ĐẠI HỌC QUỐC GIA TP HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

NGUYỄN VIẾT ĐÔNG - TRẦN NGỌC HỘI

ĐẠI SỐ ĐẠI CƯƠNG

NHÀ XUẤT BẢN ĐẠI HỌC QUỐC GIA TP HỒ CHÍ MINH - 2005

Lời nói đầu

*Giáo trình **Đại số đại cương** được viết theo chương trình qui định của học phần cùng tên, 4 tín chỉ, nhằm phục vụ cho sinh viên ngành Toán-Tin học. Với thời lượng hạn hẹp như thế, giáo trình chỉ bao gồm những kiến thức rất cơ bản về các cấu trúc đại số mà theo chúng tôi là cần thiết cho mọi sinh viên Toán-Tin học dù họ chọn bất cứ hướng nào ở giai đoạn chuyên ngành. Các cấu trúc đại số cơ bản được trình bày trong giáo trình là: Nhóm, Vành, Trường, Vành đa thức, Môđun và Đại số. Những kết quả sâu hơn về lý thuyết nhóm, lý thuyết vành,... sẽ được trình bày trong một giáo trình khác mang tên Đại số hiện đại.*

Đại số đại cương là học phần đại số trừu tượng đầu tiên trong chương trình chuyên ngành của sinh viên Toán-Tin học, là học phần cơ sở giúp sinh viên bước đầu tiếp cận với những ký hiệu và tính toán hình thức. Vì thế, với mục đích phục vụ rộng rãi cho mọi đối tượng sinh viên, bên cạnh tính chặt chẽ và logic vốn rất được chú trọng, chúng tôi còn đưa vào giáo trình nhiều ví dụ minh họa. Với phương cách như thế, chúng tôi tin rằng sinh viên sẽ dễ tiếp thu hơn và độc giả sẽ tìm thấy đôi điều bổ ích khi đọc giáo trình này.

*Cuối mỗi chương là hệ thống bài tập khá đầy đủ và phong phú giúp sinh viên rèn luyện kỹ năng tư duy nhằm tường tận hơn về những vấn đề trong lý thuyết. Một số kết quả trong lý thuyết cũng được đưa vào dưới dạng bài tập. Những bài tập có đánh dấu * là những bài khó, đòi hỏi bạn đọc phải đầu tư nhiều thời gian và công sức hơn so với các bài tập khác.*

Chúng tôi xin chân thành cảm ơn Bộ môn Đại số, Khoa Toán-Tin học, Trường Đại học Khoa học Tự nhiên, Đại học Quốc gia TP HCM và Nhà xuất bản Đại học Quốc gia TP HCM đã tạo điều kiện thuận lợi để giáo trình này sớm đến tay bạn đọc. Đặc biệt xin cảm ơn ThS Trịnh

Thanh Đèo và CN Tống Viết Phi Hùng đã góp sức biên soạn phần bài tập và đã nhiệt tình soạn thảo toàn bộ giáo trình bằng LaTeX. Mặc dù đã có nhiều cố gắng, giáo trình vẫn có thể còn nhiều khiếm khuyết. Chúng tôi rất mong nhận được sự phê bình, góp ý của quí độc giả. Mọi ý kiến xin vui lòng gửi về Bộ môn Đại số, Khoa Toán-Tin học, Trường Đại học Khoa học Tự nhiên, Đại học Quốc gia TP HCM, 227 Nguyễn Văn Cừ, Quận 5, Tp. HCM.

TP Hồ Chí Minh, tháng 6 năm 2005

CÁC TÁC GIẢ

Mục lục

Chương I
NHÓM

§1. Phép toán hai ngôi

1.1. Định nghĩa

Phép toán hai ngôi (gọi tắt là phép toán) trên tập hợp X là một ánh xạ

$$\begin{array}{rccc} f: & X \times X & \longrightarrow & X \\ & (x,y) & \longmapsto & f(x,y). \end{array}$$

Ta dùng ký hiệu xfy thay cho $f(x,y)$. Như vậy, ứng với các phép toán $*, \circ, +, ., ...$ ta có các ký hiệu $x * y$, $x \circ y$, $x + y$, $x.y$, ... Khi ký hiệu phép toán là . ta gọi đây là phép toán nhân và thường viết xy thay cho $x.y$ mà ta gọi là tích của x và y. Còn khi ký hiệu phép toán là $+$ ta gọi đây là phép toán cộng và $x + y$ là tổng của x và y.

1.2. Ví dụ

1) Phép cộng và phép nhân thông thường trên các tập hợp $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ là các phép toán; phép trừ thông thường là phép toán trên các tập hợp $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ nhưng không là phép toán trên $\mathbb{N}$.

2) Phép cộng và phép nhân ma trận là các phép toán trên $M(n, \mathbb{R})$ gồm các ma trận vuông cấp n với hệ số thực.

1.3. Định nghĩa

Cho phép toán $*$ trên tập hợp X. Ta nói phép toán $*$:

(i) *giao hoán,* nếu với mọi $x, y \in X, x * y = y * x$;

(ii) *kết hợp,* nếu với mọi $x, y, z \in X, (x * y) * z = x * (y * z)$;

(iii) có *phần tử trung hòa trái* (tương ứng, *phải*) là e nếu $e \in X$ và với mọi $x \in X$, $e * x = x$ (tương ứng, $x * e = x$). Nếu e vừa là phần tử trung hòa trái vừa là phần tử trung hòa phải thì ta nói e là *phần tử trung hòa* của phép toán $*$.

1.4. Mệnh đề. *Một phép toán có nhiều nhất một phần tử trung hòa.*

Chứng minh. Giả sử e' và e'' là hai phần tử trung hòa của phép toán $*$. Xét phần tử $e' * e''$. Vì e' là phần tử trung hòa trái nên $e' * e'' = e''$. Mặt khác,vì e'' là phần tử trung hòa phải nên $e' * e'' = e'$. Suy ra $e' = e''$. ■

1.5. Nhận xét

Từ chứng minh của Mệnh đề 1.4 ta thấy nếu e' là phần tử trung hòa trái và e'' là phần tử trung hòa phải của phép toán $*$ thì $e' = e''$. Đặc biệt, nếu trong X tồn tại phần tử trung hòa e thì đó là phần tử trung hòa trái duy nhất đồng thời cũng là phần tử trung hòa phải duy nhất.

1.6. Định nghĩa

Cho $*$ là một phép toán trên tập hợp X có phần tử trung hòa e và x là một phần tử tùy ý của X. Ta nói x *khả đối xứng trái* (tương ứng, *phải*) nếu tồn tại $x' \in X$ sao cho $x' * x = e$ (tương ứng, $x * x' = e$). Khi đó x' được gọi là *phần tử đối xứng trái* (tương ứng, *phải*) của x. Trường hợp x vừa khả đối xứng trái, vừa khả đối xứng phải thì ta nói x khả đối xứng và phần tử $x' \in X$ thỏa $x * x' = x' * x = e$ được gọi là *phần tử đối xứng* của x.

1.7. Mệnh đề. *Nếu phép toán $*$ kết hợp thì một phần tử có nhiều nhất một phần tử đối xứng.*

Chứng minh. Giả sử x' và x'' là hai phần tử đối xứng của x. Khi đó $x' * x = e$ và $x * x'' = e$. Do đó

$$x' = x' * e = x' * (x * x'') = (x' * x) * x'' = e * x'' = x''. \qquad \blacksquare$$

1.8. Nhận xét

Từ chứng minh của Mệnh đề 1.7 ta thấy, khi phép toán $*$ kết hợp, nếu x' là phần tử đối xứng trái của x và x'' là phần tử đối xứng phải của x thì $x' = x''$. Đặc biệt, nếu x khả đối xứng và x' là phần tử đối xứng của x thì x' là phần tử đối xứng trái duy nhất và cũng là phần tử đối xứng phải duy nhất của x.

1.9. Thuật ngữ và ký hiệu

1) Trường hợp phép toán cộng: Phần tử trung hòa được gọi là *phần tử không* và được ký hiệu là 0, tính chất khả đối xứng được gọi là *khả đối*, phần tử đối xứng của x được gọi là *phần tử đối* của x và ký hiệu là $-x$.

2) Trường hợp phép toán nhân: Phần tử trung hòa được gọi là *phần tử đơn vị* và được ký hiệu là e hay 1, tính chất khả đối xứng được gọi là *khả nghịch*, phần tử đối xứng của x được gọi là *phần tử nghịch đảo* của x và ký hiệu là x^{-1}.

Từ đây trở về sau, nếu không có gì gây nhầm lẫn, ta dùng phép toán nhân để chỉ một phép toán tùy ý trên tập hợp đang khảo sát.

§2. Nửa nhóm

2.1. Định nghĩa

Cho tập hợp X với phép toán nhân. Ta nói $(X, .)$ (gọi tắt là X) là:

(i) một *nửa nhóm* nếu phép toán nhân kết hợp trên X;

(ii) một *vị nhóm* nếu phép toán nhân kết hợp trên X và có phần tử trung hòa trên X.

Một nửa nhóm được gọi là *giao hoán* hay *Abel* nếu phép toán tương ứng giao hoán.

2.2. Ví dụ

1) Với phép cộng thông thường, các tập hợp $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ trở thành các vị nhóm giao hoán.

2) Với phép cộng thông thường, tập hợp $\mathbb{N}^*$ gồm các số nguyên dương trở thành một nửa nhóm giao hoán nhưng không là vị nhóm.

2.3. Ký hiệu

Trong nửa nhóm $(X, .)$, do phép toán nhân kết hợp nên với mọi x, y, z:

$$(xy)z = x(yz).$$

Giá trị chung của hai vế trong đẳng thức trên được ký hiệu là xyz và gọi là *tích* của các phần tử x, y, z theo thứ tự đó. Bằng quy nạp, ta định nghĩa *tích* của n phần tử $x_1, ..., x_n$ như sau:

$$x_1...x_n = x_1(x_2...x_n).$$

Ta có định lý sau:

2.4. Định lý. *Cho $x_1, ..., x_n$ là n phần tử tùy ý của nửa nhóm $(X, .)$ với $n \geq 3$. Khi đó:*

$$x_1...x_n = (x_1...x_i)(x_{i+1}...x_j)...(x_{k+1}...x_n),$$

trong đó $1 \leq i < j < ... < k < n$.

Chứng minh. Vì X là một nửa nhóm nên định lý đúng với $n = 3$. Xét $n > 3$, giả sử định lý đúng cho mọi tích có m phần tử với $3 \leq m < n$. Khi đó sử dụng giả thiết quy nạp và tính kết hợp ta có

$$(x_1...x_i)(x_{i+1}...x_j)...(x_{k+1}...x_n) =$$

$$= (x_1...x_i)[(x_{i+1}...x_j)...(x_{k+1}...x_n)]$$

$$= [x_1(x_2...x_i)][(x_{i+1}...x_n)]$$

$$= x_1(x_2...x_n) = x_1x_2...x_n. \qquad \blacksquare$$

2.5. Ký hiệu

Trong nửa nhóm $(X, .)$, tích của n phần tử, mỗi phần tử đều bằng x, được gọi là *lũy thừa* bậc n của x và được ký hiệu là x^n. Do Định lý 2.4 ta có

$$x^m x^n = x^{m+n} \text{ và } (x^m)^n = x^{mn}, \forall m, n \in \mathbb{N}^*.$$

Trường hợp nửa nhóm cộng $(X, +)$, tổng của n phần tử được gọi là *bội* n của x và ký hiệu là nx. Khi đó các tính chất trên trở thành

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

2.6. Định lý. *Trong nửa nhóm giao hoán, tích của n phần tử tùy ý không phụ thuộc vào thứ tự của các phần tử.*

Chứng minh. Vì phép toán giao hoán nên định lý đúng với $n = 2$. Xét $n > 2$. Giả sử định lý đúng với mọi tích của m phần tử với $m < n$. Ta chứng minh $x_1...x_n = x_{\sigma(1)}...x_{\sigma(n)}$ với mọi phép hoán vị σ của tập hợp $\{1, 2, ..., n\}$. Thật vậy, đặt $k = \sigma(n)$, bằng cách sử dụng giả thiết quy nạp và các tính chất giao hoán, kết hợp của phép nhân ta có:

$$\begin{aligned} x_1...x_n &= (x_1...x_{k-1})[x_k(x_{k+1}...x_n)] \\ &= (x_1...x_{k-1})[(x_{k+1}...x_n)x_k] \\ &= (x_1...x_{k-1}x_{k+1}...x_n)x_k \\ &= (x_{\sigma(1)}...x_{\sigma(n-1)})x_{\sigma(n)} \\ &= x_{\sigma(1)}...x_{\sigma(n)}. \end{aligned}$$

■

§3. Khái niệm về nhóm

3.1. Định nghĩa

Nhóm là một vị nhóm mà mọi phần tử đều khả đối xứng. Nói cách khác, tập hợp G khác rỗng với phép toán nhân được gọi là một nhóm nếu các tính chất sau được thỏa:

(G_1) Với mọi $x, y, z \in G, (xy)z = x(yz)$;

(G_2) Tồn tại $e \in G$ sao cho với mọi $x \in G$, $ex = xe = x$;

(G_3) Với mọi $x \in G$, tồn tại $x^{-1} \in G$ sao cho $xx^{-1} = x^{-1}x = e$.

Nếu phép toán trên G là phép cộng thì các tính chất trên trở thành:

(G_1) Với mọi $x, y, z \in G, (x + y) + z = x + (y + z)$;

(G_2) Tồn tại $0 \in G$ sao cho với mọi $x \in G$, $0 + x = x + 0 = x$;

(G_3) Với mọi $x \in G$, tồn tại $-x \in G$ sao cho $x+(-x) = (-x)+x = 0$.

Trường hợp phép toán trên nhóm G giao hoán thì ta nói G là *nhóm giao hoán* hay là *nhóm Abel*.

Nhóm G được gọi là *nhóm hữu hạn* khi tập hợp G hữu hạn. Khi đó số phần tử của G được gọi là *cấp* của nhóm G. Nếu nhóm G không hữu hạn thì ta nói G là *nhóm vô hạn*.

