $G/T(G)$ là một nhóm không xoắn.

□

Định nghĩa 2.50. Nhóm con $T(G)$ của nhóm Abel G trong mệnh đề trên được gọi là nhóm con *xoắn* của G.

Hệ quả 2.51. *Cho G là một nhóm Abel hữu hạn sinh và $T(G)$ nhóm con xoắn của G. Khi đó $T(G)$ là một nhóm hữu hạn và có một nhóm con Abel tự do K của G đẳng cấu với $G/T(G)$ sao cho $G = T(G) \oplus K$.*

Chứng minh. Trước hết ta chứng tỏ $T(G)$ là một nhóm hữu hạn. Giả sử G được sinh ra bởi r phần tử và F là nhóm Abel tự do với một cơ sở gồm r phần tử. Khi đó như trong chứng minh Hệ quả 2.40 có một toàn cấu $\varphi : F \longrightarrow G$. Theo Mệnh đề 2.45 thì nhóm con $\varphi^{-1}(T(G))$ của F cũng là Abel tự do và hữu hạn sinh, do đó $T(G) = \varphi(\varphi^{-1}(T(G)))$ là một nhóm hữu hạn sinh. Kết hợp với tính chất $T(G)$ là giao hoán và gồm các phần tử có cấp hữu hạn ta suy ra $T(G)$ là một nhóm hữu hạn.

Ta chứng minh khẳng định còn lại của hệ quả. Theo Mệnh đề 2.49 thì $G/T(G)$ là không xoắn. Vì G là hữu hạn sinh nên $G/T(G)$ cũng vậy, bởi Định lý 2.48 ta suy ra $G/T(G)$ là một nhóm Abel tự do. Bây giờ ta xét phép chiếu chính tắc $p : G \longrightarrow G/T(G)$ với $\ker p = T(G)$, theo Bổ đề 2.44 thì tồn tại một nhóm con Abel tự do K của G đẳng cấu với $G/T(G)$ sao cho $G = T(G) \oplus K$. Vậy hệ quả được chứng minh.

□

Định nghĩa 2.52. Giả sử G là một nhóm Abel hữu hạn sinh. Hạng của nhóm Abel tự do $G/T(G)$ được gọi là *hạng* của G.

Định lý 2.53. *Cho G là một nhóm Abel hữu hạn sinh. Khi đó G đẳng cấu với tích trực tiếp của một số hữu hạn các nhóm cyclic có cấp lũy thừa số nguyên tố hoặc cấp vô hạn. Các nhân tử trong tích trực tiếp được xác định duy nhất bởi G sai khác một thứ tự.*

Chứng minh. Từ Hệ quả 2.51, Định lý 2.33 và Định lý 2.41 ta có khẳng định đầu của định lý. Bây giờ giả sử G được biểu diễn như là tổng trực tiếp của các nhóm cyclic có cấp lũy thừa số nguyên tố hoặc cấp vô hạn theo hai cách, cụ thể

$$G = C_1 \oplus \cdots \oplus C_m \oplus F_1 \oplus \cdots \oplus F_n = D_1 \oplus \cdots \oplus D_k \oplus H_1 \oplus \cdots \oplus H_h,$$

ở đây C_i, D_j là các nhóm cyclic có cấp lũy thừa số nguyên tố, F_r, H_s là các nhóm cyclic có cấp vô hạn.

Khi đó $T(G)$ là tổng trực tiếp của các hạng tử trực tiếp có cấp hữu hạn trong cả hai trường hợp. Vì vậy

$$T(G) = C_1 \oplus \cdots \oplus C_m = D_1 \oplus \cdots \oplus D_k.$$

Do đó bởi Định lý 2.33 ta có $m = k$ và các C_i, D_j sai khác một thứ tự, đôi một đẳng cấu.

Ta cũng có

$$G/T(G) \cong F_1 \oplus \cdots \oplus F_n \cong H_1 \oplus \cdots \oplus H_h.$$

Do đó $n = h$ vì cùng bằng hạng của nhóm Abel tự do $G/T(G)$. Vậy định lý được chứng minh.

□

Bài tập

1. Chứng tỏ nhóm cộng $\mathbb{Q}$ các số hữu tỷ là không xoắn và không hữu hạn sinh.
2. Chứng tỏ với mọi $a, b \in \mathbb{Q}$ thì $\{a, b\}$ không độc lập. Từ đây suy ra $\mathbb{Q}$ không là nhóm Abel tự do.
3. Chứng tỏ $T(\mathbb{R}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$.
4. Cho H là một nhóm con của nhóm Abel G. Chứng tỏ nếu G/H không xoắn thì $H \supset T(G)$.
5. Tập hợp gồm phần tử 0 và tất cả các phần tử có cấp vô hạn của nhóm Abel G có phải là một nhóm con của G không?
6. Chứng minh rằng nếu tập hợp gồm phần tử 0 và tất cả phần tử có cấp vô hạn của một nhóm Abel G là một nhóm con thì G hoặc là nhóm xoắn hoặc không xoắn.
7. Cho H là một nhóm con của nhóm Abel G. Chứng tỏ $T(H) = T(G) \cap H$.
8. Cho F, G và H là những nhóm Abel hữu hạn sinh. Chứng tỏ rằng nếu $F \times G \cong F \times H$ thì $G \cong H$.

Chương 3

VÀNH

3.1 Vành và vành con

Định nghĩa 3.1. Giả sử trên tập hợp R có hai phép toán ký hiệu theo lối cộng và nhân. Ta nói R là một *vành* nếu hai phép toán thỏa mãn các điều kiện sau:

(a) R cùng với phép cộng là một nhóm Abel;

(b) Phép nhân có tính kết hợp;

(c) Phép nhân có tính phân phối với phép cộng, tức là với x, y, z tùy ý trong R ta luôn có

$$x\,(y+z) = xy + xz,$$
$$(y+z)\,x = yx + zx.$$

Nhắc lại rằng phần tử trung lập của phép cộng luôn được ký hiệu là 0 và gọi là phần tử không, phần tử đối xứng (đối với phép cộng) của phần tử x được ký hiệu là $-x$ và gọi là đối của x.

Ta nói một vành là vành *giao hoán* nếu phép nhân có tính giao hoán; là vành có *đơn vị* nếu phép nhân có đơn vị. Đơn vị của một vành nếu có thường được ký hiệu là 1 hay e.

Ví dụ 3.2. (a) Tập hợp $\mathbb{Z}$ các số nguyên, $\mathbb{Q}$ các số hữu tỷ, $\mathbb{R}$ các số thực, $\mathbb{C}$ các số phức với phép cộng và nhân thông thường là các vành giao hoán có đơn vị. Tập hợp $2\mathbb{Z}$ các số chẵn với phép cộng và nhân thông thường là một vành giao hoán nhưng không có đơn vị.

(b) Cho trước số nguyên $n \geq 2$, tập hợp $\mathbb{Z}_n$ các số nguyên mod n với phép cộng và nhân hai lớp là một vành giao hoán có đơn vị $\overline{1}$.

(c) Tập hợp $M(n, R)$ gồm các ma trận vuông cấp n ($n \geq 2$) hệ số trong R, ở đây R có thể là $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ hay $\mathbb{Z}_n$, cùng với phép cộng và nhân ma trận là một vành. Vành này không giao hoán vì phép nhân hai ma trận không có tính giao hoán, nó có đơn vị là ma trận đơn vị.

(d) Cho R và S là hai vành. Trên tích $R \times S$ ta định nghĩa các phép toán

$$(x, y) + (x', y') = (x + x', y + y'),$$

$$(x,y)(x',y') = (xx',yy')$$

với mọi $(x,y),(x',y') \in R \times S$. Khi đó $R \times S$ là một vành và gọi là *vành tích* của R và S.

(e) Giả sử G là một nhóm cộng giao hoán, ký hiệu $\mathrm{End}(G)$ là tập hợp các tự đồng cấu của G. Với bất kỳ $f, g \in \mathrm{End}(G)$ ta định nghĩa

$$(f+g)(x) = f(x) + g(x),$$
$$(f \cdot g)(x) = f(g(x))$$

với mọi $x \in G$, dễ thấy rằng $f+g$, $f \cdot g$ là hai tự đồng cấu của G nên phép cộng và phép nhân ở trên là hai phép toán trên $\mathrm{End}(G)$. Khi đó $\mathrm{End}(G)$ là một vành và gọi là *vành các tự đồng cấu* của G. Vành này có đơn vị là ánh xạ đồng nhất trên G.

(f) Cho trước tập hợp X không rỗng và vành R, đặt M là tập hợp các ánh xạ từ X đến R. Ta định nghĩa phép cộng và nhân trên M như sau: với bất kỳ $f, g \in M$ thì

$$(f+g)(x) = f(x) + g(x),$$
$$(f \cdot g)(x) = f(x)\, g(x)$$

với mọi $x \in X$. Khi đó M là một vành, vành này giao hoán nếu R giao hoán, có đơn vị nếu R có đơn vị.

Mệnh đề 3.3. *Trong một vành R ta luôn có*

(a) $0x = x0 = 0$ *với mọi* $x \in R$.

(b) $x(-y) = (-x)y = -(xy)$ *với mọi* $x, y \in R$.

(c) $(-x)(-y) = xy$ *với mọi* $x, y \in R$.

(d) $x(y-z) = xy - xz$, $(y-z)x = yx - zx$ *với mọi* $x, y, z \in R$.

(e) $x(ny) = n(xy) = (nx)y$ *với mọi* $x, y \in R$, $n \in \mathbb{Z}$.

Chứng minh. (a) Cho $x \in R$, sử dụng tính phân phối của phép nhân với phép cộng ta có $0x + 0x = (0+0)x = 0x = 0x + 0$. Giản ước hai vế cho $0x$ ta được $0x = 0$. Chứng minh tương tự đối với $x0 = 0$.

(b) Với bất kỳ $x, y \in R$ ta có $0 = x0 = x(y-y) = xy + x(-y)$. Do đó $x(-y) = -(xy)$. Chứng minh tương tự đối với khẳng định còn lại.

(c) được suy ra từ (b), (d) được suy ra từ tính phân phối của phép nhân với phép cộng và (b).

(e) Khi $n = 0$ mệnh đề hiển nhiên đúng. Giả thiết quy nạp $x(ny) = n(xy)$ với mọi số tự nhiên n. Ta có

$$\begin{aligned} x\left((n+1)\,y\right) &= x\left(ny+y\right) = x\left(ny\right)+xy \\ &= n\left(xy\right)+xy \qquad \text{bởi giả thiết quy nạp} \\ &= \left(n+1\right)xy. \end{aligned}$$

Vậy $x(ny) = n(xy)$ đúng với mọi số tự nhiên n. Kết hợp với (b) ta có $x\left(ny\right) = n\left(xy\right)$ đúng với mọi số nguyên n. Chứng minh tương tự đối với khẳng định còn lại.

□

Chú ý rằng nếu vành R có nhiều hơn một phần tử và có đơn vị 1 thì $1 \neq 0$. Thật vậy, nếu $1 = 0$, khi đó với bất kỳ $x \in R$ bởi (a) ta có $x = x \cdot 1 = x \cdot 0 = 0$ và do đó R chỉ có một phần tử.

Mệnh đề 3.4. *Cho R là một vành có đơn vị và đặt $U\left(R\right)$ là tập hợp các phần tử trong R khả nghịch. Khi đó $U\left(R\right)$ với phép nhân trong R là một nhóm.*

Chứng minh. Với bất kỳ $x, y \in U\left(R\right)$ ta có x, y là hai phần tử khả nghịch nên tích xy cũng là một phần tử khả nghịch, nói cách khác $xy \in U\left(R\right)$. Vì phép nhân trên $U\left(R\right)$ chính là phép nhân của vành R nên có tính kết hợp. 1 (đơn vị của vành R) có nghịch đảo là chính nó nên $1 \in U\left(R\right)$. Nếu $a \in U\left(R\right)$ thì a có nghịch đảo $a^{-1} \in R$, khi đó a là nghịch đảo của a^{-1} nên $a^{-1} \in U\left(R\right)$. Vậy $U\left(R\right)$ là một nhóm.

□

Ví dụ 3.5. (a) Nhóm nhân các phần tử khả nghịch của vành $\mathbb{Z}$ là $U\left(\mathbb{Z}\right) = \{1, -1\}$, nhóm nhân các phần tử khả nghịch của vành $\mathbb{Q}$ là $U\left(\mathbb{Q}\right) = \mathbb{Q} \setminus \{0\}$.

(b) Nhóm nhân các phần tử khả nghịch của vành $\mathbb{Z}_n$ là $U\left(\mathbb{Z}_n\right) = U\left(n\right)$.

(c) Xác định $\overline{a} \in \mathbb{Z}_{35}$ biết $\overline{a}^7 = \overline{2}$. Trước hết ta nhận thấy rằng 2 và 35 là hai số nguyên tố cùng nhau, suy ra a và 35 cũng nguyên tố cùng nhau và do đó $\overline{a} \in U\left(35\right)$. $U\left(35\right)$ là nhóm nhân có cấp $\varphi\left(35\right) = \varphi\left(7\right)\varphi\left(5\right) = 6 \cdot 4 = 24$, do đó $\overline{a}^{24} = \overline{1}$. Ta có $1 = 7 \cdot 7 - 2 \cdot 24$ và vì vậy

$$\overline{a} = \overline{a}^{7\cdot 7 - 2\cdot 24} = \left(\overline{a}^7\right)^{\,7}\left(\overline{a}^{24}\right)^{\,-2} = \left(\overline{2}\right)^{\,7} = \overline{23}.$$

Định nghĩa 3.6. Xét vành R và tập con S của R ổn định đối với hai phép toán cộng và nhân trên R, tức là $x + y$, $xy \in S$ với mọi $x, y \in S$. Ta nói S là một *vành con* của R nếu S là một vành với cùng hai phép toán trên R.

Định lý 3.7. *Cho vành R và tập con S không rỗng của R. Khi đó ba điều sau tương đương.*

(a) *S là một vành con của R.*

(b) *Với mọi $x, y \in S$ thì $x + y, xy \in S$ và $-x \in S$.*

(c) *Với mọi $x, y \in S$ thì $x - y, xy \in S$.*

Chứng minh. (a)⇒(b) và (b)⇒(c) là hiển nhiên. Ta chứng minh (c) ⇒(a). Bởi giả thiết (c) ta có S là một nhóm cộng giao hoán. Vì phép cộng và nhân trong S cũng là phép cộng và nhân trong R nên phép nhân có tính kết hợp và có tính phân phối với phép cộng. Vậy S là một vành và do đó là một vành con của R.

□

Ví dụ 3.8. (a) Cho R là một vành. Ta luôn có $\{0\}, R$ là hai vành con của R.

(b) $\mathbb{Z}$ là một vành con của vành $\mathbb{Q}$, $\mathbb{Q}$ là một vành con của vành $\mathbb{R}$, $\mathbb{R}$ là một vành con của vành $\mathbb{C}$.

(c) Cho số tự nhiên n. Ta chứng tỏ $n\mathbb{Z}$ là một vành con của vành $\mathbb{Z}$. Hiển nhiên $n\mathbb{Z} \neq \emptyset$. Nếu $x, y \in n\mathbb{Z}$ thì có $h, k \in \mathbb{Z}$ sao cho $x = nh$ và $y = nk$, khi đó $x - y = n(h - k) \in \mathbb{Z}$ và $xy = n(nhk) \in n\mathbb{Z}$. Theo Định lý 3.7 thì $n\mathbb{Z}$ là một vành con của $\mathbb{Z}$.

(d) $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ là một vành con của vành $\mathbb{C}$ và gọi là *vành các số nguyên Gauss.* Thật vậy, ta có $\mathbb{Z}[i] \neq \emptyset$. Nếu $x = a + bi$ và $y = c + di$ thuộc $\mathbb{Z}[i]$ thì $x - y = (a - c) + (b - d)i \in \mathbb{Z}[i]$ và $xy = (ac - bd) + (ad + bc)i \in \mathbb{Z}[i]$. Vậy $\mathbb{Z}[i]$ là một vành con của $\mathbb{C}$.

(e) Tập hợp S gồm các ma trận hệ số thực có dạng $\begin{pmatrix} x & y & z \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ là một vành con của vành các ma trận vuông cấp ba hệ số thực $M(3, \mathbb{R})$. Thật vậy, hiển nhiên $S \neq \emptyset$. Nếu $X = \begin{pmatrix} x & y & z \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ và $X' = \begin{pmatrix} x' & y' & z' \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ là hai phần tử tùy ý của S thì

$$X - X' = \begin{pmatrix} x - x' & y - y' & z - z' \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in S \text{ và } XX' = \begin{pmatrix} xx' & xy' & xz' \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in S.$$

Vậy S là một vành con của $M(3, \mathbb{R})$.

(f) Cho R là một vành. *Tâm* của R được định nghĩa là tập hợp $Z(R) = \{x \in R \mid \forall a \in R, xa = ax\}$. Ta có $Z(R) \neq \emptyset$ vì có $0 \in Z(R)$. Nếu $x, y \in Z(R)$, với bất kỳ $a \in R$ thì

$$(x - y)a = xa - ya = ax - ay = a(x - y),$$

$$a(xy) = (ax)y = (xa)y = x(ay) = (xy)a,$$

do đó $x - y, xy \in Z(R)$. Vậy $Z(R)$ là một vành con của R.

Mệnh đề 3.9. *Giao của một họ tùy ý các vành con của một vành cũng là một vành con của vành đó.*

Chứng minh. Giả sử $(S_i)_{i\in I}$ là họ các vành con của vành R. Đặt $S = \cap_{i\in I} S_i$. Ta thấy $0 \in S_i$ với mọi $i \in I$ nên $0 \in S$ và do đó $S \neq \emptyset$. Nếu $x, y \in S$ thì $x, y \in S_i$ với mọi $i \in I$, và vì S_i là các vành con của R nên $x - y, xy \in S_i$, do đó $x - y, xy \in S$. Theo Định lý 3.7 thì S là một vành con của R.

□

Cho trước vành R và tập con U của R. Xét họ các vành con của R chứa U (họ này không rỗng vì R là một phần tử của nó) và gọi $\langle U\rangle$ là giao của tất cả các vành con trong họ đó

$$\langle U\rangle = \cap_{S \text{ là vành con của } R \text{chứa } U} S.$$

Theo Mệnh đề 3.9 thì $\langle U\rangle$ là một vành con và là vành con nhỏ nhất của R chứa U. Ta gọi $\langle U\rangle$ là vành con của R *được sinh ra bởi* U.

Chú ý rằng $\langle\emptyset\rangle = \{0\}$ và $\langle U\rangle = U$ nếu U là một vành con của R.

Bài tập

1. Tập hợp nào sau đây lập thành một vành?
   (a) $\left\{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\right\}$ với phép cộng và nhân các số thực.
   (b) $\left\{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{Q}\right\}$ với phép cộng và nhân ma trận.
   (c) $\{X \in M(3, \mathbb{R}) \mid \det X = 0\}$ với phép cộng và nhân ma trận.
   (d) $\left\{\frac{m}{n} \in \mathbb{Q} \mid n \text{ lẻ}\right\}$ với phép cộng và nhân các số hữu tỷ.
   (e) $\{ri \mid r \in \mathbb{R}, i^2 = -1\}$ với phép cộng và nhân các số phức.
2. Cho R là một vành. Chứng tỏ $(a + b)(a - b) = a^2 - b^2$ với mọi $a, b \in R$ nếu và chỉ nếu R là một vành giao hoán.
3. Một vành R gọi là vành *Bool* nếu $a^2 = a$ với mọi $a \in R$.
   (a) Chứng tỏ $\mathbb{Z}_2$ và $\mathbb{Z}_2 \times \mathbb{Z}_2$ là các vành Bool.
   (b) Chứng tỏ vành Bool luôn là một vành giao hoán và $2a = 0$ với mọi $a \in R$.
4. Cho tập hợp X, trên $\mathcal{P}(X)$ ta định nghĩa hai phép toán

$$A + B = \{x \mid x \in A \cup B, x \notin A \cap B\}, \qquad A \cdot B = A \cap B$$

   với mọi $A, B \in \mathcal{P}(X)$. Chứng tỏ $\mathcal{P}(X)$ là một vành Bool có đơn vị.
5. Xác định nhóm $U(R))$ với R là một trong các vành sau.
   (a) $\mathbb{Z}_4 \times \mathbb{Z}_6$ (b) $\mathbb{Z} \times \mathbb{Q}$
   (c) $\mathbb{Z}[i]$ (d) $M(2, \mathbb{Z}_2)$ (e) $M(2, \mathbb{Z})$
6. Cho R và S là hai vành có đơn vị. Chứng tỏ

$$U(R \times S) = U(R) \times U(S).$$

7. Xác định $\overline{a} \in \mathbb{Z}_{62}$ biết $\overline{a}^{11} = \overline{5}$.
8. Phần tử a trong một vành R được gọi là *lũy đẳng* nếu $a^2 = a$. Tìm các phần tử lũy đẳng của các vành sau.

   (a) $\mathbb{Z}_{12}$ (b) $\mathbb{Z}_6 \times \mathbb{Z}_{12}$

9. Tập hợp nào sau đây là vành con của $\mathbb{C}$?

   (a) $\{0 + ib \mid b \in \mathbb{R}\}$ (b) $\{a + ib \mid a, b \in \mathbb{Q}\}$ (c) $\{z \in \mathbb{C} \mid |z| \leq 1\}$

10. Cho R là một vành tùy ý và $\mathbb{Z}$ vành các số nguyên. Trên tập hợp tích $R \times \mathbb{Z}$ ta định nghĩa phép cộng và nhân như sau:

$$(x, n) + (y, m) = (x + y, n + m),$$
$$(x, n)(y, m) = (xy + ny + mx, nm)$$

   với mọi $(x, n), (y, m) \in R \times \mathbb{Z}$.

   (a) Chứng tỏ $R \times \mathbb{Z}$ là một vành có đơn vị.

   (b) $R \times \{0\}$ là một vành con của $R \times \mathbb{Z}$.

11. Xác định các vành con của $\mathbb{Z}$.
12. Phần tử a trong một vành R được gọi là *lũy linh* nếu có số nguyên $k \geq 1$ sao cho $a^k = 0$. Chứng tỏ tập hợp các phần tử lũy linh trong một vành giao hoán R lập thành vành con của R.

3.2 Miền nguyên và trường

Định nghĩa 3.10. Giả sử R là một vành giao hoán và $a \in R$, $a \neq 0$. Ta nói a là một *ước của không* nếu có $b \in R$, $b \neq 0$ sao cho $ab = 0$.

Ví dụ 3.11. Xét vành $\mathbb{Z}_{10}$. Ta có $\overline{2} \cdot \overline{5} = \overline{0}$, $\overline{4} \cdot \overline{5} = \overline{0}$, $\overline{6} \cdot \overline{5} = \overline{0}$, $\overline{8} \cdot \overline{5} = \overline{0}$, do đó $\overline{2}, \overline{5}, \overline{4}, \overline{6}, \overline{8}$ là các ước của không. Vì $\overline{1} \cdot x \neq \overline{0}$ với mọi $x \in \mathbb{Z}_{10}$, $x \neq \overline{0}$ nên $\overline{1}$ không phải ước của không. Tương tự $\overline{3}, \overline{9}, \overline{7}$ không phải các ước của không.

Mệnh đề 3.12. *Cho R là một vành giao hoán. Khi đó R không có ước của không khi và chỉ khi trong R phép giản ước cho phần tử khác không có hiệu lực, tức là với bất kỳ $a, b, c \in R$, $a \neq 0$ mà $ab = ac$ thì ta luôn có $b = c$.*

Chứng minh. Giả sử R không có ước của không. Nếu $a, b, c \in R$, $a \neq 0$ mà $ab = ac$, ta suy ra $a(b - c) = 0$. Vì R không có ước của không và $a \neq 0$ nên $b - c = 0$, do đó $b = c$. Đảo lại, với $a \in R$ tùy ý khác không sao cho có $b \in R$ mà $ab = 0$, khi đó giản

ước hai vế cho a của phương trình $ab = 0 = a0$ ta có $b = 0$. Vậy R không có ước của không.

□

Định nghĩa 3.13. *Miền nguyên* là một vành giao hoán có nhiều hơn một phần tử, có đơn vị và không có ước của không.

Ví dụ 3.14. (a) Các vành $\mathbb{Z}$ các số nguyên, $\mathbb{Q}$ các số hữu tỉ, $\mathbb{R}$ các số thực và $\mathbb{C}$ các số phức là các miền nguyên.

(b) Các vành $\mathbb{Z}_2, \mathbb{Z}_3$ là các miền nguyên.

(c) Vành $\mathbb{Z}_{10}$ không phải miền nguyên vì có ước của không.

(d) $\mathbb{Z}$ là một miền nguyên nhưng vành tích $\mathbb{Z}\times\mathbb{Z}$ chỉ là một vành giao hoán có đơn vị, không phải là một miền nguyên vì có ước của không, chẳng hạn $(2,0)(0,3) = (0,0)$.

Định lý 3.15. *Vành $\mathbb{Z}_p$ là một miền nguyên khi và chỉ khi p là một số nguyên tố.*

Chứng minh. Giả sử $\mathbb{Z}_p$ là một miền nguyên. Nếu p là một hợp số thì có các số nguyên $1 < a, b < p$ sao cho $p = ab$, khi đó $\overline{0} = \overline{p} = \overline{a}\cdot\overline{b}$ với $\overline{a}, \overline{b}$ là hai phần tử khác không trong $\mathbb{Z}_p$. Mâu thuẩn này chứng tỏ p là một số nguyên tố. Đảo lại, giả sử p là một số nguyên tố, nếu $\overline{a} \in \mathbb{Z}_p$ tùy ý khác không sao cho có $\overline{b} \in \mathbb{Z}_p$ mà $\overline{ab} = \overline{a}\overline{b} = \overline{0}$ thì ab chia hết cho p. Vì $\overline{a} \neq \overline{0}$ nên a không chia hết cho p, do đó b chia hết cho p và $\overline{b} = \overline{0}$. Vậy $\mathbb{Z}_p$ không có ước của không và ta có điều phải chứng minh.

□

Định nghĩa 3.16. *Trường* là một vành giao hoán có nhiều hơn một phần tử, có đơn vị và mọi phần tử khác không của vành đều có nghịch đảo.

Chú ý rằng khi F là một trường thì $F^* = F \setminus \{0\}$ là một nhóm với phép toán nhân.

Ví dụ 3.17. (a) $\mathbb{Z}$ là một vành giao hoán có nhiều hơn một phần tử, có đơn vị nhưng không phải một trường vì $2 \in \mathbb{Z}$ và 2 không có nghịch đảo trong $\mathbb{Z}$.

(b) $\mathbb{Q}$, $\mathbb{R}$ và $\mathbb{C}$ là các trường.

(c) $\mathbb{Z}_4$ là một vành giao hoán có đơn vị nhưng không phải một trường vì phần tử $\overline{2} \in \mathbb{Z}_4$ không có nghịch đảo. $\mathbb{Z}_5$ là một vành giao hoán có đơn vị, hơn nữa phần tử $\overline{1}$ có nghịch đảo là chính nó, $\overline{2}$ có nghịch đảo là $\overline{3}$, $\overline{3}$ có nghịch đảo là $\overline{2}$, $\overline{4}$ có nghịch đảo là $\overline{4}$ nên $\mathbb{Z}_5$ là một trường.

Ta thấy rằng trường luôn là một miền nguyên, tức là trong một trường không có ước của không. Thật vậy, nếu F là một trường và $a \in F$, $a \neq 0$ thì a không phải ước của không, vì nếu có $b \in F$ sao cho $ab = 0$ thì

$$b = \left(a^{-1}a\right)b = a^{-1}(ab) = a^{-1}0 = 0.$$

Tuy nhiên điều ngược lại không đúng, chẳng hạn $\mathbb{Z}$ là một miền nguyên nhưng không phải một trường. Đối với miền nguyên có hữu hạn phần tử thì ta có điều ngược lại như trong định lý dưới đây.

Định lý 3.18. *Mọi miền nguyên hữu hạn đều là trường.*

Chứng minh. Giả sử $D = \{a_1, a_2, \ldots, a_n\}$ là một miền nguyên và $a \in D$, $a \neq 0$. Nếu $aa_i = aa_j$, vì $a \neq 0$ nên giản ước hai vế cho a ta có $a_i = a_j$, do đó aa_i với $1 \leq i \leq n$ là n phần tử khác nhau và $D = \{aa_1, aa_2, \ldots, aa_n\}$. Vì $1 \in D$ nên có chỉ số k sao cho $aa_k = 1$ và vì vậy a có nghịch đảo trong D, ta có điều phải chứng minh.

□

Kết hợp các Định lý 3.15 và 3.18 ta có hệ quả

Hệ quả 3.19. *$\mathbb{Z}_p$ là một trường khi và chỉ khi p là một số nguyên tố.*

Định nghĩa 3.20. Xét trường E và tập con F của E ổn định đối với hai phép toán cộng và nhân trên E, tức là $x + y$, $xy \in F$ với mọi $x, y \in F$. Ta nói F là một *trường con* của E nếu F là một trường với cùng hai phép toán trên E.

Định lý 3.21. *Cho trường E và tập con F có nhiều hơn một phần tử của E. Khi đó ba điều sau tương đương.*

(a) *F là một trường con của E.*

(b) *Với mọi $x, y \in F$ thì $x + y, xy \in F$, $-x \in F$ và nếu $x \neq 0$ thì $x^{-1} \in F$.*

(c) *Với mọi $x, y \in F$ thì $x - y \in F$ và nếu $x \neq 0$ thì $x^{-1}y \in F$.*

Chứng minh. (a)⇒(b) và (b)⇒(c) là hiển nhiên. Ta chứng minh (c) ⇒(a). Vì F có nhiều hơn một phần tử nên $F^* = F \setminus \{0\}$ không rỗng, bởi giả thiết (c) ta có F^* là một nhóm con của nhóm nhân $E^* = E \setminus \{0\}$. Nếu $x, y \in F$ thì tích xy bằng 0 khi x hay y bằng 0 hoặc là một phần tử của F^* khi x và y khác 0 và do đó tích xy luôn thuộc F. Theo Định lý 3.7 ta có F là một vành, hơn nữa vành này giao hoán có đơn vị. Nếu $x \in F$, $x \neq 0$ thì x có nghịch đảo trong F^* và do đó F là một trường. Định lý được chứng minh.

□

Ví dụ 3.22. (a) $\mathbb{Q}$ là một trường con của trường $\mathbb{R}$, $\mathbb{R}$ là một trường con của trường $\mathbb{C}$.

(b) $\mathbb{Q}(\sqrt{2}) = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$ là một trường con của trường $\mathbb{R}$. Thật vậy, ta có $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt{2}\right)$. Giả sử $x = a + b\sqrt{2}, y = c + d\sqrt{2} \in \mathbb{Q}\left(\sqrt{2}\right)$, khi đó

$$x - y = (a - c) + (b - d)\sqrt{2} \in \mathbb{Q}\left(\sqrt{2}\right).$$

Hơn nữa, nếu $x \neq 0$ thì a, b không đồng thời bằng không và do đó $a - b\sqrt{2} \neq 0$. Ta có

$$x^{-1}y = \frac{c+d\sqrt{2}}{a+b\sqrt{2}} = \frac{\left(c+d\sqrt{2}\right)\left(a-b\sqrt{2}\right)}{\left(a+b\sqrt{2}\right)\left(a-b\sqrt{2}\right)}$$
$$= \frac{ca-2db}{a^2-2b^2} + \frac{da-cb}{a^2-2b^2}\sqrt{2} \in \mathbb{Q}\left(\sqrt{2}\right).$$

Vậy $\mathbb{Q}\left(\sqrt{2}\right)$ là một trường con của $\mathbb{R}$.

Mệnh đề 3.23. *Giao tùy ý các trường con của một trường cho trước cũng là một trường con của trường đó.*

Chứng minh. Hiển nhiên được suy ra từ Định lý 3.21.

□

Bài tập

1. Tìm các ước của không trong các vành sau.
   (a) $\mathbb{Z}_{16}$ (b) $\mathbb{Z}_{13}$ (c) $\mathbb{Z}_4 \times \mathbb{Z}_6$ (d) $\mathbb{Z} \times \mathbb{Q}$
2. Tìm ví dụ về một vành giao hoán có nhiều hơn một phần tử, không có ước của không nhưng không phải là một miền nguyên.
3. Cho a là phần tử lũy linh trong vành giao hoán R có đơn vị. Chứng tỏ
   (a) $a = 0$ hoặc a là một ước của không.
   (b) ax là lũy linh với mọi $x \in R$.
   (c) $1 + a$ là phần tử khả nghịch trong R.
   (d) Nếu u là phần tử khả nghịch trong R thì $u + a$ cũng vậy.
4. Vành nào sau đây là một trường?
   (a) $\mathbb{Z}[i]$ (b) $\mathbb{Q} \times \mathbb{R}$
   (c) $\mathbb{Q}(\sqrt{5}) = \left\{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\right\}$ (d) $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$
5. Cho p là một số nguyên tố, chứng tỏ tập hợp $\mathbb{Q}(\sqrt{p}) = \left\{a + b\sqrt{p} \mid a, b \in \mathbb{Q}\right\}$ là một trường con của trường số thực.
6. Chứng tỏ tập hợp $\mathbb{Q}\left(\sqrt[3]{2}\right) = \left\{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\right\}$ là một trường con của trường số thực.
7. Chứng minh rằng trường các số hữu tỷ không có trường con nào khác ngoài chính nó.
8. Chứng minh rằng trường $\mathbb{Z}_p$ (p là số nguyên tố) không có trường con nào khác ngoài chính nó.

3.3 Iđêan và vành thương

Định nghĩa 3.24. Giả sử R là một vành và I một nhóm con của nhóm cộng R. Ta nói I là một *iđêan trái (phải)* của R nếu $rx \in I$ ($xr \in I$) với mọi $r \in R$ và $x \in I$; là một *iđêan* nếu nó vừa là iđêan trái vừa là iđêan phải.

Khi R là một vành giao hoán thì các khái niệm iđêan một phía và iđêan là trùng nhau.

Nếu I là một iđêan của vành R thì I là một vành con của R, nhưng điều ngược lại nói chung không đúng. Thật vậy, trong Ví dụ 3.8 thì S là một vành con của $M(3,\mathbb{R})$ nhưng không là một iđêan của $M(3,\mathbb{R})$ vì với $r = \begin{pmatrix} 0\,0\,0 \\ 1\,1\,1 \\ 0\,0\,0 \end{pmatrix} \in M(3,\mathbb{R})$, $x = \begin{pmatrix} 1\,1\,1 \\ 0\,0\,0 \\ 0\,0\,0 \end{pmatrix} \in S$ thì $rx = \begin{pmatrix} 0\,0\,0 \\ 1\,1\,1 \\ 0\,0\,0 \end{pmatrix} \notin S$.

Ta có mệnh đề sau là hiển nhiên.

Mệnh đề 3.25. *Cho I là một tập con không rỗng của vành R. Khi đó hai điều sau tương đương.*

(a) *I là một iđêan của R.*

(b) *$x - y \in I$ và $rx, xr \in I$ với mọi $x, y \in I$, $r \in R$.*

Ví dụ 3.26. (a) Cho R là một vành. Khi đó $\{0\}$ là một iđêan của R và gọi là iđêan *tầm thường; R* là một iđêan của chính nó và gọi là iđêan *không thật sự.* Các iđêan khác, trừ hai iđêan ở trên, gọi là các iđêan thật sự không tầm thường của R.

(b) Cho trước số nguyên n, khi đó tập hợp $n\mathbb{Z}$ gồm các bội số của n là một iđêan của vành số nguyên $\mathbb{Z}$.

Mệnh đề 3.27. *Giao tùy ý của một họ các iđêan của vành R cũng là một iđêan của R.*

Chứng minh. Giả sử $(I_j)_{j\in J}$ là một họ các iđêan của vành R. Đặt $I = \cap_{j\in J} I_j$. Ta thấy $0 \in I_j$ với mọi $j \in J$ nên $0 \in I$ và do đó $I \neq \emptyset$. Nếu $x, y \in I$, $r \in R$ thì $x, y \in I_j$, và vì I_j là iđêan của R nên $x - y, rx, xr \in I_j$ với mọi $j \in J$, do đó $x - y, rx, xr \in I$. Theo Mệnh đề 3.25 thì I là một iđêan của R.

□

Bây giờ cho trước vành R và tập con U của R. Đặt (U) là giao của tất cả iđêan của R chứa U, khi đó (U) là một iđêan và là iđêan nhỏ nhất chứa U. Ta nói (U) là *iđêan của R được sinh ra bởi U.*

Chú ý rằng $(\emptyset) = \{0\}$ và $(U) = U$ nếu U là một iđêan của R.

Mệnh đề sau mô tả cụ thể các phần tử của iđêan được sinh ra bởi U.