3.2. Ví dụ

1) Tập hợp các số nguyên $\mathbb{Z}$ cùng với phép cộng thông thường là một nhóm giao hoán mà ta gọi là nhóm cộng các số nguyên. Tương tự ta có nhóm cộng các số hữu tỷ $\mathbb{Q}$, nhóm cộng các số thực $\mathbb{R}$ và nhóm cộng các số phức $\mathbb{C}$.

2) Tập hợp các số hữu tỷ khác không $\mathbb{Q}^*$ cùng với phép nhân thông thường là một nhóm giao hoán mà ta gọi là nhóm nhân các số hữu tỷ khác không. Tương tự ta có nhóm nhân các số thực khác không $\mathbb{R}^*$ và nhóm nhân các số phức khác không $\mathbb{C}^*$.

3) Với $X = \{1, 2, ..., n\}$, đặt

$$S_n = \{\sigma | \sigma : X \longrightarrow X \text{ là một song ánh}\}.$$

Khi đó S_n với phép hợp nối ánh xạ là một nhóm (có phần tử đơn vị là ánh xạ đồng nhất Id_X và phần tử nghịch đảo của $\sigma \in S_n$ chính là ánh xạ ngược σ^{-1}). Ta gọi $(S_n, \circ)$ là nhóm hoán vị hay nhóm đối xứng bậc n. Đây là một nhóm hữu hạn có cấp $n!$ (xem §4).

4) Tập hợp $GL(n, \mathbb{R})$ gồm các ma trận vuông cấp n, khả nghịch với hệ số thực cùng với phép nhân ma trận là một nhóm không giao hoán với mọi $n > 1$ (với phần tử đơn vị là ma trận đơn vị I_n và phần tử nghịch đảo của $A \in GL(n, \mathbb{R})$ chính là ma trận nghịch đảo A^{-1}). Ta gọi $GL(n, \mathbb{R})$ là *nhóm tuyến tính đầy đủ* bậc n (hay *nhóm tuyến tính tổng quát* bậc n) trên $\mathbb{R}$.

3.3. Định lý. *Cho nhóm $(G, .)$ và $x, y, x_1, ..., x_n \in G$. Khi đó:*

(i) Phần tử đơn vị e là duy nhất.

(ii) Phần tử nghịch đảo x^{-1} của x là duy nhất và $(x^{-1})^{-1} = x$.

(iii) $xy = e$ khi và chỉ khi $yx = e$. Hơn nữa khi đó $y = x^{-1}$.

(iv) $(x_1...x_n)^{-1} = {x_n}^{-1}...{x_1}^{-1}$. Đặc biệt $(x^n)^{-1} = (x^{-1})^n$ với mọi n nguyên dương.

(v) Phép toán nhân có tính giản ước, nghĩa là với mọi $x, y, z \in G$, từ đẳng thức $xy = xz$ hay $yx = zx$ đều dẫn đến $y = z$.

Chứng minh. (i) Suy từ Mệnh đề 1.4.

(ii) Suy từ Mệnh đề 1.7.

(iii) Suy từ Nhận xét 1.8.

(iv) Chỉ cần nhận xét rằng

$$\begin{aligned}(x_1...x_n)({x_n}^{-1}...{x_1}^{-1}) &= (x_1...x_{n-1})(x_n{x_n}^{-1})({x_{n-1}}^{-1}...{x_1}^{-1}) \\ &= (x_1...x_{n-1})({x_{n-1}}^{-1}...{x_1}^{-1}) \\ &= ..... \\ &= e\end{aligned}$$

sau đó sử dụng (iii).

(v) Từ đẳng thức $xy = xz$ ta suy ra $x^{-1}(xy) = x^{-1}(xz)$ hay $(x^{-1}x)y = (x^{-1}x)z$, nghĩa là $y = z$. Tương tự, từ đẳng thức $yx = zx$ cũng dẫn đến $y = z$. ■

3.4. Ký hiệu

Trong nhóm nhân $(G, .)$ ta dùng ký hiệu x^{-n} để chỉ phần tử $(x^{-1})^n$ với mọi n nguyên dương và đặt $x^0 = e$. Như vậy ta đã định nghĩa lũy thừa bậc n của một phần tử bất kỳ trong một nhóm nhân với n nguyên. Chú ý rằng, do tính chất (iv) trong Định lý 3.3, các công thức $x^m.x^n = x^{m+n}$ và $(x^m)^n = x^{mn}$ (hay $mx + nx = (m + n)x$ và $m(nx) = (mn)x$ đối với nhóm cộng) vẫn còn đúng với mọi m, n nguyên.

3.5. Định lý. *Cho $(G, .)$ là một nửa nhóm khác rỗng. Các mệnh đề sau tương đương:*

(i) $(G, .)$ là một nhóm;

(ii) Với mọi $a, b \in G$, các phương trình $ax = b$ và $ya = b$ đều có nghiệm trong G;

(iii) Trong G có phần tử đơn vị trái e và với mọi $x \in G$, tồn tại $x' \in G$ sao cho $x'x = e$;

(iv) Trong G có phần tử đơn vị phải e' và với mọi $x \in G$, tồn tại $x'' \in G$ sao cho $xx'' = e'$.

Chứng minh. (i)⇒(ii) Ta có $x = a^{-1}b$ và $y = ba^{-1}$ lần lượt là các nghiệm của phương trình $ax = b$ và $ya = b$.

(ii)⇒(iii) Do $G \neq \emptyset$ nên tồn tại $a_0 \in G$. Gọi e là nghiệm của phương trình $ya_0 = a_0$. Khi đó e là phần tử đơn vị trái. Thật vậy, với b là một phần tử tùy ý của G, gọi c là nghiệm của phương trình $a_0x = b$, khi đó $a_0c = b$ nên

$$eb = e(a_0c) = (ea_0)c = a_0c = b.$$

Vậy e là phần tử đơn vị trái. Tính chất sau cùng trong (iii) được suy từ giả thiết mọi phương trình dạng $ya = e$ đều có nghiệm trong G.

(iii)⇒(i) Giả sử trong G có phần tử đơn vị trái e và với mọi $x \in G$,

tồn tại $x' \in G$ sao cho $x'x = e$. Ta chứng minh e là phần tử đơn vị và x' là phần tử nghịch đảo của x. Theo giả thiết, với x' như trên tồn tại $x'' \in G$ sao cho $x''x' = e$. Do đó

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

Suy ra

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

Các kết quả trên chứng tỏ e là phần tử đơn vị và $x' = x^{-1}$. Do đó $(G, .)$ là một nhóm.

Tương tự ta cũng có (i)⇒(ii); (ii)⇒(iv) và (iv)⇒(i). Do đó định lý được chứng minh. ■

§4. Nhóm hoán vị

4.1. Định nghĩa

Cho tập hợp $X \neq \emptyset$ gồm n phần tử (ta có thể đồng nhất X với $\{1, 2, \cdots, n\}$). Khi đó tập hợp S_n gồm tất cả các song ánh từ X vào X là một nhóm với phép hợp nối ánh xạ. Ta gọi S_n là *nhóm hoán vị* bậc n.

Nhóm hoán vị S_n là nhóm hữu hạn có cấp $n!$, có phần tử trung hòa là ánh xạ đồng nhất Id_X và phần tử nghịch đảo của $\sigma \in S_n$ là ánh xạ ngược σ^{-1}. Nhóm này không giao hoán nếu $n > 2$.

4.2. Một số thuật ngữ và ký hiệu

1) Mỗi phần tử $\sigma \in S_n$ được gọi là một *phép hoán vị* hay một *phép thế* bậc n và có thể được biểu diễn bởi một ma trận loại $2 \times n$:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix},$$

trong đó ở dòng thứ nhất, các phần tử của tập X được sắp xếp theo một thứ tự nào đó (thường là $1, 2, \cdots, n$), dòng thứ hai gồm ảnh của các phần tử tương ứng ở dòng thứ nhất qua song ánh σ.

2) Phép hoán vị $\sigma \in S_n$ được gọi là một *r-chu trình* hay một *chu trình có chiều dài* r nếu tồn tại các phần tử phân biệt $i_1, i_2, ..., i_r \in X$ sao cho $\sigma(i_1) = i_2, \cdots, \sigma(i_{r-1}) = i_r, \sigma(i_r) = i_1$ và $\sigma(i) = i, \forall i \in X \setminus \{i_1, i_2, \cdots, i_r\}$. Khi đó ta viết $\sigma = (i_1 i_2 \cdots i_r)$.

Hai chu trình $\sigma = (i_1 i_2 \cdots i_r)$, $\sigma' = (j_1 j_2 \cdots j_s)$ được gọi là *rời nhau* hay *độc lập* nếu $\{i_1,\ i_2, \cdots, i_r\} \cap \{j_1,\ j_2, \cdots, j_s\} = \emptyset$.

3) Mỗi 2-chu trình trong S_n được gọi là một chuyển vị. Như vậy mỗi chuyển vị có dạng $(i\ j)$ với $1 \leq i \neq j \leq n$.

Ví dụ: a) Trong nhóm hoán vị S_6, phép hoán vị σ xác định bởi $\sigma(1) = 2, \sigma(2) = 5, \sigma(3) = 4, \sigma(4) = 1, \sigma(5) = 3, \sigma(6) = 6$ được mô tả như sau:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 4 & 1 & 3 & 6 \end{pmatrix}.$$

b) Trong nhóm hoán vị S_7, chu trình $\sigma = (1\,3\,4\,7)$ có chiều dài 4 và là phép hoán vị:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 7 & 5 & 6 & 1 \end{pmatrix}.$$

c) Trong nhóm hoán vị S_8, chuyển vị $(2\ 5)$ là phép hoán vị:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 5 & 3 & 4 & 2 & 6 & 7 & 8 \end{pmatrix}.$$

d) Trong nhóm hoán vị S_5, cho

$$\sigma = (1\,2\,5\,3) \quad \text{và} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix}.$$

Ta có

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

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

$$\sigma^{-1} = (3\ 5\ 2\ 1);$$

$$\tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix}.$$

4.3. Nhận xét

Hai chu trình σ và τ rời nhau thì chúng giao hoán lẫn nhau, nghĩa là $\sigma\tau = \tau\sigma$.

4.4. Định lý. *Mọi phép hoán vị bậc n khác ánh xạ đồng nhất đều được phân tích thành tích các chu trình rời nhau có chiều dài lớn hơn hay bằng 2. Cách phân tích là duy nhất sai khác một sự đổi chỗ các chu trình.*

Chứng minh. 1) *Sự tồn tại:* Gọi k là số các phần tử i sao cho $\sigma(i) \neq i$. Chọn i_1 sao cho $i_2 = \sigma(i_1) \neq i_1;\ i_3 = \sigma(i_2); \cdots ; i_{j+1} = \sigma(i_j); \cdots$ Gọi r là số nhỏ nhất sao cho $\sigma(i_r) \in \{i_1; \cdots ; i_{r-1}\}$, khi đó $\sigma(i_r) = i_1$ (vì nếu $\sigma(i_r) = i_j \neq i_1$ thì ta có $\sigma(i_r) = i_j = \sigma(i_{j-1})$ nên σ không là song ánh).

Đặt $\sigma_1 = (i_1\, i_2 \cdots i_r)$ và $X_1 = \{i_1,\, i_2, \cdots , i_r\}$. Khi đó, nếu $r = k$ thì $\sigma_1 = \sigma$ nên σ là một chu trình, nếu $r < k$, ta gọi $i_{r+1} \notin X_1$ là một phần tử thỏa $\sigma(i_{r+1}) \neq i_{r+1}$. Thực hiện tương tự quá trình trên cho tập hợp $X_2 = X \setminus X_1$ ta được chu trình σ_2 rời nhau với σ_1. Tiếp tục thực hiện như vậy, cuối cùng ta nhận được các chu trình $\sigma_1, \sigma_2, \cdots , \sigma_p$ rời nhau từng đôi một và $\sigma = \sigma_1\sigma_2 \cdots \sigma_p$.

2) *Sự duy nhất:* Giả sử $\sigma \neq Id_X$ và σ được phân tích dưới hai dạng

$$\sigma = \sigma_1\sigma_2 \cdots \sigma_p = \sigma'_1\sigma'_2 \cdots \sigma'_q.$$

Trong đó $\sigma_1, \sigma_2, \cdots , \sigma_p$ là các chu trình rời nhau và $\sigma'_1, \sigma'_2, \cdots , \sigma'_q$cũng là các chu trình rời nhau. Đặt $\sigma_1 = (i_1 i_2 \cdots i_r)$. Khi đó tồn tại $1 \leq k \leq q$ sao cho

$$\sigma'_k(i_1) = \sigma(i_1) = \sigma_1(i_1) = i_2,$$

$$\sigma'_k(i_2) = \sigma(i_2) = \sigma_1(i_2) = i_3,$$

$$\dots$$

$$\sigma'_k(i_r) = \sigma(i_r) = \sigma_1(i_r) = i_1.$$

Do đó $\sigma'_k = \sigma_1$. Không mất tính tổng quát ta có thể giả sử $\sigma'_1 = \sigma_1$. Khi đó $\sigma_2 \cdots \sigma_p = \sigma'_2 \cdots \sigma'_q$. Tiếp tục thực hiện như trên, cuối cùng ta được $p = q$ và $\sigma'_i = \sigma_i$ với mọi $1 \le i \le p$. Định lý được chứng minh. ■

Ví dụ: Trong nhóm hoán vị S_{10} ta có

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 2 & 7 & 9 & 1 & 4 & 8 & 5 & 6 & 10 \end{pmatrix} = (1\,3\,7\,8\,5)(4\,9\,6).$$

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

Chứng minh. Cho $\sigma = (i_1 i_2 \cdots i_r)$ là một chu trình. Ta có $\sigma = (i_1 i_r)(i_1 i_{r-1}) \cdots (i_1 i_2)$. ■

4.6 Định lý. *Mọi phép hoán vị trong S_n đều được phân tích thành tích của các chuyển vị.*

Chứng minh. Suy từ Định lý 4.4 và Bổ đề 4.5. ■

Ví dụ: Với σ như trong ví dụ trên, ta có

$$\sigma = (15)(18)(17)(13)(46)(49).$$

Nhận xét rằng sự phân tích thành tích các chuyển vị của một chu trình là không duy nhất. Do đó sự phân tích trong Định lý 4.6 là không duy nhất. Tuy nhiên chúng ta sẽ chứng minh rằng tính chẵn lẻ của số các chuyển vị trong các phân tích là không thay đổi.