Mệnh đề 3.28. *Cho R là một vành giao hoán có đơn vị và $U = \{a_1, \ldots, a_n\} \subset R$. Khi đó iđêan được sinh ra bởi U gồm các phần tử có dạng $x_1a_1 + x_2a_2 + \cdots + x_na_n$, trong đó $x_1, x_2, \ldots, x_n$ là các phần tử tùy ý của R.*

Chứng minh. Đặt $I = \{x_1a_1 + x_2a_2 + \cdots + x_na_n \mid x_1, x_2, \ldots, x_n \in R\}$. Ta có $U \subset I$, nếu $u = \sum_{i=}^{n} x_ia_i$, $v = \sum_{i=}^{n} y_ia_i \in I$, $r \in R$ thì $u - v = \sum_{i=}^{n} (x_i - y_i)\, a_i \in I$ và $ru = \sum_{i=}^{n} (rx_i)\, a_i \in I$ nên I là một iđêan chứa U. Vì mỗi $x_ia_i \in (U)$ với $i = 1, \ldots, n$, do (U) là iđêan nên $\sum_{i=}^{n} x_ia_i \in (U)$, và do đó $I \subset (U)$. Vậy $I = (U)$ và ta có điều phải chứng minh.

□

Trong mệnh đề trên ta xét trường hợp đặc biệt khi $U = \{a\} \subset R$. Khi đó iđêan được sinh ra bởi a là $(a) = \{xa \mid x \in R\} = Ra$.

Ví dụ 3.29. Cho $n \in \mathbb{N}$, khi đó iđêan của $\mathbb{Z}$ được sinh ra bởi n là $(n) = n\mathbb{Z}$. Đảo lại, cho I là một iđêan tùy ý của $\mathbb{Z}$ ta chứng tỏ I có dạng $m\mathbb{Z}$ với số tự nhiên m nào đó. Thật vậy, vì I cũng là một nhóm con của $\mathbb{Z}$ nên có $m \in \mathbb{N}$ sao cho $I = m\mathbb{Z}$.

Mệnh đề 3.30. *Cho R là một vành có đơn vị. Nếu I là một iđêan của R chứa đơn vị thì $I = R$.*

Chứng minh. Giả sử 1 là đơn vị của vành R. Với x tùy ý thuộc R, vì $1 \in I$ nên $x = x \cdot 1 \in I$ và do đó $R \subset I$. Vậy $I = R$.

□

Mệnh đề 3.31. *Cho F là một vành giao hoán có đơn vị, có nhiều hơn một phần tử. Khi đó F là một trường nếu và chỉ nếu trong F chỉ có hai iđêan là $\{0\}$ và chính nó.*

Chứng minh. Giả sử F là một trường và I là iđêan tùy ý của F. Nếu I không tầm thường, khi đó có $a \in I$ và $a \neq 0$. Ta có $1 = a^{-1}a \in I$ và do đó theo Mệnh đề 3.30 thì $I = F$.

Đảo lại, vì F là một vành giao hoán có đơn vị, có hơn một phần tử, để chứng tỏ F là một trường ta chỉ cần chứng tỏ mọi phần tử khác không trong F đều có nghịch đảo. Cho $a \in F$, $a \neq 0$ và xét $(a) = Fa$ là iđêan được sinh ra bởi a, vì $(a) \neq \{0\}$, bởi giả thiết F chỉ có hai iđêan là $\{0\}$ và chính nó nên $(a) = F$. Ta có $1 \in (a) = Fa$ suy ra có $r \in F$ sao cho $1 = ra$. Vậy a có nghịch đảo và mệnh đề được chứng minh.

□

Mệnh đề 3.32. *Cho I là một iđêan của vành R. Trên nhóm cộng R/I ta định nghĩa phép nhân*

$$(x + I) \cdot (y + I) = xy + I$$

với mọi $x + I, y + I \in R/I$, khi đó R/I là một vành. Hơn nữa, nếu R là một vành giao hoán thì R/I cũng là một vành giao hoán; R có đơn vị thì R/I cũng có đơn vị.

Chứng minh. Trước hết ta chứng tỏ phép nhân ở trên được định nghĩa đúng đắn, tức là nếu $x + I = x' + I$, $y + I = y' + I$ thì ta phải có

$$xy + I = x'y' + I.$$

Thật vậy, vì $x + I = x' + I$, $y + I = y' + I$ nên có $h, k \in I$ sao cho $x = x' + h$, $y = y' + k$. Ta có

$$xy = (x' + h)(y' + k) = x'y' + (x'k + hy' + hk).$$

Vì I là iđêan nên $x'k, hy', hk \in I$ và do đó $x'k + hy' + hk \in I$. Vậy hai lớp kề $xy + I$ và $x'y' + I$ bằng nhau. Vì phép nhân trên R có tính kết hợp và phân phối với phép cộng nên trên phép nhân R/I cũng có các tính chất đó. Vậy R/I là một vành. Hơn nữa, nếu R giao hoán thì hiển nhiên R/I giao hoán. Nếu R có đơn vị 1 thì R/I có đơn vị là $1 + I$.

□

Ví dụ 3.33. (a) Cho vành R. Ta có $\{0\}$ là iđêan của R và $R/\{0\} = R$; R là iđêan của chính nó và R/R là vành chỉ có một phần tử.

(b) Xét vành $\mathbb{Z}$. Với $n \in \mathbb{N}$, $n \geq 2$ cho trước thì $n\mathbb{Z}$ là một iđêan của $\mathbb{Z}$ và $\mathbb{Z}/n\mathbb{Z}$ chính là vành $\mathbb{Z}_n$ các số nguyên mod n.

Định nghĩa 3.34. Giả sử R là một vành và I là một iđêan của R. Khi đó vành R/I được gọi là *vành thương* của R theo I.

Định nghĩa 3.35. Giả sử R là một vành giao hoán có đơn vị và I là một iđêan thực sự của R. Ta nói I là *iđêan nguyên tố* nếu với $x, y \in R$ mà tích $xy \in I$ thì ta luôn có $x \in I$ hay $y \in I$; là *iđêan tối đại* nếu R là iđêan duy nhất thực sự chứa I.

Ví dụ 3.36. (a) $2\mathbb{Z}$ là iđêan nguyên tố và cũng là iđêan tối đại của $\mathbb{Z}$. $6\mathbb{Z}$ không phải là iđêan nguyên tố vì $2 \cdot 3 \in 6\mathbb{Z}$ nhưng $2, 3 \notin 6\mathbb{Z}$. $6\mathbb{Z}$ cũng không phải iđêan tối đại của $\mathbb{Z}$ vì $6\mathbb{Z} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$.

(b) Như đã biết trong $\mathbb{Z}$ mọi iđêan đều có dạng $p\mathbb{Z}$, $p \geq 0$. Nếu $p\mathbb{Z}$ không là iđêan tầm thường ($p > 0$), ta chứng tỏ $p\mathbb{Z}$ là iđêan nguyên tố nếu và chỉ nếu p là một số nguyên tố. Thật vậy, giả sử $p\mathbb{Z}$ là iđêan nguyên tố, nếu p là một hợp số thì có $1 < a, b < p$ sao cho $p = ab$. Khi đó $ab \in p\mathbb{Z}$ nhưng $a \notin p\mathbb{Z}$ và $b \notin p\mathbb{Z}$, mâu thuẩn với $p\mathbb{Z}$ là iđêan nguyên tố. Đảo lại, nếu p là một số nguyên tố và $ab \in p\mathbb{Z}$ thì ab chia hết cho p, do đó a hoặc b chia hết cho p. Khi đó $a \in p\mathbb{Z}$ hoặc $b \in p\mathbb{Z}$ và $p\mathbb{Z}$ là iđêan nguyên tố.

Lưu ý rằng mọi iđêan tối đại đều nguyên tố. Thật vậy, giả sử I là iđêan tối đại và có tích $ab \in I$ với $a \notin I$, ta chứng tỏ $b \in I$. Vì $a \notin I$ nên $I + (a)$ là iđêan chứa I và khác I, do I tối đại nên $I + (a) = R$. Ta có $1 \in R$ và $1 = y + ra$ với $y \in I$ và

$r \in R$, suy ra $b = 1 \cdot b = yb + r(ab) \in I$ vì $y, ab \in I$ và I là iđêan. Vậy I là nguyên tố. Tuy nhiên điều ngược lại không đúng như trong ví dụ sau.

Ví dụ 3.37. Trong vành tích $R = \mathbb{Z} \times \mathbb{Z}$ xét $I = \mathbb{Z} \times \{0\}$, I là một iđêan của R. Nếu $x = (a, b), x' = (a', b') \in R$ sao cho $xx' = (aa', bb') \in I$ thì $bb' = 0$. Khi đó $b = 0$ hoặc $b' = 0$, tức là $x \in I$ hoặc $x' \in I$. Do đó I là iđêan nguyên tố. Nhưng I không phải iđêan tối đại vì

$$I = \mathbb{Z} \times \{0\} \subsetneq \mathbb{Z} \times 3\mathbb{Z} \subsetneq \mathbb{Z} \times \mathbb{Z} = R,$$

ở đây $\mathbb{Z} \times 3\mathbb{Z}$ là một iđêan của R.

Định lý sau cho ta thấy vai trò quan trọng của iđêan nguyên tố và iđêan tối đại.

Định lý 3.38. *Cho R là một vành giao hoán có nhiều hơn một phần tử, có đơn vị và I là một iđêan của R. Khi đó*

(a) *R/I là một miền nguyên nếu và chỉ nếu I là một iđêan nguyên tố.*

(b) *R/I là một trường nếu và chỉ nếu I là một iđêan tối đại.*

Chứng minh. Chú ý rằng I là iđêan thực sự của R nếu và chỉ nếu R/I là một vành giao hoán có nhiều hơn một phần tử và có đơn vị.

(a) R/I là một miền nguyên nếu và chỉ nếu nó không có ước của không. Điều này tương đương với $(a + I)(b + I) = ab + I = I$ nếu và chỉ nếu $a + I = I$ hoặc $b + I = I$. Vì vậy R/I là một miền nguyên nếu và chỉ nếu $ab \in I$ hàm ý $a \in I$ hoặc $b \in I$, và điều này nói rằng I là một iđêan nguyên tố.

(b) Giả sử R/I là một trường. Khi đó I là iđêan thực sự của R, xét iđêan J của R sao cho $I \subset J \subset R$. Ta có J/I là một iđêan của R/I. Theo Mệnh đề 3.31 thì hoặc $J/I = \{0\}$, trong trường hợp này thì $J = I$, hoặc $J/I = R/I$, trong trường hợp này thì $J = R$. Vì vậy I là iđêan tối đại. Đảo lại, Giả sử I là một iđêan tối đại và xét $a + I \in R/I$ là phần tử khác không. Khi đó $a \notin I$ và $I + (a)$ là iđêan chứa I và khác I, vì I tối đại nên $I + (a) = R$. Ta có $1 \in R$ và $1 = y + ra$ với $y \in I$ và $r \in R$, suy ra $1 + I = ra + I = (r + I)(a + I)$. Vậy $a + I$ có nghịch đảo trong R/I, vì vậy R/I là một trường.

□

Bài tập

1. Tập hợp I nào sau đây là một iđêan của vành được cho?

   (a) $I = \mathbb{Q}$ trong vành $\mathbb{R}$.

   (b) $I = 2\mathbb{Z} \times 3\mathbb{Z}$ trong vành $\mathbb{Z} \times \mathbb{Z}$.

(c) $I = \{(n, n) \mid n \in \mathbb{Z}\}$ trong vành $\mathbb{Z} \times \mathbb{Z}$.

(d) $I = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$ trong vành $\mathbb{Z}_{12}$.

(e) $I = \left\{ \begin{pmatrix} n & 0 \\ m & 0 \end{pmatrix} \mid m, n \in \mathbb{Q} \right\}$ trong vành $M(2, \mathbb{Q})$.

(f) $I = \{n + ni \mid n \in \mathbb{Z}\}$ trong vành $\mathbb{Z}[i]$.

2. Trong vành các số nguyên Gauss $\mathbb{Z}[i]$ hãy mô tả iđêan (i).
3. Trong vành các số nguyên Gauss $\mathbb{Z}[i]$ ta xét iđêan $I = (1 - i)$.
   (a) Chứng tỏ $2 \in I$.
   (b) Tìm tất cả lớp kề của I trong $\mathbb{Z}[i]$.
   (c) Mô tả vành thương $\mathbb{Z}[i]/I$.
4. Cho R là một vành tùy ý và $a \in R$. Chứng tỏ tập hợp $aR = \{ax \mid x \in R\}$ là một iđêan phải của R và $Ra = \{xa \mid x \in R\}$ là một iđêan trái của R.
5. Cho I và J là hai iđêan của vành R. Chứng minh rằng
   (a) Tập hợp $I + J = \{a + b \mid a \in I, b \in J\}$ là một iđêan.
   (b) Tập hợp $IJ = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n \mid a \in I, b_i \in J, n \in \mathbb{N}^*\}$ là một iđêan.
   (c) $IJ \subset I \cap J$.
   (d) Nếu R giao hoán và $I + J = R$ thì $IJ = I \cap J$.
6. Cho R là một vành tùy ý và n là một số nguyên cho trước. Chứng tỏ tập hợp $I = \{x \in R \mid nx = 0\}$ là một iđêan của R.
7. Cho R là một vành giao hoán và $a \in R$. Chứng tỏ iđêan được sinh ra bởi a là $(a) = \{ax \mid x \in R\}$ nếu R có đơn vị, và $(a) = \{ax + na \mid x \in R, n \in \mathbb{Z}\}$ nếu R không có đơn vị.
8. Cho D là một miền nguyên và $a, b \in D$. Chứng tỏ rằng $(a) = (b)$ nếu và chỉ nếu có phần tử $u \in D$ khả nghịch sao cho $a = ub$.
9. Cho I là một iđêan của vành R. Chứng tỏ $M(2, I)$ là một iđêan của vành $M(2, R)$.
10. Cho R là một vành giao hoán. Đặt $\mathrm{Ann}(R) = \{a \in R \mid \forall x \in R,\ ax = 0\}$, chứng tỏ $\mathrm{Ann}(R)$ là một iđêan của R.
11. Cho R là một vành giao hoán và I là một iđêan của R. Đặt

$$\mathrm{rad}(I) = \{a \in R \mid \exists n \in \mathbb{Z}, a^n \in I\},$$

chứng tỏ $\mathrm{rad}(R)$ là một iđêan của R chứa I.

12. Iđêan $(3 + i)$ có phải là một iđêan nguyên tố của vành $\mathbb{Z}[i]$ không?
13. Tìm các iđêan tối đại của $\mathbb{Z}_{20}$, và trong mỗi trường hợp hãy mô tả vành thương.
14. Tìm các iđêan tối đại của $\mathbb{Z}_6 \times \mathbb{Z}_{15}$, và trong mỗi trường hợp hãy mô tả vành thương.
15. Chứng tỏ rằng I là một iđêan tối đại của $\mathbb{Z}_n$ nếu và chỉ nếu $I = (\overline{p})$, ở đây p là một ước số nguyên tố của n.

16. Cho hai vành R và S có đơn vị. Chứng tỏ rằng
    (a) Nếu I là iđêan của R và J là iđêan của S thì $I \times J$ là iđêan của $R \times S$.
    (b) Nếu M là iđêan của $R \times S$ thì có các iđêan I của R và J của S sao cho $M = I \times J$.
    (c) M là iđêan tối đại của $R \times S$ nếu và chỉ nếu $M = I \times S$ với I iđêan tối đại của R, hoặc $M = R \times J$ với J iđêan tối đại của S.

3.4 Đồng cấu vành

Định nghĩa 3.39. Giả sử f là một ánh xạ từ vành R đến vành S. Ta nói f là một *đồng cấu vành* nếu

$$f(x+y) = f(x) + f(y) \text{ và } f(xy) = f(x) f(y)$$

với mọi $x, y \in R$.

Nếu $f : R \longrightarrow S$ là đồng cấu vành thì f cũng là một đồng cấu nhóm từ nhóm cộng R đến nhóm cộng S, do đó ta có $f(0_R) = 0_S$ và $f(-x) = -f(x)$ với mọi $x \in R$.

Định nghĩa 3.40. Giả sử $f : R \longrightarrow S$ là một đồng cấu vành. Ta nói f là một *đơn cấu* nếu f là một đơn ánh; là một *toàn cấu* nếu f là một toàn ánh; là một *đẳng cấu* nếu f là một song ánh. Một đẳng cấu từ vành R đến chính nó còn được gọi là một *tự đẳng cấu* của R.

Ví dụ 3.41. (a) Cho R và S là hai vành. Khi đó ánh xạ $x \in R \longmapsto 0 \in S$ với mọi $x \in R$ là một đồng cấu vành gọi là đồng cấu *tầm thường*.

(b) Cho S là một vành con của vành R. Khi đó ánh xạ $x \in S \longmapsto x \in R$ với mọi $x \in S$ là một đơn cấu.

(e) Cho R là một vành. Khi đó ánh xạ đồng nhất $x \in R \longmapsto x \in R$ là một tự đẳng cấu.

(f) Giả sử I là một iđêan của vành R. Khi đó phép chiếu chính tắc

$$\begin{aligned} \Pr : R &\longrightarrow R/I \\ x &\mapsto \Pr(x) = x + I \end{aligned}$$

là một toàn cấu.

(g) Xác định các đồng cấu vành $f : \mathbb{Z} \longrightarrow \mathbb{Z}$. Vì f cũng là đồng cấu nhóm với phép toán cộng nên ta có $f(m) = f(m1) = mf(1)$ với mọi $m \in \mathbb{Z}$. Vậy f hoàn toàn được xác định bởi giá trị $f(1)$. Đặt $a = f(1)$, ta có

$$a = f(1) = f(1 \cdot 1) = f(1) f(1) = a^2.$$

Do đó $a = 0$ hoặc $a = 1$. Nếu $a = 0$ thì $f(m) = 0$ với mọi $m \in \mathbb{Z}$ và f là đồng cấu không. Nếu $a = 1$ thì $f(m) = m$ với mọi $m \in \mathbb{Z}$ và f là ánh xạ đồng nhất.

(h) Chứng tỏ phương trình $8x^3 - 11x^2 + 10x - 14 = 0$ không có nghiệm nguyên. Giả sử có số nguyên a là nghiệm của phương trình đã cho, khi đó ta có

$$8a^3 - 11a^2 + 10a - 14 = 0.$$

Xét phép chiếu chính tắc $\mathrm{Pr} : \mathbb{Z} \longrightarrow \mathbb{Z}_3$ được cho bởi $\mathrm{Pr}(m) = \overline{m}$. Khi đó

$$\begin{aligned} \overline{0} &= \mathrm{Pr}(0) = \mathrm{Pr}\left(8a^3 - 11a^2 + 10a - 14\right) \\ &= \overline{8a^3 - 11a^2 + 10a - 14} = \overline{2}\overline{a}^3 - \overline{2}\overline{a}^2 + \overline{a} - \overline{2}. \end{aligned}$$

Đặt $b = \overline{a} \in \mathbb{Z}_3$ thì b là nghiệm của phương trình $\overline{2}y^3 - \overline{2}y^2 + y - \overline{2} = \overline{0}$. Mặt khác dễ thấy phương trình trên không có nghiệm trong $\mathbb{Z}_3$. Ta có điều vô lý, vậy phương trình đã cho không có nghiệm nguyên.

Mệnh đề 3.42. *Cho $f : R \longrightarrow S$ là một đồng cấu vành. Khi đó*

(a) *Nếu A là một vành con của R thì $f(A)$ là một vành con của S.*

(b) *Nếu I là một vành con của S thì $f^{-1}(I)$ cũng là một vành con của R. Hơn nữa, nếu I là một iđêan của S thì $f^{-1}(I)$ cũng là một iđêan của R.*

Chứng minh. (a) Vì A là một nhóm con của nhóm cộng R nên $f(A)$ là một nhóm con của nhóm cộng S. Xét hai phần tử tùy ý $y, y' \in f(A)$, khi đó có $x, x' \in A$ sao cho $y = f(x)$, $y' = f(x')$. Ta có

$$yy' = f(x) f(x') = f(xx') \in f(A)$$

vì $xx' \in A$. Vậy ta có (a).

(b) Vì I là một nhóm con của nhóm cộng S nên $f^{-1}(I)$ là một nhóm con của nhóm cộng R. Xét hai phần tử tùy ý $x, x' \in f^{-1}(I)$, suy ra $f(x), f(x') \in I$. Ta có

$$f(xx') = f(x) f(x') \in I$$

vì I là một vành con, và do đó $xx' \in f^{-1}(I)$. Vậy $f^{-1}(I)$ là một vành con của R.

Nếu I là một iđêan của S, khi đó với bất kỳ $r \in R$, $x \in f^{-1}(I)$ thì

$$f(rx) = f(r) f(x) \in I$$

và do đó $rx \in f^{-1}(I)$. Chứng minh tương tự ta cũng có $xr \in f^{-1}(I)$. Vậy $f^{-1}(I)$ là một iđêan của R.

□

Một hệ quả hiển nhiên là

Hệ quả 3.43. *Cho $f : R \longrightarrow S$ là một đồng cấu vành. Khi đó*
(a) $\mathrm{Im} f = f(R)$ *là một vành con của* S.
(b) $\ker f = f^{-1}(0_S)$ *là một iđêan của* R.

Khi R và S là các trường, đồng cấu vành từ R đến S còn gọi là *đồng cấu trường*. Ta thấy rằng nếu $f : R \longrightarrow S$ là một đồng cấu trường thì f là một đơn cấu hoặc đồng cấu không. Thật vậy, ta có $\ker f$ là một iđêan của R, theo Mệnh đề 3.31 R chỉ có hai iđêan là $\{0\}$ và chính nó, nếu $\ker f = \{0\}$ thì f là một đơn cấu; nếu $\ker f = R$ thì f là đồng cấu không.

Mệnh đề 3.44. *Cho $f : R \longrightarrow S$ và $g : S \longrightarrow T$ là hai đồng cấu vành. Khi đó $g \circ f$ cũng là một đồng cấu vành. Hơn nữa, nếu f, g lần lượt là các đơn cấu, toàn cấu, đẳng cấu thì $g \circ f$ cũng lần lượt là đơn cấu, toàn cấu, đẳng cấu.*

Chứng minh. Hiển nhiên từ định nghĩa của đồng cấu vành.

□

Mệnh đề 3.45. *Nếu $f : R \longrightarrow S$ là một đẳng cấu vành thì f^{-1} cũng là một đẳng cấu vành.*

Chứng minh. Giả sử $f : R \longrightarrow S$ là một đẳng cấu vành. Vì f cũng là một đẳng cấu nhóm nên f^{-1} là một đẳng cấu nhóm. Mệnh đề sẽ được chứng minh nếu ta chứng tỏ f^{-1} là một đồng cấu vành. Với bất kỳ $y, y' \in S$, do f là một song ánh nên có duy nhất $x, x' \in G$ sao cho $f(x) = y,\ f(x') = y'$. Vì $f(xx') = f(x) f(x') = yy'$ nên

$$f^{-1}(yy') = xx' = f^{-1}(y) f^{-1}(y')$$

và mệnh đề được chứng minh.

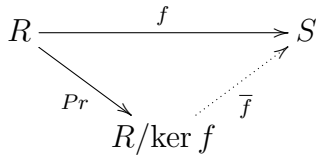
□

Định nghĩa 3.46. Ta nói vành R *đẳng cấu* với vành S, ký hiệu $R \cong S$, nếu có một đẳng cấu vành f từ R đến S.

Mệnh đề sau là hiển nhiên được suy ra từ các Mệnh đề 3.44 và 3.45.

Mệnh đề 3.47. *Quan hệ đẳng cấu là một quan hệ tương đương trên lớp các vành.*

Định lý 3.48. *Giả sử $f : R \longrightarrow S$ là một đồng cấu vành và $\mathrm{Pr} : R \longrightarrow R/\ker f$ là phép chiếu chính tắc. Khi đó*
(a) *Có duy nhất một đồng cấu vành $\overline{f} : R/\ker f \longrightarrow S$ sao cho biểu đồ*



giao hoán, tức là $\overline{f} \circ Pr = f$.

(b) $\overline{f}$ *là một đơn cấu và* $\operatorname{Im} \overline{f} = \operatorname{Im} f$.

Chứng minh. Bởi Định lý 1.91 có duy nhất đơn cấu nhóm

$$\begin{aligned} \overline{f} : R/\ker f &\longrightarrow S, \\ x + \ker f &\longmapsto f(x) \end{aligned}$$

thỏa mãn các yêu cầu của định lý. Định lý sẽ được chứng minh nếu ta chứng tỏ $\overline{f}$ là một đồng cấu vành. Thật vậy, với bất kỳ $x + \ker f, x' + \ker f \in R/\ker f$ thì

$$\begin{aligned} \overline{f}\left((x + \ker f) \cdot (x' + \ker f)\right) &= \overline{f}\left(xx' + \ker f\right) \\ &= f\left(xx'\right) \\ &= f(x) f\left(x'\right) \\ &= \overline{f}\left(x + \ker f\right) \overline{f}\left(x' + \ker f\right) \end{aligned}$$

và ta có điều phải chứng minh.

□

Hệ quả 3.49. (Định lý đẳng cấu vành thứ nhất) *Giả sử* $f : R \to S$ *là một đồng cấu vành. Khi đó*

$$R/\ker f \cong \operatorname{Im} f.$$

Định lý 3.50. *Cho các số tự nhiên* $m_1, m_2, \ldots, m_r$ *sao cho từng đôi một nguyên tố cùng nhau. Xét ánh xạ* $f : \mathbb{Z} \longrightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$ *được xác định bởi* $f(x) = (\overline{x}, \overline{x}, \ldots, \overline{x})$ *với mọi* $x \in \mathbb{Z}$. *Khi đó* f *là một toàn cấu và* $\ker f = (m_1 m_2 \cdots m_r)\,\mathbb{Z}$.

Chứng minh. Hiển nhiên f là một đồng cấu vành. Ta chứng tỏ f là một toàn ánh. Với mỗi k sao cho $1 \leq k \leq r$ đặt $n_k = \prod_{1 \leq i \leq r, i \neq k} m_i$, ta có $\gcd(m_k, n_k) = 1$. Vì $\gcd(m_k, n_k) = 1$ nên có $r_k, s_k \in \mathbb{Z}$ sao cho $r_k m_k + s_k n_k = 1$, khi đó $\overline{s_k n_k} = \overline{1}$ trong $\mathbb{Z}_{m_k}$ và $\overline{s_k n_k} = \overline{0}$ trong $\mathbb{Z}_{m_i}$ với mọi $i \neq k$. Với $(\overline{a_1}, \overline{a_2}, \ldots, \overline{a_r})$ tùy ý trong $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$, đặt $x = \sum_{j=1}^{r} (s_j n_j) a_j \in \mathbb{Z}$. Trong $\mathbb{Z}_{m_k}$ ta có

$$\begin{aligned}\overline{x} &= \overline{\sum_{j=1}^{r}(s_j n_j)a_j} \\ &= \overline{(s_k n_k)a_k} + \overline{\sum_{1\le j\le r, j\neq k}(s_j n_j)a_j} \\ &= \overline{(s_k n_k)}\,\overline{a_k} + \sum_{1\le j\le r, j\neq k}\overline{(s_j n_j)}\,\overline{a_j} \\ &= \overline{a_k}\end{aligned}$$

và f là một toàn ánh. Ta có $x \in \ker f$ nếu và chỉ nếu $f(x) = (\overline{x}, \overline{x}, \ldots, \overline{x}) = \left(\overline{0}, \overline{0}, \ldots, \overline{0}\right)$, suy ra $\overline{x} = \overline{0}$ trong $\mathbb{Z}_{m_j}$ tức là x chia hết cho m_j với mọi j. Vì các m_j, $1 \le j \le r$, từng đôi một nguyên tố cùng nhau nên x chia hết cho $\prod_{1\le j\le r} m_j$. Vậy $\ker f = (m_1 m_2 \cdots m_r)\,\mathbb{Z}$.

□

Hệ quả sau được suy ra từ Hệ quả 3.49 và Định lý 3.50.

Hệ quả 3.51. (a) *Cho các số tự nhiên $m_1, m_2, \ldots, m_r$ sao cho từng đôi một nguyên tố cùng nhau. Khi đó vành tích $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$ đẳng cấu với vành $\mathbb{Z}_{m_1 m_2 \cdots m_r}$.*

(b) *Cho $n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ là một phân tích số tự nhiên n thành tích các lũy thừa của các số nguyên tố khác nhau. Khi đó ta có đẳng cấu vành $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_r^{n_r}}$.*

Ví dụ 3.52. Vì $300 = 16 \cdot 25 = 2^4 \cdot 5^2$ nên vành $\mathbb{Z}_{300}$ đẳng cấu với vành tích $\mathbb{Z}_{2^4} \times \mathbb{Z}_{5^2} = \mathbb{Z}_{16} \times \mathbb{Z}_{25}$.

Hệ quả 3.53. *Cho hệ phương trinh đồng dư*

$$\begin{cases} x &\equiv a_1 \ mod\ m_1 \\ x &\equiv a_2 \ mod\ m_2 \\ . &\ldots\ldots\ldots\ldots \\ x &\equiv a_r \ mod\ m_r \end{cases}$$

trong đó $m_1, \ldots, m_r$ là các số tự nhiên từng đôi một nguyên tố cùng nhau. Khi đó hệ phương trình đã cho luôn có nghiệm. Giả sử $x_0 \in \mathbb{Z}$ là một nghiệm của hệ, khi đó tập hợp tất cả các nghiệm của hệ là $\{x_0 + k\,(m_1 m_2 \cdots m_r) \mid k \in \mathbb{Z}\}$.

Chứng minh. Xét ánh xạ $f : \mathbb{Z} \longrightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$ được xác định bởi $f(x) = (\overline{x}, \overline{x}, \ldots, \overline{x})$ với mọi $x \in \mathbb{Z}$. Theo Định lý 3.50 f là một toàn ánh nên với $(\overline{a_1}, \overline{a_2}, \ldots, \overline{a_r}) \in \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$ thì có $x_0 \in \mathbb{Z}$ sao cho $f(x_0) = (\overline{a_1}, \overline{a_2}, \ldots, \overline{a_r})$. Nói cách khác, với mỗi i ta có $\overline{x_0} = \overline{a_i}$ hay $x_0 \equiv a_i \bmod m_i$. Vậy x_0 là một nghiệm của hệ. Giả sử $x_1 \in \mathbb{Z}$ là một nghiệm tùy ý của hệ, khi đó

$$\begin{aligned} f(x_1 - x_0) &= f(x_1) - f(x_0) \\ &= (\overline{a_1}, \overline{a_2}, \ldots, \overline{a_r}) - (\overline{a_1}, \overline{a_2}, \ldots, \overline{a_r}) \\ &= \left(\overline{0}, \overline{0}, \ldots, \overline{0}\right). \end{aligned}$$

Do đó $x_1 - x_0 \in \ker f = (m_1 m_2 \cdots m_r)\,\mathbb{Z}$, vậy có $k \in \mathbb{Z}$ để $x_1 = x_0 + k\,(m_1 m_2 \cdots m_r)$. Khẳng định còn lại của hệ quả được chứng minh.

□

Ví dụ 3.54. (a) Tìm các giá trị nguyên x thỏa mãn hệ phương trình đồng dư

$$\begin{cases} x & \equiv 3 \bmod 5 \\ x & \equiv 2 \bmod 8 \end{cases}.$$

Nếu x_0 là một giá trị thỏa mãn hệ thì theo Hệ quả 3.53 tập hợp tất cả giá trị nguyên thỏa mãn hệ là $\{x_0 + 40k \mid k \in \mathbb{Z}\}$. Bây giờ ta tìm x_0. Vì 5 và 8 nguyên tố cùng nhau nên có $r, s \in \mathbb{Z}$ sao cho $1 = 5r + 8s$, cụ thể ta lấy $r = -3$, $s = 2$. Lấy $x_0 = (5r)\,2 + (8s)\,3 = -30 + 48 = 18$ thì thỏa mãn hệ phương trình đã cho. Vậy tập hợp tất cả giá trị nguyên cần tìm là $\{18 + 40k \mid k \in \mathbb{Z}\}$.

(b) Tìm số nguyên x sao cho khi chia cho 3 dư 2, chia cho 4 dư 1, chia cho 5 dư 3. Số nguyên x phải tìm là nghiệm của hệ phương trình đồng dư

$$\begin{cases} x & \equiv 2 \bmod 3 \\ x & \equiv 1 \bmod 4 \\ x & \equiv 3 \bmod 5 \end{cases}.$$

Ta có $1 = 7 \cdot 3 + (-1) \cdot (4 \cdot 5)$, $1 = 4 \cdot 4 + (-1) \cdot (3 \cdot 5)$, $1 = 5 \cdot 5 + (-2) \cdot (3 \cdot 4)$. Lấy

$$x_0 = 2 \cdot (-1) \cdot (4 \cdot 5) + 1 \cdot (-1) \cdot (3 \cdot 5) + 3 \cdot (-2) \cdot (3 \cdot 4) = -127$$

là một nghiệm của hệ. Khi đó tập hợp các giá trị nguyên x cần tìm là

$$\{-127 + 60k \mid k \in \mathbb{Z}\}.$$

Bài tập

1. Cho $f : R \longrightarrow S$ là một đồng cấu của các vành giao hoán. Hãy chứng tỏ
   (a) Nếu I là một iđêan nguyên tố trong S và $f^{-1}(I) \neq R$ thì $f^{-1}(I)$ cũng là một iđêan nguyên tố trong R.
   (b) Nếu I là một iđêan tối đại trong S và $f^{-1}(I) \neq R$ thì $f^{-1}(I)$ cũng là một iđêan tối đại trong R.

2. Xác định các đồng cấu vành f trong các trường hợp sau.
   (a) $f : \mathbb{Z} \longrightarrow \mathbb{Z}_6$ (b) $f : \mathbb{Z}_5 \longrightarrow \mathbb{Z}$ (c) $f : \mathbb{Z}_7 \longrightarrow \mathbb{Z}_6$
   (d) $f : \mathbb{Z}_{12} \longrightarrow \mathbb{Z}_6$ (e) $f : \mathbb{Z}[i] \longrightarrow \mathbb{C}$ (f) $f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$
3. Mô tả vành tự đồng cấu $\text{End}(\mathbb{Z}_2 \times \mathbb{Z}_2)$. Nó có phải là một vành giao hoán không?
4. Tìm số các vành không đẳng cấu có ba phần tử.
5. Chứng tỏ $\mathbb{Z}_2$ là vành Bool duy nhất (sai khác một đẳng cấu) sao cho nó là miền nguyên.
6. Cho D là một miền nguyên và n là cấp của phần tử đơn vị e trong nhóm cộng D. Hãy chứng tỏ
   (a) n là một số nguyên tố và $nx = 0$ với mọi $x \in D$.
   (b) Tập hợp $mD = \{mx \mid x \in D\}$ là một iđêan của D, trong đó m là một số nguyên tùy ý.
   (c) $D/mD \cong D$ nếu m là một bội số của n và $D/mD \cong \{0\}$ nếu m không phải bội số của n.
7. Cho $(R, +, \cdot)$ là một vành có đơn vị. Ta định nghĩa phép toán $\oplus$ và $\circ$ trên R bởi

$$x \oplus y = x + y + 1 \qquad \text{và} \qquad x \circ y = x \cdot y + x + y.$$

   Hãy chứng tỏ
   (a) $(R, \oplus, \circ)$ là một vành.
   (b) $(R, \oplus, \circ)$ đẳng cấu với $(R, +, \cdot)$.
8. Cho R là một vành và S là một tập hợp có hai phép toán cộng và nhân. Giả sử có song ánh $f : R \longrightarrow S$ có tính chất

$$f(x + y) = f(x) + f(y)$$
$$f(xy) = f(x) f(y)$$

   với mọi $x, y \in R$. Hãy chứng minh rằng
   (a) S là một vành.
   (b) S là một miền nguyên nếu R là một miền nguyên.
   (c) S là một trường nếu R là một trường.
9. Cho R là một vành có đơn vị. Chứng tỏ
   (a) Với $a \in R$ thì ánh xạ

$$h_a : R \longrightarrow R$$
$$x \longmapsto ax$$

   là một đồng cấu nhóm từ nhóm cộng Abel R đến chính nó.
   (b) Ánh xạ

$$h : R \longrightarrow \mathrm{End}\,(R)$$
$$a \longmapsto h_a$$

là một đơn cấu (vành).