4.7. Định nghĩa

Cho $\sigma \in S_n$. Ta nói rằng $\{i, j\}$ tạo thành một *nghịch thế* đối với σ nếu

$$(i - j)[\sigma(i) - \sigma(j)] < 0.$$

Nếu số các nghịch thế đối với σ là k thì dấu của σ, ký hiệu $\mathrm{sgn}(\sigma)$, là hàm được định nghĩa bởi

$$\mathrm{sgn}(\sigma) = (-1)^k.$$

Nếu $\mathrm{sgn}(\sigma) = 1$ thì σ được gọi là *hoán vị chẵn*, nếu $\mathrm{sgn}(\sigma) = -1$ thì σ được gọi là *hoán vị lẻ*.

4.8. Nhận xét

(i) $\mathrm{sgn}(Id_X) = 1$.

(ii) $\mathrm{sgn}(\sigma) = \mathrm{sgn}(\sigma^{-1})$.

(iii) Nếu σ là một chuyển vị thì $\mathrm{sgn}(\sigma) = -1$.

4.9. Định lý. *Với mọi* $\sigma, \tau \in S_n$ *thì*

$$\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau).$$

Chứng minh. Gọi k_1, k_2 và k lần lượt là số nghịch thế trong σ, τ và $\sigma\tau$. Giả sử $1 \leq i < j \leq n$. Hoán vị σ có thể được biểu diễn như sau:

$$\sigma = \begin{pmatrix} \cdots & \tau(i) & \cdots & \tau(j) & \cdots \\ \cdots & \sigma\tau(i) & \cdots & \sigma\tau(j) & \cdots \end{pmatrix}.$$

Khi đó

1^o. Nếu $\tau(i) < \tau(j)$ và $\sigma\tau(i) < \sigma\tau(j)$ thì $\{i, j\}$ không là nghịch thế trong τ; $(\tau(i), \tau(j))$ không là nghịch thế trong σ và $\{i, j\}$ không là nghịch thế trong $\sigma\tau$.

2^o. Nếu $\tau(i) < \tau(j)$ và $\sigma\tau(i) > \sigma\tau(j)$ thì $\{i, j\}$ không là nghịch thế trong τ; $(\tau(i), \tau(j))$ là nghịch thế trong σ và $\{i, j\}$ là nghịch thế trong $\sigma\tau$.

3^o. Nếu $\tau(i) > \tau(j)$ và $\sigma\tau(i) < \sigma\tau(j)$ thì $\{i, j\}$ là nghịch thế trong τ; $(\tau(i), \tau(j))$ là nghịch thế trong σ và $\{i, j\}$ không là nghịch thế trong $\sigma\tau$.

4^o. Nếu $\tau(i) > \tau(j)$ và $\sigma\tau(i) > \sigma\tau(j)$ thì $\{i, j\}$ là nghịch thế trong τ; $(\tau(i), \tau(j))$ không là nghịch thế trong σ và $\{i, j\}$ là nghịch thế trong $\sigma\tau$.

Kết hợp 4 trường hợp trên ta được $k + k_1 + k_2$ là một số chẵn nên $(-1)^k = (-1)^{k_1}(-1)^{k_2}$, nghĩa là

$$\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau). \qquad \blacksquare$$

Từ Bổ đề 4.5, Nhận xét 4.8 và Định lý 4.9 ta suy ra:

4.10. Định lý. *Với mọi hoán vị $\sigma \in S_n$, ta có*

$$\mathrm{sgn}(\sigma) = (-1)^l$$

với l là số chuyển vị trong phân tích σ thành tích các chuyển vị. Đặc biệt, tính chẵn lẻ của số các chuyển vị trong Định lý 4.6 là duy nhất.

Ví dụ: Xét tính chẵn lẻ của phép hoán vị $\sigma \in S_{10}$ sau:

$$\begin{aligned}\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 6 & 4 & 8 & 1 & 7 & 10 & 2 & 9 \end{pmatrix} \\ &= (1\,3\,6)(2\,5\,8\,10\,9) \\ &= (1\,6)(1\,3)(2\,9)(2\,10)(2\,8)(2\,5).\end{aligned}$$

Vì σ được viết dưới dạng tích của 6 chuyển vị nên $\mathrm{sgn}(\sigma) = 1$ nghĩa là σ là một hoán vị chẵn.

4.11. Hệ quả. *Nếu σ là một r-chu trình thì*

(i) $\mathrm{sgn}(\sigma) = (-1)^{r-1}$;

(ii) σ chẵn $\Leftrightarrow$ r lẻ; và σ lẻ $\Leftrightarrow$ r chẵn.

§5. Nhóm con

5.1. Định nghĩa

Một tập con H của nhóm $(G, .)$ được gọi là tập con *ổn định* của nhóm G nếu với mọi $x, y \in H, xy \in H$. Khi đó phép toán nhân thu hẹp trên H xác định một phép toán trên H mà ta gọi là phép toán cảm sinh trên H (từ phép toán trên G).

5.2. Định nghĩa

Nhóm con H của nhóm G là một tập con ổn định của nhóm G sao cho cùng với phép toán cảm sinh H là một nhóm. Ký hiệu $H \leq G$ để chỉ H là một nhóm con của G.

Định lý sau đây cho ta dấu hiệu để nhận biết nhóm con của một nhóm cho trước.

5.3. Định lý. *Cho* H *là một tập con khác rỗng của nhóm* $(G, .)$. *Các mệnh đề sau tương đương:*

(i) $H \leq G$;

(ii) Với mọi $x, y \in H, xy \in H$ *và* $x^{-1} \in H$;

(iii) Với mọi $x, y \in H, x^{-1}y \in H$.

Chứng minh. (i)⇒(ii) Trước hết ta chứng minh phần tử đơn vị e' của nhóm con H cũng chính là phần tử đơn vị e của G. Thật vậy, với mọi $x \in H$ ta có $e'x = x = ex$ nên do tính giản ước ta suy ra $e' = e$. Bây giờ gọi x' là phần tử nghịch đảo của x trong nhóm con H, ta có $x'x = e = x^{-1}x$, do đó $x^{-1} = x' \in H$. Tính chất $xy \in H$ được suy từ tính chất nhóm con H là một tập hợp con ổn định của G.

(ii)⇒(iii) Với mọi $x, y \in H$, giả thiết (ii) cho ta $x^{-1} \in H$ và do đó $x^{-1}y \in H$.

(iii)⇒(i) Vì $H \neq \emptyset$ nên tồn tại $a \in H$ và do đó $e = a^{-1}a \in H$. Bây giờ với mọi $x \in H, x^{-1} = x^{-1}e \in H$. Cuối cùng, với mọi $x, y \in H$, do $x^{-1} \in H$ nên $xy = (x^{-1})^{-1}y \in H$. Suy ra $H \leq G$. ■

5.4. Ví dụ

1) Các tập hợp $\{e\}$ và G đều là các nhóm con của G. Ta gọi đây là các *nhóm con tầm thường* của G.

2) Từ Ví dụ 3.2 ta thấy $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ và $\mathbb{Q}^* \leq \mathbb{R}^* \leq \mathbb{C}^*$.

3) Gọi A_n là tập hợp gồm tất cả những hoán vị chẵn trong nhóm hoán vị S_n. Khi đó từ Nhận xét 4.8 và các Định lý 4.9, 5.3 ta thấy $A_n \leq S_n$. Ta gọi A_n là *nhóm thay phiên* bậc n.

4) Tập hợp $SL(n,\mathbb{R})$ gồm các ma trận vuông cấp n với hệ số thực có định thức bằng 1 là một nhóm con của nhóm tuyến tính đầy đủ $GL(n,\mathbb{R})$. Ta gọi $SL(n,\mathbb{R})$ là *nhóm tuyến tính đặc biệt* bậc n trên $\mathbb{R}$.

5.5. Định lý. *Giao của một họ không rỗng các nhóm con của một nhóm G cũng là nhóm con của G.*

Chứng minh. Giả sử $\{H_i\}_{i\in I}$ là một họ không rỗng các nhóm con của nhóm $(G,.)$. Đặt $H=\bigcap_{i\in I} H_i$. Khi đó $H\neq\emptyset$ vì $e\in H$. Với mọi $x,y\in H$ ta có $x,y\in H_i,\forall i\in I$ nên theo Định lý 5.3, $x^{-1}y\in H_i,\forall i\in I$, nghĩa là $x^{-1}y\in H$. Suy ra $H\leq G$. ■

Bây giờ cho S là một tập hợp con của nhóm G. Ta xét họ tất cả các nhóm con của G chứa S. Họ này không rỗng vì chứa G. Theo Định lý 5.5 giao của họ đó là một nhóm con của G. Hiển nhiên đây là một nhóm con nhỏ nhất của G chứa S. Ta có định nghĩa sau:

5.6. Định nghĩa

Cho S là một tập con của nhóm G. *Nhóm con sinh bởi* S là nhóm con nhỏ nhất của G chứa S và được ký hiệu là $\langle S\rangle$. Tập hợp S được gọi là *tập sinh* của nhóm $\langle S\rangle$. Nếu S hữu hạn: $S=\{x_1,...,x_n\}$ thì ta nói $\langle S\rangle$ là *nhóm hữu hạn sinh* với các phần tử sinh $x_1,...,x_n$ mà ta thường ký hiệu nhóm này là $\langle x_1,...,x_n\rangle$.

Định lý sau đây mô tả các nhóm con sinh bởi một tập hợp:

5.7. Định lý. *Cho S là một tập con của nhóm G. Khi đó:*

(i) Nếu $S=\emptyset$ thì $\langle S\rangle=\{e\}$.

(ii) Nếu $S\neq\emptyset$ thì

$$\langle S\rangle=\{{x_1}^{\varepsilon_1}...{x_n}^{\varepsilon_n}|n\in\mathbb{N}^*,x_i\in S,\varepsilon_i=\pm 1\}.$$

Chứng minh. Khẳng định (i) là hiển nhiên. Ta chứng minh (ii). Thật vậy, ký hiệu vế phải của đẳng thức trong (ii) là H. Vì nhóm con $\langle S\rangle$ chứa tất cả các phần tử x_i của S nên $\langle S\rangle$ chứa H. Mặt khác, do cách đặt H ta thấy nếu $x,y\in H$ thì $xy\in H$ và $x^{-1}\in H$ nên H là một

nhóm con của G. Từ đây, do H chứa S nên ta có H chứa $\langle S\rangle$. Suy ra $H = \langle S\rangle$. ■

5.8. Ví dụ

1) Ta có $\mathbb{Z} = \langle 1\rangle$ và $\mathbb{Q} = \langle \frac{1}{n} | n \in \mathbb{N}^*\rangle$.

2) Ta có $\mathbb{Q}^* = \langle P\rangle$, trong đó

$$P = \{-1\} \cup \{p |\ p \text{ nguyên tố dương}\}.$$

3) Xét nhóm hoán vị S_n. Vì mỗi phép hoán vị đều được phân tích thành tích các chuyển vị nên S_n là nhóm sinh bởi các chuyển vị.

5.9. Chú ý

Nếu H và K là hai nhóm con của nhóm G thì $H \cup K$ không nhất thiết là một nhóm con của G (Xem bài tập 1.20). Ta ký hiệu $H \vee K$ để chỉ nhóm con sinh bởi $H \cup K$.

§6. Nhóm con cyclic và nhóm cyclic

6.1. Định nghĩa

Cho G là một nhóm. Nhóm con $\langle a\rangle$ của G sinh bởi phần tử $a \in G$ được gọi là *nhóm con cyclic sinh bởi* a. Nếu tồn tại phần tử $a \in G$ sao cho $\langle a\rangle = G$ thì ta nói G là một *nhóm cyclic* và a là *phần tử sinh* của G.

Từ Định lý 5.7 ta suy ra mệnh đề sau:

6.2. Mệnh đề. *Nhóm con cyclic sinh bởi a là tập hợp gồm tất cả các lũy thừa a^n với $n \in \mathbb{Z}$, nghĩa là $\langle a\rangle = \{a^n |\ n \in \mathbb{Z}\}$.*

Cho $(G, .)$ là một nhóm và $a \in G$. Xét nhóm con cyclic $\langle a\rangle$. Khi đó có hai trường hợp có thể xảy ra:

Trường hợp 1. Tất cả các lũy thừa $a^n (n \in \mathbb{Z})$ đều khác nhau từng đôi một. Trong trường hợp này $\langle a\rangle$ là nhóm vô hạn.

Trường hợp 2. Tồn tại những lũy thừa của a bằng nhau, chẳng hạn $a^k = a^l (k > l)$. Khi đó $a^{k-l} = e$ với $k - l > 0$. Do đó tồn tại những số nguyên dương m sao cho $a^m = e$. Gọi n là số nguyên dương nhỏ nhất sao cho $a^n = e$. Khi đó các phần tử $e, a, ..., a^{n-1}$ đôi một khác nhau và $\langle a \rangle = \{e, a, ..., a^{n-1}\}$. Thật vậy, với $0 \leq i < j \leq n-1$, vì $0 < j - i < n$ nên do tính chất nhỏ nhất của n suy ra $a^{j-i} \neq e$, nghĩa là $a^j \neq a^i$. Hơn nữa, với $x \in \langle a \rangle$, tồn tại $m \in \mathbb{Z}$ sao cho $x = a^m$. Chia m cho n ta tìm được $q, r \in \mathbb{Z}$ với $0 \leq r \leq n-1$ sao cho $m = qn + r$. Khi đó

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

và khẳng định trên được chứng minh. ■

Tóm lại, nếu tất cả các lũy thừa của a đều khác nhau thì $\langle a \rangle$ là nhóm vô hạn, còn nếu tồn tại những lũy thừa của a bằng nhau thì $\langle a \rangle$ là nhóm hữu hạn cấp n: $\langle a \rangle = \{e, a, ..., a^{n-1}\}$, trong đó n là số nguyên dương nhỏ nhất sao cho $a^n = e$. Từ đây ta có định nghĩa sau:

6.3. Định nghĩa

Cấp của một phần tử a trong nhóm G là cấp của nhóm con cyclic $\langle a \rangle$. Ta thường ký hiệu $o(a)$ hay $|a|$ để chỉ cấp của phần tử a.