10. Tìm các giá trị nguyên x thỏa mãn hệ phương trình đồng dư sau.

(a) $\begin{cases} 2x & \equiv 3 \bmod 5 \\ x & \equiv 2 \bmod 6 \end{cases}$ (b) $\begin{cases} x & \equiv 3 \bmod 15 \\ x & \equiv 2 \bmod 4 \\ x & \equiv 2 \bmod 7 \end{cases}$

11. Cho $f : R \longrightarrow S$ là một đồng cấu vành và I, J lần lượt là hai iđêan của R và S sao cho $f(I) \subset J$. Gọi $p : R \longrightarrow R/I$ và $q : S \longrightarrow S/J$ là hai phép chiếu chính tắc, khi đó chứng minh rằng tồn tại duy nhất một đồng cấu vành $\overline{f} : R/I \longrightarrow S/J$ sao cho $\overline{f} \circ p = q \circ f$. Hơn nữa, nếu f là một toàn cấu thì $\overline{f}$ cũng vậy.
12. (Định lý đẳng cấu vành thứ hai) Cho S là một vành con của vành R và I là một iđêan của R. Chứng minh rằng
    (a) $S + I = \{a + b \mid a \in S, b \in I\}$ là một vành con của R.
    (b) $S \cap I$ là một iđêan của S.
    (c) $(S + I)/I \cong S/(S \cap I)$.
13. (Định lý đẳng cấu vành thứ ba) Cho I và J là hai iđêan của vành R với $I \subset J$. Chứng minh rằng $(R/I)/(J/I) \cong R/J$.
14. Cho trường F với phần tử đơn vị e. Đặt $D = \{ne \mid n \in \mathbb{Z}\}$, chứng tỏ rằng
    (a) Trong nhóm cộng F nếu e có cấp vô hạn thì D là một vành và đẳng cấu với vành $\mathbb{Z}$ các số nguyên.
    (b) Trong trường hợp e có cấp p thì D là một trường và đẳng cấu với trường $\mathbb{Z}_p$ các số nguyên mod$p$.
15. (a) Xác định các đồng cấu trường của trường các số hữu tỷ.
    (b) Xác định các đồng cấu trường của trường các số thực.
    (c) Xác định các đồng cấu trường của trường các số phức giữ nguyên các số thực.
16. Xác định các đồng cấu trường của trường $\mathbb{Z}_p$.
17. Chứng tỏ tập hợp
$$F = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}$$
là một trường với phép cộng, phép nhân ma trận và trường này đẳng cấu với trường $\mathbb{Q}(\sqrt{2})$.
18. Chứng tỏ tập hợp
$$F = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$$

là một trường với phép cộng, phép nhân ma trận và trường này đẳng cấu với trường các số phức.

19. Chứng tỏ $\mathbb{Q}\left(\sqrt{5}\right)$ và $\mathbb{Q}\left(\sqrt{7}\right)$ là hai trường không đẳng cấu.
20. Chứng tỏ $\mathbb{R}$ và $\mathbb{C}$ là hai trường không đẳng cấu.
21. Chứng tỏ hai trường có p phần tử (p là số nguyên tố) thì đẳng cấu.
22. Chứng tỏ rằng mọi trường đều chứa một trường con nhỏ nhất (theo quan hệ bao hàm), trường này đẳng cấu với trường $\mathbb{Q}$ các số hữu tỷ hoặc trường $\mathbb{Z}_p$ các số nguyên mod$p$.

3.5 Trường các thương

Cho D là một miền nguyên, ta sẽ chứng tỏ luôn có một trường chứa D như một vành con. Để làm điều đó ta đặt $D^* = D \setminus \{0\}$, trên $D \times D^*$ xét quan hệ $(a,b) \sim (c,d)$ nếu $ad = bc$ với mọi $(a,b), (c,d) \in D \times D^*$. Quan hệ $\sim$ có những tính chất sau:

(a) Với mọi $(a,b) \in D \times D^*$ ta có $(a,b) \sim (a,b)$ vì $ab = ba$ do D là một vành giao hoán.

(b) Nếu $(a,b) \sim (c,d)$ thì $ad = bc$, suy ra $cb = da$ và vì vậy $(c,d) \sim (a,b)$.

(c) Nếu $(a,b) \sim (c,d)$ và $(c,d) \sim (e,f)$ thì $ad = bc$ và $cf = de$, suy ra

$$afd = adf = bcf = bde = bed.$$

Vì $d \neq 0$, giản ước hai vế cho d ta có $af = be$, và do đó $(a,b) \sim (e,f)$.

Vậy quan hệ $\sim$ là một tương đương. Lớp tương đương của phần tử $(a,b) \in D \times D^*$ được ký hiệu bởi $\frac{a}{b}$. Vậy ta có

$$\frac{a}{b} = \frac{c}{d} \Longleftrightarrow ad = bc.$$

Mệnh đề 3.55. *Cho D là một miền nguyên và đặt $F = \left\{\frac{a}{b} \mid a, b \in D, b \neq 0\right\}$. Khi đó F là một trường với phép cộng và phép nhân được định nghĩa*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{và} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

với mọi $\frac{a}{b}, \frac{c}{d} \in F$. Hơn nữa, nếu ta đồng nhất phần tử $a \in D$ với phần tử $\frac{a}{1} \in F$ thì D trở thành một vành con của F và mỗi phần tử của F có dạng $\frac{a}{b} = ab^{-1}$ với $a, b \in F$, $b \neq 0$.

Chứng minh. Trước hết ta chứng tỏ phép cộng được định nghĩa như trên là đúng đắn, tức là nếu $\frac{a}{b} = \frac{a'}{b'}$ và $\frac{c}{d} = \frac{c'}{d'}$ thì ta phải có

$$\frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'}.$$

Thật vậy, từ giả thiết $\frac{a}{b} = \frac{a'}{b'}$ và $\frac{c}{d} = \frac{c'}{d'}$ suy ra $ab' = ba'$ và $cd' = dc'$. Ta có

$$(ad + bc)\, b'd' = (ab')\, dd' + (cd')\, b'b = (ba')\, d'd + (dc')\, b'b = bd\,(a'd' + b'c')$$

và do đó hai lớp $\frac{ad+bc}{bd}$ và $\frac{a'd'+b'c'}{b'd'}$ bằng nhau. Tương tự như phép cộng ta cũng chứng tỏ được phép nhân là đúng đắn.

Hiển nhiên phép cộng có tính kết hợp và giao hoán, phần tử 0 là lớp $\frac{0}{1} = \frac{0}{c}$ với mọi $c \neq 0$ và đối của lớp $\frac{a}{b}$ là lớp $\frac{-a}{b}$. Ta cũng có phép nhân có tính kết hợp, giao hoán và phân phối với phép cộng, đơn vị là $\frac{1}{1} = \frac{c}{c}$ với mọi $c \neq 0$. Nếu $\frac{a}{b} \neq 0$ trong F thì $a \neq 0$ trong D, và $\frac{b}{a}$ là nghịch đảo của $\frac{a}{b}$. Vậy F là một trường.

Bây giờ xét ánh xạ $f : D \longrightarrow F$ được xác định bởi $f(a) = \frac{a}{1}$ với mọi $a \in D$. f là một đồng cấu vành vì

$$f(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = f(a) + f(b),$$
$$f(ab) = \frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1} = f(a)\, f(b).$$

Hơn nữa, f là một đơn cấu và do đó $D \cong \mathrm{Im}f$ là một vành con của F. Với mỗi phần tử $\frac{a}{b} \in F$ ta có

$$\frac{a}{b} = \frac{a}{1} \cdot \frac{1}{b} = \frac{a}{1} \cdot \left(\frac{b}{1}\right)^{-1}.$$

Nếu ta đồng nhất phần tử $a \in D$ với phần tử $\frac{a}{1} \in F$ thì ta có $\frac{a}{b} = ab^{-1}$.

□

Mệnh đề 3.56. *Cho miền nguyên D, trường F như trong mệnh đề trên và K là trường tùy ý chứa D. Khi đó có một đơn cấu η từ F đến K sao cho $\eta(a) = a$ với mọi $a \in D$.*

Chứng minh. Ta định nghĩa η như sau. Với $a \in D$ thì $\eta(a) = a$. Với bất kỳ $\frac{a}{b} \in F$, vì $b \in D$ và $b \neq 0$ nên $\eta(b) \neq 0$ trong K, ta định nghĩa $\eta\left(\frac{a}{b}\right) = \eta(a)\,\eta(b)^{-1}$. Ánh xạ η được định nghĩa đúng đắn vì nếu $\frac{a}{b} = \frac{c}{d}$, khi đó $ad = bc$ trong D và $\eta(a)\,\eta(d) = ad = bc = \eta(b)\,\eta(c)$ trong K, vì vậy $\eta(a)\,\eta(b)^{-1} = \eta(c)\,\eta(d)^{-1}$. Dễ thấy rằng η là một đồng cấu trường, và do η khác không nên là một đơn cấu.

□

Định nghĩa 3.57. Cho miền nguyên D. Ta nói một trường F là trường các thương của D nếu có một đơn cấu vành f từ D đến F sao cho mọi phần tử của F đều có dạng $f(a)\, f(b)^{-1}$ với $a, b \in D$, $b \neq 0$.

Định lý 3.58. *Trường các thương của một miền nguyên là tồn tại và được xác định duy nhất sai khác một đẳng cấu.*

Chứng minh. Cho D là một miền nguyên. Bởi Mệnh đề 3.55 trường các thương F của D luôn tồn tại. Nếu K là trường các thương khác của D và $g : D \longrightarrow K$ là đơn cấu vành như trong định nghĩa của trường các thương K, đồng nhất $a \in D$ với $g(a) \in K$ ta xem K chứa D như một vành con, khi đó có đơn cấu η như trong chứng minh của Mệnh đề 3.56 từ F đến K. Vì K gồm các phần tử có dạng $g(a)\, g(b)^{-1}$ với $a, b \in D$, $b \neq 0$ nên η là một toàn ánh. Vậy η là một đẳng cấu.

□

Mệnh đề 3.59. *Mọi trường E chứa miền nguyên D đều chứa trường các thương của D.*

Chứng minh. Được suy ra từ Mệnh đề 3.56.

□

Như vậy ta có thể nói rằng một miền nguyên D tùy ý đều được chứa trong một trường các thương của nó, trường các thương của D được cấu tạo gồm các phần tử trong D, nghịch đảo các phần tử khác không của D và lấy tích của chúng, đây là trường nhỏ nhất trong các trường chứa D. Trường các thương được xác định duy nhất sai khác một đẳng cấu.

Ví dụ 3.60. (a) Trường các thương của miền nguyên $\mathbb{Z}$ là trường $\mathbb{Q}$ các số hữu tỷ.

(b) Cho trường F, khi đó F là một miền nguyên. Vì trường các thương của F là trường nhỏ nhất chứa F nên trường các thương của F là chính nó.

Bài tập

1. Xác định trường các thương của các miền nguyên sau.
   (a) $\mathbb{Z}[i]$ (b) $\mathbb{R}$ (c) $\mathbb{Z}_5$
   (d) $\mathbb{Z}[\sqrt{3}] = \left\{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\right\}$ (e) $\mathbb{Q}\left(\sqrt{3}\right)$
2. Cho p là một số nguyên tố. Chứng tỏ 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.

Chương 4
VÀNH ĐA THỨC

Đa thức luôn đóng một vai trò quan trọng trong đại số và giải tích. Tập hợp các đa thức với phép cộng và nhân hai đa thức tạo thành một vành. Trong chương này chúng ta sẽ tìm hiểu về chúng. Đặc biệt ta sẽ tìm hiểu vành đa thức một biến, kết quả quan trọng trong vành các số nguyên như phân tích số tự nhiên lớn hơn một thành tích của những số nguyên tố được mở rộng cho vành đa thức một biến. Cuối chương dành cho việc tìm hiểu đa thức nhiều biến, đặc biệt là các đa thức đối xứng.

4.1 Vành đa thức một biến

Cho R là một vành giao hoán có đơn vị. Ta nói một đa thức với hệ số trong R là dãy $(a_0, a_1, a_2, \ldots, a_n, \ldots)$, trong đó $a_n \in R$ và các a_n bằng không với hầu hết ngoại trừ hữu hạn các chỉ số n. Đặt P là tập hợp các đa thức với hệ số trong R. Với hai đa thức $f = (a_0, a_1, a_2, \ldots, a_n, \ldots)$ và $g = (b_0, b_1, b_2, \ldots, b_n, \ldots)$ tùy ý trong P ta định nghĩa

$$f + g = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n, \ldots)$$

và

$$f \cdot g = (c_0, c_1, c_2, \ldots, c_n, \ldots),$$

trong đó $c_n = \sum_{i+j=n} a_i b_j$. Vì chỉ có hữu hạn các chỉ số n sao cho $a_n + b_n$, c_n khác không nên $f + g, f \cdot g \in P$ và do đó phép cộng và phép nhân ở trên là hai phép toán trên P. Dễ thấy rằng P là một vành giao hoán, có đơn vị với hai phép toán đã cho, phần tử không còn gọi đa thức không là dãy $(0, 0, \ldots)$ các phần tử đều bằng không, phần tử đơn vị là dãy $(1, 0, \ldots, 0, \ldots)$.

Xét ánh xạ $\eta : R \longrightarrow P$ được xác định bởi $\eta(a) = (a, 0, \ldots, 0, \ldots)$ với mọi $a \in R$. Khi đó η là một đơn cấu, đồng nhất phần tử $a \in R$ với đa thức gọi là đa thức hằng $(a, 0, \ldots, 0, \ldots) \in P$ ta xem R là một vành con của P.

Bây giờ đặt $x = (0, 1, \ldots, 0, \ldots)$, ta có

$$\begin{aligned} x^2 &= (0,0,1,0,\ldots,0,\ldots) \\ x^3 &= (0,0,0,1,0,\ldots,0,\ldots) \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ x^n &= \Big(\underbrace{0,\ldots,0}_{n \text{ số không}},1,0,\ldots,0,\ldots\Big). \end{aligned}$$

Hơn nữa, $a \in R$ thì

$$ax^n = \Big(\underbrace{0,\ldots,0}_{n \text{ số không}},a,0,\ldots,0,\ldots\Big).$$

Nếu $f = (a_0, a_1, a_2, \ldots, a_n, \ldots) \in P$ thì f được viết ở dạng

$$f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \cdots,$$

tổng ở đây chỉ là hữu hạn vì các a_n đều bằng không với hầu hết ngoại trừ hữu hạn các chỉ số n và biểu diễn trên là duy nhất. Các số a_n gọi là hệ số của đa thức. Lưu ý rằng hai đa thức $a_0 + a_1x + \cdots + a_nx^n$ và $b_0 + b_1x + \cdots + b_mx^m$ $(n \le m)$ bằng nhau nếu và chỉ nếu $a_0 = b_0$, $a_1 = b_1, \ldots, a_n = b_n$ và $b_{n+1} = \cdots = b_m = 0$.

Định nghĩa 4.1. Cho R là một vành giao hoán có đơn vị. Ký hiệu $R[x]$ là tập hợp tất cả đa thức với hệ số trong R, khi đó $R[x]$ là một vành giao hoán, có đơn vị và được gọi là *vành đa thức một biến.*

Định nghĩa 4.2. Cho đa thức $f = a_0 + a_1x + \cdots + a_nx^n \in R[x]$. Nếu $a_n \neq 0$ thì f được gọi là đa thức *bậc* n và viết $\deg f = n$. Hệ số a_n gọi là hệ số dẫn đầu, nếu $a_n = 1$ thì f gọi là *đơn hệ*.

Để cho tiện ta quy ước bậc của đa thức không bằng $-\infty$.

Ví dụ 4.3. (a) Xét hai đa thức $f = \bar{2}x^3 + \bar{3}x + \bar{1}$ và $g = \bar{3}x^2 + \bar{1}$ trong $\mathbb{Z}_6[x]$. Khi đó

$$\begin{aligned} f \cdot g &= \left(\bar{2}x^3 + \bar{3}x + \bar{1}\right)\left(\bar{3}x^2 + \bar{1}\right) \\ &= \bar{2}x^3 + \bar{3}x^3 + \bar{3}x + \bar{3}x^2 + \bar{1} \\ &= \bar{5}x^3 + \bar{3}x^2 + \bar{3}x + \bar{1} \end{aligned}$$

chỉ là đa thức bậc 3 khác với tổng hai bậc của f và g là 5.

(b) Xét hai đa thức khác không $f = \bar{2}x^3$ và $g = \bar{3}x^2$ trong $\mathbb{Z}_6[x]$, nhưng đa thức tích $f \cdot g$ lại là đa thức không.

Mệnh đề 4.4. *Cho D là một miền nguyên và hai đa thức $f, g \in D[x]$. Khi đó ta có* $\deg(f \cdot g) = \deg f + \deg g$.

Chứng minh. Nếu f hay g là đa thức không thì mệnh đề hiển nhiên đúng. Giả sử $f = \sum_{i=0}^{n} a_i x^i$ là đa thức bậc n và $g = \sum_{j=0}^{m} a_j x^j$ là đa thức bậc m, khi đó đa thức tích $f \cdot g = a_n b_m x^{n+m} + \sum_{i=0}^{n+m-1} c_i x^i$. Ta có $a_n \neq 0$ và $b_m \neq 0$, vì D là một miền nguyên nên $a_n b_m \neq 0$ và do đó $f \cdot g$ là đa thức có bậc $n+m$. Mệnh đề được chứng minh.

□

Hệ quả sau được suy ra từ mệnh đề trên là

Hệ quả 4.5. *Nếu D là một miền nguyên thì $D[x]$ cũng là một miền nguyên.*

Mệnh đề 4.6. *Cho D là một miền nguyên. Khi đó những phần tử khả nghịch trong $D[x]$ chính là những phần tử khả nghịch trong D.*

Chứng minh. Cho f là phần tử khả nghịch trong $D[x]$ và g là nghịch đảo của nó trong $D[x]$. Khi đó $f \cdot g = 1$ là đa thức có bậc không, theo Mệnh đề 4.4 thì f và g phải là các đa thức bậc không nên là các đa thức hằng thuộc D. Mệnh đề được chứng minh.

□

Từ mệnh đề trên ta thấy rằng $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{Z}_p[x]$, ở đây p là số nguyên tố, chỉ là các miền nguyên nhưng không phải là trường.

Định nghĩa 4.7. Cho D là một miền nguyên. Khi đó trường các thương của $D[x]$, ký hiệu $D(x)$, gọi là trường các *phân thức* với hệ số trong D, nó gồm các phần tử có dạng f/g, ở đây $f, g \in D[x]$ với $g \neq 0$.

Chú ý rằng hai phần tử f/g và h/k trong $D(x)$ là bằng nhau nếu và chỉ nếu $f \cdot k = g \cdot h$.

Trong phần còn lại của chương này, nếu không nói gì thêm thì ta hiểu đa thức được xét là đa thức với hệ số trong một trường.

Bài tập

1. Tính $f \cdot g$ với f, g được cho trong $R[x]$ trong các trường hợp sau.
   (a) $f = \overline{2}x^2 + x + \overline{1}$, $g = \overline{3}x^3 + \overline{2}x + \overline{1}$ trong $\mathbb{Z}_6[x]$.
   (b) $f = \overline{2}x^2 + x + \overline{1}$, $g = \overline{3}x^3 + \overline{2}x + \overline{1}$ trong $\mathbb{Z}_5[x]$.
2. Tìm tất cả đa thức có bậc nhỏ hơn bốn trong $\mathbb{Z}_2[x]$.
3. Tìm tất cả đa thức có bậc nhỏ hơn ba trong $\mathbb{Z}_3[x]$.
4. Chứng tỏ ánh xạ $\psi : \mathbb{R}[x] \longrightarrow \mathbb{C}$ được định nghĩa bởi: với $f = \sum_{k=1}^{n} a_k x^k \in \mathbb{R}[x]$ thì $\psi(f) = f(i) = \sum_{k=1}^{n} a_k i^k \in \mathbb{C}$ là một đồng cấu vành. Xác định $\ker \psi$ và $\mathrm{Im}\psi$.

5. Xác định hạt nhân và ảnh của đồng cấu vành $\psi : \mathbb{R}[x] \longrightarrow \mathbb{C}$ được định nghĩa bởi $\psi(f) = f\left(1 + i\sqrt{2}\right)$.
6. Cho $\eta : R \longrightarrow S$ là một đồng cấu vành. Ta định nghĩa $\eta^* : R[x] \longrightarrow S[x]$ như sau: với bất kỳ $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ thì $\eta^*(f) = \sum_{i=0}^{n} \eta(a_i) x^i$. Chứng tỏ η^* là một đồng cấu vành. Nó được gọi là đồng cấu cảm sinh.
7. Cho $\mathrm{Pr} : \mathbb{Z} \longrightarrow \mathbb{Z}_7$ là phép chiếu chính tắc. Chứng tỏ đồng cấu cảm sinh $\mathrm{Pr}^* : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_7[x]$ là một toàn cấu, xác định $\ker(\mathrm{Pr}^*)$.
8. Chứng tỏ nếu R và S là hai vành đẳng cấu thì $R[x]$ và $S[x]$ cũng vậy.
9. Chứng tỏ nếu S là một vành con của R thì $S[x]$ cũng là một vành con của $R[x]$.
10. Tìm những phần tử khả nghịch của các vành sau.
    (a) $\mathbb{Z}[x]$ (b) $\mathbb{R}[x]$ (c) $\mathbb{Z}_7[x]$ (d) $\mathbb{Z}(x)$
11. Tìm một số tự nhiên $n > 1$ và đa thức $f \in \mathbb{Z}_n[x]$ có bậc dương sao cho nó là một phần tử khả nghịch trong $\mathbb{Z}_n[x]$.

4.2 Phép chia Euclid

Như đã biết trong vành các số nguyên có phép chia có dư của một số nguyên cho một số nguyên khác không, phép chia này còn gọi là phép chia Euclid. Phép chia Euclid vẫn còn đúng trong vành đa thức được thể hiện qua định lý sau.

Định lý 4.8. *Cho hai đa thức $f, g \in F[x]$ và $g \neq 0$. Khi đó tồn tại duy nhất hai đa thức q (gọi là đa thức thương) và r (đa thức dư) với $r = 0$ hay $\deg r < \deg g$ sao cho $f = qg + r$. Nếu $r = 0$ thì ta nói f chia hết cho g.*

Chứng minh. Ta chứng minh bằng quy nạp theo bậc của f. Trước hết ta chứng tỏ sự tồn tại của biểu diễn. Nếu $\deg f < \deg g$, ta lấy $q = 0$ và $r = f$ thì $f = qg + r$. Nếu $\deg f \geq \deg g$, giả sử $f = a_0 + a_1 x + \cdots + a_n x^n$ và $g = b_0 + b_1 x + \cdots + b_m x^m$, $b_m \neq 0$. Xét đa thức $f_1 = f - a_n b_m^{-1} x^{n-m} g$ thì $\deg f_1 < \deg f$, bởi giả thiết quy nạp tồn tại hai đa thức q_1 và r với $r = 0$ hay $\deg r < \deg g$ sao cho $f_1 = q_1 g + r$. Do đó

$$\begin{aligned} f &= f_1 + a_n b_m^{-1} x^{n-m} g \\ &= q_1 g + r + a_n b_m^{-1} x^{n-m} g \\ &= \left(q_1 + a_n b_m^{-1} x^{n-m}\right) g + r \\ &= qg + r \end{aligned}$$

với $q = q_1 + a_n b_m^{-1} x^{m-n}$.

Bây giờ ta chứng minh tính duy nhất của biểu diễn. Giả sử $f = q'g + r'$ với $r' = 0$ hay $\deg r' < \deg g$ là một biểu diễn khác, khi đó ta có

$$(q - q')\, g = r' - r.$$

Nếu $q \neq q'$ thì bậc của đa thức bên trái lớn hơn bậc của đa thức bên phải. Mâu thuẩn này chứng tỏ $q = q'$, do đó $r' - r = 0$ và $r = r'$. Định lý được chứng minh.

□

Ví dụ 4.9. Cho $f, g \in \mathbb{Z}_5[x]$, $f = \overline{2}x^4 + x^3 + \overline{3}x^2 + \overline{3}x + \overline{1}$, $g = \overline{2}x^2 - x + \overline{2}$. Tìm q và r trong phép chia f cho g. Thực hiện phép chia đa thức như phép chia đa thức hệ số nguyên ta được $f = \left(x^2 + x + \overline{1}\right) g + \overline{2}x - \overline{1}$, do đó $q = x^2 + x + \overline{1}$ và $r = \overline{2}x - \overline{1}$.

Định nghĩa 4.10. Cho đa thức $f = a_0 + a_1 x + \cdots + a_n x^n$ với hệ số trong F và phần tử $c \in F$. Ta nói $f(c) = a_0 + a_1 c + \cdots + a_n c^n \in F$ là giá trị của f tại $x = c$, nếu $f(c) = 0$ thì c gọi là một *nghiệm* của f.

Mệnh đề 4.11. *Dư của phép chia đa thức f cho $x - c$ là $f(c)$.*

Chứng minh. Theo Định lý 4.8 tồn tại hai đa thức q và r với $\deg r < 1$ sao cho

$$f = q(x - c) + r.$$

Vì $\deg r < 1$ nên r là một đa thức hằng. Cho $x = c$ suy ra $f(c) = r$.

□

Một hệ quả hiển nhiên là

Hệ quả 4.12. *Đa thức $f \in F[x]$ chia hết cho $x - c$ với $c \in F$ khi và chỉ khi c là một nghiệm của f.*

Chú ý rằng hệ quả trên vẫn đúng khi F là một vành giao hoán có đơn vị. Thật vậy, cho $f = \sum_{i=1}^{n} a_i x^i \in F[x]$ và $c \in F$. c là một nghiệm của f thì $\sum_{i=1}^{n} a_i c^i = 0$. Điều này tương đương với

$$\begin{aligned} f &= \sum_{i=1}^{n} a_i x^i - \sum_{i=1}^{n} a_i c^i \\ &= \sum_{i=1}^{n} a_i \left(x^i - c^i\right) \\ &= (x - c) \left(\sum_{i=1}^{n} a_i \left(x^{i-1} + c x^{i-2} + \cdots + c^{i-1}\right) \right) \end{aligned}$$

và f chia hết cho $x - c$.

Định nghĩa 4.13. Cho $f \in F[x]$ và $c \in F$ là một nghiệm của f. Ta nói c là nghiệm bội s nếu

$$f = (x - c)^s g,$$

ở đây $g \in F[x]$ và $g(c) \neq 0$. Khi đó ta có thể xem f có s nghiệm c.

Ví dụ 4.14. (a) $f = x^3 - 1 = (x-1)(x^2+x+1) \in \mathbb{Q}[x]$, ta có $1 \in \mathbb{Q}$ là nghiệm đơn (bội 1) của f.

(b) $f = x^3 - \overline{1} = \left(x - \overline{1}\right)^3 \in \mathbb{Z}_3[x]$, do đó $\overline{1} \in \mathbb{Z}_3$ là nghiệm bội 3 của f.

Mệnh đề 4.15. *Cho $f \in F[x]$ là đa thức bậc n ($n \geq 1$). Khi đó f có nhiều nhất n nghiệm trong F.*

Chứng minh. Ta chứng minh mệnh đề bằng quy nạp theo bậc n của đa thức. Với $n = 1$ mệnh đề hiển nhiên đúng. Cho $n > 1$ và giả sử mệnh đề đúng với mọi đa thức có bậc nhỏ hơn n. Xét đa thức f có bậc n. Nếu f không có nghiệm thì mệnh đề đúng. Ngược lại, gọi c là một nghiệm của f, khi đó có đa thức $g \in F[x]$ sao cho $f = (x-c)g$. Vì $\deg f = n$ nên $\deg g = n-1$. Theo giả thiết quy nạp g có nhiều nhất $n-1$ nghiệm và nghiệm của g cũng là nghiệm của f nên f có nhiều nhất n nghiệm.

□

Định lý 4.16. *Cho F là một trường có hữu hạn phần tử. Khi đó $F^* = F \setminus \{0\}$ là một nhóm nhân cyclic.*

Chứng minh. Theo định lý cơ bản của nhóm Abel hữu hạn thì $F^* \cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_n}$, ở đây d_i là lũy thừa của số nguyên tố và C_{d_i} là nhóm nhân cyclic cấp d_i. Đặt $N = \prod_{i=1}^{n} d_i$ và M là bội số chung nhỏ nhất của $d_1, d_2, \ldots, d_n$, ta có $M \leq N$. Với mỗi $b_i \in C_{d_i}$ ta có $(b_i)^{d_i} = 1$ nên $(b_i)^M = 1$. Do đó với mỗi $a \in F^*$ thì $a^M = 1$ hay nói cách khác, mọi phần tử của F^* đều là nghiệm của đa thức $x^M - 1$ trong $F[x]$. Bởi Mệnh đề 4.15 thì $|F^*| \leq M$, nhưng ta đã biết $|F^*| = N$ và do đó $N = M$. Điều này chỉ xảy ra khi và chỉ khi các số d_i và d_j với $i \neq j$ là nguyên tố cùng nhau và bởi Hệ quả 2.15 ta có $F^* \cong C_N$ là nhóm cyclic cấp N.

□

Bài tập

1. Tìm đa thức thương và dư trong mỗi trường hợp sau.
   (a) Chia $3x^4 + 4x^3 - x^2 + 5x - 1$ cho $2x^2 + x + 1$ trong $\mathbb{Q}[x]$.
   (b) Chia $x^7 + x^6 + x^4 + x + \overline{1}$ cho $x^2 + x + \overline{1}$ trong $\mathbb{Z}_2[x]$.
   (c) Chia $\overline{2}x^5 + x^4 + \overline{2}x^3 + x + \overline{1}$ cho $x^3 + x + \overline{1}$ trong $\mathbb{Z}_3[x]$.
2. Tìm nghiệm của các đa thức sau.
   (a) $x^3 + \overline{3}x + \overline{5}$ trong $\mathbb{Z}_7$.
   (b) $x^4 + \overline{3}x + \overline{2}$ trong $\mathbb{Z}_5$.
   (c) $x^3 + \overline{2}x + \overline{5}$ trong $\mathbb{Z}_6$.
   d) $x^2 - \overline{1}$ trong $\mathbb{Z}_{15}$.

(e) x^3+x^2+x+1 trong $\mathbb{R}$.

(f) $x^4+x^3+x^2+x+1$ trong $\mathbb{C}$.

3. Cho D là một miền nguyên. Chứng minh rằng nếu đa thức $f \in D[x]$ có hai nghiệm phân biệt $a, b \in D$ thì f chia hết cho đa thức $(x-a)(x-b)$.
4. (a) Chứng tỏ đa thức hệ số thực $x^{92}+x^{61}+x^{30}$ luôn chia hết cho x^2+x+1.

   (b) Chứng tỏ đa thức hệ số thực $x^{2p}-x^p+1$ luôn chia hết cho x^2-x+1 với mọi số nguyên tố $p>3$.
5. Cho các đa thức hệ số thực f, g và h thỏa mãn $f(x^3)+xg(x^3)=(1+x+x^3)h(x)$. Chứng tỏ f, g, h luôn chia hết cho $x-1$.
6. Trong vành đa thức $\mathbb{Z}[x]$ chứng tỏ $f=(x-2)^{2n}+(x-1)^n-1$ luôn chia hết cho x^2-3x+2. Tìm thương của phép chia.
7. Cho đa thức $f=ax^{n+1}+bx^n+1 \in \mathbb{Z}[x]$. Xác định a và b để f chia hết cho $(x-1)^2$. Tìm thương của phép chia.
8. Trong $\mathbb{R}[x]$ tìm đa thức dư trong phép chia đa thức f cho đa thức g trong mỗi trường hợp sau.

   (a) $f=(\cos\alpha - x\sin\alpha)^n$, $g=x^2+1$, trong đó n là số tự nhiên dương và α là số thực cho trước.

   (b) $f=(x-1)^n+(x-2)^n$, $g=(x-1)^2(x-2)^2$, trong đó n là số tự nhiên dương cho trước.
9. Cho $a_1, a_2, \ldots, a_{n+1}$là các phần tử khác nhau trong trường F và $b_1, b_2, \ldots, b_{n+1}$ là các phần tử của F. Chứng tỏ có nhiều nhất một đa thức $f \in F[x]$ có bậc không vượt quá n sao cho $f(a_i)=b_i$ với mọi $i=1,\ldots,n+1$.
10. Cho $a_1, a_2, \ldots, a_{n+1}$là các phần tử khác nhau trong trường F và $b_1, b_2, \ldots, b_{n+1}$ là các phần tử của F. Chứng tỏ đa thức

$$f=\sum_{i=1}^{n+1} B_i(x-a_1)\cdots(x-a_{i-1})(x-a_{i+1})\cdots(x-a_{n+1}),$$

   trong đó $B_i = b_i/(a_i-a_1)\cdots(a_i-a_{i-1})(a_i-a_{i+1})\cdots(a_i-a_{n+1})$, là đa thức duy nhất bậc n trong $F[x]$ sao cho $f(a_i)=b_i$ với mọi $i=1,\ldots,n+1$.
11. Cho trường F và $f, g \in F[x]$ với $\deg f, \deg g \geq 1$. Chứng tỏ tồn tại duy nhất các đa thức $q_0, q_1, \ldots, q_r \in F[x]$ sao cho $\deg q_i < \deg g$, $i=0,1,\ldots,r$, và

$$f=q_r g^r+\cdots+q_2 g^2+q_1 g+q_0.$$

12. Tìm các q_i trong bài tập trên trong mỗi trường hợp sau.

   (a) $f=x^4+2x+3$, $g=x+1$ trong $\mathbb{Q}[x]$.

   (b) $f=x^4+x+\overline{1}$, $g=x+\overline{1}$ trong $\mathbb{Z}_2[x]$.

   (c) $f=x^5+x+\overline{3}$, $g=x^2+\overline{1}$ trong $\mathbb{Z}_5[x]$.

13. (*Định lý Wilson*) Chứng minh rằng $(n-1)! \equiv -1 \bmod n$ nếu và chỉ nếu n là một số nguyên tố.

4.3 Hàm đa thức

Định nghĩa 4.17. Cho đa thức $f = \sum_{i=0}^{n} a_i x^i \in F[x]$. Ta nói *hàm đa thức* cảm sinh từ f là ánh xạ $\tilde{f} : F \longrightarrow F$ được xác định bởi $\tilde{f}(c) = \sum_{i=0}^{n} a_i c^i$ với mỗi $c \in F$.

Đặt M là tập hợp các hàm đa thức. Với $\tilde{f}, \tilde{g} \in M$ tùy ý ta định nghĩa

$$\left(\tilde{f} + \tilde{g}\right)(c) = \tilde{f}(c) + \tilde{g}(c), \qquad \left(\tilde{f} \cdot \tilde{g}\right)(c) = \tilde{f}(c)\,\tilde{g}(c)$$

với mọi $c \in F$. Ta thấy rằng $\tilde{f} + \tilde{g}$ và $\tilde{f} \cdot \tilde{g}$ là hai hàm đa thức lần lượt được cảm sinh từ hai đa thức $f + g$ và $f \cdot g$, do đó phép cộng và phép nhân ở trên là các phép toán trên M.

Mệnh đề 4.18. *M là một vành giao hoán có đơn vị và gọi là vành các hàm đa thức.*

Chứng minh. Kiểm tra trực tiếp từ định nghĩa ta có M là một vành giao hoán có đơn vị. Phần tử không là hàm không, phần tử đơn vị là hàm hằng nhận giá trị bằng 1.

□

Nhận xét rằng ánh xạ $f \longmapsto \tilde{f}$ là một đồng cấu vành từ $F[x]$ đến M. Nó là một toàn ánh nhưng nói chung không phải là một đơn ánh. Thật vậy, ta xét khi $F = \mathbb{Z}_p$ là trường có p phần tử, ở đây p là số nguyên tố. Khi đó đa thức $x^p - x$, bởi định lý Fermat, và đa thức không cùng cảm sinh một hàm đa thức không. Do đó ánh xạ nói trên không phải là một đơn ánh. Tuy nhiên khi F là trường có vô hạn phần tử thì ta có

Mệnh đề 4.19. *Cho F là một trường có vô hạn phần tử, khi đó ánh xạ $f \longmapsto \tilde{f}$ là một đẳng cấu từ vành $F[x]$ đến vành M.*

Chứng minh. Gọi η là ánh xạ từ $F[x]$ đến M được xác định bởi $\eta(f) = \tilde{f}$. Hiển nhiên η là một toàn cấu. Nếu $\eta(h) = \eta(k)$ ta suy ra $\eta(h-k) = \eta(h) - \eta(k)$ là hàm không. Nói cách khác, với mọi $c \in F$ đều là nghiệm của đa thức $h - k$. Vì F có vô hạn phần tử nên theo Mệnh đề 4.15 thì $h - k$ là đa thức không, và do đó $h = k$. Vậy η là một đơn ánh nên là một đẳng cấu.

□

Khi F là $\mathbb{Q}$, $\mathbb{R}$ hay $\mathbb{C}$, bởi mệnh đề trên ta thường đồng nhất một đa thức với một hàm đa thức và ngược lại.

Bài tập

1. Giả sử F là một trường có hữu hạn phần tử, chứng minh rằng mọi ánh xạ từ F đến chính nó đều là hàm đa thức.
2. Giả sử F là một trường có q phần tử $a_1, \ldots, a_q$. Chứng minh rằng
   (a) Trong $F[x]$ ta có $x^q - x = (x - a_1)(x - a_2) \cdots (x - a_q)$.
   (b) Với bất kỳ $f, g \in F[x]$, $\tilde{f} = \tilde{g}$ nếu và chỉ nếu $f - g$ chia hết $x^q - x$.

4.4 Đa thức bất khả quy

Bây giờ xét hai đa thức $f, g \in F[x]$, nếu có đa thức $h \in F[x]$ sao cho $f = hg$ thì ta nói f là một bội của g hay g là một ước của f. Chú ý rằng mọi đa thức đều là ước của đa thức không. Nếu đa thức d vừa là một ước của f vừa là một ước của g thì d gọi là một ước chung của f và g.

Định nghĩa 4.20. Cho hai đa thức f và g thuộc $F[x]$. Đa thức $d \in F[x]$ gọi là một *ước chung lớn nhất* của f và g nếu d là một ước chung của f và g và bất kỳ ước chung nào khác của f và g đều là một ước của d. Ta ký hiệu $\gcd(f, g)$ để chỉ ước chung lớn nhất đơn hệ của f và g.

Mệnh đề 4.21. *Ước chung lớn nhất của hai đa thức f và g trong $F[x]$ nếu tồn tại thì duy nhất sai khác một nhân tử khác không trong F, tức là nếu d, d' là hai ước chung lớn nhất của f và g thì có $a \in F$, $a \neq 0$ sao cho $d = ad'$.*

Chứng minh. Giả sử d và d' là hai ước chung lớn nhất của f và g. Khi đó d là một ước của d' và ngược lại, do đó có các đa thức h, k sao cho $d = hd'$ và $d' = kd$. Nếu $d = 0$ thì $d' = 0$. Nếu $d \neq 0$, ta có $d = hkd$, vì $F[x]$ là một miền nguyên nên giản ước hai vế cho d ta được $hk = 1$. Vậy $h \in F$ là phần tử khác không và mệnh đề được chứng minh.

□

Mệnh đề 4.22. *Trong vành đa thức $F[x]$ cho hai đa thức f và g không đồng thời bằng không. Khi đó ước chung lớn nhất của chúng luôn tồn tại. Đặt $d = \gcd(f, g)$ thì có hai đa thức $u, v \in F[x]$ sao cho $d = uf + vg$.*

Chứng minh. Đặt $I = \{rf + sg \mid r, s \in F[x]\}$ và gọi $d \in I$ là đa thức khác không có bậc nhỏ nhất. Ta chứng tỏ d là ước chung lớn nhất của f và g. Vì $d \in I$ nên có $u, v \in F[x]$ sao cho $d = uf + vg$. Thực hiện chia f cho d ta được $f = qd + r$, trong đó q và r là hai đa thức nào đó với $r = 0$ hay $\deg r < \deg d$. Khi đó

$$r = f - qd = (1 - qu) f + (-qv) g \in I,$$

bởi tính nhỏ nhất của $\deg d$ suy ra $r = 0$, và do đó $f = qd$. Nói cách khác d là một ước của f. Tương tự, ta cũng có d là một ước của g nên d là một ước chung của f và g. Mặt khác, nếu h là một ước chung của f và g thì h là một ước của $uf + vg = d$ và do đó d là một ước chung lớn nhất của f và g.

□

Định nghĩa 4.23. Cho đa thức $p \in F[x]$ với $\deg p \geq 1$. Ta nói p là *bất khả quy* trên F (hay bất khả quy trong $F[x]$) nếu có sự phân tích $p = f \cdot g$ trong $F[x]$ thì f hoặc g phải là đa thức hằng, tức là p không thể phân tích được thành tích của hai đa thức trong $F[x]$ có bậc ≥ 1.

Chú ý rằng nếu đa thức p là bất khả quy trên F thì đa thức ap cũng vậy với mọi $a \in F$, $a \neq 0$. Một đa thức không bất khả quy trên F còn gọi là *khả quy* trên F (hay khả quy trong $F[x]$).

Ví dụ 4.24. (a) Đa thức $x^2 - 2$ là bất khả quy trên $\mathbb{Q}$ nhưng khả quy trên $\mathbb{R}$ vì $x^2 - 2 = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right)$.

(b) Đa thức $x^2 + 1$ là bất khả quy trên $\mathbb{R}$ nhưng khả quy trên $\mathbb{C}$ vì $x^2 + 1 = (x - i)(x + i)$.

(c) Đa thức

$$x^4 + 1 = \left(x^2 + 1\right)^2 - 2x^2 = \left(x^2 - \sqrt{2}x + 1\right)\left(x^2 + \sqrt{2}x + 1\right)$$

là khả quy trên $\mathbb{R}$.

(d) Đa thức $x^2 + \overline{1}$ là bất khả quy trên $\mathbb{Z}_3$ nhưng khả quy trên $\mathbb{Z}_2$ vì $x^2 + \overline{1} = x^2 - \overline{1} = \left(x - \overline{1}\right)\left(x + \overline{1}\right)$.

Mệnh đề sau là hiển nhiên.

Mệnh đề 4.25. *Đa thức bậc nhất luôn là bất khả quy.*

Mệnh đề 4.26. *Các đa thức bậc hai hoặc bậc ba với hệ số trong F là bất khả quy trên F nếu và chỉ nếu chúng không có nghiệm trong F.*

Chứng minh. Giả sử p là đa thức bậc hai hay bậc ba với hệ số trong F. Khi đó p là khả quy trên F nếu và chỉ nếu p phân tích được thành tích của hai đa thức trong đó có một đa thức bậc nhất. Điều này tương đương với p có nghiệm trong F và ta có điều phải chứng minh.

□

Ví dụ 4.27. (a) Tìm các đa thức bậc hai bất khả quy trên $\mathbb{Z}_2$. Xét đa thức bậc hai $p = x^2 + ax + b$ với $a, b \in \mathbb{Z}_2$, p là bất khả quy nếu và chỉ nếu $p\left(\overline{0}\right) \neq \overline{0}$ và $p\left(\overline{1}\right) \neq \overline{0}$. Nói cách khác, $p\left(\overline{0}\right) = b = \overline{1}$ và $p\left(\overline{1}\right) = \overline{1} + a + b = \overline{1}$, từ đây suy ra $a = b = \overline{1}$. Vậy có duy nhất một đa thức bậc hai bất khả quy trên $\mathbb{Z}_2$ là $x^2 + x + \overline{1}$.

(b) Tương tự như trên ta xét đa thức bậc ba $q = x^3+ax^2+bx+c$ với $a, b, c \in \mathbb{Z}_2$, q là bất khả quy nếu và chỉ nếu $q\left(\overline{0}\right) = \overline{1}$ và $q\left(\overline{1}\right) = \overline{1}$, do đó $c = \overline{1}$ và $\overline{1}+a+b+c = \overline{1}$. Từ đây suy ra $a = c = \overline{1}$, $b = \overline{0}$ hay $a = \overline{0}$, $b = c = \overline{1}$. Vậy có hai đa thức bậc ba bất khả quy trên $\mathbb{Z}_2$ là $x^3 + x^2 + \overline{1}$ và $x^3 + x + \overline{1}$.

Ta xét đa thức có bậc lớn hơn ba. Nếu đa thức là bất khả quy thì rõ ràng nó không có nghiệm trong trường hệ số bởi vì nếu có nghiệm thì nó phân tích được thành tích của hai đa thức trong đó có một đa thức bậc nhất. Tuy nhiên điều ngược lại không đúng, tức là có những đa thức không có nghiệm trong trường hệ số nhưng vẫn khả quy. Chẳng hạn đa thức $(x^2 + 1)^2$ không có nghiệm trong $\mathbb{R}$ và là đa thức khả quy.

Bây giờ ta sẽ chứng tỏ mọi đa thức khác hằng luôn được phân tích thành tích của những đa thức bất khả quy. Trước hết ta cần bổ đề

Bổ đề 4.28. *Cho đa thức bất khả quy p và hai đa thức f, g với hệ số trong F. Nếu p là một ước của $f \cdot g$ thì p là một ước của f hay g.*

Chứng minh. Giả sử p không phải ước của f. Vì p là bất khả quy nên 1 là ước chung lớn nhất của p và f. Theo Mệnh đề 4.22 thì có $u, v \in F[x]$ sao cho $1 = uf + vp$. Nhân hai vế cho g ta có $g = u(fg) + (vg)p$, vì p là một ước của vế phải nên p là một ước của g.

□

Định lý 4.29. *Mọi đa thức với hệ số trong F có bậc $n \geq 1$ đều phân tích được thành tích của những đa thức bất khả quy. Nếu không kể thứ tự trong phân tích thì các đa thức bất khả quy này được xác định duy nhất sai khác các hằng số nhân khác không.*

Chứng minh. Ta chứng minh sự tồn tại của phân tích bằng quy nạp theo bậc n của đa thức. Với $n = 1$ thì định lý hiển nhiên đúng. Cho $n > 1$ và giả thiết quy nạp định lý đúng đối với các đa thức có bậc nhỏ hơn n. Xét đa thức f có bậc n. Nếu f bất khả quy thì định lý đúng, ngược lại $f = gh$ với g và h là hai đa thức nào đó có bậc nhỏ hơn n. Theo quy nạp ta có $g = p_1p_2 \cdots p_r$ và $h = p_{r+1}p_{r+2} \cdots p_s$, trong đó các p_i, $1 \leq i \leq s$, là những đa thức bất khả quy nào đó và do đó $f = p_1p_2 \cdots p_rp_{r+1}p_{r+2} \cdots p_s$.

Tiếp theo ta chứng tỏ tính duy nhất của phân tích. Giả sử $f = q_1q_2 \cdots q_t$ là một phân tích khác thành tích của những đa thức bất khả quy. Ta có q_1 là một ước của f, áp dụng liên tiếp Bổ đề 4.28 thì q_1 là một ước của p_j nào đó. Bằng cách đánh số lại các chỉ số, ta giả sử q_1 là ước của p_1, vì p_1 bất khả quy nên có $a_1 \in F$, $a_1 \neq 0$ sao cho $q_1 = a_1p_1$. Giản ước hai vế cho p_1 ta được $p_2 \cdots p_s = a_1q_2 \cdots q_t$, lập luận tương tự như trên sau một số hữu hạn bước ta có $t = s$ và $p_i = a_iq_i$ với $a_i \in F$, $a_i \neq 0$, $i = 1, \ldots, t$.

□

Bài tập

1. Chứng tỏ $x^3 + \overline{2}x + \overline{1}$ là bất khả quy trên $\mathbb{Z}_5$.
2. Chứng tỏ $x^3 + x + \overline{1}$ là bất khả quy trên $\mathbb{Z}_7$.
3. Chứng tỏ $x^4 - 2x^2 - 4$ là bất khả quy trên $\mathbb{Q}$.
4. Tìm tất cả đa thức bậc hai bất khả quy trên $\mathbb{Z}_3$.
5. Tìm tất cả đa thức bậc bốn, bậc năm bất khả quy trên $\mathbb{Z}_2$.
6. Phân tích các đa thức sau thành tích của các đa thức bất khả quy trong vành được cho.
   (a) $x^4 + \overline{1} \in \mathbb{Z}_2[x]$.
   (b) $x^4 + \overline{4} \in \mathbb{Z}_5[x]$.
   (c) $x^3 + x^2 + \overline{2}x + \overline{3} \in \mathbb{Z}_7[x]$.
7. Cho trước số nguyên tố p, chứng tỏ số các đa thức có dạng $x^2 + ax + b$ bất khả quy trên $\mathbb{Z}_p$ bằng $p(p-1)/2$.
8. Cho trước số nguyên tố p và phần tử a tùy ý trong $\mathbb{Z}_p$, chứng tỏ các đa thức $x^p + a$, $x^p - a$ luôn khả quy trên $\mathbb{Z}_p$.
9. Chứng tỏ nếu đa thức $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ bậc $n \geq 1$ là bất khả quy trên một trường F nào đó thì đa thức $a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$ cũng vậy.
10. Tìm ảnh và ker của đồng cấu vành $\psi : \mathbb{R}[x] \longrightarrow \mathbb{C}$ trong mỗi trường hợp sau:
    (a) $\psi(f) = f(i)$ với mỗi $f \in \mathbb{R}[x]$.
    (b) $\psi(f) = f\left(1 + i\sqrt{3}\right)$ với mỗi $f \in \mathbb{R}[x]$.
11. Cho F là một trường. Hãy chứng tỏ
    (a) Nếu I là một iđêan của $F[x]$ thì I được sinh ra bởi một đa thức p nào đó thuộc $F[x]$.
    (b) Iđêan được sinh ra bởi p là tối đại nếu và chỉ nếu p là bất khả quy.

4.5 Nhân tử hóa đa thức hệ số phức và thực

Ta chấp nhận định lý sau gọi là định lý cơ bản của đại số mà chứng minh của nó có thể xem trong [7].

Định lý 4.30. *Mọi đa thức hệ số phức, không là đa thức hằng luôn có ít nhất một nghiệm phức.*

Hệ quả 4.31. *Mọi đa thức hệ số phức, bậc $n > 0$ đều có đúng n nghiệm phức (kể cả số bội của nghiệm).*

Chứng minh. Ta chứng minh hệ quả bằng quy nạp theo bậc n của đa thức. Nếu f là đa thức bậc nhất thì hiển nhiên định lý đúng. Cho $n > 1$ và giả sử định lý đúng với các đa thức có bậc nhỏ hơn n. Xét f là một đa thức bậc n, theo Định lý 4.30 thì

f có một nghiệm và do đó f được phân tích thành tích của một đa thức bậc nhất và một đa thức g bậc $n-1$. Bởi giả thiết quy nạp, g có $n-1$ nghiệm và nghiệm của g cũng là nghiệm của f nên f có đúng n nghiệm.

□

Tiếp theo ta chứng tỏ nghiệm phức của đa thức hệ số thực sẽ xuất hiện theo từng cặp liên hợp.

Mệnh đề 4.32. *Nếu z là một nghiệm phức của một đa thức hệ số thực thì số phức liên hợp $\overline{z}$ cũng là một nghiệm của đa thức nói trên.*

Chứng minh. Giả sử z là một nghiệm phức của đa thức hệ số thực $f = \sum_{i=1}^{n} a_i x^i$, khi đó ta có $\sum_{i=1}^{n} a_i z^i = 0$. Vì liên hợp của một tổng hai số phức bằng tổng hai số phức liên hợp, liên hợp của một tích hai số phức bằng tích hai số phức liên hợp và liên hợp của một số thực thì bằng chính nó nên ta có

$$0 = \overline{0} = \overline{\sum_{i=1}^{n} a_i z^i} = \sum_{i=1}^{n} \overline{a_i}\,\overline{z}^i = \sum_{i=1}^{n} a_i \overline{z}^i.$$

Vậy $\overline{z}$ cũng là một nghiệm của f.

□

Hệ quả 4.33. (a) *Đa thức bất khả quy trên $\mathbb{C}$ chỉ là các đa thức bậc nhất.*

(b) *Đa thức bất khả quy trên $\mathbb{R}$ chỉ là các đa thức bậc nhất hoặc các đa thức bậc hai có biệt số âm.*

Chứng minh. (a) Hiển nhiên được suy ra từ Định lý 4.30.

(b) Nếu $f \in \mathbb{R}[x]$ là đa thức bậc hai, theo Mệnh đề 4.26 thì f là bất khả quy khi và chỉ khi nó không có nghiệm thực, điều này có nghĩa là f có biệt số âm.

Xét $f \in \mathbb{R}[x]$ là đa thức bậc $n > 2$, bởi Định lý 4.30 f có một nghiệm phức z. Nếu z là nghiệm thực thì f được phân tích trong $\mathbb{R}[x]$ thành tích của hai đa thức bậc nhất và bậc $n-1$. Nếu z không là nghiệm thực, theo Mệnh đề 4.32 thì $\overline{z}$ cũng là một nghiệm và khi đó f chia hết cho $(x-z)(x-\overline{z})$. Vì $(x-z)(x-\overline{z}) = x^2 - 2\mathrm{Re}(z)\,x + |z|^2$ là đa thức với hệ số thực nên f có phân tích trong $\mathbb{R}[x]$ thành tích của hai đa thức bậc hai và bậc $n-2$. Vậy f là khả quy trong $\mathbb{R}[x]$ và mệnh đề được chứng minh.

□

Kết hợp Định lý 4.29 và Hệ quả 4.33 ta có

Hệ quả 4.34. (a) *Mọi đa thức hệ số phức không phải đa thức hằng luôn phân tích được thành tích của những đa thức bậc nhất.*

(b) *Mọi đa thức hệ số thực không phải đa thức hằng đều phân tích được thành tích của những đa thức bậc nhất và những đa thức bậc hai hệ số thực có biệt số âm.*

Ví dụ 4.35. (a) Phân tích x^2+i trong $\mathbb{C}[x]$ thành tích của các đa thức bậc nhất. Ta có

$$\begin{aligned} x^2+i &= x^2-\left(\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2}\right)^2 \\ &= \left[x-\left(\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2}\right)\right]\left[x+\left(\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2}\right)\right]. \end{aligned}$$

b) Phân tích x^4-1-i trong $\mathbb{C}[x]$ thành tích của các đa thức bậc nhất. Ta viết $1+i$ ở dạng lượng giác $1+i=\sqrt{2}\left(\cos\frac{\pi}{4}+i\sin\frac{\pi}{4}\right)$ và đặt $\alpha=\sqrt[8]{2}\left(\cos\frac{\pi}{16}+i\sin\frac{\pi}{16}\right)$ là một căn bậc bốn của $1+i$. Vì $x^4-1-i=x^4-\alpha^4$ nên ta có

$$\begin{aligned} x^4-1-i &= \left(x-\alpha^2\right)\left(x+\alpha^2\right) \\ &= (x-\alpha)(x+\alpha)(x-i\alpha)(x+i\alpha). \end{aligned}$$

(c) Phân tích đa thức $p=x^4+x^3+x^2+x+1$ trong $\mathbb{R}[x]$ thành tích của những đa thức bất khả quy. Các nghiệm của đa thức x^5-1 là các căn bậc năm của đơn vị, đó là 1 và $z_k=\cos\left(\frac{k2\pi}{5}\right)+i\sin\left(\frac{k2\pi}{5}\right)$ với $k=1,2,3,4$. Vì $x^5-1=(x-1)p$ do đó z_1,z_2,z_3,z_4 là các nghiệm của p. Ta có phân tích p thành tích của những đa thức với hệ số phức như sau

$$p=(x-z_1)(x-z_4)(x-z_2)(x-z_3).$$

Vì z_1 và z_4 là hai số phức liên hợp, z_2 và z_3 là hai số phức liên hợp do đó

$$\begin{aligned} p &= \left(x^2-2\mathrm{Re}(z_1)\,x+|z_1|^2\right)\left(x^2-2\mathrm{Re}(z_2)\,x+|z_2|^2\right) \\ &= \left(x^2-2\cos\left(\frac{2\pi}{5}\right)x+1\right)\left(x^2-2\cos\left(\frac{4\pi}{5}\right)x+1\right). \end{aligned}$$

Bài tập

1. Với số tự nhiên n dương cho trước hãy giải phương trình

$$(x+i)^n+(x-i)^n=0.$$

2. Chứng tỏ $1-i$ là một nghiệm của phương trình

$$x^6+(1+2i)\,x^4+(1+2i)\,x^2+2i=0.$$

Hãy giải phương trình đã cho.

3. Chứng tỏ i là một nghiệm kép của đa thức

$$x^6 + x^5 + 3x^4 + 2x^3 + 3x^2 + x + 1.$$

Hãy phân tích đa thức trên thành tích của những đa thức bất khả quy trên $\mathbb{R}$.

4. Hãy phân tích các đa thức hệ số thực sau thành tích của những đa thức bất khả quy trên $\mathbb{R}$.
   (a) $1 + x^8$
   (b) $1 + x^4 + x^8$
   (c) $8x^3 + (1 - x^2)^3$
5. Gọi q và r là thương và dư trong phép chia một đa thức f cho một đa thức $g \neq 0$ trong $\mathbb{C}[x]$. Chứng minh rằng nếu f và g là các đa thức hệ số thực thì q và r cũng vậy.
6. Chứng tỏ vành thương $\mathbb{C}[x]/(x^2+1)$ không phải miền nguyên.
7. Cho đa thức hệ số thực $x^2 + x + 1$. Chứng tỏ $\mathbb{R}[x]/(x^2+x+1)$ là một trường và trường này đẳng cấu với trường $\mathbb{C}$ các số phức.

4.6 Nhân tử hóa đa thức hệ số hữu tỷ và hệ số nguyên

Cho đa thức f với hệ số hữu tỷ . Nếu nhân với f một bội số chung của các mẫu số của các hệ số của đa thức f thì ta được đa thức g hệ số nguyên. Vì f và g chỉ khác nhau một hằng số nhân khác không nên nghiệm hữu tỷ của chúng là như nhau. Vì vậy việc tìm nghiệm hữu tỷ của đa thức hệ số hữu tỷ được quy về tìm nghiệm hữu tỷ của đa thức hệ số nguyên.

Định lý 4.36. *Cho $f = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$. Nếu r/s ($\gcd(r,s)=1$) là một nghiệm hữu tỷ của f thì $r \mid a_0$ và $s \mid a_n$. Đặc biệt nếu f đơn hệ thì mọi nghiệm hữu tỷ của f đều là nghiệm nguyên.*

Chứng minh. Nếu $f(r/s) = 0$ thì $a_n(r/s)^n + \cdots + a_1(r/s) + a_0 = 0$ và

$$a_nr^n + a_{n-1}r^{n-1}s + \cdots + a_1rs^{n-1} + a_0s^n = 0.$$

Ta có $a_nr^n = -s(a_{n-1}r^{n-1} + \cdots + a_1rs^{n-2} + a_0s^{n-1})$, suy ra $s \mid a_nr^n$. Vì $\gcd(r,s) = 1$ nên $s \mid a_n$. Tương tự ta cũng có $r \mid a_0$.

□

Vì mỗi hệ số a_0 và a_n chỉ có hữu hạn các ước số nên định lý cũng chỉ ra rằng việc tìm nghiệm hữu tỷ của một đa thức hệ số nguyên trở nên đơn giản bằng cách thử trên tập hợp hữu hạn các phần tử r/s.

Lưu ý rằng việc tìm nghiệm hữu tỷ của đa thức hệ số nguyên có thể đưa về việc tìm nghiệm nguyên của đa thức hệ số nguyên đơn hệ nhờ phép biến đổi như sau. Cho đa

thức $f = a_0 + a_1x + \cdots + a_nx^n$, nếu c là một nghiệm của f thì $a_0 + a_1c + \cdots + a_nc^n = 0$. Nhân hai vế với a_n^{n-1} ta được

$$a_n^{n-1}a_0 + a_n^{n-2}a_1\left(a_nc\right) + \cdots + \left(a_nc\right)^n = 0.$$

Đặt $b = a_nc$ thì b là nghiệm của đa thức hệ số nguyên đơn hệ

$$g = a_n^{n-1}a_0 + a_n^{n-2}a_1x + \cdots + x^n.$$

Do đó để tìm nghiệm của f ta chỉ việc tìm nghiệm của g.

Ví dụ 4.37. (a) Phân tích đa thức $f = 2x^3 + 3x^2 - 1$ trong $\mathbb{Q}[x]$. Nếu r/s là một nghiệm của f thì $r \mid 1$ và $s \mid 2$. Do đó các giá trị có thể có của r/s là $\pm 1, \pm 1/2$. Thử lại ta có $-1, 1/2$ là hai nghiệm của f. Lấy f chia cho $(x+1)(x-1/2)$ ta được thương là $2(x+1)$. Vậy $f = (x+1)^2(2x-1)$.

(b) Phân tích đa thức $f = x^5 - 8x^4 + 20x^3 - 20x^2 + 19x - 12$ trong $\mathbb{Q}[x]$. Dễ thấy rằng 1 là một nghiệm của f, lấy f chia cho $x - 1$ ta có $f = (x-1)g$ với

$$g = x^4 - 7x^3 + 13x^2 - 7x + 12.$$

Ta thấy ± 1 không phải là nghiệm của g, do đó theo Định lý 4.36 thì nghiệm của g chỉ có thể là $\pm 2, \pm 3, \pm 4, \pm 6, \pm 12$. Vì có khá nhiều giá trị phải thử xem có phải là nghiệm của g hay không nên ta cần đưa thêm vài tiêu chuẩn phụ để giảm bớt việc thử nghiệm. Chẳng hạn ta thấy $g(\alpha) > 0$ với mọi $\alpha < 0$ nên nghiệm của g chỉ có thể là $2, 3, 4, 6, 12$. Hơn nữa, nếu c là một nghiệm của g, bởi chú ý sau Hệ quả 4.12 ta có $g = (x-c)h$ trong đó h là một đa thức hệ số nguyên nào đó, nếu x nhận giá trị bằng 1 thì $1 - c$ là một ước số của $g(1)$ và nếu x nhận giá trị bằng-1 thì $1 + c$ là một ước số của $g(-1)$. Với nhận xét này ta thấy khi c là một trong các giá trị $2, 6, 12$ thì hoặc$1 - c$ không phải ước của $g(1) = 12$ hoặc $1 + c$ không phải ước của $g(-1) = 40$ nên không phải là nghiệm. Khi c bằng 3 hay 4 đều làm cho $1 - c$ ước của $g(1)$ và $1 + c$ ước của $g(-1)$ nên chúng có thể là nghiệm của g. Thử lại ta thấy chúng là hai nghiệm của g. Vậy ta có

$$f = (x-1)(x-3)(x-4)\left(x^2+1\right)$$

là một phân tích f thành tích của các đa thức bất khả quy trong $\mathbb{Q}[x]$.

(c) Chứng minh $\sqrt[8]{3}$ là một số vô tỷ. Ta thấy rằng $\sqrt[8]{3}$ là một nghiệm của đa thức $x^8 - 3$. Theo Định lý 4.36 nghiệm hữu tỷ nếu có của đa thức là $\pm 1, \pm 3$. Dễ thấy rằng chúng không phải là nghiệm của đa thức. Vậy nghiệm của đa thức phải là vô tỷ, suy ra $\sqrt[8]{3}$ là một số vô tỷ.

Ta nhận thấy rằng việc tìm nghiệm hữu tỷ của một đa thức hệ số nguyên rồi dựa vào đó để phân tích thành tích các nhân tử bất khả quy không phải khi nào cũng thành công vì có những đa thức có bậc lớn hơn ba khả quy trong $\mathbb{Q}[x]$ nhưng lại không có nghiệm trong $\mathbb{Q}$.

Bây giờ ta xét vấn đề sau. Cho đa thức hệ số nguyên, nếu nó nhân tử hóa được trong $\mathbb{Z}[x]$ thì hiển nhiên nhân tử hóa được trong $\mathbb{Q}[x]$, ngược lại nếu nó nhân tử hóa được trong $\mathbb{Q}[x]$ thì có thể nhân tử hóa được trong $\mathbb{Z}[x]$ không? Để trả lời cho câu hỏi này ta cần khái niệm và bổ đề

Định nghĩa 4.38. Cho $f \in \mathbb{Z}[x]$ không phải đa thức hằng. Ta nói f là *nguyên bản* nếu 1 là ước chung lớn nhất của các hệ số của f.

Với đa thức g hệ số hữu tỷ cho trước, gọi v là bội số chung nhỏ nhất của các mẫu số của các hệ số của g thì $g = (1/v)\,\overline{g}$, trong đó $\overline{g}$ là đa thức hệ số nguyên. Đặt u là ước số chung lớn nhất của các hệ số của $\overline{g}$ thì $g = (u/v)\,G$, ở đây G là đa thức nguyên bản.

Bổ đề 4.39. (Bổ đề Gauss) *Tích của hai đa thức nguyên bản là một đa thức nguyên bản.*

Chứng minh. Giả sử $G = b_0 + b_1x + \cdots + b_nx^n$ và $H = c_0 + c_1x + \cdots + c_mx^m$ là hai đa thức nguyên bản. Để chứng minh bổ đề ta chỉ cần chứng tỏ cho một số nguyên tố p tùy ý thì p không chia hết các hệ số của đa thức tích $G \cdot H$ là đủ. Vì G và H nguyên bản nên p không chia hết các hệ số của G và H, gọi i, j là hai số nguyên nhỏ nhất sao cho b_i và c_j là hai hệ số của G và H tương ứng mà p không chia hết. Hệ số của x^{i+j} trong $G \cdot H$ là

$$b_{i+j}c_0 + \cdots + b_{i+1}c_{j-1} + b_ic_j + b_{i-1}c_{j+1} + \cdots + b_0c_{i+j}.$$

Vì p chia hết $c_0, \cdots, c_{j-1}, b_{i-1}, \ldots, b_0$ và p không chia hết b_ic_j nên p không chia hết hệ số này và bổ đề được chứng minh.

□

Định lý 4.40. *Cho đa thức $f \in \mathbb{Z}[x]$. Nếu f phân tích được trong $\mathbb{Q}[x]$ thành tích của hai đa thức có bậc m và n thì f cũng phân tích được trong $\mathbb{Z}[x]$ thành tích của hai đa thức có bậc m và n.*

Chứng minh. Giả sử $f = g \cdot h$ là tích của hai đa thức trong $\mathbb{Q}[x]$ có bậc m và n. Ta viết $g = (u/v)\,G$ và $h = (r/s)\,H$, ở đây G, H là hai đa thức nguyên bản và $u, v, r, s \in \mathbb{Z}$. Bây giờ

$$f = \left(\frac{u}{v}G\right)\left(\frac{r}{s}H\right) = \frac{ur}{vs}G \cdot H = \frac{p}{q}G \cdot H$$

với p, q nguyên tố cùng nhau. Nếu e_i là hệ số của $G \cdot H$ thì $\frac{pe_i}{q}$ là hệ số của f và là một số nguyên. Vì p, q nguyên tố cùng nhau nên q chia hết mọi e_i, bởi Bổ đề 4.39 $G \cdot H$ là nguyên bản tức là các e_i chỉ có ước chung là ± 1 nên $q = \pm 1$. Vậy $f = \pm pG \cdot H$ và định lý được chứng minh.

□

Ví dụ 4.41. (a) Phân tích đa thức $f = x^4 - 3x^2 + 2x + 1$ thành các nhân tử bất khả quy trong $\mathbb{Q}[x]$. Bởi Định lý 4.36, nghiệm hữu tỷ của đa thức chỉ có thể là ± 1. Tuy nhiên, ta thấy chúng không phải là nghiệm, vì thế f không có nhân tử bậc nhất. Do đó nếu f có nhân tử thì nhân tử phải bậc hai. Bởi Định lý 4.40 ta có thể chọn nhân tử là các đa thức hệ số nguyên. Giả sử

$$\begin{aligned} x^4 - 3x^2 + 2x + 1 &= \left(x^2 + ax + b\right)\left(x^2 + cx + d\right) \\ &= x^4 + (a + c)\, x^3 + (b + d + ac)\, x^2 + (bc + ad)\, x + bd. \end{aligned}$$

Vì vậy ta cần phải giải hệ phương trình sau để tìm nghiệm nguyên:

$$\begin{cases} a + c & = 0 \\ b + d + ac & = -3 \\ bc + ad & = 2 \\ bd & = 1 \end{cases}.$$

Ta suy ra $b = d = \pm 1$ và $c + a = \pm 2$, đây là một mâu thuẩn. Vậy f không thể phân tích thành tích hai đa thức bậc hai và do đó nó là bất khả quy trong $\mathbb{Q}[x]$.

(b) Phân tích đa thức $f = x^5 - 9x^4 + 8x^3 - 5x^2 + 3x + 9$ thành các nhân tử bất khả quy trong $\mathbb{Q}[x]$. Nhận xét rằng ánh xạ $\eta : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_2[x]$ được xác định với mọi $g = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$, $\eta(g) = \overline{g} = \sum_{i=0}^{n} \overline{a_i} x^i \in \mathbb{Z}_2[x]$ là một toàn cấu vành. Nếu $f = h \cdot k$ là một phân tích của f trong $\mathbb{Q}[x]$, bởi Định lý 4.40 ta có thể chọn h, k là các đa thức hệ số nguyên, khi đó

$$\overline{f} = \eta(f) = \eta(h) \cdot \eta(k) = \overline{h} \cdot \overline{k}$$

là một phân tích của $\overline{f}$ trong $\mathbb{Z}_2[x]$. Mặt khác ta có $\overline{f} = x^5 + x^4 + x^2 + x + \overline{1}$. $\overline{f}$ không có nghiệm trong $\mathbb{Z}_2$ nên không có nhân tử bậc nhất. Do đó nếu $\overline{f}$ có nhân tử thì có nhân tử bất khả quy bậc hai. Như trong Ví dụ 4.27, trong $\mathbb{Z}_2[x]$ chỉ có duy nhất $x^2 + x + \overline{1}$ là đa thức bất khả quy bậc hai. Kiểm tra trực tiếp bằng cách lấy $\overline{f}$ chia cho $x^2 + x + \overline{1}$ ta thấy $x^2 + x + \overline{1}$ không phải nhân tử của $\overline{f}$ nên $\overline{f}$ là bất khả quy trong $\mathbb{Z}_2[x]$, từ đây suy ra f là bất khả quy trong $\mathbb{Q}[x]$.

Với một đa thức hệ số nguyên cho trước, làm thế nào để biết đa thức đã cho là bất khả quy trên $\mathbb{Q}$ hay không? Định lý sau cho ta một điều kiện đủ để trả lời câu hỏi trên.

Định lý 4.42. (Tiêu chuẩn Eisenstein) *Cho* $f = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$. *Giả sử có số nguyên tố* p *sao cho* p *chia hết* $a_0, a_1, \ldots, a_{n-1}$, p *không chia hết* a_n, p^2 *không chia hết* a_0 *thì* f *bất khả quy trên* $\mathbb{Q}$.

Chứng minh. Giả sử f khả quy trên $\mathbb{Q}$. Bởi Định lý 4.40, f được phân tích thành tích hai đa thức trong $\mathbb{Z}[x]$, đó là

$$f = (b_0 + b_1x + \cdots + b_rx^r)(c_0 + c_1x + \cdots + c_sx^s),$$

ở đây $b_i, c_j \in \mathbb{Z}$, $r, s > 0$ và $r + s = n$. Vì $a_0 = b_0c_0$ và $p \mid a_0, p^2 \nmid a_0$ nên p chia hết một trong hai số b_0 hoặc c_0 và không chia hết đồng thời cả hai. Không mất tính tổng quát, giả sử $p \mid b_0$ và $p \nmid c_0$. Bây giờ p không thể chia hết tất cả các hệ số $b_0, b_1, \ldots, b_r$ được vì như thế p sẽ chia hết a_n. Gọi t là số nguyên dương nhỏ nhất sao cho p không chia hết b_t, $1 \leq t \leq r < n$. Khi đó

$$a_t = b_0c_t + b_1c_{t-1} + \cdots + b_{t-1}c_1 + b_tc_0$$

và $p \mid a_t, p \mid b_0, p \mid b_1, \ldots, p \mid b_{t-1}$ suy ra $p \mid b_tc_0$. Tuy nhiên ta lại có $p \nmid b_t$ và $p \nmid c_0$, đây là một mâu thuẩn và định lý được chứng minh.

□

Ví dụ 4.43. (a) Các đa thức $x^7 - 2$, $x^5 - 4x^3 + 6x^2 - 8x - 2$ là bất khả quy trên $\mathbb{Q}$ theo tiêu chuẩn Eisenstein với $p = 2$.

(b) Cho đa thức $f = x^4 + 1$. Ta không thể áp dụng tiêu chuẩn Eisenstein cho f được. Đặt $f = f(x)$ và $g = f(x + a)$ với a hằng số hữu tỷ tùy ý. Ta nhận thấy rằng $f = h \cdot k$ nếu và chỉ nếu $g = h(x + a)\, k(x + a)$, do đó f và g cùng khả quy hoặc cùng bất khả quy. Lấy $a = 1$, ta có

$$g = f(x + 1) = (x + 1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$$

và g là bất khả quy trên $\mathbb{Q}$ theo tiêu chuẩn Eisenstein với $p = 2$, do nhận xét trên f là bất khả quy trên $\mathbb{Q}$.

(c) Chứng tỏ đa thức $\phi = \phi(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ là bất khả quy trên $\mathbb{Q}$ với mọi số nguyên tố p. ϕ được gọi là đa thức cyclotomic và có thể viết ở dạng $\phi = (x^p - 1)/(x - 1)$. Để chứng tỏ ϕ là bất khả quy ta xét đa thức

$$\begin{aligned}\psi &= \phi(x+1)\\ &= \frac{1}{x}\left[(x+1)^p - 1\right]\\ &= x^{p-1} + C_p^{p-1}x^{p-2} + \cdots + C_p^2 x + C_p^1.\end{aligned}$$

Với $1 \leq i \leq p-1$, $C_p^i = \frac{p!}{i!(p-i)!}$ suy ra $i!\,(p-i)!C_p^i = p!$. Vì p là số nguyên tố, vế phải chia hết cho p và $i!, (p-i)!$ không chia hết cho p suy ra C_p^i chia hết cho p. Vì $C_p^1 = p$ không chia hết cho p^2, theo tiêu chuẩn Eisenstein ψ là bất khả quy trên $\mathbb{Q}$ và do đó ϕ cũng vậy.