Từ Định nghĩa 6.3 và theo lý luận trên ta có hệ quả sau:

6.4. Hệ quả. *Cho $(G, .)$ là một nhóm và $a \in G$. Ta có:*

(i) a có cấp vô hạn khi và chỉ khi với mọi $k \in \mathbb{Z}$, nếu $a^k = e$ thì $k = 0$.

(ii) a có cấp hữu hạn khi và chỉ khi tồn tại $k \in \mathbb{Z}^*$ sao cho $a^k = e$.

(iii) Nếu a có cấp hữu hạn thì cấp của a là số nguyên dương n nhỏ nhất sao cho $a^n = e$. Hơn nữa, khi đó với mọi $k \in \mathbb{Z}$, $a^k = e$ khi và chỉ khi k là bội số của n.

6.5. Ví dụ

1) Nhóm cộng các số nguyên $\mathbb{Z}$ là nhóm cyclic sinh bởi 1.

2) Với mỗi n nguyên dương, quan hệ đồng dư modulo n trên $\mathbb{Z}$ định

bởi

$$x \equiv y(\text{mod } n) \Leftrightarrow x - y \text{ chia hết cho } n.$$

Đây là một quan hệ tương đương trên $\mathbb{Z}$ với các lớp tương đương là

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

Tập thương của $\mathbb{Z}$ theo quan hệ đồng dư modulo n định bởi

$$\mathbb{Z}_n = \{\overline{x} | x \in \mathbb{Z}\} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}.$$

Trên $\mathbb{Z}_n$ ta định nghĩa phép toán cộng như sau:

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

Kiểm chứng dễ dàng rằng định nghĩa trên được hoàn toàn xác định và $\mathbb{Z}_n$ trở thành một nhóm giao hoán. Hơn nữa, $\mathbb{Z}_n$ là nhóm cyclic hữu hạn cấp n sinh bởi $\overline{1}$. Ta gọi $\mathbb{Z}_n$ là *nhóm cộng các số nguyên modulo* n.

3) Trong nhóm hoán vị S_n, một r-chu trình $\sigma = (i_1\ i_2\ ...\ i_r)$ luôn luôn có cấp r vì $\sigma^r = Id$ và $\sigma^l \neq Id$ với mọi $0 < l < r$.

6.6. Định lý. *Mọi nhóm con của nhóm cyclic đều là nhóm cyclic. Hơn nữa, nếu* $H \leq \langle a \rangle$ *và* $H \neq \{e\}$ *thì* $H = \langle a^n \rangle$ *trong đó* n *là số nguyên dương nhỏ nhất sao cho* $a^n \in H$.

Chứng minh. Giả sử $H \subset \langle a \rangle$. Nếu $H = \{e\}$ thì hiển nhiên H là nhóm con cyclic sinh bởi e. Xét trường hợp $H \neq \{e\}$. Khi đó tồn tại $k \in \mathbb{Z}^*$ sao cho $a^k \in H$. Vì a^k và $a^{-k} = (a^k)^{-1}$ đều thuộc H nên có thể khẳng định rằng tồn tại $l \in \mathbb{N}^*$ sao cho $a^l \in H$. Gọi n là số nguyên dương nhỏ nhất sao cho $a^n \in H$. Ta chứng minh $H = \langle a^n \rangle$. Thật vậy, hiển nhiên $\langle a^n \rangle \subseteq H$. Ngược lại, cho $x = a^m \in H$. Lấy m chia cho n ta tìm được $q, r \in \mathbb{Z}$ sao cho $m = qn + r$ với $0 \leq r < n$. Vì $a^r = a^m(a^n)^{-q} \in H$ nên theo định nghĩa của n ta phải có $r = 0$, nghĩa là $m = qn$ và $x = (a^n)^q \in \langle a^n \rangle$. Điều này chứng tỏ $H \subset \langle a^n \rangle$. Vậy $H = \langle a^n \rangle$. ■

Từ Định lý 6.6 ta suy ra hệ quả sau:

6.7. Hệ quả. H *là một nhóm con của nhóm cộng các số nguyên* $\mathbb{Z}$ *khi và chỉ khi* H *có dạng* $n\mathbb{Z}$ *với* $n \in \mathbb{N}$, *trong đó*

$$n\mathbb{Z} = \{nk | k \in \mathbb{Z}\}.$$

§7. Nhóm con chuẩn tắc và nhóm thương

7.1. Định lý. *Cho $(G,.)$ là một nhóm và H là một nhóm con của G. Xét quan hệ $\sim$ trên G như sau:*

$$x \sim y \Leftrightarrow x^{-1}y \in H.$$

Khi đó

(i) $\sim$ là một quan hệ tương đương trên G.

(ii) Lớp tương đương chứa x là $\overline{x} = xH$, trong đó

$$xH = \{xh | h \in H\}.$$

Ta gọi xH là *lớp ghép trái* của H (bởi phần tử x). Tập hợp thương của G theo quan hệ $\sim$, ký hiệu là G/H, được gọi là *tập thương* của G trên H và $|G/H|$ là *chỉ số* của nhóm con H trong G, ký hiệu là $[G : H]$.

Chứng minh. (i) Tính phản xạ: Với mọi $x \in G, x \sim x$ vì $x^{-1}x = e \in H$.

Tính đối xứng: Với mọi $x, y \in G$, nếu $x \sim y$ thì $x^{-1}y \in H$ nên $y^{-1}x = (x^{-1}y)^{-1} \in H$, nghĩa là $y \sim x$.

Tính bắc cầu: Với mọi $x, y, z \in G$, nếu $x \sim y$ và $y \sim z$ thì $x^{-1}y \in H$ và $y^{-1}z \in H$ nên $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$, nghĩa là $x \sim z$.

Vậy $\sim$ là một quan hệ tương đương trên G.

(ii) Ta có

$$\begin{aligned} x \sim y &\Leftrightarrow x^{-1}y \in H \\ &\Leftrightarrow \exists h \in H, x^{-1}y = h \\ &\Leftrightarrow \exists h \in H, y = xh. \end{aligned}$$

Suy ra $\overline{x} = \{y \in G | x \sim y\} = \{xh | h \in H\} = xH$. ■

7.2. Chú ý

Hoàn toàn tương tự, ta định nghĩa được quan hệ $\sim'$ trên G như sau:

$$x \sim' y \Leftrightarrow xy^{-1} \in H.$$

Khi đó $\sim'$ cũng là một quan hệ tương đương trên G và lớp tương đương chứa x là $\overline{x} = Hx$, trong đó $Hx = \{hx | h \in H\}$. Ta gọi Hx là *lớp ghép phải* của H (bởi phần tử x).

Định lý sau đây cho ta thông tin về cấp của các nhóm con của các nhóm hữu hạn.

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

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

Chứng minh. Trước hết nhận xét rằng nếu xH là một lớp ghép trái thì ánh xạ

$$\begin{array}{rccc} \varphi : & H & \longrightarrow & xH \\ & h & \longmapsto & xh \end{array}$$

là một song ánh. Thật vậy, φ là toàn ánh do định nghĩa của tập hợp xH, φ là đơn ánh vì nếu $xh = xk$ thì $h = k$ do tính giản ước của phép toán nhân trong nhóm G. Như vậy số phần tử của các lớp ghép trái đều bằng nhau và bằng $|H|$, số lớp ghép là $[G : H]$. Do đó

$$|G| = |H|[G : H]. \qquad \blacksquare$$

Từ Định lý Lagrange ta suy ra ngay hệ quả sau:

7.4. Hệ quả. *Cho G là một nhóm hữu hạn. Khi đó:*

(i) Cấp của mỗi nhóm con của G là một ước số của cấp của G.

(ii) Cấp của mỗi phần tử thuộc G là một ước số của cấp của G.

(iii) Nếu G có cấp nguyên tố thì G là nhóm cyclic và G được sinh bởi một phần tử bất kỳ khác e.

Chú ý rằng nếu H là một nhóm con tùy ý của G thì tập thương G/H như đã xây dựng trong Định lý 7.1 không nhất thiết là một nhóm. Sau

đây chúng ta đề cập đến một loại nhóm con đặc biệt mà ứng với nhóm con loại đó tập hợp thương trở thành một nhóm.

7.5. Định nghĩa

Một nhóm con H của nhóm $(G,.)$ được gọi là *chuẩn tắc* nếu với mọi $x \in G$ và $h \in H,\ x^{-1}hx \in H$. Ký hiệu $H \lhd G$ để chỉ H là một nhóm con chuẩn tắc của G.

7.6. Mệnh đề. *Cho H là một nhóm con của nhóm $(G,.)$. Các mệnh đề sau tương đương:*

(i) $H \lhd G$;

(ii) $\forall x \in G, x^{-1}Hx \subset H$;

(iii) $\forall x \in G, x^{-1}Hx = H$;

(iv) $\forall x \in G, xH = Hx$;

trong đó $x^{-1}Hx = \{x^{-1}hx | h \in H\}$.

Chứng minh. (i)⇒(ii) Hiển nhiên do định nghĩa.

(ii)⇒(iii) Với giả thiết (ii) ta có $x^{-1}Hx \subset H$. Mặt khác

$$xHx^{-1} = (x^{-1})^{-1}H(x^{-1}) \subset H$$

nên $H \subset x^{-1}Hx$. Từ đó $x^{-1}Hx = H$.

(iii)⇒(iv) Theo giả thiết (iii), $x^{-1}Hx = H$ nên

$$xH = x(x^{-1}Hx) = Hx.$$

(iv)⇒(i) Với mọi $x \in G$ và $h \in H$ ta có $hx \in Hx = xH$ nên tồn tại $k \in H$ sao cho $hx = xk$. Suy ra $x^{-1}hx = k \in H$. Điều này chứng tỏ $H \lhd G$. ■

7.7. Nhận xét

1) Nếu G giao hoán thì mọi nhóm con của G đều chuẩn tắc.

2) Các nhóm con tầm thường $\{e\}$ và G đều chuẩn tắc trong G.

7.8. Ví dụ

1) Nhóm thay phiên bậc n (Xem Ví dụ 5.4) là nhóm con chuẩn tắc của nhóm hoán vị S_n vì với mọi hoán vị chẵn τ ta có $\sigma^{-1}\tau\sigma$ cũng là hoán vị chẵn với mọi hoán vị $\sigma \in S_n$.

2) Nhóm tuyến tính đặc biệt $SL(n,\mathbb{R})$ (Xem Ví dụ 5.4) là nhóm con chuẩn tắc của nhóm tuyến tính đầy đủ $GL(n,\mathbb{R})$ vì với mọi $X \in GL(n,\mathbb{R})$ và $A \in SL(n,\mathbb{R})$ ta có

$$\det(X^{-1}AX) = (\det X)^{-1}(\det A)(\det X) = \det(A) = 1,$$

nghĩa là $X^{-1}AX \in SL(n,\mathbb{R})$.

Khi H là một nhóm con chuẩn tắc của G thì tập thương G/H trở thành một nhóm như trong định lý sau:

7.9. Định lý. *Cho G là một nhóm và H là nhóm con chuẩn tắc của G. Khi đó:*

(i) Lớp xyH chỉ phụ thuộc vào các lớp xH và yH mà không phụ thuộc vào sự lựa chọn của các phần tử đại diện x, y của các lớp đó.

(ii) Tập thương G/H cùng với phép toán nhân định bởi

$$(xH)(yH) = xyH$$

là một nhóm, gọi là nhóm thương của G trên H .

Chứng minh. (i) Giả sử $x_1H = xH$ và $y_1H = yH$, nghĩa là $x^{-1}x_1 \in H$ và $y^{-1}y_1 \in H$. Ta cần chứng minh $x_1y_1H = xyH$, nghĩa là $(xy)^{-1}(x_1y_1) \in H$. Thật vậy

$$(xy)^{-1}(x_1y_1) = y^{-1}x^{-1}x_1y_1 = [y^{-1}x^{-1}x_1y][y^{-1}y_1].$$

Phần tử sau cùng thuộc H do $x^{-1}x_1$ và $y^{-1}y_1$ đều thuộc H và $H \lhd G$.

(ii) Do (i) phép toán nhân được định nghĩa như trong (ii) được hoàn toàn xác định. Tính kết hợp của phép toán nhân trên G/H được suy từ tính kết hợp của phép toán nhân trên G. Phần tử đơn vị trong G/H chính là lớp $eH = H$, trong đó e là phần tử đơn vị của G, còn phần tử nghịch đảo của lớp xH chính là $x^{-1}H$.

7.10. Nhận xét

1) Nếu G là một nhóm giao hoán thì nhóm thương G/H cũng giao hoán. Chiều đảo không đúng.

2) Với $H \leq G$, nếu tập thương G/H là một nhóm với phép toán được định nghĩa như trên ($(xH)(yH) = xyH$) thì $H \lhd G$. Thật vậy, với mọi $x \in G$ và $h \in H$ ta có $x^{-1}hxH = (x^{-1}H)(hH)(xH) = (x^{-1}H)H(xH) = (x^{-1}H)(xH) = x^{-1}xH = H$ nên $x^{-1}hx \in H$.

7.11. Ví dụ

1) Vì nhóm cộng các số nguyên $\mathbb{Z}$ giao hoán nên với mỗi n nguyên dương nhóm con $n\mathbb{Z}$ chuẩn tắc trong $\mathbb{Z}$. Ứng với nhóm con $H = n\mathbb{Z}$, quan hệ $\sim$ trong Định lý 7.1 định bởi

$$\begin{aligned} x \sim y &\Leftrightarrow x - y \in n\mathbb{Z} \\ &\Leftrightarrow x - y \text{ chia hết cho } n. \end{aligned}$$

Như vậy, $\sim$ chính là quan hệ đồng dư modulo n trên $\mathbb{Z}$ và nhóm thương $\mathbb{Z}/n\mathbb{Z}$ chính là nhóm cộng $\mathbb{Z}_n$ các số nguyên modulo n trong Ví dụ 6.5.