Bài tập

1. Chứng tỏ $\sqrt{2}/\sqrt[3]{7}$ là một số vô tỷ.
2. Tìm một đa thức trong $\mathbb{Q}[x]$ nhận $\sqrt{2}+\sqrt{3}$ làm nghiệm. Sau đó chứng tỏ $\sqrt{2}+\sqrt{3}$ là một số vô tỷ.
3. Đa thức hệ số nguyên nào dưới đây là bất khả quy trên $\mathbb{Q}$?
   (a) $10x^7 - 6x^4 + 15x^2 + 18x - 6$
   (b) $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
   (c) $3x^4 + 5x + 1$
   (d) $x^6 + 2x^3 - 3x^2 + 1$
   (e) $x^4 + 4$
4. Phân tích các đa thức sau thành các nhân tử bất khả quy trong $\mathbb{Z}[x]$.
   (a) $1 + x + x^2 + x^3 + x^4 + x^5$
   (b) $1 + x + x^2 + x^3 + x^4 + x^5 + x^6$
   (c) $1 + x + x^2 + x^3 + x^4 + x^5 + x^7$
5. Chứng tỏ đa thức $x^{n-1} + x^{n-2} + \cdots + x + 1 \in \mathbb{Q}[x]$, ở đây n không phải số nguyên tố, luôn khả quy trên $\mathbb{Q}$.

4.7 Phương trình bậc ba và bậc bốn

Trong mục này ta sẽ tìm hiểu cách giải phương trình bậc ba và bậc bốn hệ số phức.

Xét phương trình bậc ba $x^3 + ax^2 + bx + c = 0$. Đặt $x = y - a/3$, khi đó phương trình trở thành $y^3 + py + q = 0$. Để giải phương trình này ta đặt $y = u + v$, thay vào phương trình ta được

$$u^3 + v^3 + (u+v)(3uv + p) + q = 0.$$

Ta tìm một cặp u, v sao cho $3uv + p = 0$ $(*)$ và $u^3 + v^3 + q = 0$. Từ đây suy ra $u^3v^3 = -(1/27)\, p^3$, $u^3 + v^3 = -q$ và khi đó u^3, v^3 là các nghiệm của phương trình bậc hai

$$z^2 + qz - \frac{1}{27}p^3 = 0.$$

Ta có $u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ và $v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$, trong đó $\sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ là một căn bậc hai của $\frac{q^2}{4} + \frac{p^3}{27}$ (Lưu ý rằng không có vấn đề gì trong cách chọn u^3 và v^3 vì u và v do ta đặt và vai trò của u và v hoàn toàn đối xứng). Gọi u_1 là một căn bậc ba của $-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ và v_1 là một căn bậc ba của $-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ sao cho thỏa mãn $(*)$, khi đó ta còn có hai cặp u_2, v_2 và u_3, v_3 cũng thỏa mãn $(*)$, ở đây

$$u_2 = \omega u_1,\ v_2 = \omega^2 v_1 \quad \text{và} \quad u_3 = \omega^2 u_1,\ v_3 = \omega v_1$$

với ω căn bậc ba phức của đơn vị, cụ thể $\omega = \frac{-1+i\sqrt{3}}{2}$. Đặt

$$\begin{aligned} y_1 &= u_1 + v_1, \\ y_2 &= \omega u_1 + \omega^2 v_1, \\ y_3 &= \omega^2 u_1 + \omega v_1, \end{aligned}$$

ta sẽ chứng tỏ y_1, y_2, y_3 là ba nghiệm của phương trình đã cho. Lưu ý rằng $\omega^2 = \overline{\omega}$, $(\omega)^3 = (\omega^2)^3 = 1$ và $1 + \omega + \omega^2 = 0$. Ta thấy $y_1 + y_2 + y_3 = 0$, $y_1y_2 + y_1y_3 + y_2y_3 = p$ và $y_1y_2y_3 = -q$. Xét phương trinh

$$\begin{aligned} 0 &= (y - y_1)(y - y_2)(y - y_3) \\ &= y^3 - (y_1 + y_2 + y_3)\, y^2 + (y_1y_2 + y_1y_3 + y_2y_3)\, y - y_1y_2y_3 \\ &= y^3 + py + q. \end{aligned}$$

Vậy y_1, y_2, y_3 là ba nghiệm của phương trình đã cho.

Ví dụ 4.44. Giải phương trình $x^3 + 3x + 1 = 0$. Đặt $x = u + v$, ta tìm u, v thỏa mãn hệ

$$\begin{cases} u^3 + v^3 + 1 &= 0 \\ uv + 1 &= 0 \end{cases}.$$

Từ đây ta suy ra u^3, v^3 là nghiệm của phương trình $z^2 + z - 1 = 0$. Ta tìm được

$$u^3 = \frac{-1 + \sqrt{5}}{2} \text{ và } v^3 = \frac{-1 - \sqrt{5}}{2}.$$

Khi đó một nghiệm của phương trình là

$$u+v=\sqrt[3]{\frac{-1+\sqrt{5}}{2}}+\sqrt[3]{\frac{-1-\sqrt{5}}{2}}.$$

Hai nghiệm khác là

$$\omega u+\omega^2 v=\frac{-1+i\sqrt{3}}{2}\cdot\sqrt[3]{\frac{-1+\sqrt{5}}{2}}+\frac{-1-i\sqrt{3}}{2}\cdot\sqrt[3]{\frac{-1-\sqrt{5}}{2}},$$
$$\omega^2 u+\omega v=\frac{-1-i\sqrt{3}}{2}\cdot\sqrt[3]{\frac{-1+\sqrt{5}}{2}}+\frac{-1+i\sqrt{3}}{2}\cdot\sqrt[3]{\frac{-1-\sqrt{5}}{2}}.$$

Xét phương trình bậc bốn $x^4+ax^3+bx^2+cx+d=0$. Trước hết ta chuyển số hạng bx^2+cx+d sang bên phải rồi viết bên trái ở dạng một nhị thức bình phương

$$\left(x^2+\frac{ax}{2}\right)^2=\left(\frac{a^2}{4}-b\right)x^2-cx-d.$$

Cộng vào hai vế của phương trình trên một đại lượng $\left(x^2+\frac{ax}{2}\right)y+\frac{y^2}{4}$, trong đó y là một tham số, ta có

$$\left(x^2+\frac{ax}{2}+\frac{y}{2}\right)^2=\left(\frac{a^2}{4}-b+y\right)x^2+\left(\frac{ay}{2}-c\right)x+\frac{y^2}{4}-d.$$

Ta chọn tham số y sao cho vế phải là một nhị thức bình phương, muốn thế chỉ cần chọn y sao cho biệt số của tam thức bậc hai đối với x ở vế phải

$$\left(\frac{ay}{2}-c\right)^2-4\left(\frac{a^2}{4}-b+y\right)\left(\frac{y^2}{4}-d\right)=0$$

và điều này tương đương với y là nghiệm của phương trình bậc ba

$$y^3-by^2+(ac-4d)\,y-\left[d\left(a^2-4b\right)+c^2\right]=0.$$

Giả sử y_0 là một nghiệm của phương trình bậc ba trên, khi đó ta có

$$\left(x^2+\frac{ax}{2}+\frac{y_0}{2}\right)^2=(\alpha x+\beta)^2.$$

Từ đây ta suy ra nghiệm của phương trinh bậc bốn đã cho chính là nghiệm của hai phương trình bậc hai

$$\left(x^2+\frac{ax}{2}+\frac{y_0}{2}\right)=\pm(\alpha x+\beta).$$

Ví dụ 4.45. Giải phương trình bậc bốn $x^4+x^3+2x^2+x+1=0$. Ta chuyển $2x^2+x+1$ sang bên phải rồi viết bên trái ở dạng một nhị thức bình phương

$$\left(x^2+\frac{x}{2}\right)^2=-\frac{7}{4}x^2-x-1.$$

Cộng vào hai vế của phương trình trên một đại lượng $\left(x^2+\frac{x}{2}\right)y+\frac{y^2}{4}$, trong đó y là một tham số, ta có

$$\left(x^2+\frac{x}{2}+\frac{y}{2}\right)^2=\left(-\frac{7}{4}+y\right)x^2+\left(\frac{y}{2}-1\right)x+\frac{y^2}{4}-1.$$

Ta chọn tham số y sao cho vế phải là một nhị thức bình phương, muốn thế chọn y sao cho biệt số của tam thức bậc hai đối với x ở vế phải

$$\left(\frac{y}{2}-1\right)^2-4\left(-\frac{7}{4}+y\right)\left(\frac{y^2}{4}-1\right)=0$$

và điều này tương đương với y là nghiệm của phương trình bậc ba

$$y^3-2y^2-3y+6=0.$$

Ta thấy $y=2$ là một nghiệm của phương trình bậc ba trên, khi đó ta có

$$\left(x^2+\frac{x}{2}+1\right)^2=\frac{1}{4}x^2.$$

Từ đây ta suy ra nghiệm của phương trinh bậc bốn đã cho chính là nghiệm của hai phương trình bậc hai

$$x^2+\frac{x}{2}+1=\pm\frac{1}{2}x.$$

Vậy phương trình đã cho có bốn nghiệm là $-\frac{1}{2}+i\frac{\sqrt{3}}{2}$, $-\frac{1}{2}-i\frac{\sqrt{3}}{2}$, i, $-i$.

Bài tập

1. Giải các phương trình bậc ba hệ số phức sau.
   (a) $x^3-x^2+2x+1=0$
   (b) $x^3-6x+1=0$
   (c) $2x^3-3x+1=0$
2. Giải các phương trình bậc bốn hệ số phức sau.
   (a) $x^4+x^3-x^2-x+1=0$
   (b) $x^4+2x^3-3x^2+4x-1=0$
   (c) $4x^4-5x^2-4x-3=0$

4.8 Đa thức nhiều biến

Định nghĩa 4.46. Cho R là một vành giao hoán có đơn vị. Vành đa thức n biến được định nghĩa bằng quy nạp như sau: đặt $R_1 = R[x_1]$ gọi là vành đa thức một biến, giả thiết quy nạp vành đa thức $n-1$ biến $R_{n-1} = R[x_1, x_2, \ldots, x_{n-1}]$ được định nghĩa, khi đó *vành đa thức n biến* được định nghĩa $R[x_1, x_2, \ldots, x_n] = R_{n-1}[x_n]$.

Từ định nghĩa ta có dãy các vành con sau:

$$R \subset R[x_1] \subset R[x_1,x_2] \subset \cdots \subset R[x_1, x_2, \ldots, x_n].$$

Phần tử $f \in R[x_1, \ldots, x_n]$ được gọi là một đa thức n biến, nó được viết duy nhất ở dạng

$$f = c_1 x_1^{a_{11}} \cdots x_n^{a_{1n}} + \cdots + c_m x_1^{a_{m1}} \cdots x_n^{a_{mn}}$$

với $c_i \in R$, còn $a_{i1}, \ldots, a_{in}$, $i = 1, \ldots, m$, là những số tự nhiên và $(a_{i1}, \ldots, a_{in}) \neq (a_{j1}, \ldots, a_{jn})$ khi $i \neq j$. Ta nói c_i là hệ số và $c_i x_1^{a_{i1}} \cdots x_n^{a_{in}}$ là một hạng tử của f. Hai đa thức bằng nhau khi và chỉ khi các hạng tử của chúng giống nhau. Đặc biệt đa thức bằng đa thức không khi và chỉ khi các hệ số của nó đều bằng không.

Ta gọi bậc của hạng tử $cx_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ $(c \neq 0)$ là tổng của các số mũ $a_1 + a_2 + \cdots + a_n$ và bậc của đa thức là số lớn nhất trong các bậc của các hạng tử của nó. Đa thức không được quy ước có bậc $-\infty$. Nếu các hạng tử của đa thức có cùng bậc n thì đa thức được gọi là đa thức đẳng cấp bậc n.

Để sắp xếp các hạng tử của một đa thức khác không thì có nhiều cách sắp xếp. Có một cách sắp xếp mà ta gọi là cách sắp xếp theo thứ tự từ điển dựa trên quan hệ thứ tự toàn phần trong tích Descartes $\mathbb{N}^n$. Ta nói

$$(a_1, \ldots, a_n) > (b_1, \ldots, b_n)$$

nếu có một chỉ số i sao cho $a_1 = b_1, \ldots, a_{i-1} = b_{i-1}$ và $a_i > b_i$. Chẳng hạn

$$(2,1,0) > (2,0,0) > (1,3,5) > (1,3,2) > (0,5,1) > (0,0,9).$$

Đa thức sau là sự sắp xếp theo thứ tự từ điển

$$f = -x_1^2 x_2 + x_1^2 + 2x_1 x_2^3 x_3^5 - 5x_1 x_2^3 x_3^2 - 4x_2^5 x_3 + x_3^9.$$

Hạng tử tương ứng với dãy số mũ lớn nhất $(2,1,0)$ gọi là *hạng tử cao nhất* của f. Mệnh đề sau là hiển nhiên.

Mệnh đề 4.47. *Cho $f, g \in R[x_1, x_2, \ldots, x_n]$ là hai đa thức khác không có các hạng tử cao nhất lần lượt là $ax_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ và $bx_1^{b_1} x_2^{b_2} \cdots x_n^{bn}$. Khi đó*

(a) *Nếu* $(a_1, a_2, \ldots, a_n) > (b_1, b_2, \ldots, b_n)$ *thì hạng tử cao nhất của* $f + g$ *là* $ax_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}$.

(b) *Nếu* $ab \neq 0$ *thì hạng tử cao nhất của* $f \cdot g$ *là* $abx_1^{a_1+b_1}x_2^{a_2+b_2}\cdots x_n^{a_n+b_n}$.

Hệ quả sau dễ dàng được suy ra từ Mệnh đề 4.47.

Hệ quả 4.48. *Nếu* R *là một miền nguyên thì* $R[x_1, \ldots, x_n]$ *cũng là một miền nguyên.*

Bài tập

1. Trong $\mathbb{C}[x, y, z]$ cho $f = x + y + z$, $g = x + jy + j^2z$ và $h = x + j^2y + jz$, trong đó $j = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Hãy tính $f + g + h$, $f \cdot g \cdot h$.
2. Cho đa thức $f = y(x+1)^n - x(y+1)^n + x - y \in R[x, y]$, trong đó n là số tự nhiên. Chứng tỏ tồn tại đa thức $g \in R[x, y]$ sao cho $f = xy(x - y)g$.

4.9 Đa thức đối xứng

Trong phần này đa thức f của n biến sẽ được ký hiệu là $f(x_1, x_2, \ldots, x_n)$.

Định nghĩa 4.49. Giả sử R là một vành giao hoán có đơn vị và $f(x_1, x_2, \ldots, x_n) \in R[x_1, x_2, \ldots, x_n]$. Ta nói $f(x_1, \ldots, x_n)$ là *đa thức đối xứng* của n biến nếu

$$f\left(x_{\tau(1)}, \ldots, x_{\tau(n)}\right) = f(x_1, \ldots, x_n)$$

với mọi hoán vị $\tau = \begin{pmatrix} 1 & 2 & \ldots & n \\ \tau(1) & \tau(2) & \ldots & \tau(n) \end{pmatrix} \in S_n$.

Ví dụ 4.50. Trong vành $\mathbb{Z}[x_1, x_2, x_3]$ đa thức

$$f(x_1, x_2, x_3) = x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2$$

là đối xứng vì

$$\begin{aligned} f(x_1, x_2, x_3) &= f(x_2, x_1, x_3) = f(x_1, x_3, x_2) \\ &= f(x_3, x_2, x_1) = f(x_2, x_3, x_1) = f(x_3, x_1, x_2). \end{aligned}$$

Mệnh đề 4.51. *Tập hợp gồm các đa thức đối xứng của* $R[x_1, \ldots, x_n]$ *là một vành con của* $R[x_1, \ldots, x_n]$.

Chứng minh. Đặt S là tập hợp gồm các đa thức đối xứng của $R[x_1, \ldots, x_n]$. Ta có đa thức không thuộc S. Nếu $f(x_1, x_2, \ldots, x_n)$ và $g(x_1, x_2, \ldots, x_n)$ là hai đa thức đối

xứng tùy ý trong S, đặt $h(x_1, x_2, \ldots, x_n) = f(x_1, x_2, \ldots, x_n) - g(x_1, x_2, \ldots, x_n)$ thì

$$\begin{aligned} h\left(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)}\right) &= f\left(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)}\right) - g\left(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)}\right) \\ &= f(x_1, x_2, \ldots, x_n) - g(x_1, x_2, \ldots, x_n) \\ &= h(x_1, x_2, \ldots, x_n) \end{aligned}$$

với mọi $\tau \in S_n$ và do đó $f(x_1, x_2, \ldots, x_n) - g(x_1, x_2, \ldots, x_n) \in S$. Tương tự ta cũng có $f(x_1, x_2, \ldots, x_n)\, g(x_1, x_2, \ldots, x_n) \in S$. Vậy S là một vành con của $R[x_1, \ldots, x_n]$. □

Sau đây là các đa thức đối xứng đặc biệt mà ta gọi là các *đa thức đối xứng cơ bản*.

Trong $R[x_1, x_2]$ có hai đa thức đối xứng cơ bản là $\sigma_1 = x_1 + x_2$, $\sigma_2 = x_1 x_2$.

Trong $R[x_1, x_2, x_3]$ có ba đa thức đối xứng cơ bản là $\sigma_1 = x_1 + x_2 + x_3$, $\sigma_2 = x_1x_2 + x_1x_3 + x_2x_3$, $\sigma_3 = x_1x_2x_3$.

Tổng quát trong $R[x_1, \ldots, x_n]$ có n đa thức đối xứng cơ bản là

$$\begin{aligned} \sigma_1 &= x_1 + x_2 + \cdots + x_n \\ \sigma_2 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n \\ \sigma_3 &= x_1x_2x_3 + x_1x_2x_4 + \cdots + x_{n-2}x_{n-1}x_n \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ \sigma_n &= x_1x_2\cdots x_n. \end{aligned}$$

Kết quả chính ở đây là chứng tỏ mọi đa thức đối xứng luôn được biểu diễn qua các đa thức đối xứng cơ bản. Để chứng tỏ điều đó ta cần các bổ đề sau.

Bổ đề 4.52. *Nếu $ax_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}$ là hạng tử cao nhất của đa thức đối xứng khác không của n biến thì $a_1 \geq a_2 \geq \cdots \geq a_n$.*

Chứng minh. Cho $f(x_1, x_2, \ldots, x_n)$ là đa thức đối xứng của n biến có hạng tử cao nhất là $ax_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}$. Giả sử có $i < j$ mà $a_i < a_j$, lấy τ là chuyển vị (i, j), khi đó trong $f\left(x_{\tau(1)}, \ldots, x_{\tau(n)}\right) = f(x_1, x_2, \ldots, x_n)$ xuất hiện hạng tử

$$ax_1^{a_1}x_2^{a_2}\cdots x_j^{a_i}\cdots x_i^{a_j}\cdots x_n^{a_n} = ax_1^{a_1}x_2^{a_2}\cdots x_i^{a_j}\cdots x_j^{a_i}\cdots x_n^{a_n}$$

với dãy số mũ $(a_1, a_2, \ldots, a_j, \ldots, a_i, \ldots, a_n)$ lớn hơn dãy số mũ của hạng tử cao nhất $ax_1^{a_1}x_2^{a_2}\cdots x_i^{a_i}\cdots x_j^{a_j}\cdots x_n^{a_n}$. Đây là một mâu thuẩn và bổ đề được chứng minh. □

Bổ đề 4.53. *Cho $a_1, a_2, \ldots, a_n$ là dãy các số tự nhiên sao cho $a_1 \geq a_2 \geq \cdots \geq a_n$. Khi đó đa thức*

$$f(x_1,\ldots,x_n)=\sigma_1^{a_1-a_2}\sigma_2^{a_2-a_3}\cdots\sigma_{n-1}^{a_{n-1}-a_n}\sigma_n^{a_n}$$

có hạng tử cao nhất là $x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}$.

Chứng minh. Thay $\sigma_1 = x_1+\cdots+x_n$, $\sigma_2 = x_1x_2+\cdots+x_{n-1}x_n,\ldots$, $\sigma_n = x_1x_2\cdot\cdots\cdot x_n$ vào $f(x_1,\ldots,x_n)$ ta có

$$f(x_1,\ldots,x_n)=(x_1+\cdots+x_n)^{a_1-a_2}(x_1x_2+\cdots+x_{n-1}x_n)^{a_2-a_3}\cdots \\ \cdots(x_1x_2\cdot\cdots\cdot x_n)^{a_n}$$

Khi đó hạng tử cao nhất của $f(x_1,\ldots,x_n)$ là

$$x_1^{a_1-a_2}(x_1x_2)^{a_2-a_3}\cdots(x_1x_2\cdots x_{n-1})^{a_{n-1}-a_n}(x_1x_2\cdots x_n)^{a_n}=x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}$$

và bổ đề được chứng minh.

□

Bổ đề 4.54. *Nếu đa thức*

$$f(x_1,\ldots,x_n)=c_1\sigma_1^{a_{11}}\cdots\sigma_n^{a_{1n}}+\cdots+c_m\sigma_1^{a_{m1}}\cdots\sigma_n^{a_{mn}}$$

là đa thức không, trong đó $(a_{i1},\ldots,a_{in})\neq(a_{j1},\ldots,a_{jn})$ *với* $i\neq j$ *thì các* $c_i=0$ *với mọi* $i=1,\ldots,m$.

Chứng minh. Với mỗi $i=1,\ldots,m$, bởi Bổ đề 4.53, đa thức $c_i\sigma_1^{a_{i1}}\cdots\sigma_n^{a_{in}}$ có hạng tử cao nhất là $c_ix_1^{b_{i1}}x_2^{b_{i2}}\cdots x_n^{b_{in}}$, ở đây

$$\begin{aligned}b_{i1} &= a_{i1}+a_{i2}+\cdots+a_{in}\\ b_{i2} &= a_{i2}+\cdots+a_{in}\\ &\cdots\cdots\cdots\cdots\\ b_{in} &= a_{in}.\end{aligned}$$

Với $i\neq j$ thì dãy số mũ $(b_{i1},b_{i2},\ldots,b_{in})\neq(b_{j1},b_{j2},\ldots,b_{jn})$, vì nếu ngược lại thì

$$\begin{aligned}a_{i1}+a_{i2}+\cdots+a_{in} &= a_{j1}+a_{j2}+\cdots+a_{jn}\\ a_{i2}+\cdots+a_{in} &= a_{j2}+\cdots+a_{jn}\\ &\cdots\cdots\cdots\cdots\\ a_{in} &= a_{jn}\end{aligned}$$

và suy ra $(a_{i1},\ldots,a_{in})=(a_{j1},\ldots,a_{jn})$ là một mâu thuẩn. Khi đó trong tập hợp hữu hạn các dãy số mũ $(b_{i1},b_{i2},\ldots,b_{in})$ có phần tử lớn nhất, không mất tính tổng quát giả sử đó là $(b_{11},b_{12},\ldots,b_{1n})$ và $c_1x_1^{b_{11}}x_2^{b_{12}}\cdots x_n^{b_{1n}}$ là hạng tử cao nhất của

$f(x_1,\ldots,x_n)=0$ nên $c_1=0$. Lập luận tương tự cho các hệ số c_i còn lại, tất cả đều bằng không và bổ đề được chứng minh.

□

Định lý 4.55. *Cho $f(x_1,\ldots,x_n)$ là một đa thức đối xứng khác không của $R[x_1,x_2,\ldots,x_n]$. Khi đó $f((x_1,\ldots,x_n)$ được biểu diễn duy nhất như một đa thức của $\sigma_1,\sigma_2,\ldots,\sigma_n$.*

Chứng minh. Ta chứng minh định lý bằng quy nạp theo thứ tự từ điển trên tập hợp các dãy số mũ của hạng tử cao nhất trong đa thức. Giả sử $ax_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}$ với dãy số mũ tương ứng $(a_1,a_2,\ldots,a_n)$ là hạng tử cao nhất của $f(x_1,\ldots,x_n)$. Giả thiết quy nạp mọi đa thức đối xứng có hạng tử cao nhất với dãy số mũ tương ứng nhỏ hơn $(a_1,a_2,\ldots,a_n)$ đều được biểu diễn như một đa thức của $\sigma_1,\sigma_2,\ldots,\sigma_n$. Theo Bổ đề 4.52 thì $a_1\geq a_2\geq\cdots\geq a_n$, bởi Bổ đề 4.53, đa thức $\sigma_1^{a_1-a_2}\sigma_2^{a_2-a_3}\cdots\sigma_{n-1}^{a_{n-1}-a_n}\sigma_n^{a_n}$ có hạng tử cao nhất là $x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}$. Bây giờ xét

$$f_1(x_1,\ldots,x_n)=f(x_1,\ldots,x_n)-a\sigma_1^{a_1-a_2}\sigma_2^{a_2-a_3}\cdots\sigma_{n-1}^{a_{n-1}-a_n}\sigma_n^{a_n}$$

thì $f_1(x_1,\ldots,x_n)$ cũng là đa thức đối xứng có hạng tử cao nhất với dãy số mũ tương ứng nhỏ hơn $(a_1,a_2,\ldots,a_n)$. Theo giả thiết quy nạp $f_1(x_1,\ldots,x_n)$ được biểu diễn như một đa thức của $\sigma_1,\sigma_2,\ldots,\sigma_n$ và do đó $f(x_1,\ldots,x_n)$ cũng vậy.

Bây giờ ta chứng tỏ tính duy nhất của biểu diễn. Giả sử $f(x_1,\ldots,x_n)$ có hai biểu diễn, bằng cách thêm những hạng tử có hệ số bằng không nếu cần, ta giả sử

$$\begin{aligned}f(x_1,\ldots,x_n)&=c_1\sigma_1^{a_{11}}\cdots\sigma_n^{a_{1n}}+\cdots+c_m\sigma_1^{a_{m1}}\cdots\sigma_n^{a_{mn}}\\&=d_1\sigma_1^{a_{11}}\cdots\sigma_n^{a_{1n}}+\cdots+d_m\sigma_1^{a_{m1}}\cdots\sigma_n^{a_{mn}}.\end{aligned}$$

Khi đó ta có $(c_1-d_1)\sigma_1^{a_{11}}\cdots\sigma_n^{a_{1n}}+\cdots+(c_m-d_m)\sigma_1^{a_{m1}}\cdots\sigma_n^{a_{mn}}=0$. Theo Bổ đề 4.54 thì $c_i-d_i=0$ và $c_i=d_i$ với $i=1,\ldots,m$ và định lý được chứng minh.

□

Ví dụ 4.56. Trong vành $\mathbb{Z}[x_1,x_2,x_3]$ hãy biểu thị đa thức đối xứng $f(x_1,x_2,x_3)=x_1^3+x_2^3+x_3^3$ theo các đa thức đối xứng cơ bản. Hạng tử cao nhất của $f(x_1,x_2,x_3)$ là $x_1^3=x_1^3x_2^0x_3^0$ và dãy số mũ tương ứng là $(3,0,0)$. Các dãy số mũ không tăng nhỏ hơn $(3,0,0)$ là $(3,0,0)>(2,1,0)>(1,1,1)$, do đó

$$\begin{aligned}f(x_1,x_2,x_3)&=\sigma_1^{3-0}\sigma_2^{0-0}\sigma_3^0+a\sigma_1^{2-1}\sigma_2^{1-0}\sigma_3^0+b\sigma_1^{1-1}\sigma_2^{1-1}\sigma_3^1\\&=\sigma_1^3+a\sigma_1\sigma_2+b\sigma_3.\end{aligned}$$

Cho x_1,x_2,x_3 lần lượt bằng $1,1,0$ ta được $a=-3$, cho x_1,x_2,x_3 lần lượt bằng $1,1,-1$ ta có $b=3$. Vậy

$$f(x_1,x_2,x_3)=\sigma_1^3-3\sigma_1\sigma_2+3\sigma_3.$$

Phương pháp để xác định các hệ số a, b ở trên gọi là phương pháp hệ tử bất định.

Chú ý rằng trong trường hợp đa thức là đối xứng nhưng không cùng bậc thì những hạng tử có cùng bậc của đa thức là một đa thức đối xứng và đa thức đã cho là tổng của những đa thức đối xứng cùng bậc với những bậc khác nhau.

Bây giờ ta sẽ chỉ ra một vài ứng dụng của đa thức đối xứng.

Ví dụ 4.57. (a) Tìm các số nguyên α, β, γ thỏa mãn hệ

$$\begin{cases} \alpha\beta\gamma & = -2, \\ \alpha^3 + \beta^3 + \gamma^3 & = 8, \\ \alpha + \beta + \gamma & = 2. \end{cases}$$

Theo ví dụ trên thì

$$\alpha^3 + \beta^3 + \gamma^3 = (\alpha + \beta + \gamma)^3 - 3(\alpha + \beta + \gamma)(\alpha\beta + \alpha\gamma + \beta\gamma) + 3\alpha\beta\gamma.$$

Ta suy ra $\alpha\beta + \alpha\gamma + \beta\gamma = -1$. Mặt khác, xét đa thức

$$f(x) = (x - \alpha)(x - \beta)(x - \gamma)$$

thì đa thức này có nghiệm là α, β, γ. Khai triển $f(x)$ ta được

$$\begin{aligned} f(x) &= x^3 - (\alpha + \beta + \gamma)x^2 + (\alpha\beta + \alpha\gamma + \beta\gamma)x - \alpha\beta\gamma \\ &= x^3 + 2x^2 - x - 2. \end{aligned}$$

$f(x)$ có ba nghiệm là $-1, 1, 2$. Vậy hệ đã cho có nghiệm là $(-1, 1, 2)$ và các hoán vị của nó.

(b) Tìm điều kiện cần và đủ để đa thức $x^3 + ax + b$ hệ số phức có ba nghiệm phân biệt.

Gọi α, β, γ là ba nghiệm của đa thức đã cho. Ta có $\sigma_1 = \alpha + \beta + \gamma = 0$, $\sigma_2 = \alpha\beta + \alpha\gamma + \beta\gamma = a$ và $\sigma_3 = \alpha\beta\gamma = -b$. Mặt khác ta có

$$(\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2 = \sigma_1^2\sigma_2^2 - 4\sigma_1^3\sigma_3 - 4\sigma_2^3 + 18\sigma_1\sigma_2\sigma_3 - 27\sigma_3^2,$$

do đó $(\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2 = -(4a^3 + 27b^2)$. Vậy điều kiện cần và đủ để đa thức $x^3 + ax + b$ có ba nghiệm phân biệt là $4a^3 + 27b^2 \neq 0$.

Bài tập

1. Trong $R[x, y, z]$ viết dạng tổng quát của đa thức đối xứng đẳng cấp có bậc 2, 3.

2. Trong $R[x,y,z,t]$ viết dạng tổng quát của đa thức đối xứng đẳng cấp biết rằng đa thức đó có hạng tử cao nhất là
   (a) xy (b) x^2y
3. Cho đa thức $f_n = x^n(y-z) + y^n(z-x) + z^n(x-y) \in \mathbb{Z}[x,y,z]$, trong đó n là một số tự nhiên lớn hơn 1.
   (a) Chứng minh rằng tồn tại đa thức $g_n \in \mathbb{Z}[x,y,z]$ sao cho
   $$f_n = (x-y)(x-z)(y-z)g_n.$$
   (b) Xác định g_n với $n = 2,3,4$.
   (c) Chứng tỏ $g_n = \sum x^p y^q z^r$, trong đó tổng được lấy trong tập hợp các bộ số (p,q,r) các số nguyên không âm sao cho $p+q+r = n-2$.
4. Cho đa thức $f_n = (x+y+z)^n - x^n - y^n - z^n \in \mathbb{Z}[x,y,z]$, trong đó n là một số tự nhiên không âm.
   (a) Chứng minh rằng nếu n là số lẻ thì có đa thức $g_n \in \mathbb{Z}[x,y,z]$ sao cho $f_n = (x+y)(y+z)(z+x)g_n$.
   (b) Xác định g_n với $n = 5$.
5. Trong $\mathbb{Z}[x,y,z]$ hãy biểu diễn đa thức đối xứng $x^4+y^4+z^4$ theo các đa thức đối xứng cơ bản.
6. Trong $\mathbb{Z}[x,y,z]$ hãy biểu diễn các đa thức đối xứng sau theo các đa thức đối xứng cơ bản.
   (a) $x^2y + x^2z + xy^2 + y^2z + xz^2 + yz^2$
   (b) $(x+y)(y+z)(z+x)$
   (c) $(x+y-z)(y+z-x)(z+x-y)$
   (d) $(x^2+y^2)(y^2+z^2)(z^2+x^2)$
7. Trong $\mathbb{Z}[x,y,z,t]$ chứng tỏ các đa thức sau là đa thức đối xứng và biểu diễn chúng theo các đa thức đối xứng cơ bản.
   (a) $(x+y-z-t)^2 + (x+z-t-y)^2 + (x+t-z-y)^2$
   (c) $(x+y-z-t)(x+z-t-y)(x+t-z-y)$
   (d) $(x+y+z-t)(x+y+t-z)(x+z+t-y)(y+z+t-x)$
   (e) $(xy-zt)(xz-yt)(xt-yz)$
8. Trong $\mathbb{Z}_2[x,y,z]$ hãy biểu diễn đa thức đối xứng $x^4+y^4+z^4$ theo các đa thức đối xứng cơ bản.
9. Cho a,b,c là ba nghiệm của đa thức hệ số thực
   $$x^3 + x^2 - 3x - 1.$$
   Tính giá trị của biểu thức $a^3b + a^3c + ab^3 + b^3c + ac^3 + bc^3$.
10. Tìm nghiệm thực của hệ phương trình

$$\begin{cases} x+y+z & =2 \\ x^2+y^2+z^2 & =6 \\ x^3+y^3+z^3 & =8 \end{cases}.$$

Chương 5

MIỀN EUCLID - MIỀN IĐÊAN CHÍNH

Trong chương này vành luôn được giả thiết là miền nguyên với đơn vị 1. Lớp các miền nguyên đặc biệt được khảo sát là lớp các miền Euclid và lớp các miền iđêan chính.

5.1 Tính chất số học trong một miền nguyên

Định nghĩa 5.1. Giả sử D là một miền nguyên và $a, b \in D$. Ta nói *a chia hết cho b* hay *b chia hết a*, ký hiệu $b \mid a$, nếu có $c \in D$ sao cho $a = bc$.

Chú ý rằng 0 luôn chia hết cho mọi phần tử trong D. Khi a chia hết cho b ta còn nói a là một bội của b hoặc b là một ước của a. Mệnh đề sau đây là hiển nhiên.

Mệnh đề 5.2. *Cho $a, b, c \in D$. Ta có*

(a) $a \mid a$.

(b) *$c \mid b$ và $b \mid a$ thì $c \mid a$.*

Mệnh đề 5.3. *Cho $a, b \in D$. Khi đó các khẳng định sau là tương đương.*

(a) *b chia hết a và a chia hết b.*

(b) *Có phần tử khả nghịch u trong D sao cho $a = ub$.*

(c) *Iđêan được sinh ra bởi a và iđêan được sinh ra bởi b là bằng nhau.*

Chứng minh. (a)⇒(b) Giả sử $b \mid a$ và $a \mid b$ khi đó có $u, v \in D$ sao cho $a = ub$ và $b = va$. Nếu $a = 0$ thì $b = 0$ và khi đó $a = 1 \cdot b$. Nếu $a \neq 0$, ta có $a = (uv)\, a$, trong miền nguyên D giản ước hai vế cho a, $uv = 1$ và u khả nghịch. Ta có (b).

(b)⇒(c) Ta có $a = ub$, suy ra $a \in (b)$ và do đó $(a) \subset (b)$. Mặt khác, vì u khả nghịch nên $b = u^{-1}a$ và tương tự ta cũng có $(b) \subset (a)$. Vậy $(a) = (b)$.

(c)⇒(a) là hiển nhiên.

□

Định nghĩa 5.4. Ta nói hai phần tử a và b thuộc miền nguyên D là *liên kết* nếu có phần tử khả nghịch u trong D sao cho $a = ub$.

Dễ thấy quan hệ liên kết là một quan hệ tương đương trên D.

Ví dụ 5.5. (a) Trong vành $\mathbb{Z}$ các số nguyên, a và $-a$ là liên kết.

(b) Trong vành đa thức $F[x]$, ở đây F là một trường, hai đa thức f và af ($a \in F$, $a \neq 0$) là liên kết.

(c) Trong miền nguyên D, hai phần tử khả nghịch bất kỳ là liên kết.

Bây giờ cho $a \in D$. Nếu u khả nghịch thì u là một ước của 1 và 1 luôn là ước của a nên theo Mệnh đề 5.2 thì u là một ước của a. Các phần tử liên kết với a cũng là các ước của a. Các ước khả nghịch và các ước liên kết của a gọi là các *ước không thật sự*, các ước khác gọi là *ước thật sự*. Chẳng hạn trong $\mathbb{Z}$, $\pm 1, \pm 6$ là các ước không thật sự của 6, còn $\pm 2, \pm 3$ là các ước thật sự của 6.

Định nghĩa 5.6. Trong miền nguyên D cho phần tử p khác không và không khả nghịch. Ta nói

(a) p là *bất khả quy* nếu p không có ước thật sự, tức là nếu có sự phân tích $p = ab$ trong D thì a hoặc b phải là phần tử khả nghịch. Một phần tử không bất khả quy gọi là *khả quy*.

(b) p là *nguyên tố* nếu với bất kỳ $a, b \in D$ mà $p \mid ab$ thì ta luôn có $p \mid a$ hoặc $p \mid b$.

Ví dụ 5.7. Trong $\mathbb{Z}$ và $F[x]$, ở đây F là một trường, phần tử nguyên tố cũng là phần tử bất khả quy và ngược lại.

Mệnh đề 5.8. *Cho phần tử p khác không trong miền nguyên D. Khi đó p là nguyên tố nếu và chỉ nếu iđêan được sinh ra bởi p là một iđêan nguyên tố.*

Chứng minh. Giả sử p là nguyên tố và $I = (p)$ là iđêan được sinh ra bởi p. Khi đó với mọi $a, b \in D$ mà $ab \in I$ thì $p \mid ab$, p là nguyên tố nên $p \mid a$ hoặc $p \mid b$. Vì vậy a hay b thuộc I và do đó I là một iđêan nguyên tố. Đảo lại, giả sử $I = (p)$ là một iđêan nguyên tố. Vì (p) là iđêan thực sự của D nên p không khả nghịch. Với mọi $a, b \in D$ nếu $p \mid ab$ thì $ab \in I$. Vì I là một iđêan nguyên tố nên a hay b thuộc I, do đó $p \mid a$ hay $p \mid b$ và p là nguyên tố.

□

Mệnh đề 5.9. *Trong một miền nguyên, mọi phần tử nguyên tố đều bất khả quy.*

Chứng minh. Giả sử p là một phần tử nguyên tố của miền nguyên D. Nếu $p = ab$ là một phân tích trong D thì $p \mid a$ hay $p \mid b$. Khi $p \mid a$ thì $a = up$ với phần tử u nào đó trong D. Ta có $p = ab = (ub)\, p$, trong miền nguyên D giản ước hai vế cho $p \neq 0$ ta có $ub = 1$, và b là phần tử khả nghịch. Tương tự, khi $p \mid b$ thì a là một phần tử khả nghịch. Vì thế p là bất khả quy và ta có điều phải chứng minh.

□

Tuy nhiên điều ngược lại không đúng như trong ví dụ sau.

Ví dụ 5.10. Xét miền nguyên $\mathbb{Z}\left[\sqrt{5}i\right] = \left\{a + b\sqrt{5}i \mid a, b \in \mathbb{Z}\right\}$ và phần tử $2 \in \mathbb{Z}\left[\sqrt{5}i\right]$. Giả sử $2 = uv$ là một phân tích trong $\mathbb{Z}\left[\sqrt{5}i\right]$, khi đó $4 = |uv|^2 = |u|^2 |v|^2$. Ta viết $u = a + b\sqrt{5}i$ thì $|u|^2 = a^2 + 5b^2$ chia hết 4. Vì không có a, b nguyên thỏa $a^2 + 5b^2 = 2$ nên $|u|^2$ phải bằng 1 hay 4. Nếu $|u|^2 = 1$, vì $u \in \mathbb{Z}\left[\sqrt{5}i\right]$ nên $u = \pm 1$ là phần tử khả nghịch, nếu $|u|^2 = 4$ thì $|v|^2 = 1$ và $v = \pm 1$ là phần tử khả nghịch. Vậy 2 là bất khả quy. Đặt $z = 1 + \sqrt{5}i$ và $w = 1 - \sqrt{5}i$. Ta thấy 2 chia hết $zw = 6$, nhưng 2 không chia hết z cũng như không chia hết w nên 2 không phải nguyên tố.

Định nghĩa 5.11. Cho hai phần tử a và b thuộc miền nguyên D. Nếu phần tử $c \in D$ là một ước của a và b thì ta nói c là một *ước chung* của a và b. Một ước chung của a và b gọi là *ước chung lớn nhất*, ký hiệu $\gcd(a, b)$, nếu mọi ước chung khác của a và b đều là ước của nó.

Ta thấy rằng ước chung lớn nhất của a và b nếu có thì không hẳn duy nhất. Thật vậy, nếu d là một ước chung lớn nhất của a và b, theo Mệnh đề 5.3 thì mọi phần tử liên kết với d cũng là ước chung lớn nhất của a và b, tức là chúng sai khác một nhân tử khả nghịch.

5.2 Miền Euclid

Định nghĩa 5.12. Giả sử D là một miền nguyên và D^* là tập hợp các phần tử khác không của D. Ta nói D cùng với ánh xạ δ (gọi là ánh xạ Euclid) từ D^* đến tập hợp các số tự nhiên $\mathbb{N}$ là một *miền Euclid* nếu δ có các tính chất:

(a) $\delta(a) \leq \delta(ab)$ với mọi $a, b \in D^*$;

(b) Với a, b tùy ý trong D và $b \neq 0$ thì có $q, r \in D$ sao cho $a = qb + r$, trong đó $r = 0$ hoặc $\delta(r) < \delta(b)$.

Ví dụ 5.13. (a) Vành các số nguyên $\mathbb{Z}$ cùng với ánh xạ $n \in \mathbb{Z}^* \longmapsto |\, n \,| \in \mathbb{N}$ là một miền Euclid.

(b) Trường F cùng với ánh xạ hằng $x \in \mathbb{F}^* \longmapsto 0 \in \mathbb{N}$ là một miền Euclid.

(c) Vành đa thức $F[x]$, ở đây F là một trường, cùng với ánh xạ $f \in \mathbb{F}[x]^* \longmapsto \deg f \in \mathbb{N}$ là một miền Euclid.

Mệnh đề 5.14. *Cho miền Euclid D với ánh xạ Euclid δ. Khi đó*

(a) $\delta(1) \leq \delta(a)$ với mọi $a \in D^*$.

(b) $\delta(1) = \delta(u)$, *trong đó u là phần tử khả nghịch tùy ý trong D.*

Chứng minh. (a) Với mọi $a \in D^*$ ta có $\delta(1) \leq \delta(1 \cdot a) = \delta(a)$.

(b) Với u khả nghịch trong D, theo (a) ta có $\delta(1) \leq \delta(u)$. Mặt khác $\delta(u) \leq \delta(uu^{-1}) = \delta(1)$. Vậy $\delta(1) = \delta(u)$.

□

Mệnh đề 5.15. *Vành các số nguyên Gauss $\mathbb{Z}[i] = \{a + bi/a, b \in \mathbb{Z}\}$ cùng với ánh xạ $\delta(a + bi) = a^2 + b^2$ với mọi $a + bi \in \mathbb{Z}[i]$ và $a + bi \neq 0$ là một miền Euclid.*

Chứng minh. Với $z = a + bi \in \mathbb{Z}[i]$ và $z \neq 0$, từ định nghĩa ta có $\delta(z) = |z|^2$. Khi đó $\delta(vw) = \delta(v)\delta(w)$ và $\delta(v), \delta(w) \geq 1$ với mọi $v, w \in \mathbb{Z}[i]$, v, w khác không, và do đó $\delta(v) \leq \delta(vw)$.

Ta chứng tỏ thuật toán chia tồn tại trong $\mathbb{Z}[i]$. Cho trước z và $w \neq 0$ trong $\mathbb{Z}[i]$. Xem chúng như là những phần tử trong $\mathbb{C}$ thì $\frac{z}{w} = s + ti$, $s, t \in \mathbb{Q}$. Ta viết $s = a + s'$ và $t = b + t'$, ở đây a và b lần lượt là các số nguyên gần nhất với s và t. Vì vậy $|s'|, |t'| \leq \frac{1}{2}$. Khi đó $z = (a + bi)w + (s' + t'i)w$, ta thấy $(s' + t'i)w = z - (a + bi)w \in \mathbb{Z}[i]$ và do đó $z = qw + r$, trong đó $q = a + bi$ và $r = (s' + t'i)w$ là những phần tử trong $\mathbb{Z}[i]$. Phần còn lại là chứng tỏ $r = 0$ hoặc $\delta(r) < \delta(w)$. Nếu $r \neq 0$ thì

$$\begin{aligned}\delta(r) &= |(s' + t'i)w|^2 = |s' + t'i|^2 |w|^2 \\ &= \left(s'^2 + t'^2\right)|w|^2 \\ &\leq \left(\frac{1}{4} + \frac{1}{4}\right)|w|^2 = \frac{1}{2}\delta(w) < \delta(w)\end{aligned}$$

và mệnh đề được chứng minh.

□

Chú ý rằng trong định nghĩa của miền Euclid thì thương q và dư r không đòi hỏi duy nhất. Chẳng hạn trong $\mathbb{Z}[i]$ ta có

$$\begin{aligned}3 - 2i &= (3 + i)(1 - i) - 1, \\ 3 - 2i &= 3(1 - i) + i.\end{aligned}$$

Trong cả hai trường hợp, $\delta(r) = 1 < 2 = \delta(1 - i)$.

Bây giờ ta xét hai phần tử a và b tùy ý không đồng thời bằng không trong miền Euclid, chứng minh tương tự như Mệnh đề 4.22 ước chung lớn nhất d của chúng luôn tồn tại. Tuy nhiên ở đây ta sẽ dùng thuật toán chia gọi là thuật toán Euclid mà qua đó ta tìm được u, v sao cho $d = ua + vb$. Trước hết ta cần bổ đề sau.

Bổ đề 5.16. *Cho $a, b, q, r \in D$ thỏa mãn quan hệ $a = qb + r$. Khi đó ước chung lớn nhất của a và b cũng là ước chung lớn nhất của b và r.*

Chứng minh. Nếu d là một ước chung của a và b thì d chia hết a và chia hết b, do đó d chia hết r, suy ra d là một ước chung của b và r. Tương tự nếu d là một ước

chung của b và r thì d cũng là một ước chung của a và b. Vậy ước chung lớn nhất của a và b là ước chung lớn nhất của b và r.

□

Định lý 5.17. *Trong miền Euclid D cho hai phần tử a và b không đồng thời bằng không. Khi đó ước chung lớn nhất của chúng luôn tồn tại. Gọi $d = \gcd(a, b)$ thì có $u, v \in D$ sao cho $d = ua + vb$.*

Chứng minh. Theo bổ đề trên, để tìm ước chung lớn nhất của hai phần tử a và b ta đưa về tìm ước chung lớn nhất của b và dư r khi chia a cho b. Quá trình này được gọi là *Thuật toán Euclid.*

Nếu $b = 0$ thì ước chung lớn nhất của chúng là a. Vì vậy ta giả sử b khác không, thực hiện phép chia a cho b ta có $a = q_0 b + r_1$. Nếu $r_1 \neq 0$ ta lại chia b cho r_1, $b = q_1 r_1 + r_2$. Nếu $r_2 \neq 0$ ta lại chia r_1 cho r_2, $r_1 = q_2 r_2 + r_3$. Quá trình chia ở trên phải chấm dứt sau một số hữu hạn bước vì dãy các số tự nhiên $\delta(b) > \delta(r_1) > \delta(r_2) > \delta(r_3) > \cdots$ không thể giảm vô hạn, cuối cùng ta đi đến một phép chia có dư bằng không, $r_{m-1} = q_m r_m + 0$. Khi đó theo Bổ đề 5.16 ta có

$$\begin{aligned}\gcd(a, b) &= \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots \\ &= \gcd(r_{m-1}, r_m) = \gcd(r_m, 0) = r_m.\end{aligned}$$

Như vậy trong thuật toán Euclid đối với phần tử a và phần tử khác không b, phần tử dư cuối cùng khác không r_m là một ước chung lớn nhất của a và b. Đặt $d = \gcd(a, b)$, thực hiện thuật toán Euclid ta tìm được $d = r_m$, thế các giá trị $r_{m-1}, r_{m-2}, ..., r_2, r_1$ ngược từ dưới lên và ta tìm được $u, v \in D$ sao cho $d = ua + vb$.

□

Ví dụ 5.18. Cho $f = 4x^4 - 2x^3 - 16x^2 + 5x + 9$ và $g = 2x^3 - x^2 - 5x + 4$ là hai đa thức hệ số thực. Tìm ước chung lớn nhất của chúng. Trước khi thực hiện phép chia Euclid ta nhận xét rằng ước chung lớn nhất của hai đa thức h và k cũng là ước chung lớn nhất của ah và bk với a, b hai hằng số khác không. Bây giờ lấy f chia cho g ta có $f = 2x\, g + r_1$ với $r_1 = -6x^2 - 3x + 9$. Nếu lấy g chia cho r_1 ta sẽ được các đa thức hệ số không là số nguyên, do nhận xét trên ta lấy $3g$ chia cho r_1 ta được $3g = (-x + 1)\, r_1 + r_2$ với $r_2 = -3x + 3$. Tiếp tục lấy r_1 chia cho r_2 ta có $r_1 = (2x + 3) r_2$. Vậy $\gcd(f, g) = d = -\frac{1}{3} r_2 = x - 1$. Thay $r_1 = f - 2xg$ vào $3g = (-x + 1)\, r_1 + r_2$ ta có

$$\begin{aligned}r_2 &= 3g - (-x + 1)\, r_1 \\ &= 3g - (-x + 1)\, (f - 2xg) \\ &= (3 + 2x\, (-x + 1))\, g - (-x + 1)\, f \\ &= \left(-2x^2 + 2x + 3\right) g + (x - 1)\, f.\end{aligned}$$

Do đó $d = -\frac{1}{3}r_2 = \left(\frac{2}{3}x^2 - \frac{2}{3}x - 1\right)g + \left(-\frac{1}{3}x + \frac{1}{3}\right)f$.

Bài tập

1. Chứng tỏ miền nguyên $\mathbb{Z}[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{Z}\}$ cùng với ánh xạ $\delta(z) = |z\overline{z}|$, ở đây $z = a + b\alpha$, $\overline{z} = a - b\alpha$, là một miền Euclid trong các trường hợp sau.
   (a) $\mathbb{Z}\left[\sqrt{2}\right]$ (b) $\mathbb{Z}\left[\sqrt{3}\right]$ (c) $\mathbb{Z}\left[\sqrt{2}i\right]$
2. Tìm thương q và phần dư r trong miền Euclid, ở đây $a = qb + r$ trong các trường hợp sau.
   (a) $a = 3 - 4i$, $b = 4 + 3i$ trong $\mathbb{Z}[i]$.
   (b) $a = 5 - 2\sqrt{2}$, $b = 3 - \sqrt{2}$ trong $\mathbb{Z}\left[\sqrt{2}\right]$.
3. Tìm ước chung lớn nhất d của a và b trong miền Euclid và biểu diễn nó ở dạng $d = ua + vb$ trong các trường hợp sau.
   (a) $a = 4 + 7i$, $b = 1 + 8i$ trong $\mathbb{Z}[i]$.
   (b) $a = 7 + 5\sqrt{2}$, $b = 1 + \sqrt{2}$ trong $\mathbb{Z}\left[\sqrt{2}\right]$.
   (c) $a = 3 - 7\sqrt{3}$, $b = 7 - \sqrt{3}$ trong $\mathbb{Z}\left[\sqrt{3}\right]$.
4. Trong mỗi trường hợp sau, cho trước f, g là hai đa thức trong $R[x]$, hãy xác định $\gcd(f, g)$ và tìm $u, v \in R[x]$ sao cho $\gcd(f, g) = uf + vg$.
   (a) $f = x^4 - x^2 - 2$, $g = x^3 + x^2 + x + 1$ trong $\mathbb{Q}[x]$.
   (b) $f = x^4 + x^3 + x^2 + \overline{1}$, $g = x + \overline{1}$ trong $\mathbb{Z}_2[x]$.
   (c) $f = x^4 + \overline{2}$, $g = x^3 + \overline{3}$ trong $\mathbb{Z}_5[x]$.
5. (a) Chứng tỏ rằng với bất kỳ $f \in \mathbb{Z}_3[x]$ luôn tồn tại $u, v \in \mathbb{Z}_3[x]$ sao cho $f = \left(x^2 + x + \overline{2}\right)u + \left(x + \overline{1}\right)v$.
   (b) Tìm $u, v \in \mathbb{Z}_3[x]$ sao cho $x^4 + x^2 + \overline{2} = \left(x^2 + x + \overline{2}\right)u + \left(x + \overline{1}\right)v$.
6. Tìm $u, v \in \mathbb{Q}[x]$ sao cho $x = (x^3 + 1)u + (x^2 + 1)v$.
7. Tìm phần tử sinh của iđêan I trong miền Euclid trong các trường hợp sau.
   (a) I được sinh ra bởi $x^3 - 2x^2 + 1$ và $x^3 + 2x - 5$ trong $\mathbb{Q}[x]$.
   (b) I được sinh ra bởi $3 - \sqrt{i}$, $5 + 5\sqrt{i}$ trong $\mathbb{Z}[i]$.
   (c) I được sinh ra bởi $3 - 2\sqrt{3}$, $b = 1 + \sqrt{3}$ trong $\mathbb{Z}\left[\sqrt{3}\right]$.
8. Nếu F là một trường thì vành $F[x, y]$ có phải là một miền Euclid không?
9. Cho D cùng với ánh xạ δ là một miền Euclid và $a, b \in D^*$. Chứng tỏ rằng
   (a) Nếu a và b liên kết thì $\delta(a) = \delta(b)$.
   (b) Nếu $\delta(a) = \delta(b)$ và $a \mid b$ thì a và b liên kết.
10. Cho D cùng với ánh xạ δ là một miền Euclid và $a, b \in D^*$. Chứng tỏ rằng $\delta(a) < \delta(ab)$ nếu và chỉ nếu b không phải phần tử khả nghịch.

5.3 Miền iđêan chính

Trong phần này ta xét lớp các miền nguyên đặc biệt gọi là lớp các miền iđêan chính và chứng tỏ dãy các bao hàm

$$\text{Miền nguyên} \supset \text{Miền iđêan chính} \supset \text{Miền Euclid} \supset \text{Trường}.$$

Các định lý trong lớp các miền Euclid như sự tồn tại ước chung lớn nhất, nhân tử hóa một phần tử không khả nghịch vẫn còn đúng trong lớp các vành này.

Xét miền nguyên D, một iđêan I của D được gọi là *iđêan chính* nếu I được sinh ra bởi một phần tử nào đó trong D.

Định nghĩa 5.19. Ta nói một miền nguyên là *miền iđêan chính* nếu mọi iđêan của nó đều là iđêan chính.

Mệnh đề 5.20. *Một miền Euclid là một miền iđêan chính.*

Chứng minh. Cho I là một iđêan trong miền Euclid D cùng với ánh xạ Euclid δ. Nếu $I = \{0\}$ thì $I = (0)$. Nếu $I \neq \{0\}$, gọi $a \in I$, $a \neq 0$ là phần tử sao cho $\delta(a) \leq \delta(x)$ với mọi $x \in I$, $x \neq 0$. Ta chứng tỏ $I = (a)$. Với b tùy ý trong I, tồn tại $q, r \in D$ sao cho $b = qa + r$ với $r = 0$ hay $\delta(r) < \delta(b)$. Vì $r = b - qa \in I$, bởi tính nhỏ nhất của $\delta(a)$ ta suy ra $r = 0$ và $b = qa \in I$. Vì vậy $I = (a)$.

□

Mệnh đề 5.21. *Trong miền iđêan chính D cho hai phần tử a và b không đồng thời bằng không. Khi đó ước chung lớn nhất của chúng luôn tồn tại. Nếu $d = \gcd(a, b)$ thì có $u, v \in D$ sao cho $d = ua + vb$.*

Chứng minh. Gọi I là iđêan được sinh ra bởi a và b. Vì D là một miền iđêan chính nên có $d \in D$ sao cho $I = (d)$. Ta chứng tỏ d là một ước chung lớn nhất của a và b. Vì $a, b \in I = (d)$ nên d là một ước chung của a và b. Mặt khác, $d \in I = (a, b)$ nên có $u, v \in D$ sao cho $d = ua + vb$. Nếu c là một ước chung của a và b thì c là một ước của $ua + vb = d$ và do đó d là một ước chung lớn nhất của a và b.

□

Định nghĩa 5.22. Ta nói hai phần tử a và b trong miền nguyên D là *nguyên tố cùng nhau* nếu 1 là một ước chung lớn nhất của chúng.

Hệ quả 5.23. *Cho miền iđêan chính D và $a, b \in D$. Khi đó a và b nguyên tố cùng nhau nếu và chỉ nếu có $u, v \in D$ sao cho $ua + vb = 1$.*

Chứng minh. Chiều thuận được suy ra từ Mệnh đề 5.21. Đảo lại, nếu có $u, v \in D$ sao cho $ua + vb = 1$, khi đó mọi ước chung của a và b đều là ước của 1, do đó 1 là ước chung lớn nhất của a và b.

□

Mệnh đề 5.24. *Cho phần tử p khác không trong miền iđêan chính D. Khi đó p là bất khả quy nếu và chỉ nếu iđêan được sinh ra bởi p là một iđêan tối đại.*

Chứng minh. Giả sử D là một miền iđêan chính. Cho $p \in D$ là bất khả quy. Nếu I là một iđêan sao cho $(p) \subset I \subset D$, khi đó vì D là một miền iđêan chính nên $I = (q)$ với phần tử q nào đó trong D. Vì $p \in I$ nên $p = rq$ với phần tử r trong D, p là bất khả quy nên r hay q khả nghịch. Nếu r khả nghịch thì $(p) = (q) = I$. Nếu q khả nghịch thì $I = D$. Vậy (p) là iđêan tối đại.

Giả sử (p) là một iđêan tối đại. Vì (p) là iđêan thực sự của D nên p không khả nghịch. Nếu $p = xy$ là một phân tích trong D, khi đó $(p) \subset (x) \subset D$. Vì I là tối đại nên $(p) = (x)$ hoặc $(x) = D$. Nếu $(p) = (x)$, theo Mệnh đề 5.3 thì p và x liên kết, và khi đó y là phần tử khả nghịch. Nếu $(x) = D = (1)$ thì x và 1 liên kết, và x là phần tử khả nghịch. Vậy nếu $p = xy$ thì x hay y là phần tử khả nghịch, và p là bất khả quy.

□

Mệnh đề 5.25. *Trong một miền iđêan chính, mọi phần tử bất khả quy đều nguyên tố.*

Chứng minh. Cho D là một miền iđêan chính và $p \in D$ là bất khả quy. Giả sử $p \mid ab$ với $a, b \in D$. Vì p chỉ có ước không thật sự, do đó nếu $p \nmid a$ thì ước chung của p và a phải là những phần tử khả nghịch. Trong trường hợp này p và a nguyên tố cùng nhau nên có $r, s \in D$ sao cho $1 = rp + sa$. Nhân hai vế với b ta được $b = (rb)\, p + s\,(ab)$. p chia hết vế phải nên p chia hết b và p là nguyên tố.

□

Như vậy trong một miền iđêan chính, bởi các Mệnh đề 5.9, 5.25 thì phần tử nguyên tố là bất khả quy và ngược lại, và bởi các Mệnh đề 5.8, 5.24, trong tập hợp các iđêan không tầm thường thì các iđêan nguyên tố và các iđêan tối đại là trùng nhau.

Ví dụ 5.26. (a) $\mathbb{Z}\left[\sqrt{5}i\right]$ trong Ví dụ 5.10 không phải miền iđêan chính vì $2 \in \mathbb{Z}\left[\sqrt{5}i\right]$ là bất khả quy nhưng không là nguyên tố.

(b) $\mathbb{Z}[x]$ không phải là một miền iđêan chính vì iđêan được sinh ra bởi 2 và x không phải là một iđêan chính.

Bây giờ ta sẽ chứng tỏ mọi phần tử khác không và không khả nghịch trong một miền iđêan chính luôn phân tích được thành tích các phần tử bất khả quy. Trước hết ta cần các bổ đề sau.

Bổ đề 5.27. *Cho miền iđêan chính D và $I_1 \subset I_2 \subset \cdots$ là một dãy tăng các iđêan trong D. Khi đó tồn tại số nguyên dương m sao cho $I_n = I_m$ với mọi $n \geq m$.*

Chứng minh. Đặt $I = \cup_i I_i$, ta chứng tỏ I là một iđêan trong D. Thật vậy, ta có $I \neq \emptyset$ và nếu $x, y \in I$, $r \in D$ thì có k, l sao cho $x \in I_k$ và $y \in I_l$. Gọi h là số lớn hơn k và l thì $x, y \in I_h$, vì I_h là một iđêan nên $x - y, rx \in I_h \subset I$. Vậy I là một iđêan. D là một miền iđêan chính nên $I = (a)$ với phần tử a nào đó trong D. Vì $a \in I$ nên có m sao cho $a \in I_m$. Khi đó với mọi $n \geq m$ thì

$$(a) \subset I_m \subset I_n \subset I = (a).$$

Vậy $I_n = I_m$ với mọi $n \geq m$.

□

Bổ đề 5.28. *Cho miền iđêan chính D và phần tử $a \in D$ khác không, không khả nghịch. Khi đó a có ước bất khả quy.*

Chứng minh. Nếu a là bất khả quy thì một ước bất khả quy của a là chính nó. Giả sử a khả quy, khi đó a có một ước thật sự, tức là có một phân tích $a = x_1 y_1$ trong D, trong đó x_1, y_1 là hai phần tử không khả nghịch nào đó và $(a) \subsetneq (y_1)$. Nếu y_1 là bất khả quy thì a có một ước bất khả quy, ngược lại có một phân tích $y_1 = x_2 y_2$ trong D, ở đây x_2, y_2 là hai phần tử không khả nghịch và $(y_1) \subsetneq (y_2)$. Tiếp tục cách này ta có một dãy các iđêan

$$(a) \subset (y_1) \subset (y_2) \subset \cdots$$

trong đó $y_i = x_{i+1} y_{i+1}$. Bởi Bổ đề 5.27 có m sao cho $(y_n) = (y_m)$ với mọi $n \geq m$. Khi đó y_{m+1} liên kết với y_m và x_{m+1} là phần tử khả nghịch, do đó y_m là một ước bất khả quy của a.

□

Định lý 5.29. *Cho miền iđêan chính D và phần tử $a \in D$ khác không, không khả nghịch. Khi đó*

(a) *a được viết dưới dạng $a = p_1 p_2 \cdots p_n$, trong đó các phần tử p_i, $i = 1, \ldots, n$, là bất khả quy;*

(b) *Nếu $a = q_1 q_2 \cdots q_m$ là một phân tích khác của a thành tích các phần tử bất khả quy thì $n = m$ và với một cách đánh số thích hợp ta có $q_i = u_i p_i$ với u_i khả nghịch, $i = 1, \ldots n$.*

Chứng minh. (a) Cho $a \in D$ khác không và không khả nghịch. Bởi Bổ đề 5.28, $a = p_1 y_1$, trong đó p_1 là bất khả quy. Nếu y_1 khả nghịch thì (a) được chứng minh. Ngược lại, $y_1 = p_2 y_2$ với p_2 bất khả quy. Nếu y_2 khả nghịch thì a là tích của những phần tử bất khả quy. Ngược lại, tiếp tục cách trên ta có một dãy các iđêan

$$(a) \subset (y_1) \subset (y_2) \subset \cdots$$

Theo Bổ đề 5.27 thì dãy trên dừng tại một số n nào đó, khi đó y_{n+1} là khả nghịch và $a = p_1 p_2 \cdots p_n$, ở đây các p_i, $i = 1, \ldots, n$, là bất khả quy.

(b) Giả sử a có một phân tích khác $a = q_1 q_2 \cdots q_m$, q_j bất khả quy và $m \geq n$. Khi đó $p_1 \mid q_1 q_2 \cdots q_m$, bởi Mệnh đề 5.25 ta có p_1 là nguyên tố nên p_1 chia hết một q_j nào đó. Bằng cách đánh số lại các chỉ số, ta giả sử $p_1 \mid q_1$ và khi đó p_1 và $q_1$liên kết, tức là có u_1 khả nghịch sao cho $q_1 = u_1 p_1$. Bởi tính giản ước trong miền nguyên ta có $p_2 \cdots p_n = u_1 q_2 \cdots q_m$. Tiếp tục cách này với các p_i còn lại, ta có

$$1 = u_1 \cdots u_n q_{n+1} \cdots q_m.$$

Vì các $q_{m+1}, \ldots, q_m$ là bất khả quy nên $m = n$ và mỗi p_i và q_i là liên kết. Định lý được chứng minh.

□

Ví dụ 5.30. Trong vành số nguyên $\mathbb{Z}$ ta có

$$12 = 2 \cdot 2 \cdot 3 = (-2) \cdot 2 \cdot (-3) = 2 \cdot (-2) \cdot (-3).$$

Bây giờ ta chuyển qua vấn đề nhân tử hóa một đa thức liên quan đến trường các thương. Như đã biết, nếu f là một đa thức trong $\mathbb{Z}[x]$, bởi Định lý 4.40, f có nhân tử hóa thành tích các đa thức bất khả quy trong $\mathbb{Q}[x]$ thì f cũng có nhân tử hóa thành tích các đa thức bất khả quy trong $\mathbb{Z}[x]$. Định lý sau là mở rộng của định lý trên đối với miền idêan chính mà chứng minh của nó hoàn toàn tương tự.

Định lý 5.31. *Cho miền idêan chính D, Q là trường các thương của D và đa thức $f \in D[x]$. Nếu f phân tích được trong $Q[x]$ thành tích của hai đa thức có bậc r và s thì f cũng phân tích được trong $D[x]$ thành tích của hai đa thức có bậc r và s.*

Bài tập

1. Xác định các phần tử khả nghịch trong mỗi miền nguyên sau.
   (a) $\mathbb{Z}\left[\sqrt{2}i\right]$ (b) $\mathbb{Z}_5[x]$ (c) $\mathbb{Z}[i][x]$ (a) $\mathbb{R}[x]$
2. Cặp nào sau đây là liên kết trong miền nguyên đã cho.
   (a) $3 + 2\sqrt{2}$ và $-1 + \sqrt{2}$ trong $\mathbb{Z}\left[\sqrt{2}\right]$.
   (b) 2 và $2 + \sqrt{3}$ trong $\mathbb{Z}\left[\sqrt{3}\right]$.
   (c) $4x - 8$ và $x - 2$ trong $\mathbb{Z}[x]$.
   (d) $\overline{5}x^3 + x - \overline{4}$ và $x^3 + \overline{3}x + \overline{2}$ trong $\mathbb{Z}_7[x]$.
   (e) $1 + \sqrt{5}i$ và $1 - \sqrt{5}i$ trong $\mathbb{Z}\left[\sqrt{5}i\right]$.
3. Phần tử nào sau đây trong miền nguyên tương ứng là nguyên tố hay bất khả quy?
   (a) $7x - 5$ trong $\mathbb{Z}[x]$, trong $\mathbb{C}[x]$, trong $\mathbb{Z}_{11}[x]$.

(b) -5 trong $\mathbb{Z}\left[\sqrt{5}i\right]$, trong $\mathbb{Z}$, trong $\mathbb{Q}$.

(c) 11 trong $\mathbb{Z}\left[\sqrt{3}\right]$, trong $\mathbb{Z}$, trong $\mathbb{R}$.

(d) 19 trong $\mathbb{Z}\left[\sqrt{3}i\right]$, trong $\mathbb{Z}\left[\sqrt{2}i\right]$, trong $\mathbb{C}$.

4. Chứng tỏ $\mathbb{Z}\left[\sqrt{3}i\right]$ không phải miền Euclid.
5. $\mathbb{Z}[x]$ có phải là miền Euclid không?
6. 5 có phải là phần tử bất khả quy trong $\mathbb{Z}[i]$ không?
7. Chứng tỏ rằng một số nguyên Gauss là bất khả quy nếu và chỉ nếu nó là tích của một phần tử khả nghịch với một số nguyên Gauss có dạng sau:

   (a) Số nguyên tố p tùy ý trong $\mathbb{Z}$ với $p \equiv 3 \bmod 4$.

   (b) $1+i$.

   (c) $a+bi$, ở đây a là số nguyên dương và chẵn và $a^2+b^2=p$ là một số nguyên tố trong $\mathbb{Z}$ sao cho $p \equiv 1 \bmod 4$.
8. Cho D là một miền nguyên. Chứng tỏ các khẳng định sau là tương đương.

   (a) D là một trường.

   (b) $D[x]$ là một miền Euclid.

   (c) $D[x]$ là một miền iđêan chính.

Chương 6

TRƯỜNG

Trong chương này chúng ta sẽ tìm hiểu các trường mở rộng của một trường cho trước. Đặc biệt với một đa thức hệ số trên một trường đã cho, ta chứng tỏ luôn tồn tại một trường mở rộng sao cho đa thức được phân tích thành tích của các nhân tử bậc nhất trên trường đó. Cuối chương dành cho việc tìm hiểu trường hữu hạn.

6.1 Đặc số của một trường

Định nghĩa 6.1. Giả sử F là một trường. Nếu đơn vị 1 với phép toán cộng có cấp là một số p hữu hạn thì ta nói F có *đặc số* p và viết $\text{Char}F = p$. Ngược lại, ta nói F có đặc số 0 và viết $\text{Char}F = 0$.

Chú ý rằng nếu $\text{Char}F{=}p > 0$thì $px = (p1)\,x = 0x = 0$ với mọi $x \in F$.

Mệnh đề 6.2. *Cho F là một trường. Khi đó* $\text{Char}F = 0$ *hay* $\text{Char}F{=}p$*, ở đây p là một số nguyên tố.*

Chứng minh. Giả sử $\text{Char}F = p > 0$. Nếu p không là số nguyên tố thì có hai số nguyên dương m, n nhỏ hơn p sao cho $p = mn$. Khi đó

$$0 = p1 = (mn)\,1 = (m1)\,(n1)\,.$$

Vì F là một trường nên không có ước của không, do đó $m1 = 0$ hay $n1 = 0$. Trong cả hai trường hợp đều mâu thuẩn với p là cấp của 1. Vậy p phải là một số nguyên tố.

□

Ví dụ 6.3. (a) Các trường $\mathbb{Q}$, $\mathbb{R}$ và $\mathbb{C}$ là các trường có đặc số 0.

(b) Trường Z_p các số nguyên mod$p$ (p nguyên tố) có đặc số p.

Định nghĩa 6.4. Trong một trường F đặt P là giao của tất cả các trường con của F thì P cũng là một trường con của F. Ta nói trường con P như thế là *trường con nguyên tố* của F.

Ta thấy rằng trường con nguyên tố của F là trường con nhỏ nhất của F theo quan hệ bao hàm. Định lý sau đây mô tả cụ thể trường con nguyên tố của một trường tùy ý.

Định lý 6.5. *Cho F là một trường. Khi đó*

(a) *Nếu* $\mathrm{Char}F = 0$ *thì trường con nguyên tố P của F đẳng cấu với trường $\mathbb{Q}$.*

(b) *Nếu* $\mathrm{Char}F = p > 0$ *thì trường con nguyên tố P của F đẳng cấu với trường $\mathbb{Z}_p$.*

Chứng minh. Xét đồng cấu vành $f : \mathbb{Z} \to F$ được xác định bởi $f(m) = m1$ với mọi $m \in \mathbb{Z}$. Vì $1 \in P$ nên $\mathrm{Im}f \subset P$. Ta có $\ker f$ là một iđêan của $\mathbb{Z}$ nên có dạng $\ker f = s\mathbb{Z}$ với số nguyên $s \geq 0$ nhỏ nhất thuộc $\ker f$. Vì $f(s) = s1 = 0$ và bởi tính chất của s nên s chính là đặc số của trường F.

(a) Nếu F có đặc số $s = 0$ thì $\ker f = \{0\}$, khi đó ta có đẳng cấu miền nguyên $f : \mathbb{Z} \cong \mathrm{Im}f \subset P$. Do đó trường các thương $\mathbb{Q}$ của $\mathbb{Z}$ đẳng cấu với trường các thương K của $\mathrm{Im}f$. Vì $\mathrm{Im}f \subset P$, bởi Hệ quả **??** ta có $K \subset P$. Mặt khác, vì K là một trường con của F nên chứa trường con nguyên tố P. Vậy $K = P$, nói cách khác $P \cong \mathbb{Q}$.

(b) Nếu F có đặc số $s = p$ (p nguyên tố), theo Hệ quả 3.49 thì

$$\mathbb{Z}/\ker f = \mathbb{Z}/p\mathbb{Z} \cong \mathrm{Im}f \subset P.$$

$\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$ là một trường, suy ra $\mathrm{Im}f$ cũng là một trường. Trường này chứa trong trường con nguyên tố P và do đó $\mathbb{Z}_p \cong \mathrm{Im}f = P$.

□

Như vậy, theo định lý trên $\mathbb{Q}$ là trường nhỏ nhất có đặc số 0 và $\mathbb{Z}_p$ trường nhỏ nhất có đặc số p. Mọi trường đều chứa một trường con đẳng cấu với $\mathbb{Q}$ hoặc $\mathbb{Z}_p$ tùy theo đặc số của nó là 0 hay p.

Mệnh đề 6.6. *Trong một trường F có đặc số p ta luôn có $(a+b)^p = a^p + b^p$ với mọi $a, b \in F$.*

Chứng minh. Ta có

$$(a+b)^p = a^p + b^p + \sum_{i=1}^{p-1} C_p^i a^i b^{p-i}.$$

Với $1 \leq i \leq p-1$, C_p^i chia hết cho p và do đó

$$C_p^i a^i b^{p-i} = \left(C_p^i 1\right)\left(a^i b^{p-i}\right) = 0.$$

Mệnh đề được chứng minh.