2) Theo Ví dụ 7.8, $A_n \lhd S_n$. Nếu σ và τ là hai hoán vị lẻ thì $\sigma^{-1}\tau$ là hoán vị chẵn nên $\sigma^{-1}\tau \in A_n$, từ đó $\sigma A_n = \tau A_n$. Điều này chứng tỏ nhóm thương S_n/A_n có đúng hai phần tử:

$$S_n/A_n = \{A_n, \overline{A_n}\},$$

trong đó $\overline{A_n} = S_n \setminus A_n$.

§8. Đồng cấu

8.1. Định nghĩa

Một ánh xạ f từ nhóm G vào nhóm G' được gọi là một *đồng cấu* (*nhóm*) nếu f bảo toàn phép toán, nghĩa là với mọi $x, y \in G$,

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

Một đồng cấu từ nhóm G vào G được gọi là một *tự đồng cấu* của G. Một đồng cấu đồng thời là đơn ánh, toàn ánh hay song ánh được gọi lần lượt là *đơn cấu, toàn cấu* hay *đẳng cấu*. Một tự đồng cấu song ánh được gọi là một tự đẳng cấu. Nếu tồn tại một đẳng cấu từ nhóm G vào nhóm G' thì ta nói G đẳng cấu với G', ký hiệu $G \simeq G'$.

8.2. Ví dụ

1) Ánh xạ đồng nhất id_G của nhóm G là một tự đẳng cấu, gọi là *tự đẳng cấu đồng nhất* của G.

2) Giả sử H là một nhóm con của nhóm G. Khi đó ánh xạ bao hàm $i_H : H \longrightarrow G$ $(i_H(x) = x)$ là một đơn cấu, gọi là *đơn cấu* chính tắc.

3) Giả sử H là một nhóm con chuẩn tắc của nhóm G. Khi đó ánh xạ $\pi : G \longrightarrow G/H$ định bởi $\pi(x) = xH$ là một toàn cấu, gọi là *toàn cấu chính tắc*.

4) Giả sử G và G' là hai nhóm tùy ý. Khi đó ánh xạ $f : G \longrightarrow G'$ định bởi $f(x) = e'$ (e' là phần tử trung hòa của G') là một đồng cấu, gọi là *đồng cấu tầm thường*.

5) Ánh xạ $x \mapsto \cos 2\pi x + i \sin 2\pi x$ là một đồng cấu từ nhóm cộng các số thực $\mathbb{R}$ vào nhóm nhân các số phức khác không $\mathbb{C}^*$.

6) Ánh xạ $x \mapsto e^x$ là một đẳng cấu từ nhóm cộng các số thực $\mathbb{R}$ lên nhóm nhân $\mathbb{R}^+$ các số thực dương.

7) Ánh xạ $x \mapsto \ln x$ là một đẳng cấu từ nhóm nhân $\mathbb{R}^+$ các số thực dương lên nhóm cộng các số thực $\mathbb{R}$.

8) Ánh xạ $\mathrm{sgn} : S_n \longrightarrow (\{-1; 1\}, .)$ là một đồng cấu.

9) Ánh xạ $\det : GL(n,\mathbb{R}) \longrightarrow \mathbb{R}^*$ là một toàn cấu.

10) Cho $(G,.)$ là một nhóm và $a \in G$. Ánh xạ $\varphi_a : G \longrightarrow G$ định bởi $\varphi_a(x) = axa^{-1}$ là một tự đẳng cấu của G. Thật vậy, φ_a là một đồng cấu vì

$$\forall x, y \in G, \varphi_a(xy) = a(xy)a^{-1} = (axa^{-1})(aya^{-1}) = \varphi_a(x)\varphi_a(y).$$

Mặt khác, φ_a là một song ánh vì với mỗi $y \in G$, tồn tại duy nhất $x = a^{-1}ya \in G$ sao cho $y = \varphi_a(x)$. Ta gọi φ_a là một *tự đẳng cấu trong* của nhóm G.

Từ Định nghĩa 8.1 ta suy ra các tính chất cơ bản của đồng cấu nhóm như sau:

8.3. Mệnh đề. *Nếu $f : G \longrightarrow G'$ là một đồng cấu nhóm thì*

$$f(e) = e' \text{ và } f(x^{-1}) = (f(x))^{-1} \text{ với mọi } x \in G$$

(e và e' lần lượt là các phần tử đơn vị của các nhóm G và G').

Chứng minh. Từ đẳng thức $ee = e$ ta có $f(e)f(e) = f(e)$ và tính giản ước của phép nhân trong nhóm G' cho ta $f(e) = e'$. Mặt khác, với mọi $x \in G$, từ đẳng thức $x^{-1}x = e$ ta suy ra $f(x^{-1})f(x) = e'$ nên $f(x^{-1}) = (f(x))^{-1}$.

8.4. Mệnh đề. *Tích của hai đồng cấu nhóm là một đồng cấu nhóm. Đặc biệt, tích của hai đơn cấu (tương ứng: toàn cấu, đẳng cấu) là một đơn cấu (tương ứng: toàn cấu, đẳng cấu).*

Chứng minh. Giả sử $f : G \longrightarrow G'$ và $g : G' \longrightarrow G''$ là các đồng cấu nhóm. Xét ánh xạ tích $g_\circ f$, ta có với mọi $x, y \in G$, $(g_\circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g_\circ f)(x)(g_\circ f)(y)$ nên $g_\circ f$ vẫn còn là đồng cấu nhóm. ■

8.5. Mệnh đề. *Ánh xạ ngược của một đẳng cấu nhóm là một đẳng cấu nhóm.*

Chứng minh. Giả sử $f : G \longrightarrow G'$ là một đẳng cấu nhóm. Vì $f^{-1} : G' \longrightarrow G$ cũng là song ánh nên ta chỉ cần chứng minh f^{-1} là đồng cấu. Thật vậy, với mọi $x', y' \in G'$, tồn tại $x, y \in G$ sao cho $x' = f(x)$ và

$y' = f(y)$ nên $f^{-1}(x'y') = f^{-1}(f(x)f(y)) = f^{-1}(f(xy)) = (f^{-1}_{\circ}f)(xy)$ $= xy = f^{-1}(x')f^{-1}(y')$. Vậy f^{-1} là đồng cấu và do đó là đẳng cấu. ■

8.6. Chú ý

Do các Mệnh đề 8.4 và 8.5 ta thấy quan hệ đẳng cấu $\simeq$ giữa các nhóm là một quan hệ tương đương, nghĩa là có ba tính chất phản xạ, đối xứng và bắc cầu.

8.7. Định lý. *Cho đồng cấu nhóm $f : G \longrightarrow G'$ và H là một nhóm con của G, H' là một nhóm con của G'. Khi đó:*

(i) $f(H)$ là một nhóm con của G'.

(ii) $f^{-1}(H')$ là một nhóm con của G. Hơn nữa, nếu H' là nhóm con chuẩn tắc của G' thì $f^{-1}(H')$ là nhóm con chuẩn tắc của G.

Đặc biệt, $Imf = f(G)$ là nhóm con của G' và $\mathrm{Ker}f = f^{-1}(e')$ là nhóm con chuẩn tắc của G.

Ta gọi Imf là *ảnh* của f và $\mathrm{Ker}f$ là *hạt nhân* của f.

Chứng minh. (i) Vì $e \in H$ nên $e' = f(e) \in f(H)$. Với mọi $x', y' \in f(H)$, tồn tại $x, y \in H$ sao cho $x' = f(x), y' = f(y)$ nên $(x')^{-1}y' = f(x)^{-1}f(y) = f(x^{-1})f(y) = f(x^{-1}y) \in f(H)$ do $x^{-1}y \in H$. Theo Định lý 5.3, $f(H) \leq G'$.

(ii) Vì $f(e) = e' \in H'$ nên $e \in f^{-1}(H')$. Với mọi $x, y \in f^{-1}(H')$ ta có $f(x) \in H'$ và $f(y) \in H'$ nên $f(x^{-1}y) = (f(x))^{-1}f(y) \in H'$, nghĩa là $x^{-1}y \in f^{-1}(H')$. Điều này chứng tỏ $f^{-1}(H') \leq G$. Bây giờ giả sử $H' \lhd G'$. Khi đó với mọi $x \in G$ và $h \in f^{-1}(H')$ ta có $f(h) \in H'$ nên $f(x^{-1}hx) = (f(x))^{-1}f(h)f(x) \in H'$ do H' chuẩn tắc. Từ đó $x^{-1}hx \in f^{-1}(H')$. Lý luận trên chứng tỏ $f^{-1}(H') \lhd G$.

Cuối cùng nhận xét rằng $G \leq G$ và $\{e'\} \lhd G'$ nên theo kết quả trên ta có khẳng định sau cùng của định lý. ■

Theo lý thuyết ánh xạ, hiển nhiên một đồng cấu nhóm $f : G \longrightarrow G'$ là toàn cấu khi và chỉ khi $Imf = G'$. Định lý sau đây cho ta một dấu hiệu rất đơn giản để nhận biết một đồng cấu có là đơn cấu hay không.

8.8. Định lý. *Đồng cấu nhóm $f : G \longrightarrow G'$ là đơn cấu khi và chỉ khi* $\mathrm{Ker}f = \{e\}$.

Chứng minh. Chiều thuận là hiển nhiên vì $\mathrm{Ker}f \leq G$ và $\mathrm{Ker}f$ chứa không quá một phần tử do f là đơn ánh. Đảo lại, giả sử $\mathrm{Ker}f = \{e\}$. Khi đó với mọi $x, y \in G$ thỏa $f(x) = f(y)$ ta có $f(x^{-1}y) = (f(x))^{-1}f(y) = e'$ nên $x^{-1}y \in \mathrm{Ker}f$, suy ra $x^{-1}y = e$, nghĩa là $x = y$. Vậy f đơn ánh. ■

8.9. Định lý đẳng cấu 1. *Cho đồng cấu nhóm $f : G \longrightarrow G'$. Khi đó ánh xạ $\overline{f} : G/\mathrm{Ker}f \longrightarrow G'$ định bởi $\overline{f}(x\mathrm{Ker}f) = f(x)$ là một đơn cấu. Đặc biệt, $G/\mathrm{Ker}f \simeq Imf$.*

Chứng minh. Đặt $H = \mathrm{Ker}f$. Vì $H \lhd G$ nên ta lập được nhóm thương G/H. Xét tương ứng $f : G/H \longrightarrow G'$ định bởi $\overline{f}(xH) = f(x)$ ta có với mọi $x, y \in G$:

$$\begin{aligned}
\overline{f}(xH) = \overline{f}(yH) &\Leftrightarrow f(x) = f(y) \\
&\Leftrightarrow (f(x))^{-1}f(y) = e' \\
&\Leftrightarrow f(x^{-1})f(y) = e' \\
&\Leftrightarrow f(x^{-1}y) = e' \\
&\Leftrightarrow x^{-1}y \in H \\
&\Leftrightarrow xH = yH.
\end{aligned}$$

Chiều $(\Leftarrow)$ chứng tỏ $\overline{f}$ là một ánh xạ, chiều $(\Rightarrow)$ chứng tỏ $\overline{f}$ là một đơn ánh. Bây giờ ta kiểm chứng $\overline{f}$ là một đồng cấu. Thật vậy, với mọi $x, y \in G$:

$$\overline{f}((xH)(yH)) = \overline{f}(xyH) = f(xy) = f(x)f(y) = \overline{f}(xH)\overline{f}(yH).$$

Vậy $\overline{f}$ là đơn cấu. Khẳng định sau cùng trong Định lý được suy từ lý thuyết về ánh xạ. ■

8.10. Định lý đẳng cấu 2. *Cho G là một nhóm và H, K là hai nhóm con của G, hơn nữa H chuẩn tắc trong G. Khi đó $HK \leq G, H \lhd HK, H \cap K \lhd K$ và $K/H \cap K \simeq HK/H$ qua đẳng cấu $k(H \cap K) \mapsto kH$, trong đó $HK = \{hk | h \in H, k \in K\}$.*

Chứng minh. 1) $HK \leq G$: Hiển nhiên $e = ee \in HK$. Giả sử

h_1k_1, h_2k_2 là hai phần tử của HK. Khi đó

$$(h_1k_1)^{-1}(h_2k_2) = {k_1}^{-1}{h_1}^{-1}h_2k_2 = [{k_1}^{-1}({h_1}^{-1}h_2)k_1][{k_1}^{-1}k_2].$$

Chú ý rằng ${h_1}^{-1}h_2 \in H$ nên ${k_1}^{-1}({h_1}^{-1}h_2)k_1 \in H$ do $H \lhd G$, hơn nữa ${k_1}^{-1}k_2 \in K$ do $K \leq G$. Do đó $(h_1k_1)^{-1}(h_2k_2) \in HK$. Suy ra $HK \leq G$.

2) $H \lhd HK$: Vì $H \subset HK$ và $H \lhd G$ nên $H \lhd HK$.

3) Xét ánh xạ $f : K \longrightarrow HK/H$ định bởi $f(k) = kH$. Hiển nhiên f là một đồng cấu nhóm, hơn nữa f còn là toàn cấu vì với mọi $hkH \in HK/H$ ta có $hkH = (hH)(kH) = H(kH) = kH = f(k)$. Mặt khác

$$\begin{aligned} \mathrm{Ker}f &= \{k \in K | f(k) = H\} \\ &= \{k \in K | kH = H\} \\ &= \{k \in K | k \in H\} \\ &= H \cap K. \end{aligned}$$

Do đó $H \cap K \lhd K$ và theo Định lý 8.9 ta có đẳng cấu

$$K/H \cap K \simeq HK/H,$$

trong đó $k(H \cap K) \mapsto kH$. ■

8.11. Định lý đẳng cấu 3. *Cho G là một nhóm và H là một nhóm con chuẩn tắc của G. Ta có*

(i) $\mathcal{K}$ là một nhóm con của G/H khi và chỉ khi $\mathcal{K}$ có dạng $\mathcal{K} = K/H$ với $K \leq G$ và $H \leq K$.

(ii) $\mathcal{K}$ là một nhóm con chuẩn tắc của G/H khi và chỉ khi $\mathcal{K}$ có dạng $\mathcal{K} = K/H$ với $K \lhd G$ và $H \leq K$. Hơn nữa, khi đó

$$(G/H)/(K/H) \simeq G/K$$

qua đẳng cấu $xH(K/H) \mapsto xK$.