□

Mệnh đề 6.7. *Cho F là một trường có đặc số p. Khi đó ánh xạ Frobenius $\varphi : F \longrightarrow F$ được xác định bởi $\varphi(x) = x^p$ với mọi $x \in F$ là một đơn cấu.*

Chứng minh. Cho $x, y \in F$, bởi Mệnh đề 6.6 ta có

$$f(x+y) = (x+y)^p = x^p + y^p = f(x) + f(y).$$

Hiển nhiên $f(xy) = (xy)^p = x^p y^p = f(x) f(y)$ và f là một đồng cấu trường. Vì f không phải đồng cấu tầm thường nên f là một đơn cấu.

□

6.2 Mở rộng đại số

Cho F là một trường con của trường E, khi đó ta còn nói E là một trường mở rộng của F. Với phép cộng trên E và phép nhân phần tử trong F với phần tử trong E thì E là một F-không gian véc-tơ.

Định nghĩa 6.8. Cho E là một trường mở rộng của trường F và $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$. Ta ký hiệu $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ là trường con nhỏ nhất của E chứa F và $\alpha_1, \alpha_2, \ldots, \alpha_n$, gọi là trường mở rộng của F bởi các phần tử $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Đặt $F_0 = F$, với mỗi $i \geq 1$, đặt $F_i = F(\alpha_1, \alpha_2, \ldots, \alpha_i)$ thì $F_{i+1} = F_i(\alpha_{i+1})$. Ta nói $F_i(\alpha_{i+1})$ là *mở rộng đơn* của F_i bởi phần tử α_{i+1} và ta có dãy các mở rộng đơn $F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n$. Như vậy $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ là mở rộng của F nhận được bởi liên tiếp các mở rộng đơn.

Mệnh đề sau mô tả các phần tử của trường mở rộng đơn $F(\alpha)$ của F.

Mệnh đề 6.9. *Cho E là một trường mở rộng của trường F và $\alpha \in E$. Khi đó*

$$F(\alpha) = \left\{ \frac{P(\alpha)}{Q(\alpha)} \mid P, Q \in F[x], Q(\alpha) \neq 0 \right\}.$$

Chứng minh. Đặt $K = \left\{ \frac{P(\alpha)}{Q(\alpha)} \mid P, Q \in F[x], Q(\alpha) \neq 0 \right\}$. Dễ thấy K chứa phần tử 0 và 1, K ổn định với các phép cộng, trừ, nhân và nghịch đảo của phần tử khác không nên K là một trường con của E. Hơn nữa, K chứa F và α nên chứa $F(\alpha)$. Mặt khác, mọi phần tử của K đều nhận được từ các phần tử của F và α bởi các phép toán cộng, trừ, nhân và chia nên là một phần tử của $F(\alpha)$ và do đó $K \subset F(\alpha)$. Vậy $K = F(\alpha)$.

□

Định nghĩa 6.10. Cho E là một trường mở rộng của trường F và $\alpha \in E$. Ta nói α là *đại số* trên F nếu có đa thức $f \in F[x]$ khác không sao cho $f(\alpha) = 0$. Ngược lại, ta nói α là siêu việt trên F.

Ví dụ 6.11. (a) $\sqrt{2}$ là nghiệm của đa thức $x^2 - 2 \in \mathbb{Q}[x]$ nên $\sqrt{2}$ là đại số trên $\mathbb{Q}$.

(b) Cho trường F, khi đó mọi phần tử $a \in F$ đều đại số trên F vì là nghiệm của đa thức $x - a \in F[x]$.

(c) Người ta chứng tỏ được số π không là nghiệm của bất kỳ đa thức khác không nào với hệ số hữu tỷ nên số π là siêu việt trên $\mathbb{Q}$.

Mệnh đề 6.12. *Cho E là một trường mở rộng của trường F và $\alpha \in E$ đại số trên F. Khi đó*

(a) *Có duy nhất đa thức bất khả quy đơn hệ $p \in F[x]$ nhận α làm nghiệm.*

(b) *Nếu có đa thức $f \in F[x]$ nhận α làm nghiệm thì f chia hết cho p.*

Chứng minh. Vì α đại số trên F nên có đa thức khác không thuộc $F[x]$ nhận α làm nghiệm. Gọi $p \in F[x]$ là đa thức khác không có bậc nhỏ nhất nhận α làm nghiệm. Đa thức p được chọn đơn hệ bằng cách nhân với một phần tử khác không thích hợp trong F. Ta chứng tỏ p là bất khả quy trên F. Giả sử $p = gh$ là một phân tích trong $F[x]$ thành tích của hai đa thức có bậc nhỏ hơn bậc của p. Vì α là nghiệm của p nên là nghiệm của g hay h. Trong cả hai trường hợp ta đều có α là nghiệm của đa thức có bậc nhỏ hơn bậc của p, đây là một mâu thuẩn. Vậy p là bất khả quy trên F. Bây giờ giả sử $f \in F[x]$ nhận α làm nghiệm, lấy f chia cho p ta được $f = sp + r$, trong đó $r = 0$ hoặc r là đa thức có bậc nhỏ hơn bậc của p. Vì α là nghiệm của f và p nên α là nghiệm của r, và do bậc của r nhỏ hơn bậc của p nên r phải là đa thức không. Vậy f chia hết cho p và ta có (b).

Cuối cùng chỉ còn phải chứng tỏ p là duy nhất. Giả sử $q \in F[x]$ là đa thức bất khả quy đơn hệ nhận α làm nghiệm. Theo (b) thì q chia hết cho p, và bởi q là bất khả quy nên có $a \in F$ sao cho $q = ap$. Vì p và q đều đơn hệ nên $a = 1$ và $q = p$. Vậy ta có (a).

□

Định nghĩa 6.13. Cho E là một trường mở rộng của trường F và $\alpha \in E$ đại số trên F. Khi đó có duy nhất đa thức bất khả quy đơn hệ $p \in F[x]$ nhận α làm nghiệm. Đa thức này còn gọi là *đa thức cực tiểu* của α trên F và bậc của nó được ký hiệu là $\deg_F(\alpha)$.

Ví dụ 6.14. (a) Cho trường F. Khi đó với mọi $a \in F$ thì $x - a$ là đa thức cực tiểu của a trên F và $\deg_F(a) = 1$.

(b) $\sqrt{2}$ là nghiệm của đa thức $x^2 - 2 \in \mathbb{Q}[x]$, $x^2 - 2$ là đa thức cực tiểu của $\sqrt{2}$ trên $\mathbb{Q}$ và $\deg_{\mathbb{Q}}\left(\sqrt{2}\right) = 2$.

Khi α là một phần tử đại số trên F, mệnh đề sau mô tả cấu trúc của $F(\alpha)$.

Mệnh đề 6.15. *Cho E là một trường mở rộng của trường F và $\alpha \in E$ đại số trên F. Đặt $n = \deg_F(\alpha)$ và p là đa thức cực tiểu của α trên F. Khi đó*

(a) *Trường $F(\alpha)$ đẳng cấu với trường $F[x]/(p)$.*

(b) *$F(\alpha)$ là một F-không gian véc-tơ với cơ sở $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$.*

Chứng minh. (a) Gọi $p \in F[x]$ là đa thức cực tiểu của α, p có bậc n. Xét ánh xạ $\eta : F[x] \longrightarrow E$ được xác định bởi $\eta(f) = f(\alpha)$ với mỗi $f \in F[x]$. Hiển nhiên η là một đồng cấu vành và $\text{Im}\eta = \{f(\alpha) \mid f \in F[x]\} \subset F(\alpha)$. Nếu $h \in \ker\eta$ thì $h(\alpha) = 0$, bởi Mệnh đề 6.12 thì h chia hết cho p và do đó $\ker\eta = (p)$. Theo Hệ quả 3.49 thì $F[x]/(p)$ đẳng cấu với $\text{Im}\eta$. Tiếp theo ta chứng tỏ $\text{Im}f = F(\alpha)$. Vì p là đa thức bất khả quy trong $F[x]$ nên iđêan được sinh ra bởi p là tối đại và do đó $F[x]/(p)$ là một trường. Vậy $\text{Im}f$ là một trường và là trường chứa F và α nên $\text{Im}f = F(\alpha)$.

(b) Khẳng định còn lại của mệnh đề được chứng minh như sau. Với mỗi $f \in F[x]$ ta viết $f = qp + r$, ở đây r là đa thức có bậc nhỏ hơn bậc của đa thức p. Khi đó $f(\alpha) = q(\alpha)p(\alpha) + r(\alpha) = r(\alpha)$ vì $p(\alpha) = 0$, tức là $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ là một hệ sinh của F-không gian véc-tơ $F(\alpha)$. Nếu có $b_0, b_1, \ldots, b_{n-1} \in F$ sao cho

$$b_0 1 + b_1\alpha_1 + \cdots + b_{n-1}\alpha^{n-1} = 0,$$

ta đặt $u = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} \in F[x]$, là đa thức có bậc nhỏ hơn n nhận α làm nghiệm nên phải là đa thức không, tức là $b_0 = b_1 = \cdots = b_{n-1} = 0$. Vậy $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ độc lập tuyến tính và là một cơ sở của F-không gian véc-tơ $F(\alpha)$. □

Ví dụ 6.16. (a) $\mathbb{Q}\left(\sqrt[3]{2}\right)$ là một trường mở rộng của $\mathbb{Q}$. Vì $\sqrt[3]{2}$ là nghiệm của đa thức $x^3 - 2$, $x^3 - 2$ không có nghiệm trong $\mathbb{Q}$ nên bất khả quy trên $\mathbb{Q}$. Do đó $\mathbb{Q}\left(\sqrt[3]{2}\right)$ là một không gian véc-tơ trên $\mathbb{Q}$ với cơ sở $1, \sqrt[3]{2}, \left(\sqrt[3]{2}\right)^2$. Mọi phần tử trong $\mathbb{Q}\left(\sqrt[3]{2}\right)$ có dạng $b_0 + b_1\sqrt[3]{2} + b_2\left(\sqrt[3]{2}\right)^2$ với $b_0, b_1, b_2 \in \mathbb{Q}$.

(b) $\mathbb{Q}\left(\sqrt[5]{2}\right)$ là một trường mở rộng của $\mathbb{Q}$. $\sqrt[5]{2}$ là nghiệm của đa thức $x^5 - 2 \in \mathbb{Q}[x]$. Bởi tiêu chuẩn Eisenstein, $x^5 - 2$ là bất khả quy trên $\mathbb{Q}$. $\mathbb{Q}\left(\sqrt[5]{2}\right)$ là một không gian véc-tơ trên $\mathbb{Q}$ với cơ sở $1, \sqrt[5]{2}, \left(\sqrt[5]{2}\right)^2, \left(\sqrt[5]{2}\right)^3, \left(\sqrt[5]{2}\right)^4$.

Định nghĩa 6.17. Giả sử E là một trường mở rộng của trường F. Ta nói E là *mở rộng hữu hạn* của F nếu E là một F-không gian véc-tơ hữu hạn chiều, khi đó ký hiệu $[E : F]$ là chiều của F-không gian véc-tơ E và gọi là bậc của E trên F. Ngược lại, ta nói E là mở rộng vô hạn của F.

Ví dụ 6.18. (a) $\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3$.

(b) $[\mathbb{C} : \mathbb{R}] = 2$.

(c) F là một trường tùy ý thì $[F : F] = 1$.

(d) α là một phần tử đại số trên trường F thì $[F(\alpha) : F] = \deg_F(\alpha)$.

(e) $\mathbb{R}$ là một mở rộng vô hạn của $\mathbb{Q}$. Thật vậy, nếu $[\mathbb{R} : \mathbb{Q}] = n$ hữu hạn thì $\mathbb{R}$ đẳng cấu với $\mathbb{Q}^n$ như các $\mathbb{Q}$-không gian véc-tơ. Đây là một mâu thuẩn vì $\mathbb{R}$ là tập hợp vô hạn không đếm được trong khi đó $\mathbb{Q}^n$ là tập hợp đếm được.

Định lý 6.19. *Cho E là một trường mở rộng hữu hạn của trường F và K một trường mở rộng hữu hạn của E. Khi đó*

(a) *K là trường mở rộng hữu hạn của F và $[K:F] = [K:E]\,[E:F]$.*

(b) *Đặt $m = [K:E]$ và $\{u_1, u_2, \ldots, u_m\}$là một cơ sở của K trên E, $n = [E:F]$ và $\{v_1, v_2, \ldots, v_n\}$là một cơ sở của E trên F thì $\{u_i v_j \mid 1 \le i \le m, 1 \le j \le n\}$ là một cơ sở của K trên F.*

Chứng minh. Định lý sẽ được chứng minh nếu ta chứng tỏ

$$\{u_i v_j \mid 1 \le i \le m, 1 \le j \le n\}$$

là một cơ sở của K trên F. Cho $\alpha \in K$ là một phần tử tùy ý, vì $\{u_1, u_2, \ldots, u_m\}$là một cơ sở của K trên E nên có các phần tử $c_i \in E$, $1 \le i \le m$, sao cho $\alpha = \sum_{i=1}^{m} c_i u_i$. Với mỗi $c_i \in E$, vì $\{v_1, v_2, \ldots, v_n\}$là một cơ sở của E trên F nên có các phần tử $d_{ij} \in F$, $1 \le j \le n$, sao cho $c_i = \sum_{j=1}^{n} d_{ij} v_j$. Khi đó $\alpha = \sum_{i=1}^{m} \sum_{j=1}^{n} d_{ij}\,(u_i v_j)$ và do đó $\{u_i v_j \mid 1 \le i \le m, 1 \le j \le n\}$ là một hệ sinh của F-không gian véc-tơ K.

Tiếp theo ta chứng tỏ $\{u_i v_j \mid 1 \le i \le m, 1 \le j \le n\}$ là độc lập tuyến tính trên F. Giả sử $\sum_{i=1}^{m} \sum_{j=1}^{n} k_{ij}\,(u_i v_j) = 0$, trong đó $k_{ij} \in F$. Ta có $\sum_{i=1}^{m} \left(\sum_{j=1}^{n} k_{ij} v_j\right) u_i = 0$, vì $\{u_1, u_2, \ldots, u_m\}$ độc lập tuyến tính trên E nên $\sum_{j=1}^{n} k_{ij} v_j = 0$ với mọi i. Vì $\{v_1, v_2, \ldots, v_n\}$ độc lập tuyến tính trên F nên $k_{ij} = 0$ với mọi i, j. Ta có điều phải chứng minh.

□

Ví dụ 6.20. (a) Xác định bậc của $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ trên $\mathbb{Q}$. Xét dãy các mở rộng

$$\mathbb{Q} \subset \mathbb{Q}\left(\sqrt{2}\right) \subset \mathbb{Q}\left(\sqrt{2}\right)\left(\sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right).$$

Đa thức cực tiểu của $\sqrt{2}$ trên $\mathbb{Q}$ là $x^2 - 2$, do đó $\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2$. Ta có $\mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$. Mặt khác $\sqrt{3}$ là một nghiệm của đa thức $x^2 - 3$, nếu đa thức này có nghiệm trong $\mathbb{Q}\left(\sqrt{2}\right)$ thì có $a, b \in \mathbb{Q}$ sao cho $\left(a + b\sqrt{2}\right)^2 - 3 = 0$. Điều này tương đương với $a^2 + 2b^2 - 3 = -2ab\sqrt{2}$, khi đó nếu $a = 0$ thì $b = \pm\sqrt{\frac{3}{2}}$ hoặc nếu $b = 0$ thì $a = \pm\sqrt{3}$ hoặc $ab \neq 0$ thì $\sqrt{2} = \frac{a^2 + 2b^2 - 3}{-2ab}$, trong cả ba trường hợp ta đều có sự vô lý. Vậy đa thức $x^2 - 3$ không có nghiệm trong $\mathbb{Q}\left(\sqrt{2}\right)$, do đó bất khả quy trên $\mathbb{Q}\left(\sqrt{2}\right)$ và $\left[\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) : \mathbb{Q}\left(\sqrt{2}\right)\right] = 2$. Ta có

$$\left[\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) : \mathbb{Q}\left(\sqrt{2}\right)\right]\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 4.$$

(b) Xác định bậc của $\mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}\right)$ trên $\mathbb{Q}$. Đa thức cực tiểu của $\sqrt[3]{2}$ trên $\mathbb{Q}$ là $x^3 - 2$, do đó $\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3$. Nếu $\sqrt{3} \in \mathbb{Q}\left(\sqrt[3]{2}\right)$ thì ta có dãy các trường mở rộng $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt{3}\right) \subset \mathbb{Q}\left(\sqrt[3]{2}\right)$, bởi Định lý 6.19 thì $\left[\mathbb{Q}\left(\sqrt{3}\right) : \mathbb{Q}\right] = 2$ là một ước số của $\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3$, đây là một mâu thuẩn. Do đó $\sqrt{3} \notin \mathbb{Q}\left(\sqrt[3]{2}\right)$, tức là $x^2 - 3$ bất

khả quy trên $\mathbb{Q}\left(\sqrt[3]{2}\right)$ và do đó $\left[\mathbb{Q}\left(\sqrt[3]{2}\right)\left(\sqrt{3}\right):\mathbb{Q}\left(\sqrt[3]{2}\right)\right]=2$. Khi đó

$$\left[\mathbb{Q}\left(\sqrt[3]{2},\sqrt{3}\right):\mathbb{Q}\right]=\left[\mathbb{Q}\left(\sqrt[3]{2},\sqrt{3}\right):\mathbb{Q}\left(\sqrt[3]{2}\right)\right]\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right]=2\cdot 3=6.$$

(c) Tìm đa thức cực tiểu của phần tử $\sqrt[3]{2}+\sqrt{3}$ trên $\mathbb{Q}$. Đặt $\alpha=\sqrt[3]{2}+\sqrt{3}$, khi đó

$$\left(\alpha-\sqrt{3}\right)^3=\alpha^3+9\alpha-3\sqrt{3}\left(\alpha^2+1\right)=2\quad(*),$$

suy ra $27\left(\alpha^2+1\right)^2=\left(\alpha^3+9\alpha-2\right)^2$ và rút gọn ta được

$$\alpha^6-9\alpha^4-4\alpha^3+27\alpha^2-36\alpha-23=0.$$

Vậy α là một nghiệm của đa thức $p=x^6-9x^4-4x^3+27x^2-36x-23\in\mathbb{Q}[x]$. Ta có $\mathbb{Q}(\alpha)\subset\mathbb{Q}\left(\sqrt[3]{2},\sqrt{3}\right)$. Mặt khác, từ $(*)$ ta suy ra $\sqrt{3}=\frac{\alpha^3+9\alpha-2}{3(\alpha^2+1)}\in\mathbb{Q}(\alpha)$, và $\sqrt[3]{2}=\alpha-\sqrt{3}=\alpha-\frac{\alpha^3+9\alpha-2}{3(\alpha^2+1)}\in\mathbb{Q}(\alpha)$. Vậy $\mathbb{Q}(\alpha)=\mathbb{Q}\left(\sqrt[3]{2},\sqrt{3}\right)$. Theo (b) thì $\left[\mathbb{Q}\left(\sqrt[3]{2},\sqrt{3}\right):\mathbb{Q}\right]=\left[\mathbb{Q}\left(\sqrt[3]{2}+\sqrt{3}\right):\mathbb{Q}\right]=6$, tức là đa thức cực tiểu của phần tử $\sqrt[3]{2}+\sqrt{3}$ trên $\mathbb{Q}$ có bậc 6, do đó đa thức p chính là đa thức cực tiểu của phần tử $\sqrt[3]{2}+\sqrt{3}$ trên $\mathbb{Q}$.

Định nghĩa 6.21. Giả sử E là một trường mở rộng của trường F. Ta nói E là *mở rộng đại số* của F nếu mọi phần tử của E đều đại số trên F.

Mệnh đề 6.22. *Mọi trường mở rộng hữu hạn của trường F đều là mở rộng đại số của F.*

Chứng minh. Cho E là một trường mở rộng hữu hạn của F với $[E:F]=n$. Cho α là phần tử tùy ý trong E. Vì E là F-không gian véc-tơ có chiều n nên tập hợp $\{1,\alpha,\ldots,\alpha^n\}$ gồm $n+1$ phần tử trong E phải phụ thuộc tuyến tính. Điều này có nghĩa là có các phần tử $c_0,c_1,\ldots,c_n\in F$ không đồng thời bằng không sao cho

$$c_0+c_1\alpha+\cdots+c_n\alpha^n=0.$$

Khi đó đa thức $f=c_0+c_1x+\cdots+c_nx^n\in F[x]$ là đa thức khác không nhận α làm nghiệm. Vậy α là đại số trên F và ta có điều phải chứng minh.

□

Ví dụ 6.23. (a) Xét phần tử $\alpha=\sqrt[5]{3}-2\left(\sqrt[5]{3}\right)^2+4\left(\sqrt[5]{3}\right)^4$, α có phải đại số trên $\mathbb{Q}$ không? Ta có x^5-3 bất khả quy trên $\mathbb{Q}$ theo tiêu chuẩn Eisenstein và nhận $\sqrt[5]{3}$ làm nghiệm, do đó $\left[\mathbb{Q}\left(\sqrt[5]{3}\right):\mathbb{Q}\right]=5$. Bởi Mệnh đề 6.22, $\mathbb{Q}\left(\sqrt[5]{3}\right)$ là mở rộng đại số của $\mathbb{Q}$. Mặt khác $\alpha\in\mathbb{Q}\left(\sqrt[5]{3}\right)$, suy ra α đại số trên $\mathbb{Q}$.

Hệ quả 6.24. *Cho E là một trường mở rộng hữu hạn của trường F và $\alpha\in E$. Khi đó $\deg_F\alpha$ là một ước số của $[E:F]$.*

Chứng minh. E là một trường mở rộng hữu hạn của F, theo Mệnh đề 6.22 thì E là mở rộng đại số của F và do đó α là đại số trên F. Ta có $F \subset F(\alpha) \subset E$, bởi Định lý 6.19 thì

$$[E : F] = [E : F(\alpha)]\,[F(\alpha) : F].$$

Do đó $\deg_F \alpha = [F(\alpha) : F]$ là một ước số của $[E : F]$.

□

Hệ quả 6.25. *Cho E là một trường mở rộng của trường F và $\alpha, \beta \in E$ là hai phần tử đại số trên F với $n = \deg_F \alpha$, $m = \deg_F \beta$. Khi đó $[F(\alpha, \beta) : F] \leq nm$.*

Chứng minh. Ta có $F \subset F(\alpha) \subset F(\alpha)(\beta) = F(\alpha, \beta)$, bởi Định lý 6.19 thì

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)]\,[F(\alpha) : F].$$

Vì $[F(\alpha, \beta) : F(\alpha)] = [F(\alpha)(\beta) : F(\alpha)] = \deg_{F(\alpha)} \beta$ và $[F(\alpha) : F] = \deg_F \alpha = n$, do đó chỉ cần chứng tỏ $\deg_{F(\alpha)} \beta \leq \deg_F \beta = m$ là đủ. β là phần tử đại số trên F nên β là nghiệm của một đa thức $p \in F[x]$ nào đó có bậc m và bất khả quy trên F. Nếu p cũng bất khả quy trên $F(\alpha)$ thì $\deg_{F(\alpha)} \beta = \deg_F \beta$. Ngược lại, p có phân tích thành tích của những đa thức bất khả quy trên $F(\alpha)$ có bậc nhỏ hơn bậc của p và β là nghiệm của một trong các đa thức này và khi đó $\deg_{F(\alpha)} \beta < \deg_F \beta$. Hệ quả được chứng minh.

□

Mệnh đề 6.26. *Cho E là một trường mở rộng của trường F và $\alpha, \beta \in E$ là hai phần tử đại số trên F. Khi đó $\alpha \pm \beta, \alpha\beta$ và (nếu $\beta \neq 0$) $\alpha\beta^{-1}$ là những phần tử đại số trên F.*

Chứng minh. Bởi Hệ quả 6.25, $F(\alpha, \beta)$ là trường mở rộng hữu hạn của F nên là mở rộng đại số của F. Vì các phần tử $\alpha \pm \beta, \alpha\beta$ và (nếu $\beta \neq 0$) $\alpha\beta^{-1}$ thuộc $F(\alpha, \beta)$ nên là các phần tử đại số trên F.

□

Một hệ quả hiển nhiên từ mệnh đề trên là

Hệ quả 6.27. *Cho E là một trường mở rộng của trường F. Khi đó tập hợp các phần tử trong E mà những phần tử đó đại số trên F lập thành một trường con của E chứa F.*

Định nghĩa 6.28. Đặt $\overline{\mathbb{Q}}$ là tập hợp các số phức đại số trên $\mathbb{Q}$. Khi đó $\overline{\mathbb{Q}}$ là một trường gọi là *trường các số đại số* .

Như đã biết mọi mở rộng hữu *hạn* của một trường F đều là mở rộng đại số. Tuy nhiên, điều ngược lại không đúng tức là có những mở rộng đại số của F nhưng không

là mở rộng hữu hạn. Chẳng hạn, $\overline{\mathbb{Q}}$ là một mở rộng đại số của $\mathbb{Q}$ nhưng không phải mở rộng hữu hạn của $\mathbb{Q}$. Để thấy điều này ta lấy n là số tự nhiên dương tùy ý, khi đó đa thức $x^n - 3$ bất khả quy trên $\mathbb{Q}$ bởi tiêu chuẩn Eisenstein và $\left[\mathbb{Q}\left(\sqrt[n]{3}\right) : \mathbb{Q}\right] = n$. Vì $\mathbb{Q}\left(\sqrt[n]{3}\right) \subset \overline{\mathbb{Q}}$ nên $\left[\overline{\mathbb{Q}} : \mathbb{Q}\right] \geq n$ và do đó $\overline{\mathbb{Q}}$ là mở rộng vô hạn của $\mathbb{Q}$.

Định lý 6.29. *Cho E là một trường mở rộng đại số của trường F và K một trường mở rộng đại số của E. Khi đó K là một trường mở rộng đại số của F.*

Chứng minh. Cho α là phần tử tùy ý trong K. Khi đó α đại số trên E và có đa thức $p = c_0 + c_1 x + \cdots + c_n x^n \in E[x]$ bất khả quy trên E nhận α làm nghiệm. Đặt $L = F(c_o, c_1, \ldots, c_n)$ và xét dãy các trường mở rộng $F \subset L \subset L(\alpha)$. Ta có $c_0, c_1, \ldots, c_n \in E$ là những phần tử đại số trên F, áp dụng liên tiếp Hệ quả 6.25 thì L là mở rộng hữu hạn của F. Ta cũng có $L(\alpha)$ là mở rộng hữu hạn của L, bởi Định lý 6.19 thì $L(\alpha)$ là mở rộng hữu hạn của F và do đó là mở rộng đại số của F. Vậy α là đại số trên F và định lý được chứng minh.

□

Bài tập

1. Cho E là một trường mở rộng của trường F. Với $f \in F[x_1, \ldots, x_n]$ và $\alpha_1, \ldots, \alpha_n \in E$ ta đặt $f(\alpha_1, \ldots, \alpha_n)$ là phần tử thuộc E nhận được khi thay các biến x_i trong f bởi các giá trị α_i. Hãy chứng tỏ
$$F(\alpha_1, \ldots, \alpha_n) = \left\{ \frac{P(\alpha_1, \ldots, \alpha_n)}{Q(\alpha_1, \ldots, \alpha_n)} \mid P, Q \in F[x_1, \ldots, x_n], Q(\alpha_1, \ldots, \alpha_n) \neq 0 \right\}.$$
2. Chứng tỏ các số phức sau là đại số trên $\mathbb{Q}$.
   (a) $2 - \sqrt{7}$ (b) $\sqrt{3} + \sqrt{5}$ (c) $\sqrt[3]{2} - \sqrt{3}$
   (d) $1 - 2i$ (e) $\sqrt{2 - \sqrt{3}}$
3. Cho số phức α là một nghiệm của $x^5 + 2x + 2 \in \mathbb{Q}[x]$. Trong mở rộng đơn $\mathbb{Q}(\alpha)$ của $\mathbb{Q}$ hãy biểu diễn $(\alpha^3 + 2\alpha)(\alpha^3 + 3)$, $\alpha^4(\alpha^3 - \alpha^2 + 3\alpha - 7)$ và $(\alpha + 2)/(\alpha^2 + 4)$ theo một cơ sở của $\mathbb{Q}(\alpha)$.
4. Xác định bậc của trường mở rộng của $\mathbb{Q}$ trong mỗi trường hợp sau.
   (a) $\mathbb{Q}\left(\sqrt{18}, \sqrt[4]{2}\right)$ (b) $\mathbb{Q}\left(\sqrt{10}, 3 + \sqrt{8}\right)$ (c) $\mathbb{Q}\left(\sqrt[5]{3}, i\right)$
   (d) $\mathbb{Q}\left(i, \sqrt{2}, \sqrt{5}\right)$ (e) $\mathbb{Q}\left(\sqrt[3]{3}, \alpha\right)$, α là một nghiệm của $x^4 + 4x + 2$.
5. Chứng tỏ các số phức α sau là đại số trên $\mathbb{Q}$ và xác định $\deg_{\mathbb{Q}}(\alpha)$.
   (a) $\sqrt{7} - i$ (b) $\sqrt{3} + i\sqrt{3}$ (c) $\sqrt[4]{5} + \sqrt{5}$ (d) $\sqrt[3]{2} + \sqrt{5}$
6. Tìm $\deg_F\left(\sqrt{2} + \sqrt{5}\right)$ trên trường F trong các trường hợp sau.
   (a) $\mathbb{Q}$ (b) $\mathbb{Q}\left(\sqrt{10}\right)$ (c) $\mathbb{Q}\left(\sqrt{3}\right)$ (d) $\mathbb{Q}\left(\sqrt{2}, \sqrt{5}\right)$
7. Tìm đa thức cực tiểu trong $\mathbb{Q}[x]$ nhận số được cho làm nghiệm trong các trường hợp sau:

(a) $\sqrt{2}-3$ (b) $\sqrt{3}+\sqrt[4]{3}$ (c) $\sqrt[3]{2}+\sqrt[3]{4}$
(d) $\alpha^2+\alpha$, α là một nghiệm của x^3+3x^2-3.

8. Trong các trường hợp sau đa thức có bất khả quy trên trường được cho không?
(a) x^3+3 trên $\mathbb{Q}\left(\sqrt{5}\right)$.
(b) $x^4-2x^3+4x^2-8x+6$ trên $\mathbb{Q}\left(\sqrt[5]{3}\right)$.
(c) x^3+8x-2 trên $\mathbb{Q}\left(\sqrt{2},i\right)$.
(d) x^5+3x+3 trên $\mathbb{Q}\left(\sqrt{5},\sqrt{7},1+i\right)$.
9. Trong mỗi trường hợp sau, hãy xét xem phần tử α có sinh ra mở rộng được cho của $\mathbb{Q}$ không?
(a) $\alpha=\sqrt{3}+\sqrt{7}$ trong $\mathbb{Q}\left(\sqrt{3},\sqrt{7}\right)$.
(b) $\alpha=\frac{\sqrt{3}-1}{\sqrt{3}+5}$ trong $\mathbb{Q}\left(\sqrt{3}\right)$.
(c) $\alpha=\beta^2+\beta+1$ trong $\mathbb{Q}(\beta)$, ở đây β là một nghiệm của x^3+5x-5.
10. Chứng tỏ $\mathbb{Q}\left(\sqrt{2},\sqrt{11},\sqrt{13}\right)=\mathbb{Q}\left(\sqrt{2}+\sqrt{11}+\sqrt{13}\right)$.
11. Chứng tỏ $\mathbb{Q}\left(\sqrt{5}\right)$ và $\mathbb{Q}\left(\sqrt{7}\right)$ không đẳng cấu.
12. Chứng tỏ rằng nếu F là một trường mở rộng bậc hai của $\mathbb{Q}$ thì $F=\mathbb{Q}\left(\sqrt{d}\right)$, trong đó d là một số nguyên không có ước là một số bình phương. Kết quả như thế nào nếu $\mathbb{Q}$ được thay bởi $\mathbb{R}$?
13. Cho F là một trường con của trường E và cho $\alpha\in E$ đại số trên F. Chứng tỏ $I=\{f\in F[x]\mid f(\alpha)=0\}$ là một iđêan thức sự của $F[x]$.
14. Cho F là một trường con của trường E và $\alpha\in E$. Chứng tỏ $F(\alpha)$ là F-không gian véc-tơ hữu hạn chiều nếu và chỉ nếu α đại số trên F.
15. Cho F là một trường con của trường E và $\alpha\in E$. Chứng tỏ α đại số trên F nếu và chỉ nếu $F[\alpha]=\{f(\alpha)\mid f\in F[x]\}$ là một trường.
16. Cho F là một trường con của trường E và $\alpha\in E$. Chứng tỏ α siêu việt trên F nếu và chỉ nếu $F[\alpha]=\{f(\alpha)\mid f\in F[x]\}$ đẳng cấu với vành đa thức $F[x]$.
17. Cho f và g là hai đa thức bất khả quy trên trường F với $\deg f=10$ và $\deg g=9$. Giả sử α là một nghiệm của f trong một trường mở rộng của F, chứng tỏ g vẫn còn bất khả quy trên $F(\alpha)$.
18. Cho F là một trường con của trường E và $\alpha,\beta\in E$. Nếu α và β đại số trên F với $\deg_F(\alpha)=m$ và $\deg_F(\beta)=n$, ở đây $\gcd(m,n)=1$, chứng tỏ $[F(\alpha,\beta):F]=mn$.
19. Cho F là một trường con của trường E. Chứng tỏ E là một mở rộng hữu hạn của F nếu và chỉ nếu có $\alpha_1,\ldots,\alpha_n\in E$ là những phần tử đại số trên F và $E=F(\alpha_1,\ldots,\alpha_n)$.
20. Cho F là một trường con của trường E, $\alpha\in E$ và $f\in F[x]$ một đa thức khác không. Chứng tỏ rằng nếu $f(\alpha)$ là đại số trên F thì α đại số trên F.
21. Cho F là một trường con của trường E và $\alpha\in E$. Chứng minh rằng nếu $[F(\alpha):F]$ là một số lẻ thì $F(\alpha^2)=F(\alpha)$.

22. Cho p và q là hai số nguyên tố khác nhau.
    (a) Chứng tỏ $\mathbb{Q}\left(\sqrt{p}+\sqrt{q}\right)=\mathbb{Q}\left(\sqrt{p},\sqrt{q}\right)$.
    (b) Tìm đa thức cực tiểu của $\sqrt{p}+\sqrt{q}$ trên $\mathbb{Q}$.
23. Cho trường F và p là đa thức bất khả quy bậc m trong $F[x]$. Chứng minh rằng nếu E là một trường mở rộng hữu hạn bậc n của F và $\gcd(m,n)=1$ thì p cũng bất khả quy trong $E[x]$.
24. Cho F là một trường con của trường E và $\alpha,\beta\in E$. chứng tỏ rằng nếu $\alpha+\beta$ và $\alpha\beta$ đều đại số trên F thì α và β đều đại số trên F.
25. Chứng tỏ trường $\overline{\mathbb{Q}}$ các số đại số là đóng đại số, tức là mọi đa thức khác hằng hệ số trong $\overline{\mathbb{Q}}$ đều có nghiệm trong $\overline{\mathbb{Q}}$.
26. Chứng tỏ mọi trường mở rộng hữu hạn của trường số thực $\mathbb{R}$ là chính nó hoặc đẳng cấu với trường các số phức $\mathbb{C}$.

6.3 Trường phân rã

Bây giờ cho trước đa thức $f\in F[x]$, ở đây F là một trường. Giả sử f không phải đa thức hằng và không có nghiệm trong F. Câu hỏi đặt ra là có tồn tại hay không một trường mở rộng của F để f có nghiệm? Trong $F[x]$ đa thức f luôn phân tích được thành tích của các đa thức bất khả quy, do đó f có nghiệm khi và chỉ khi một nhân tử nào đó của f có nghiệm. Câu trả lời là như sau.

Định lý 6.30. *Cho p là một đa thức bất khả quy trong $F[x]$. Khi đó luôn tồn tại một trường mở rộng E của F sao cho E chứa ít nhất một nghiệm của p.*

Chứng minh. Vì p là đa thức bất khả quy trong $F[x]$ nên iđêan được sinh ra bởi p là tối đại và do đó $E=F[x]/(p)$ là một trường. Ta có ánh xạ $a\in F\longrightarrow\overline{a}=a+(p)\in E$ là một đơn cấu, và nếu đồng nhất a với $\overline{a}$ thì F là một trường con của E. Giả sử $p=a_nx^n+\cdots+a_1x+a_0\in F[x]$. Đặt $\alpha=\overline{x}=x+(p)\in E$ thì

$$\begin{aligned}p(\alpha)&=a_n\overline{x}^n+\cdots+a_1\overline{x}+a_0\\&=\overline{a_nx^n+\cdots+a_1x+a_0}\\&=\overline{p}=\overline{0}.\end{aligned}$$

Vậy p có nghiệm trong E.