Chứng minh. Xét toàn cấu chính tắc $\pi : G \longrightarrow G/H$. Với $\mathcal{K} \leq G/H$, đặt $K = \pi^{-1}(\mathcal{K})$ thì $H \leq K \leq G$ và $\pi(K) = \mathcal{K}$. Do đó khẳng định (i) được chứng minh. Mặt khác, nếu $\mathcal{K} \lhd G/H$ thì $K \lhd G$ nên ta có khẳng định đầu trong (ii). Hơn nữa, khi đó xét tương ứng $f : G/H \longrightarrow G/K$ định bởi $f(xH) = xK$ ta thấy ngay f là một ánh xạ vì nếu $xH = yH$

thì $x^{-1}y \in H$, từ đó $x^{-1}y \in K$, nghĩa là $xK = yK$. Hiển nhiên f là toàn ánh. Ngoài ra do $f((xH)(yH)) = f(xyH) = xyK = (xK)(yK) = f(xH)f(yH)$ nên f là đồng cấu. Cuối cùng ta có

$$\begin{aligned} \mathrm{Ker}f &= \{xH \in G/H | f(xH) = K\} \\ &= \{xH \in G/H | xK = K\} \\ &= \{xH \in G/H | x \in K\} \\ &= K/H \end{aligned}$$

nên theo Định lý 8.9 $(G/H)/(K/H) \simeq G/K$ trong đó

$$(xH)(KH) \longmapsto xK. \qquad \blacksquare$$

8.12. Hệ quả. *Mọi nhóm cyclic vô hạn đều đẳng cấu với nhóm cộng các số nguyên $\mathbb{Z}$. Mọi nhóm cyclic hữu hạn cấp n đều đẳng cấu với nhóm cộng $\mathbb{Z}_n$ các số nguyên mod n.*

Chứng minh. Giả sử G là nhóm cyclic sinh bởi x. Xét ánh xạ $f : \mathbb{Z} \longrightarrow G$ định bởi $f(m) = x^m$. Dễ thấy f là một đồng cấu từ nhóm cộng các số nguyên $\mathbb{Z}$ vào G. Khi đó $\mathrm{Ker}f$ là một nhóm con của $\mathbb{Z}$ nên $\mathrm{Ker}f$ có dạng $\mathrm{Ker}f = n\mathbb{Z}$ với $n \in \mathbb{N}$ (Hệ quả 6.7).

Nếu $n = 0$ thì $\mathrm{Ker}f = \{0\}$ nên f là đơn cấu và do đó cũng là đẳng cấu. Trong trường hợp này G vô hạn và $G \simeq \mathbb{Z}$.

Nếu $n > 0$ thì theo Định lý 8.9 $\mathbb{Z}/n\mathbb{Z} \simeq G$. Vì nhóm thương $\mathbb{Z}/n\mathbb{Z}$ chính là nhóm $\mathbb{Z}_n$ (Xem Ví dụ 7.11) nên trong trường hợp này G hữu hạn cấp n và $G \simeq \mathbb{Z}_n$. $\blacksquare$

8.13. Ví dụ

Từ Ví dụ 8.2 ta thấy

1) Đồng cấu $f : \mathbb{R} \longrightarrow \mathbb{C}^*$ định bởi $f(x) = \cos 2\pi x + i \sin 2\pi x$ có $\mathrm{Ker}f = \mathbb{Z}$ và $\mathrm{Im}f = U$ trong đó $U = \{z \in \mathbb{C}^* | \ |z| = 1\}$. Do đó theo Định lý 8.9 $\mathbb{R}/\mathbb{Z} \simeq U$.

2) Đồng cấu $f = \mathrm{sgn} : S_n \longrightarrow (\{-1; 1\}, .)$ có $\mathrm{Ker}f = A_n$ và $\mathrm{Im}f = \{\pm 1\}$ nên $S_n/A_n \simeq \{\pm 1\}$.

3) Toàn cấu $f : GL(n, \mathbb{R}) \longrightarrow \mathbb{R}^*$ định bởi $f(A) = detA$ có

$$\mathrm{Ker}f = \{A \in GL(n, \mathbb{R}) | \mathrm{det}A = 1\} = SL(n, \mathbb{R})$$

nên $GL(n, \mathbb{R})/SL(n, \mathbb{R}) \simeq \mathbb{R}^*$.

Bài tập

Bài 1.1 Trong các trường hợp sau hãy xét xem cấu trúc $(G, *)$ có là nửa nhóm, vị nhóm hay nhóm không, và xét tính giao hoán của chúng. Trong trường hợp $(G, *)$ là nhóm, hãy mô tả tất cả các phần tử có cấp hữu hạn của nhóm này.

a) $G = \mathbb{Q} \setminus \{-6\}, x * y = 90xy + 540x + 540y + 3234$.

b) $G = \mathbb{R}^+ \setminus \{1\}, x * y = x^{\ln y}$.

c) $G = \mathbb{R}, x * y = \sqrt[n]{x^n + y^n}$, trong đó n là một số nguyên dương lẻ cho trước.

d) $G = \mathbb{R}, x * y = (\sqrt[n]{x} + \sqrt[n]{y})^n$, trong đó n là một số nguyên dương lẻ cho trước.

e) $G = \mathbb{R}^+, x * y = ln(e^x + e^y - 1)$.

f) $G = \mathbb{R} \times \mathbb{R}^*, (x, y) * (z, t) = (x + yz, yt)$.

g) $G = \mathbb{R} \times \mathbb{R}^*, (x, y) * (z, t) = (xz - yt, xt + yz)$.

h) $G = \mathbf{R^2} \setminus \{(\mathbf{0}, \mathbf{0})\}, (x, y) * (z, t) = (xz - yt, xt + yz)$.

Bài 1.2 a) Chứng minh rằng một nửa nhóm khác rỗng, hữu hạn là nhóm khi và chỉ khi phép toán tương ứng có tính giản ước. Chỉ ra rằng điều kiện hữu hạn không thể bỏ được.

b) Chứng minh rằng mọi tập con khác rỗng, hữu hạn, kín đối với phép toán tương ứng trong một nhóm đều là các nhóm con của nhóm đó.

Bài 1.3 Cho $(X, .)$ là một nửa nhóm khác rỗng. Với mỗi $a \in X$ ta đặt

$$aX = \{ax | x \in X\};$$

$$Xa = \{xa | x \in X\}.$$

Chứng minh các khẳng định sau là tương đương:

a) $(X, .)$ là nhóm;

b) Với mọi $a \in X$, $aX = Xa = X$.

Bài 1.4 Cho nhóm $(G, .)$ và $a \in G$. Trên G ta định nghĩa phép toán $*$ như sau: $\forall x, y \in G, x * y = xay$. Chứng minh rằng $(G, *)$ cũng là nhóm.

Bài 1.5 Cho G là một nhóm trong đó có duy nhất một phần tử a có cấp 2. Chứng minh rằng với mọi $x \in G,\ ax = xa$.

Bài 1.6 Cho G là một nhóm mà mọi phần tử khác e đều có cấp 2. Chứng minh G giao hoán.

Bài 1.7 Cho nhóm $(G, .)$. Trên G ta định nghĩa một quan hệ $\sim$ như sau:

$$\forall x, y \in G, x \sim y \Leftrightarrow \exists a \in G, x = a^{-1}ya.$$

Chứng minh rằng

a) $\sim$ là quan hệ tương đương trên G;

b) $\sim$ là quan hệ thứ tự trên G khi và chỉ khi G giao hoán.

Bài 1.8 Cho nhóm $(G,.)$. Giả sử tồn tại ba số nguyên i liên tiếp sao cho với mọi $x, y \in G,\ (xy)^i = x^i y^i$. Chứng minh rằng G giao hoán.

Bài 1.9 Chứng minh rằng nếu $(G,.)$ là một nhóm giao hoán có đúng n phần tử khác nhau là $x_1, x_2, ..., x_n$ thì $(x_1 x_2 ... x_n)^2 = e$.

Bài 1.10 Chứng minh rằng trong nhóm hoán vị S_n, nếu một hoán vị có cấp lẻ thì đó phải là một hoán vị chẵn. Xét chiều đảo.

Bài 1.11 Trong nhóm hoán vị S_{10}, xét các phép hoán vị

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 3 & 5 & 7 & 6 & 1 & 8 & 4 & 10 & 9 \end{pmatrix};$$

$$\sigma_2 = (1\ 3\ 4\ 7)(2\ 5)(1\ 2\ 4\ 3).$$

a) Viết σ_1 và σ_2 dưới dạng tích các chu trình rời nhau và dưới dạng tích các chuyển vị. Suy ra tính chẵn, lẻ và cấp của chúng.

b) Viết $\sigma_1\sigma_2; \sigma_2^2; \sigma_2^{-1}; \sigma_2^{-2}; \sigma_1^2\sigma_2; \sigma_1\sigma_2^2$ dưới dạng tích các chu trình rời nhau. Xét tính chẵn, lẻ và cấp của chúng.

c) Tìm $\sigma \in S_n$ thỏa $\sigma_1 \sigma \sigma_2^{-2} = \sigma_1^3$.

Bài 1.12 Cho σ và τ là hai hoán vị rời nhau trong S_n. Chứng minh rằng $(\sigma\tau)^k = \sigma^k\tau^k, \forall k \in \mathbb{N}$.

Bài 1.13 Cho một ví dụ chứng tỏ rằng lũy thừa của một chu trình không nhất thiết là một chu trình.

Bài 1.14 * Xét nhóm hoán vị S_n và σ là một k-chu trình. Chứng minh rằng với $l \in \mathbb{N}$, σ^l là k-chu trình khi và chỉ khi $(k,l) = 1$.

Bài 1.15 Chứng minh các khẳng định sau:

a) $H = \left\{ \begin{pmatrix} x & y \\ 2y & x \end{pmatrix} \mid x; y \in \mathbb{Q} \right\}$ là một nhóm con của nhóm $(M(2,\mathbb{Q}),+)$.

b) $H = \left\{ \begin{pmatrix} x & y \\ 2y & x \end{pmatrix} \mid x; y \in \mathbb{Q}; x^2 + y^2 > 0 \right\}$ là một nhóm con của nhóm $(GL(2, \mathbb{Q}), .)$.

c) $U_n = \{z \in \mathbb{C} | z^n = 1\}$ với $n \in \mathbb{N}$; $U = \{z \in \mathbb{C} | \ \exists k \in \mathbb{N}^*, z^k = 1\}$ và $T = \{z \in \mathbb{C} | \ |z| = 1\}$ là các nhóm con của nhóm $(\mathbb{C}^*, .)$.

Bài 1.16 a) Chứng minh rằng H là một nhóm con của nhóm $(\mathbb{Z}, +)$ khi và chỉ khi H có dạng $n\mathbb{Z}$ với $n \in \mathbb{N}$.

b) Cho $m, n \in \mathbb{N}$. Chứng minh rằng

$$m\mathbb{Z} \cap n\mathbb{Z} = [m, n]\mathbb{Z} \quad \text{và} \quad m\mathbb{Z} + n\mathbb{Z} = (m, n)\mathbb{Z}.$$

Bài 1.17 Cho $(G, .)$ là một nhóm và H là một nhóm con của G. Chứng minh rằng với $x \in G$ các khẳng định sau là tương đương:

a) xH là nhóm con của G;

b) Hx là nhóm con của G;

c) $x \in H$.

Bài 1.18 Cho $(G, .)$ là một nhóm và H là một nhóm con của G. Chứng minh rằng với mỗi $x \in G$, tập hợp $x^{-1}Hx$ cũng là nhóm con của G (Ta gọi đây là các *nhóm con liên hợp* với H).

Bài 1.19 Cho nhóm $(G, .)$ và $a \in G$. Ta định nghĩa

1) *Tâm hóa tử* của a trong G là tập hợp

$$C(a) = \{x \in G | ax = xa\}.$$

2) *Tâm* của G là tập hợp

$$C(G) = \{x \in G | xy = yx, \forall y \in G\}.$$

Chứng minh rằng:

a) $C(G) \leq C(a) \leq G$;

b) $C(G) = \bigcap_{b \in G} C(b)$;

c) G giao hoán $\Leftrightarrow C(G) = G$.

d) Mọi nhóm con của $C(G)$ đều là nhóm con chuẩn tắc của G.

e) Tìm tâm của nhóm tuyến tính tổng quát $GL(n, \mathbb{R})$.

Bài 1.20 Cho H, K là các nhóm con của nhóm G. Chứng minh rằng $H \cup K$ là nhóm con của G khi và chỉ khi $H \subset K$ hay $K \subset H$.

Bài 1.21 Cho nhóm $(G, .)$. Với $A, B \subset G$, ta đặt

$$AB = \{ab | a \in A, b \in B\};$$

$$A^{-1} = \{a^{-1} | a \in A\}.$$

Chứng minh rằng với $A, B, C \subset G$:

a) $(AB)C = A(BC)$;

b) $(A^{-1})^{-1} = A$;

c) $(AB)^{-1} = B^{-1}A^{-1}$;

d) Với $A \neq \emptyset$ các khẳng định sau tương đương:

i) A là nhóm con của G;

ii) $AA = A$ và $A^{-1} = A$;

iii) $A^{-1}A = A$.

e) Nếu A, B là các nhóm con của G thì AB là nhóm con của G khi và chỉ khi $AB = BA$; hơn nữa khi đó $AB = A \vee B$, trong đó $A \vee B = \langle A \cup B \rangle$.

Bài 1.22 Cho $(G, .)$ là một nhóm Abel và H là một nhóm con của G. Với mỗi $n \in \mathbb{N}$ ta đặt

$$H_n = \{x \in G | \ x^n \in H\}.$$

Chứng minh rằng với $m, n \in \mathbb{N}$ ta có

a) H_n là nhóm con của G, và H_n chứa H.

b) $H_m \cap H_n = H_d$, trong đó $d = (m, n)$. Suy ra điều kiện để $H_m \cap H_n = H$.

Bài 1.23 Cho $(G, .)$ là một nhóm Abel và H là một nhóm con của G. Đặt

$$K = \{x \in G | \ \exists n \in \mathbb{N}^*, x^n \in H\}.$$

Chứng minh rằng

a) K là nhóm con chuẩn tắc của G, và K chứa H.

b) trong nhóm thương G/K không có phần tử nào có cấp hữu hạn lớn hơn 1.

Bài 1.24 Cho nhóm $(G, .)$ và H, K là hai nhóm con của G. Chứng minh rằng nếu H và K có chỉ số hữu hạn trong G thì nhóm con $H \cap K$ cũng có chỉ số hữu hạn trong G.

Bài 1.25 * Cho nhóm $(G, .)$ hữu hạn và H, K là hai nhóm con của G. Chứng minh rằng $|HK||H \cap K| = |H||K|$.

Bài 1.26 Chứng minh rằng trong nhóm hoán vị S_n, mọi k-chu trình đều có cấp k và cấp của tích các chu trình rời nhau bằng bội chung nhỏ nhất của các cấp của các chu trình nầy.

Bài 1.27 a) Hãy mô tả tất cả các phần tử có cấp 20 trong S_9.

b) Chứng minh rằng trong S_9 không tồn tại phần tử nào có cấp 18.

Bài 1.28 * Giả sử G là một nhóm con Abel có cấp 1111 trong S_{999}. Chứng minh rằng tồn tại $i \in \{1, 2, ..., 999\}$ sao cho $\sigma(i) = i, \forall \sigma \in G$.

Bài 1.29 Tìm hai phần tử a, b của một nhóm G sao cho a, b đều có cấp hữu hạn nhưng ab lại có cấp vô hạn.

Bài 1.30 Cho nhóm $(G, .)$ và $a, b \in G$. Chứng minh rằng

a) Cấp của ab bằng cấp của ba.

b) Cấp của a^{-1} bằng cấp của a.

c) Giả sử $ab = ba$ và a có cấp r, b có cấp s, trong đó r, s nguyên tố cùng nhau; khi đó ab có cấp rs.

d) Giả sử $ab = ba$ và a có cấp r, b có cấp s, trong đó $\langle a \rangle \cap \langle b \rangle = \{e\}$; khi đó ab có cấp $[r, s]$.

Bài 1.31 Chứng minh rằng nếu G là một nhóm có hơn một phần tử và chỉ có hai nhóm con là $\{e\}$ và G thì G phải là nhóm cyclic cấp nguyên tố.

Bài 1.32 Chứng minh rằng điều kiện cần và đủ để nhóm G chỉ có hữu hạn nhóm con là G hữu hạn.

Bài 1.33 Chứng minh:

a) Mọi nhóm cyclic đều giao hoán.

b) Mọi nhóm con của một nhóm cyclic cũng cyclic.

c) Ảnh đồng cấu của một nhóm cyclic cũng cyclic.

Bài 1.34 Cho nhóm cyclic $G = \langle x \rangle$ hữu hạn cấp n. Chứng minh rằng với $k, l \in \mathbb{Z}$ ta có

a) Cấp của x^k bằng n/d, trong đó $d = (n, k)$.

b) $\langle x^k \rangle = \langle x^l \rangle$ khi và chỉ khi $(n, k) = (n, l)$.

c) $G = \langle x^k \rangle$ khi và chỉ khi $(n, k) = 1$. Từ đó suy ra số các phần tử sinh của G.

d) Hãy mô tả tất cả các nhóm con của G.

Bài 1.35 Cho hai nhóm G_1 và G_2, trong đó mỗi nhóm có ít nhất hai phần tử. Chứng minh rằng nhóm $G_1 \times G_2$ cyclic khi và chỉ khi G_1 và G_2 là các nhóm cyclic hữu hạn có cấp nguyên tố cùng nhau.

Bài 1.36 Chỉ ra rằng quan hệ "chuẩn tắc" trên tập hợp các nhóm con không có tính bắc cầu.

Bài 1.37 Cho $(G, .)$ là một nhóm và H là một nhóm con của G. *Chuẩn hóa tử* của H trong G là tập con của G định bởi:

$$N_G(H) = \{x \in G | \ xH = Hx\}.$$

Chứng minh rằng

a) $N_G(H)$ là nhóm con của G.

b) H là nhóm con chuẩn tắc của $N_G(H)$.

c) H là nhóm con chuẩn tắc của G khi và chỉ khi $N_G(H) = G$.

d) $N_G(H)$ là nhóm con lớn nhất của G nhận H làm nhóm con chuẩn tắc.

Bài 1.38 Cho H, K là hai nhóm con của nhóm $(G, .)$. Chứng minh rằng:

a) Nếu H chuẩn tắc trong G thì HK là nhóm con của G.

b) Nếu H, K đều chuẩn tắc trong G thì HK là nhóm con chuẩn tắc của G.

Bài 1.39 Cho H, K là hai nhóm con chuẩn tắc của nhóm $(G, .)$ thỏa $H \cap K = \{e\}$. Chứng minh rằng $xy = yx$ với mọi $x \in H,\ y \in K$.

Bài 1.40 Cho nhóm $(G, .)$ và $S \subset G$ thỏa $x^{-1}Sx \subset \langle S \rangle$ với mọi $x \in G$. Chứng minh $\langle S \rangle$ chuẩn tắc trong G.

Bài 1.41 Cho G là một nhóm hữu hạn và H là một nhóm con của G có chỉ số $[G : H] = 2$. Chứng minh H là một nhóm con chuẩn tắc của G. Hãy tổng quát hóa kết quả trên.

Bài 1.42 a) Cho nhóm G với tâm là $C(G)$. Chứng minh rằng nhóm thương $G/C(G)$ cyclic khi và chỉ khi G giao hoán.

b) Dùng kết quả câu a) để chứng minh rằng mọi nhóm hữu hạn cấp p^2 với p nguyên tố đều giao hoán.

Bài 1.43 Cho nhóm $(G, .)$. Ta gọi *hoán tử* của hai phần tử x và y trong G là phần tử $[x, y] = x^{-1}y^{-1}xy$. Nhóm con của G sinh bởi tất cả các hoán tử của các phần tử trong G được gọi là *nhóm hoán tử* của G và được ký hiệu là $[G, G]$. Chứng minh rằng:

a) $[G, G]$ là nhóm con chuẩn tắc của G.

b) Với H là nhóm con chuẩn tắc của G, nhóm thương G/H giao hoán khi và chỉ khi $[G, G] \subset H$. Suy ra nhóm thương $G/[G, G]$ giao hoán.

Bài 1.44 Xét nhóm hoán vị S_4. Chứng minh rằng tập hợp

$$K = \{Id, (12)(34), (13)(24), (14)(23)\}$$

là nhóm con chuẩn tắc của G (Ta gọi K là nhóm Klein).

Bài 1.45 Chứng minh rằng:

a) Nhóm hoán vị S_n được sinh bởi các chuyển vị.

b) Nhóm thay phiên A_n là nhóm con chuẩn tắc của S_n và được sinh bởi các 3-chu trình.

c) Nếu H là một nhóm con chuẩn tắc của A_n và H có chứa ít nhất một 3-chu trình thì $H = A_n$.

Bài 1.46 Cho $(G, .)$ là một nhóm giao hoán. Chứng minh rằng ánh xạ $f : x \mapsto x^k$ với k là một số nguyên cho trước, là một đồng cấu nhóm. Hãy xác định $Kerf$.

Bài 1.47 Cho $(G, .)$ là một nhóm. Chứng minh rằng ánh xạ $x \mapsto x^{-1}$ là một tự đẳng cấu của nhóm G khi và chỉ khi G giao hoán.

Bài 1.48 Xét đồng cấu nhóm cộng $f : \mathbb{Z} \longrightarrow \mathbb{Z}$. Chứng minh rằng

a) Imf có dạng $n\mathbb{Z}$ với $n \in \mathbb{N}$;

b) $Kerf = \{0\}$ hoặc $Kerf = \mathbb{Z}$;

c) Tìm tất cả các tự đồng cấu của nhóm cộng $\mathbb{Z}$.

Bài 1.49 Xét đồng cấu nhóm cộng $f : \mathbb{Q} \longrightarrow \mathbb{Z}$.

a) Chứng minh rằng với $n \in \mathbb{N}^*$, $f(1) = nf(1/n)$.

b) Suy ra $f(1) = 0$ và f phải là đồng cấu tầm thường.

Bài 1.50 Hãy mô tả tất cả các tự đồng cấu $f : \mathbb{Z}_{12} \longrightarrow \mathbb{Z}_{12}$.

Bài 1.51 Cho G là một nhóm và $f : G \longrightarrow G$ là một ánh xạ xác định bởi $f(a) = a^{-1}, \forall a \in G$. Chứng minh rằng G abel khi và chỉ khi f là một đồng cấu.

Bài 1.52 Chứng minh rằng

a) Mọi nhóm cyclic hữu hạn cấp n đều đẳng cấu với nhóm $(\mathbb{Z}_n, +)$.

b) Mọi nhóm cyclic vô hạn đều dẳng cấu với nhóm $(\mathbb{Z}, +)$.

Bài 1.53 Chứng minh rằng tồn tại duy nhất (sai khác một đẳng cấu) một nhóm hữu hạn cấp 8 sinh bởi hai phần tử a, b thoả hệ thức

$$a^4 = e, \quad ba = a^{-1}b, \quad a^2 = b^2.$$

Nhóm này được gọi là *nhóm Quaternion*.

Hướng dẫn: Chứng minh sự tồn tại của Nhóm bằng cách xét nhóm con của nhóm $GL(2,\mathbb{C})$ sinh bởi hai ma trận $a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ và $b = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$.

Bài 1.54 Chứng minh rằng mọi nhóm con của nhóm quaternion đều chuẩn tắc.

Bài 1.55 Chứng minh rằng với mỗi số nguyên dương n tồn tại duy nhất (sai khác một đẳng cấu) một nhóm hữu hạn cấp $2n$ sinh bởi hai phần tử a, b thoả hệ thức

$$a^2 = e, \quad b^n = e, \quad ab = b^{-1}a.$$

Nhóm nầy được gọi là *nhóm nhị diện* D_n.

Hướng dẫn: Chứng minh sự tồn tại của Nhóm bằng cách xét nhóm con của nhóm $GL(2,\mathbb{C})$ sinh bởi hai ma trận $a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ và $b = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}$, trong đó ζ là một căn nguyên thủy bậc n của 1.

Bài 1.56 Chứng minh rằng trong nhóm nhị diện D_n với $n \geq 3$ nhóm con $\langle b \rangle$ chuẩn tắc nhưng nhóm con $\langle a \rangle$ thì không.

Bài 1.57 a) Cho G là một nhóm hữu hạn có cấp $|G| \leq 5$. Chứng minh G giao hoán.

b) Cho G là một nhóm hữu hạn có cấp 6. Chứng minh rằng nếu G giao hoán thì G là nhóm cyclic đẳng cấu với $\mathbb{Z}_6$; nếu G không giao hoán thì G đẳng cấu với nhóm nhị diện D_3.

Bài 1.58 Chứng minh rằng:

a) $GL(n,\mathbb{R})/SL(n,\mathbb{R}) \simeq \mathbb{R}^*$.

b) Nhóm thương $\mathbb{R}/\mathbb{Z}$ đẳng cấu với nhóm nhân T gồm các số phức có môđun bằng 1.

Bài 1.59 Cho nhóm cyclic $G = \langle x \rangle$ hữu hạn cấp n.

a) Với $f : G \longrightarrow G'$ là một đồng cấu nhóm, đặt $y = f(x)$. Chứng minh $y^n = e$, nghĩa là, y có cấp là một ước số của n.

b) Chứng minh rằng tương ứng $f \mapsto f(x)$ là một song ánh giữa tập các đồng cấu nhóm từ G vào G' và tập các phần tử y của G' có cấp là ước số của n.

Bài 1.60 Chứng minh rằng với đồng cấu $f : G \longrightarrow G'$ từ một nhóm hữu hạn G vào một nhóm G', ta có:

a) Cấp của $x \in G$ chia hết cho cấp của $f(x)$.

b) Cấp của G chia hết cho cấp của Imf.

Bài 1.61 Chứng minh rằng nhóm G' là ảnh đồng cấu của một nhóm cyclic hữu hạn G khi và chỉ khi G' là nhóm cyclic hữu hạn có cấp chia hết cho cấp G.

Bài 1.62 Ký hiệu $\mathbb{C}^*$ là nhóm nhân các số phức khác 0. Chứng minh rằng nếu H là nhóm con có chỉ số hữu hạn trong $\mathbb{C}^*$ thì $H = \mathbb{C}^*$.

Bài 1.63 Cho G_1, G_2 là hai nhóm với các phần tử đơn vị lần lượt là e_1, e_2. Xét tích trực tiếp $G = G_1 \times G_2$ và các tập con $H_1 = G_1 \times \{e_2\}$ và $H_2 = \{e_1\} \times G_2$. Chứng minh rằng

a) Các phép chiếu $p_j : G \longrightarrow G_j$ định bởi $p_j(x_1, x_2) = x_j$ là các toàn cấu nhóm và $Kerp_1 = H_2$; $Kerp_2 = H_1$. Suy ra H_j là nhóm con chuẩn tắc của G $(j = 1, 2)$.

b) Các phép nhúng $i_1 : G_1 \longrightarrow G$ định bởi $i_1(x_1) = (x_1, e_2)$ và $i_2 : G_2 \longrightarrow G$ định bởi $i_2(x_2) = (e_1, x_2)$ là các đơn cấu nhóm và $Imi_1 = H_1; Imi_2 = H_2$.

c) $G/H_1 \simeq H_2$ và $G/H_2 \simeq H_1$.

d) $G = H_1H_2$ và $H_1 \cap H_2 = \{(e_1, e_2)\}$.

Mở rộng kết quả trên cho tích trực tiếp $G_1 \times G_2 \times ... \times G_n$.

Bài 1.64 Cho nhóm $(G, .)$.

a) Chứng minh rằng tập hợp tất cả các tự đẳng cấu của G cùng với phép toán tích các ánh xạ là một nhóm. Ta ký hiệu nhóm nầy là $Aut(G)$.

b) Với mỗi $g \in G$, ánh xạ $\varphi_g : x \mapsto gxg^{-1}$ là một tự đẳng cấu của G. Ta gọi đây là các *tự đẳng cấu trong* của G.

c) Gọi $Int(G)$ là tập tất cả các tự đẳng cấu trong của G. Chứng minh rằng $Int(G)$ là một nhóm con chuẩn tắc của $Aut(G)$.

d) Chứng minh $G/C(G) \simeq Int(G)$, trong đó $C(G)$ là tâm của G.