□

Như vậy với mỗi đa thức $f\in F[x]$ không phải đa thức hằng thì f luôn phân tích được trong $E[x]$ thành tích của hai đa thức trong đó có một đa thức bậc nhất, ở đây E là một trường mở rộng nào đó của F. Bằng cách mở rộng liên tiếp trường

E thì f được phân tích thành tích của những đa thức bậc nhất. Từ đây ta có định nghĩa

Định nghĩa 6.31. Giả sử F là một trường, $f \in F[x]$ không phải đa thức hằng và E một trường mở rộng của F. Ta nói f *phân rã* trên E nếu trong $E[x]$ đa thức f được nhân tử hóa

$$f = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

thành tích các đa thức bậc nhất. Đặt K là giao của tất cả các trường con của E chứa F mà f phân rã, đây là trường con nhỏ nhất của E chứa F mà f phân rã. Ta nói trường K như thế là *trường phân rã* trong E của f trên F.

Chú ý rằng vì a là hệ số dẫn đầu của f nên $a \in F$.

Ví dụ 6.32. (a) $f = x^2 - 2 \in \mathbb{Q}[x]$, $f = \left(x-\sqrt{2}\right)\left(x+\sqrt{2}\right)$ là phân rã trên $\mathbb{Q}\left(\sqrt{2}\right)$.
(b) $f = x^2+1 \in \mathbb{Q}[x]$, $f = (x-i)(x+i)$ là phân rã trên $\mathbb{Q}(i)$.

Mệnh đề sau cho thấy trường phân rã của f chính là mở rộng của F bởi các nghiệm của nó.

Mệnh đề 6.33. *Cho F là một trường, $f \in F[x]$ không phải đa thức hằng và E một trường mở rộng của F mà trên trường đó f phân rã thành*

$$f = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n).$$

Khi đó $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ là trường phân rã trong E của f trên F.

Chứng minh. Đặt $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$, hiển nhiên f phân rã trên K. Nếu L là một trường con tùy ý của E chứa F mà trên đó f phân rã thành $f = a(x-\beta_1)(x-\beta_2)\cdots(x-\beta_n)$, bởi tính duy nhất của nhân tử hóa đa thức trong $E[x]$ thì $x-\alpha_i$ và $x-\beta_j$ chỉ khác nhau thứ tự. Vì thế $\alpha_i \in L$ với mọi i, hơn nữa L chứa F và do đó $K \subset L$. Ta có điều phải chứng minh.

□

Ví dụ 6.34. (a) Xét đa thức $f = x^4 - 7x^2 + 1 \in \mathbb{Q}[x]$. f có bốn nghiệm trong $\mathbb{C}$ là $\frac{\pm 3 \pm \sqrt{5}}{2}$, do đó trường phân rã của f trong $\mathbb{C}$ trên $\mathbb{Q}$ là

$$\mathbb{Q}\left(\frac{3+\sqrt{5}}{2}, \frac{-3+\sqrt{5}}{2}, \frac{3-\sqrt{5}}{2}, \frac{-3-\sqrt{5}}{2}\right) = \mathbb{Q}\left(\sqrt{5}\right).$$

(b) Xét đa thức $x^n - 1 \in \mathbb{Q}[x]$, trong đó n là số nguyên dương cho trước. Đa thức này có n nghiệm phức là $\alpha, \alpha^2, \ldots, \alpha^{n-1}$ với $\alpha = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$, do đó trường phân rã trong $\mathbb{C}$ của đa thức này trên $\mathbb{Q}$ là $\mathbb{Q}(\alpha, \alpha^2, \ldots, \alpha^{n-1}) = \mathbb{Q}(\alpha)$.

(c) Cho p là một số nguyên tố. Xác định trường phân rã trong $\mathbb{C}$ của đa thức $x^p - 5$ trên $\mathbb{Q}$ và bậc mở rộng của nó. Các căn bậc p của đơn vị lập thành một nhóm

con cyclic cấp p của nhóm nhân $\mathbb{C}^*$. Vì p là số nguyên tố nên mọi căn bậc p khác 1 của đơn vị đều là phần tử sinh của nhóm cyclic. Gọi α là một căn bậc p tùy ý của 1 và $\alpha \neq 1$, khi đó $\sqrt[p]{5}\alpha^i$ với $0 \leq i \leq p-1$ là p nghiệm khác nhau của đa thức đã cho. Do đó trường phân rã trong $\mathbb{C}$ của đa thức $x^p - 5$ trên $\mathbb{Q}$ là $\mathbb{Q}\left(\alpha, \sqrt[p]{5}\right)$. Ta xác định $\left[\mathbb{Q}\left(\alpha, \sqrt[p]{5}\right) : \mathbb{Q}\right]$. Vì

$$x^p - 1 = (x-1)\left(x^{p-1} + \cdots + x + 1\right),$$

do đó α là nghiệm của đa thức $x^{p-1} + \cdots + x + 1$, theo (c) của Ví dụ 4.43 thì đa thức này bất khả quy trên $\mathbb{Q}$ nên $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p - 1$. Ta cũng có $\deg_{\mathbb{Q}}\left(\sqrt[p]{5}\right) = p$ vì $\sqrt[p]{5}$ là nghiệm của đa thức $x^p - 5$ bất khả quy trên $\mathbb{Q}$. Nếu $\deg_{\mathbb{Q}(\alpha)}\left(\sqrt[p]{5}\right) = m < p$ thì

$$\left[\mathbb{Q}\left(\alpha, \sqrt[p]{5}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\alpha, \sqrt[p]{5}\right) : \mathbb{Q}(\alpha)\right][\mathbb{Q}(\alpha) : \mathbb{Q}] = m(p-1),$$

bởi Hệ quả 6.24 $\deg_{\mathbb{Q}}\left(\sqrt[p]{5}\right) = p$ là một ước số của $\left[\mathbb{Q}\left(\alpha, \sqrt[p]{5}\right) : \mathbb{Q}\right] = m(p-1)$, đây là một mâu thuẩn vì một số nguyên tố không thể là ước số của tích các số tự nhiên khác không nhỏ hơn nó. Vậy $\deg_{\mathbb{Q}(\alpha)}\left(\sqrt[p]{5}\right) = p$ và $\left[\mathbb{Q}\left(\alpha, \sqrt[p]{5}\right) : \mathbb{Q}\right] = p(p-1)$.

Định lý sau đây chứng tỏ trường phân rã như thế luôn tồn tại.

Định lý 6.35. *Cho F là một trường và $f \in F[x]$ không phải đa thức hằng. Khi đó luôn tồn tại một trường phân rã của f trên F.*

Chứng minh. Trước hết ta chứng tỏ luôn tồn tại một trường mở rộng E của F mà trên đó f phân rã. Ta chứng minh bằng quy nạp theo bậc n của f. Khi $n = 1$ thì f là đa thức bậc nhất, ta lấy $E = F$. Giả sử định lý đúng đối với các đa thức bậc $n-1$ trên các trường tùy ý. Xét f là đa thức bậc n, theo Định lý 6.30 tồn tại trường mở rộng L của F sao cho một nhân tử bất khả quy của f có nghiệm và do đó f có một nghiệm β, và trong $L[x]$ f có phân tích $f = (x-\beta)g$ với g có bậc $n-1$. Bởi giả thiết quy nạp có một trường mở rộng E của L sao cho trên E g phân rã thành

$$g = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{n-1}),$$

và f phân rã thành $f = a(x-\beta)(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{n-1})$. Khi đó đặt K là giao của tất cả các trường con của E chứa F mà f phân rã, K chính là trường phân rã của f trên F và định lý được chứng minh.

□

Tiếp theo ta sẽ chứng tỏ trường phân rã của một đa thức như thế là duy nhất sai khác một đẳng cấu.

Bây giờ xét $\tau : F \longrightarrow F'$ là một đẳng cấu giữa các trường. Ánh xạ cảm sinh $\tau^* : F[x] \longrightarrow F'[x]$ được xác định với bất kỳ $f = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$ thì

$$\tau^*(f) = \tau(a_n)\,x^n + \cdots + \tau(a_1)\,x + \tau(a_0) \in F'[x]$$

là một đẳng cấu giữa các vành đa thức.

Bổ đề 6.36. *Cho $\tau : F \to F'$ là một đẳng cấu và $p \in F[x]$ là một đa thức bất khả quy. Nếu α và β lần lượt là nghiệm của p và $\tau^*(p)$ thì τ được mở rộng thành một đẳng cấu $\varphi : F(\alpha) \longrightarrow F'(\beta)$ sao cho $\varphi(\alpha) = \beta$.*

Chứng minh. Để cho tiện ta ký hiệu $f' = \tau^*(f)$ với mọi $f \in F[x]$ và lưu ý f, f' có cùng bậc. Trước hết ta chứng tỏ $p' = \tau^*(p)$ là bất khả quy trên F'. Thật vậy, vì τ^* là một đẳng cấu nên nếu $p' = g'h'$ là một phân tích trong $F'[x]$ thành tích của hai đa thức có bậc nhỏ hơn bậc của p' thì $p = gh$ là một phân tích trong $F[x]$ thành tích của hai đa thức có bậc nhỏ hơn bậc của p, điều này không thể được vì p là bất khả quy và do đó p' là bất khả quy. Khi đó ta có $F[x]/(p)$ và $F'[x]/(p')$ là hai trường. Định nghĩa ánh xạ $\psi : F[x]/(p) \longrightarrow F'[x]/(p')$ được xác định bởi $\psi(f + (p)) = f' + (p')$ với mọi $f + (p) \in F[x]/(p)$. Ta chứng tỏ ψ được định nghĩa đúng đắn. Thật vậy, nếu $f + (p) = g + (p)$ thì có $h \in (p)$ sao cho $f = g + h$. Ta có

$$\begin{aligned}\psi(f + (p)) &= \psi((g + h) + (p)) \\ &= (g + h)' + (p') \\ &= g' + h' + (p').\end{aligned}$$

Vì $h \in (p)$ suy ra $h' = \tau^*(h) \in (p')$, và do đó

$$\psi(f + (p)) = g' + h' + (p') = g' + (p') = \psi(g + (p)).$$

Lúc này dễ thấy rằng ψ là một đẳng cấu. Bởi Mệnh đề 6.15, ta có $F(\alpha) \cong F[x]/(p)$ và $F'[x]/(p') \cong F'(\beta)$. Khi đó đẳng cấu $\varphi : F(\alpha) \longrightarrow F'(\beta)$ là hợp thành của ba đẳng cấu từ $F(\alpha)$ đến $F[x]/(p)$, đẳng cấu ψ và đẳng cấu từ $F'[x]/(p')$ đến $F(\beta)$. Cụ thể với phần tử tùy ý $f(\alpha) \in F(\alpha)$, qua đẳng cấu thứ nhất thành $f + (p)$, qua đẳng cấu thứ hai thành $f' + (p')$ và qua đẳng cấu thứ ba thành $f'(\beta) \in F(\beta)$. Đẳng cấu này thỏa mãn các yêu cầu của bổ đề.

□

Mệnh đề 6.37. *Cho p là một đa thức bất khả quy trong $F[x]$. Nếu α và β là hai nghiệm của p thì $F(\alpha)$ đẳng cấu với $F(\beta)$.*

Chứng minh. Trong Bổ đề 6.36 lấy τ là ánh xạ đồng nhất trên F, khi đó mệnh đề được chứng minh.

□

Như vậy cấu trúc của trường $F(\alpha)$ chỉ phụ thuộc vào đa thức bất khả quy p và không phụ thuộc vào nghiệm của p trong trường mở rộng.

Định lý 6.38. *Cho $\tau : F \longrightarrow F'$ là một đẳng cấu, $f \in F[x]$ không phải đa thức hằng, K và K' lần lượt là hai trường phân rã của f trên F và của $\tau^*(f)$ trên F'. Khi đó tồn tại một đẳng cấu $\psi : K \longrightarrow K'$ sao cho ψ bằng τ trên F.*

Chứng minh. Ta chứng minh bằng quy nạp theo bậc n của f. Khi $n = 1$ thì f và $\tau^*(f)$ là hai đa thức bậc nhất, do đó $K = F$ và $K' = F'$. Khi đó $\psi = \tau$ là đẳng cấu giữa K và K'. Giả sử định lý đúng đối với các đa thức bậc $n-1$ trên các trường tùy ý. Xét f là đa thức bậc n và p là một nhân tử bất khả quy của f. Nếu $\alpha \in K$ là một nghiệm của p và $\beta \in K'$ là một nghiệm của $\tau^*(p)$, bởi Bổ đề 6.36 thì τ được mở rộng thành một đẳng cấu $\varphi : F(\alpha) \longrightarrow F'(\beta)$ sao cho $\varphi(\alpha) = \beta$. Đẳng cấu trường này cảm sinh đẳng cấu vành $\varphi^* : F(\alpha)[x] \longrightarrow F'(\beta)[x]$. Trong $F(\alpha)[x]$ f có phân tích $f = (x-\alpha)g$ với đa thức g có bậc $n-1$ nên $\varphi^*(f)$ cũng có phân tích trong $F'(\beta)[x]$ là $\varphi^*(f) = (x-\beta)\varphi^*(g)$. Chú ý rằng K là trường phân rã của g trên $F(\alpha)$ và K' là trường phân rã của $\varphi^*(g)$ trên $F'(\beta)$. Theo giả thiết quy nạp φ được mở rộng thành một đẳng cấu $\psi : K \longrightarrow K'$ và ψ bằng τ trên F.

□

Hệ quả 6.39. *Cho $f \in F[x]$ không phải đa thức hằng, K và K' là hai trường phân rã của f trên F. Khi đó K và K' là đẳng cấu.*

Chứng minh. Trong Định lý 6.38 lấy τ là ánh xạ đồng nhất và hệ quả được suy ra.

□

Bài tập

1. Tìm một trường không chứa trong trường các số thực đẳng cấu với trường được cho trong các trường hợp sau.
   (a) $\mathbb{Q}\left(\sqrt[3]{2}\right)$ (b) $\mathbb{Q}\left(\sqrt[4]{3}\right)$
2. Xác định các tự đẳng cấu của trường được cho trong các trường hợp sau.
   (a) $\mathbb{Q}\left(\sqrt{5}\right)$ (b) $\mathbb{Q}\left(\sqrt[3]{2}\right)$ (c) $\mathbb{Q}(i)$
3. Cho α là một nghiệm của đa thức $x^2 + x + \overline{2} \in \mathbb{Z}_3[x]$ trong một trường mở rộng của $\mathbb{Z}_3$. Xác định $[\mathbb{Z}_3(\alpha) : \mathbb{Z}_3]$ và tìm tất cả tự đẳng cấu của $\mathbb{Z}_3(\alpha)$.
4. Tìm trường phân rã K trong $\mathbb{C}$ của đa thức f trên $\mathbb{Q}$ và xác định $[K : \mathbb{Q}]$ trong các trường hợp sau.
   (a) $f = x^4 - 1$ (b) $f = x^3 + 1$ (c) $f = x^4 - 9$
   (d) $f = x^4 + 1$ (e) $f = x^3 - 7$ (f) $f = x^4 - 2x^2 + 1$
   (g) $f = x^3 + x + 1$ (h) $f = x^4 - 2x^3 - x + 2$
5. Cho α là một nghiệm của $f = x^3 + x^2 + \overline{1} \in \mathbb{Z}_2[x]$. Chứng tỏ f phân rã trên $\mathbb{Z}_2(\alpha)$.
6. Xác định trường phân rã trong $\mathbb{C}$ của $f = x^8 - 3$ trên $\mathbb{Q}$.

7. Cho F là một trường. Chứng minh rằng trường phân rã K của đa thức $f \in F[x]$ có bậc n dương trên F có bậc mở rộng không vượt quá $n!$.

6.4 Trường hữu hạn

Định nghĩa 6.40. *Trường hữu hạn* là một trường có số phần tử hữu hạn.

Ví dụ 6.41. $\mathbb{Z}_p$ với p nguyên tố là một trường hữu hạn gồm p phần tử.

Mệnh đề 6.42. *Mỗi trường hữu hạn đều có số phần tử là lũy thừa của một số nguyên tố nào đó.*

Chứng minh. Giả sử F là một trường hữu hạn. Bởi Định lý 6.5, F có đặc số p và là một trường mở rộng hữu hạn của $P \cong Z_p$. Khi đó F là một không gian véc-tơ trên P, và $F \cong P^n$ như không gian véc-tơ với $n = \dim_P F$. Vậy số phần tử của F bằng p^n.

□

Bây giờ ta chứng tỏ mọi trường hữu hạn đều là mở rộng đơn của trường con nguyên tố của nó.

Mệnh đề 6.43. *Cho F là một trường hữu hạn có đặc số p. Khi đó F là mở rộng đơn hữu hạn của trường con nguyên tố $P \cong \mathbb{Z}_p$, tức là có $\alpha \in F$ sao cho $F = P(\alpha)$.*

Chứng minh. F có đặc số p, theo Định lý 6.5 F là trường mở rộng của trường con nguyên tố $P \cong \mathbb{Z}_p$. Từ Định lý 4.16 ta có $F^* = F \setminus \{0\} = \langle \alpha \rangle$ là một nhóm cyclic được sinh ra bởi phần tử α nào đó trong F, khi đó mọi phần tử khác không của F là một lũy thừa nào đó của α và do đó thuộc $P(\alpha)$. Vậy $F = P(\alpha)$ và ta có điều phải chứng minh.

□

Ví dụ 6.44. Trong Ví dụ 4.27 đa thức $p = x^2 + x + \overline{1}$ là bất khả quy trên $\mathbb{Z}_2$. Gọi α là một nghiệm của p trong một trường mở rộng của $\mathbb{Z}_2$, khi đó $\mathbb{Z}_2(\alpha)$ là mở rộng bậc hai của $\mathbb{Z}_2$ và là trường gồm bốn phần tử

$$\mathbb{Z}_2(\alpha) = \{a + b\alpha \mid a, b \in \mathbb{Z}_2\}.$$

Phép cộng và phép nhân trên $\mathbb{Z}_2(\alpha)$ được xác định bởi các bảng bên dưới với lưu ý $\alpha^2 + \alpha + \overline{1} = \overline{0}$.

$+$	$\overline{0}$	$\overline{1}$	α	$\overline{1}+\alpha$
$\overline{0}$	$\overline{0}$	$\overline{1}$	α	$\overline{1}+\alpha$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{1}+\alpha$	α
α	α	$\overline{1}+\alpha$	$\overline{0}$	$\overline{1}$
$\overline{1}+\alpha$	$\overline{1}+\alpha$	α	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$	α	$\overline{1}+\alpha$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	α	$\overline{1}+\alpha$
α	$\overline{0}$	α	$\overline{1}+\alpha$	$\overline{1}$
$\overline{1}+\alpha$	$\overline{0}$	$\overline{1}+\alpha$	$\overline{1}$	α

Mệnh đề 6.45. *Cho F là một trường hữu hạn có đặc số p. Khi đó đồng cấu Frobenius $\varphi : F \longrightarrow F$ là một tự đẳng cấu.*

Chứng minh. Bởi Mệnh đề 6.7, φ là một đơn cấu. Vì một đơn ánh từ một tập hữu hạn đến chính nó luôn là một song ánh, do đó φ là một đẳng cấu.

□

Bây giờ ta sẽ chứng tỏ điều ngược lại, tức là cho trước số nguyên tố p và số nguyên dương n, khi đó luôn tồn tại một trường hữu hạn có số phần tử bằng p^n. Để làm điều này ta cần một số khái niệm sau.

Định nghĩa 6.46. Cho đa thức $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$. Ta nói đa thức

$$f' = na_n x^{n-1} + (n-1)\, a_{n-1}x^{n-2} + \cdots + a_1 \in F[x]$$

là *đạo hàm* của f. Khi f là đa thức hằng thì ta quy ước đạo hàm của f là đa thức không.

Ta có các tính chất sau của đạo hàm đa thức mà phép chứng minh của nó là hiển nhiên.

Mệnh đề 6.47. *Cho F là một trường và $c \in F$, $f, g \in F[x]$. Khi đó*
(a) $(cf)' = cf'$.
(b) $(f+g)' = f' + g'$.
(c) $(fg)' = f'g + fg'$.
(d) $[(x-c)^n]' = n\,(x-c)^{n-1}$ *với mọi số nguyên n dương.*

Mệnh đề 6.48. *Cho $f \in F[x]$ và α là một nghiệm của f trong một trường mở rộng của F. Khi đó α là nghiệm bội của f nếu và chỉ nếu α là một nghiệm của f'.*

Chứng minh. Nếu α là phần tử trong một trường mở rộng E của F và là một nghiệm bội của f thì trong $E[x]$ f có phân tích

$$f = (x-\alpha)^m\, g$$

với $m \geq 2$. Khi đó $f' = (x-\alpha)^{m-1}\, g + (x-\alpha)^m\, g'$ và do đó $f'(\alpha) = 0$.

Đảo lại, nếu α là một nghiệm đơn của f thì trong $E[x]$ f có phân tích

$$f = (x-\alpha)\, g,$$

trong đó $g(\alpha) \neq 0$. Khi đó $f' = g + (x-\alpha)\, g'$ và do đó $f'(\alpha) = g(\alpha) \neq 0$.

□

Định lý 6.49. *Cho trước số nguyên tố p và số nguyên dương n. Khi đó luôn tồn tại một trường có số phần tử bằng p^n.*

Chứng minh. Gọi F là trường phân rã của đa thức $f = x^{p^n} - x \in \mathbb{Z}_p[x]$ trên $\mathbb{Z}_p$. Vì đạo hàm $f' = p^n x^{p^n-1} - \overline{1} = -\overline{1} \neq \overline{0}$ nên theo Mệnh đề 6.48 f không có nghiệm bội. Như vậy tập hợp F_f gồm tất cả các nghiệm của f trong F có đúng p^n phần tử. Ta chứng tỏ F_f là một trường con của F . Thật vậy $\overline{0}, \overline{1} \in F_f$. Với mọi $a, b \in F_f$, áp dụng liên tiếp Mệnh đề 6.6 ta có

$$(a-b)^{p^n} = a^{p^n} - b^{p^n} = a - b,$$

suy ra $a - b \in F_f$ và nếu $a \neq 0$ thì

$$\left(a^{-1}b\right)^{p^n} = \left(a^{-1}\right)^{p^n} b^{p^n} = \left(a^{p^n}\right)^{-1} b^{p^n} = a^{-1}b,$$

do đó $a^{-1}b \in F_f$. Vậy F_f là một trường con của F chứa $\mathbb{Z}_p$ và tất cả các nghiệm của f. Bởi định nghĩa của trường phân rã thì $F = F_f$ và F có p^n phần tử.

Hệ quả 6.50. *Với mỗi số nguyên n dương cho trước luôn có một đa thức bất khả quy bậc n trong $\mathbb{Z}_p[x]$.*

Chứng minh. Gọi F là một trường mở rộng của $\mathbb{Z}_p$ với p^n phần tử, theo Mệnh đề 6.43 thì $F = \mathbb{Z}_p(\alpha)$ là mở rộng đơn của $\mathbb{Z}_p$ bởi một phần tử α nào đó trong F. Khi đó $[\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = n$ nên đa thức bất khả quy trên $\mathbb{Z}_p$ nhận α làm nghiệm phải là đa thức bậc n và hệ quả được chứng minh.

□

Mệnh đề 6.51. *Hai trường hữu hạn bất kì có cùng số phần tử thì đẳng cấu.*

Chứng minh. Giả sử F là một trường với p^n phần tử, khi đó F là trường mở rộng của trường $P \cong \mathbb{Z}_p$ gồm p phần tử. Ta chứng tỏ F là trường phân rã của đa thức $x^{p^n} - x \in P[x]$. Ta có nhóm nhân $F^* = F \setminus \{0\}$ có cấp $p^n - 1$. Khi đó với mọi $a \in F^*$ thì $a^{p^n-1} = 1$, nói cách khác mọi phần tử của F đều là những nghiệm khác nhau của đa thức $f = x^{p^n} - x \in P[x]$. Ta có

$$x^{p^n} - x = \prod_{a \in F} (x - a).$$

Vậy F chính là trường phân rã của f trên P vì mọi trường con thật sự của F có số phần tử nhỏ hơn p^n thì không thể chứa đủ nghiệm của f. Bởi Hệ quả 6.39 hai trường phân rã của cùng một đa thức thì đẳng cấu, từ đây ta có điều phải chứng minh.

□

Ví dụ 6.52. Trong Ví dụ 4.27 đa thức $x^3 + x + \overline{1}$ là bất khả quy trên $\mathbb{Z}_2$. Nếu α là một nghiệm của đa thức trên trong một trường mở rộng của $\mathbb{Z}_2$ thì $\mathbb{Z}_2(\alpha)$ là mở rộng bậc ba của $\mathbb{Z}_2$ và là trường gồm tám phần tử

$$\mathbb{Z}_2(\alpha) = \left\{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Z}_2\right\}.$$

Tương tự như trên, nếu lấy đa thức bất khả quy $x^3 + x^2 + \overline{1}$ trên $\mathbb{Z}_2$ và β là một nghiệm của nó trong một trường mở rộng của $\mathbb{Z}_2$ thì $\mathbb{Z}_2(\beta)$ là trường gồm tám phần tử

$$\mathbb{Z}_2(\beta) = \left\{a + b\beta + c\beta^2 \mid a, b, c \in \mathbb{Z}_2\right\}.$$

Theo Mệnh đề 6.51 có một đẳng cấu từ $\mathbb{Z}_2(\alpha)$ đến $\mathbb{Z}_2(\beta)$, ta xác định đẳng cấu này. Xét ánh xạ $\eta : \mathbb{Z}_2(\alpha) \longrightarrow \mathbb{Z}_2(\beta)$ được xác định bởi

$$\eta\left(a + b\alpha + c\alpha^2\right) = a + b\left(\overline{1} + \beta\right) + c\left(\overline{1} + \beta\right)^2$$

với mọi $a+b\alpha+c\alpha^2 \in \mathbb{Z}_2(\alpha)$. Dễ thấy f là một song ánh, ta chứng tỏ f là một đồng cấu. Thậy vậy, cho bất kỳ $u(\alpha), v(\alpha) \in \mathbb{Z}_2(\alpha)$, ở đây $u, v \in \mathbb{Z}_2[x]$. Hiển nhiên

$$f(u(\alpha) + v(\alpha)) = f(u(\alpha)) + f(v(\alpha)).$$

Đặt $p = x^3 + x + \overline{1}$, ta viết

$$uv = qp + r$$

với r đa thức dư trong phép chia uv cho p. Khi đó ta có

$$u(\alpha)v(\alpha) = q(\alpha)p(\alpha) + r(\alpha) = r(\alpha)$$

vì α là một nghiệm của p, và bởi

$$p\left(\overline{1} + \beta\right) = \left(\overline{1} + \beta\right)^3 + \left(\overline{1} + \beta\right) + \overline{1} = \beta^3 + \beta^2 + \overline{1} = \overline{0}$$

nên ta cũng có

$$r\left(\overline{1} + \beta\right) = q\left(\overline{1} + \beta\right)p\left(\overline{1} + \beta\right) + r\left(\overline{1} + \beta\right) = u\left(\overline{1} + \beta\right)v\left(\overline{1} + \beta\right).$$

Do đó

$$\begin{aligned} f(u(\alpha)v(\alpha)) &= f(r(\alpha)) \\ &= r\left(\overline{1} + \beta\right) \\ &= u\left(\overline{1} + \beta\right)v\left(\overline{1} + \beta\right) \\ &= f(u(\alpha))f(v(\alpha)). \end{aligned}$$

Vậy f là một đẳng cấu.

Định lý 6.53. *Cho E là trường hữu hạn gồm p^n phần tử, trong đó p là một số nguyên tố và n nguyên dương.*

(a) *Nếu F là một trường con của E thì F gồm p^r phần tử, trong đó r là một ước số của n.*

(b) Nếu r *là một ước số của n thì có duy nhất một trường con F của E gồm p^r phần tử, được xác định bởi*

$$F = \left\{\alpha \in E \mid \alpha^{p^r} - \alpha = 0\right\}.$$

Chứng minh. (a) Vì E có p^n phần tử suy ra E có đặc số p. Gọi P là trường con nguyên tố của E, ta có dãy các mở rộng $P \subset F \subset E$. Theo Định lý 6.19

$$n = [E : P] = [E : F]\,[F : P].$$

Do đó $r = [F : P]$ là một ước số của n.

(b) Nếu r là một ước số của n thì $p^r - 1$ là một ước số của $p^n - 1$. Nhóm nhân $E^* = E \setminus \{0\}$ là một nhóm cyclic cấp $p^n - 1$, theo Định lý 1.42 có duy nhất nhóm con cyclic F^* cấp $p^r - 1$ gồm các phần tử trong E^*có cấp là ước số của $p^r - 1$, cụ thể

$$F^* = \left\{\alpha \in| \ \alpha^{p^r-1} = 1\right\}.$$

Như trong chứng minh của Định lý 6.49 ta có $F = F^* \cup \{0\} = \left\{\alpha \in E \mid \alpha^{p^r} - \alpha = 0\right\}$ là trường phân rã trong E của đa thức $x^{p^r} - x$ và là trường con duy nhất của E gồm p^r phần tử.

□

Bài tập

1. Trong mỗi trường hợp hãy tìm một đa thức bất khả quy bậc n trên trường F đã cho.
   (a) $n = 3$, $F = \mathbb{Z}_{11}$ (b) $n = 5$, $F = \mathbb{Z}_3$
   (c) $n = 3$, F là trường có bốn phần tử.
2. Giải các hệ phương trình sau trong $\mathbb{Z}_2(\alpha)$ trường mở rộng bậc hai của $\mathbb{Z}_2$.
   (a) $\begin{cases} \alpha x + \left(\alpha + \overline{1}\right) y & = \alpha + \overline{1} \\ x + \alpha y & = \overline{1} \end{cases}$ (b) $\begin{cases} \left(\alpha + \overline{1}\right) x + y & = \alpha \\ x + \left(\alpha + \overline{1}\right) y & = \alpha + \overline{1} \end{cases}$
3. Lập bảng công và nhân của các trường gồm N phần tử trong mỗi trường hợp sau.
   (a) $N = 5$ (b) $N = 9$ (c) $N = 8$
4. (a) Nếu $p(x) \in \mathbb{Z}_2[x]$, hãy chứng tỏ $[p(x)]^2 = p(x^2)$.
   (b) Nếu β là một nghiệm của $p \in \mathbb{Z}_2[x]$, hãy chứng tỏ β^{2^m} cũng là nghiệm với mọi $m \in \mathbb{N}$.

(c) Cho trường $\mathbb{Z}_2(\alpha)$ với $\alpha^4+\alpha+\overline{1}=\overline{0}$. Hãy tìm một đa thức bất khả quy trong $\mathbb{Z}_2[x]$ nhận α^3 làm nghiệm.

5. Tìm cấu trúc trường F (nếu có) gồm N phần tử các phần tử sinh của nhóm nhân $F^* = F \setminus \{0\}$ trong các trường hợp sau.
   (a) $N=7$ (b) $N=9$ (c) $N=15$ (d) $N=16$
6. Xác định cấu trúc của các trường con của trường E gồm N phần tử trong các trường hợp sau.
   (a) $N=8$ (b) $N=16$ (c) $N=3^3$ (d) $N=3^4$
7. Chứng tỏ $x^8+x \in \mathbb{Z}_2[x]$ phân rã trên trường E mở rộng bậc ba của $\mathbb{Z}_2$ nhưng không phân rã trên bất kỳ trường nào nhỏ hơn.
8. Cho F là một trường hữu hạn với đặc số p và $\varphi : F \longrightarrow F$ là tự đẳng cấu Frobenius. Chứng tỏ $K = \{\alpha \in F \mid \varphi^n(\alpha) = \alpha\}$ với n nguyên dương cho trước là một trường con của F.
9. Liệt kê tất cả đa thức bất khả quy bậc 1, 2 và 4 trên $\mathbb{Z}_2$ và chứng tỏ tích của chúng bằng $x^{16}-x$.
10. Cho trước số n nguyên dương. Chứng tỏ $x^{p^n}-x$ là tích của tất cả các đa thức bất khả quy đơn hệ trên trường $\mathbb{Z}_p$ mà bậc của nó chia hết n.
11. Chứng tỏ nếu F có đặc số 0 thì mọi đa thức bất khả quy trên F không có nghiệm bội trong một trường mở rộng của F.

Tài liệu tham khảo

1. B. Baumslag and B.Chandler, *Theory and Problems of Group Theory,* McGraw-Hill, 1968.
2. William J. Gilbert and W. Keith Nicholson, *Modern Algebra with Applications,* John Wiley and Sons, Inc., Hobekon, New Jersey, 2004.
3. Lê Thanh Hà, *Giáo trình Da thức và Nhân tử hóa,* Tài liệu lưu hành nội bộ, Huế, 1995.
4. Lê Thanh Hà, *Giáo trình Các trường số đại số và lý thuyết Galois,* Tài liệu lưu hành nội bộ, Huế, 1996.
5. Nguyễn Hữu Việt Hưng, *Đại số đại cương,* Nhà xuất bản Giáo dục, 1998.
6. Aigli Papantonopoulou, *Algebra Pure and Aplied,* Upper Saddle River, NJ 07458, Prentice Hall, 2002.
7. Hoàng Xuân Sính, *Đại số đại cương,* Nhà xuất bản Giáo dục, 2010.

Chỉ mục

ánh xạ, 6
ánh xạ ngược, 13
ánh xạ ngược bên phải, 13
ánh xạ ngược bên trái, 13
đếm được, 16
đồng cấu (nhóm), 58
đồng cấu tầm thường, 58
đồng cấu trường, 107
đồng cấu vành, 105
đặc số, 161
độ dài của chu trình, 46
độc lập, 83
đại số, 163
đạo hàm, 177
đẳng cấu, 58
đơn ánh, 10
đơn cấu, 58
được sắp, 22
được sắp thẳng, 22
đa thức đối xứng, 141
đa thức đối xứng cơ bản, 142
đa thức cực tiểu, 164
ước của không, 96
ước chung lớn nhất, 151

bất khả quy, 150
Bổ đề Zorn, 24

cấp của nhóm, 31
cấp của phần tử, 40
cùng lực lượng, 16
cơ sở, 83
chặn dưới, 23
chặn trên, 23
chia hết, 149
chu trình, 46
chuyển vị, 46

dấu của hoán vị, 47

giao tùy ý các tập hợp, 4

hàm đa thức, 124
hợp tùy ý các tập hợp, 4
hợp thành của hai ánh xạ, 9
hạng của nhóm Abel hữu hạn sinh, 89
hạng của nhóm Abel tự do, 86
hoán vị, 45
hoán vị chẵn, 48
hoán vị lẻ, 48

iđêan, 100
iđêan được sinh ra bởi U, 100
iđêan chính, 155
iđêan nguyên tố, 102
iđêan tối đại, 102
iđêan trái (phải), 100
infimum, 23

lớp kề phải, 51
lớp kề trái, 50
lớp tương đương, 19
liên kết, 149

mở rộng, 7
mở rộng đại số, 167
mở rộng đơn, 163
mở rộng hữu hạn, 165
miền Euclid, 151
miền iđêan chính, 155
miền nguyên, 97

nửa nhóm, 30
nguyên bản, 133
nguyên tố, 150
nguyên tố cùng nhau, 155
nhóm, 31

nhóm đối xứng, 45
nhóm Abel, 31
nhóm Abel không xoắn, 87
nhóm Abel tự do, 83
nhóm con, 35
nhóm con chuẩn tắc, 54
nhóm con xoắn, 89
nhóm cyclic, 40
nhóm hữu hạn, 31
nhóm thương, 56
nhóm thay phiên, 49

p-nhóm, 80
phép chiếu chính tắc, 58
phép nhân các hoán vị, 45
phép toán hai ngôi, 27
phân hoạch, 21
phần tử, 1
phần tử đối xứng, 29
phần tử đối xứng phải, 29
phần tử đối xứng trái, 29
phần tử lớn nhất, 22
phần tử nhỏ nhất, 22
phần tử tối đại, 22
phần tử tối tiểu, 22
phần tử trung lập, 27
phần tử trung lập phải, 28
phần tử trung lập trái, 28

quan hệ tương đương, 19
quan hệ thứ tự, 22

song ánh, 10
supremum, 23

tích Descartes của tùy ý các tập hợp, 5
tích trực tiếp của hai nhóm, 68
tính giao hoán, 27
tính kết hợp, 27
tập con, 1
tập hợp, 1
tập sinh của một nhóm, 37
tự đẳng cấu, 58
tạo ảnh của một tập hợp , 7
tổng trực tiếp của hai nhóm Abel, 74
thứ tự bộ phận, 22
thứ tự tốt, 24
thứ tự từ điển, 24
thứ tự toàn phần, 22
thu hẹp, 7
toàn ánh, 10
toàn cấu, 58
trường, 97
trường các số đại số, 168
trường các thương, 114
trường con, 98
trường con nguyên tố, 161
trường hữu hạn, 176
trường phân rã, 172

vành, 91
vành đa thức một biến, 118
vành đa thức n biến, 140
vành con, 93
vành tích, 92
vành thương, 102
vị nhóm, 30