Bài 1.65 Cho f là một đẳng cấu từ nhóm $(G, .)$ đến nhóm $(G', .)$.

a) Chứng minh rằng tương ứng $H \mapsto f(H)$ là một song ánh giữa tập hợp các nhóm con của G và của G'.

b) Chứng minh rằng tương ứng $H \mapsto f(H)$ là một song ánh giữa tập hợp các nhóm con chuẩn tắc của G và của G'.

c) Giả sử H là một nhóm con chuẩn tắc của G. Chứng minh rằng tương ứng $xH \mapsto f(x)f(H)$ là một đẳng cấu từ nhóm thương G/H đến nhóm thương $G'/f(H)$.

Bài 1.66 Xét ánh xạ $f : \mathbb{Z} \mapsto \mathbb{Z}$ định bởi $f(x) = nx$, trong đó $n \in \mathbb{N}^*$ cho trước. Chứng minh rằng:

a) f là một đồng cấu nhóm cộng. Tìm Imf và $Kerf$.

b) f là một đẳng cấu nhóm cộng từ $\mathbb{Z}$ đến $n\mathbb{Z}$. Từ đó, hãy mô tả tất cả các nhóm con của nhóm $n\mathbb{Z}$.

c) Với $m \in \mathbb{N},\ \mathbb{Z}/m\mathbb{Z} \simeq n\mathbb{Z}/mn\mathbb{Z}$.

Bài 1.67 Cho $(G,.)$ là một nhóm hữu hạn cấp n. Chứng minh rằng ánh xạ $x \mapsto f_x$, trong đó f_x thuộc nhóm hoán vị $S(G)$ của G định bởi $f_x(y) = xy$ với mọi $y \in G$, là một đơn cấu từ nhóm G vào nhóm $S(G)$. Từ đó suy ra rằng mọi nhóm hữu hạn đều là nhóm con (sai khác một đẳng cấu) của các nhóm hoán vị.

Bài 1.68 Cho G, G' lần lượt là hai nhóm cyclic hữu hạn cấp m và n với các phần tử sinh lần lượt là x và y. Xét tương ứng $f : G \longrightarrow G'$ định bởi $f(x^k) = y^{kl}$ với mọi $k \in \mathbb{N}$, trong đó $l \in \mathbb{N}^*$ cho trước.

a) Chứng minh rằng f là một đồng cấu nhóm khi và chỉ khi ml chia hết cho n.

b) f là một đẳng cấu nhóm khi và chỉ khi $m = n$ và $(m, l) = 1$.

c) Áp dụng tìm tất cả các đồng cấu từ nhóm cyclic cấp 8 đến nhóm cyclic cấp 12 và từ nhóm cyclic cấp 12 đến nhóm cyclic cấp 8.

d) Áp dụng tìm tất cả các tự đẳng cấu của nhóm cyclic cấp 8.

Bài 1.69 a) Cho nhóm $(G,.)$ và $G_1, G_2, ..., G_n$ là các nhóm con chuẩn tắc của G thoả các điều kiện sau:

$$G = G_1G_2...G_n \quad \text{và} \quad G_i \cap (G_1...G_{i-1}G_{i+1}...G_n) = \{e\}, \forall 1 \leq i \leq n.$$

Chứng minh rằng

i) Mọi phần tử $x \in G$ được viết duy nhất dưới dạng $x = x_1x_2...x_n$ trong đó $x_i \in G_i, \forall 1 \leq i \leq n$.

ii) G đẳng cấu với nhóm tích trực tiếp $G_1 \times G_2 \times ... \times G_n$.

Ta nói G là một *nội tích trực tiếp* của các nhóm con $G_i, 1 \leq i \leq n$.

b) Chứng minh rằng nếu nhóm $(G,.)$ đẳng cấu với tích trực tiếp của những nhóm con $H_i, 1 \leq i \leq n$ thì trong G sẽ tồn tại các nhóm con

G_i đẳng cấu với H_i sao cho G là nội tích trực tiếp của các nhóm con $G_i, 1 \leq i \leq n$.

Bài 1.70 Chứng minh rằng mọi nhóm hữu hạn cấp p^2 với p nguyên tố hoặc đẳng cấu với nhóm $\mathbb{Z}_{p^2}$ hoặc đẳng cấu với nhóm $\mathbb{Z}_p \times \mathbb{Z}_p$.

Chương II
VÀNH VÀ TRƯỜNG

§1. Khái niệm về vành

1.1. Định nghĩa

Vành là một tập hợp R cùng với hai phép toán cộng và nhân thỏa các tính chất sau:

(R_1) $(R,+)$ là nhóm Abel;

(R_2) $(R,.)$ là nửa nhóm;

(R_3) Phép nhân phân phối đối với phép cộng, nghĩa là với mọi $x,y,z \in R$, ta có

$$x(y+z) = xy + xz;$$

$$(y+z)x = yx + zx.$$

Phần tử trung hòa của phép cộng được gọi là *phần tử không*, ký hiệu là 0; phần tử đối xứng của phần tử $x \in R$ là *phần tử đối* của x ký hiệu là $-x$. Nếu phép nhân giao hoán thì ta nói vành R *giao hoán*; nếu phép nhân có phần tử đơn vị thì vành R được gọi là *vành có đơn vị*. Phần tử đơn vị được ký hiệu là e hay 1.

1.2. Nhận xét

Cho R là vành có đơn vị e. Phần tử $x \in R$ được gọi là khả nghịch nếu x khả đối xứng với phép nhân, nghĩa là tồn tại $y \in R$ sao cho $xy = yx = e$. Ký hiệu

$$R^* = \{x \in R | \, x \text{ khả nghịch}\}.$$

Khi đó R^* là một nhóm đối với phép nhân, gọi là *nhóm các phần tử khả nghịch* của R.

1.3. Ví dụ

1) Tập hợp các số nguyên $\mathbb{Z}$ với phép cộng và phép nhân thông thường là vành giao hoán, có đơn vị, gọi là *vành các số nguyên*. Tương tự ta cũng có *vành các số hữu tỷ* $\mathbb{Q}$, *vành các số thực* $\mathbb{R}$, *vành các số phức* $\mathbb{C}$.

2) Trên nhóm cộng $\mathbb{Z}_n$ các số nguyên modulo n, ta định nghĩa phép toán nhân như sau: với mọi $\overline{x}$, $\overline{y} \in \mathbb{Z}_n$, $\overline{x}\ \overline{y} = \overline{xy}$. Khi đó $\mathbb{Z}_n$ trở thành vành giao hoán có đơn vị $\overline{1}$.

3) Tập $M(n, \mathbb{R})$ các ma trận vuông cấp n với hệ số thực cùng với phép cộng và nhân ma trận thông thường là vành có đơn vị. Vành này không giao hoán nếu $n \geq 2$.

4) Cho $(G, +)$ là một nhóm Abel. Tập hợp $End(G)$ các tự đồng cấu của nhóm G là vành có đơn vị với phép cộng định bởi:

$$(f + g)(x) = f(x) + g(x), \forall f,\ g \in End(G), \forall x \in G,$$

và phép nhân là phép hợp nối ánh xạ. Vành này không giao hoán nếu $|G| \geq 2$.

5) Giả sử $R_1,\ R_2, \cdots, R_n$ là các vành. Khi đó tích Descartes

$$\prod_{i=1}^{n} R_i = \{(x_1, x_2, \cdots, x_n) | x_1 \in R_1, x_2 \in R_2, \cdots, x_n \in R_n\}$$

cùng với phép cộng $(x_i)+(y_i) = (x_i+y_i)$ và phép nhân $(x_i)(y_i) = (x_i y_i)$, là một vành, gọi là *vành tích trực tiếp* của $R_1, R_2, \cdots, R_n$. Hiển nhiên

nếu mọi vành R_i đều giao hoán (tương ứng, có đơn vị) thì vành tích trực tiếp cũng giao hoán (tương ứng, có đơn vị).

Từ Định nghĩa 1.1 ta có mệnh đề sau :

1.4. Mệnh đề. *Cho R là một vành. Khi đó với mọi $x, y, z \in R$ và $n \in \mathbb{Z}$ ta có*

(i) $x(y-z) = xy - xz$ *và* $(y-z)x = yx - zx$.

(ii) $0x = x0 = 0$.

(iii) $x(-y) = (-x)y = -(xy)$ *và* $(-x)(-y) = xy$.

(iv) $(nx)y = x(ny) = n(xy)$. *Đặc biệt, nếu R có đơn vị e thì* $nx = (ne)x = x(ne)$.

Chứng minh. (i) Do tính phân phối của phép nhân đối với phép cộng ta có

$$xy = x[(y-z)+z] = x(y-z) + xz.$$

Suy ra $x(y-z) = xy - xz$. Đẳng thức còn lại được chứng minh tương tự.

(ii) Do (i) ta có $0x = (y-y)x = yx - yx = 0$. Tương tự $x0 = 0$.

(iii) Từ (i) và (ii) ta có $x(-y) = x(0-y) = x0 - xy = -xy$. Tương tự $(-x)y = -(xy)$. Hơn nữa, $(-x)(-y) = -(-xy) = xy$.

(iv) Ta chứng minh $(nx)y = n(xy)$. Với $n = 0$, đẳng thức hiển nhiên đúng. Xét $n > 0$, ta có

$$(nx)y = (x + x + \cdots + x)y = xy + xy + \cdots + xy = n(xy).$$

Với $n < 0$, đặt $m = -n > 0$, ta có

$$(nx)y = [m(-x)]y = m[(-x)y] = m(-xy) = (-m)(xy) = n(xy).$$

Vậy $(nx)y = n(xy)$ với mọi $n \in \mathbb{Z}$. Tương tự $x(ny) = n(xy)$.

Nếu R có đơn vị thì $nx = n(ex) = (ne)x$. Tương tự, $nx = x(ne)$. ■

§2. Vành con, Ideal và vành thương

2.1. Định nghĩa

Cho R là một vành.

(i) Tập con A khác rỗng của R được gọi là một *vành con* của R nếu A ổn định đối với hai phép toán trong vành R và A cùng với hai phép toán cảm sinh là một vành.

(ii) Vành con I của R được gọi là một *ideal trái* (tương ứng, *ideal phải*) của R nếu với mọi $r \in R$ và $x \in I$ ta có $rx \in I$ (tương ứng, $xr \in I$). Ta nói I là một *ideal* của R nếu I vừa là ideal trái vừa là ideal phải của R.

2.2. Định lý (Đặc trưng của vành con). *Cho A là một tập con khác rỗng của vành R. Các mệnh đề sau tương đương:*

(i) A là một vành con của R;

(ii) Với mọi $x, y \in A$, $x + y \in A$, $xy \in A$, $-x \in A$;

(iii) Với mọi $x, y \in A$, $x - y \in A$ và $xy \in A$.

Chứng minh. $(i) \Rightarrow (ii)$. Vì A là một vành con của R nên A ổn định đối với phép cộng và phép nhân, nghĩa là $x + y \in A$, và $xy \in A$. Mặt khác, do $(A, +)$ là một nhóm con của $(R, +)$ nên $-x \in A$.

$(ii) \Rightarrow (iii)$. Với mọi $x, y \in A$, ta có $x, (-y) \in A$ nên $x - y = x + (-y) \in A$.

$(iii) \Rightarrow (i)$. Từ giả thiết (iii), theo Định lý 5.3, Chương I. $(A, +)$ là nhóm con của $(R, +)$. Mặt khác, các phép toán cảm sinh cũng có tính chất kết hợp và phân phối nên A là một vành, nghĩa là A là một vành con của R. ■

2.3. Định lý (Đặc trưng của ideal). *Cho I là một tập con khác rỗng của vành R. Các mệnh đề sau tương dương:*

(i) I là một ideal của R;

(ii) Với mọi $x, y \in I$ và $r \in R, x + y \in I$, $-x \in I$, $rx \in I$ và $xr \in I$;

(iii) Với mọi $x, y \in I$ và $r \in R$, $x - y \in I, xr \in I$ và $rx \in I$.

Chứng minh. Dựa vào Định lý 2.2 và Định nghĩa 2.1. ■

2.4. Nhận xét

1) Các tập con $\{0\}$ và R đều là các ideal của R, gọi là các *ideal tầm thường*.

2) Nếu vành R giao hoán thì các khái niệm ideal trái, ideal phải và ideal là trùng nhau.

3) Giả sử R là vành có đơn vị và I là một ideal trái hay phải của R. Khi đó $I = R \Leftrightarrow I$ chứa ít nhất một phần tử khả nghịch $\Leftrightarrow I$ chứa phần tử đơn vị.

4) Với $I,\ J$ là hai ideal của R, đặt

$$I + J = \{x + y | x \in I,\ y \in J\};$$

$$IJ = \{\sum_{i=1}^{n} x_i y_i | x_i \in I,\ y_i \in J,\ n \in \mathbb{N}^*\}.$$

Khi đó $I + J$ và IJ cũng là các ideal của R, gọi là *tổng* và *tích* của các ideal I và J.

2.5. Ví dụ

1) I là ideal của $\mathbb{Z}$ khi và chỉ khi I có dạng $n\mathbb{Z}$ với $n \in \mathbb{Z}$.

2) $M(n, \mathbb{Z})$ là vành con của $M(n, \mathbb{Q})$ nhưng không là ideal.

3) $M(n, 2\mathbb{Z})$ là ideal của $M(n, \mathbb{Z})$.

Từ Định nghĩa 2.1 ta thấy giao của một họ khác rỗng các vành con (tương ứng, ideal) của một vành R cũng là một vành con (tương ứng, ideal) của vành R.

Giả sử S là một tập con của vành R. Khi đó S chứa trong ít nhất một vành con (tương ứng, ideal) của R, chẳng hạn $S \subset R$. Giao của tất cả các vành con (tương ứng, ideal) của R có chứa S là một vành con (tương ứng, ideal) của R có chứa S. Ta có định nghĩa sau:

2.6. Định nghĩa

Cho S là một tập con khác rỗng của vành R. Ta định nghĩa:

(i) Giao của tất cả các vành con của R có chứa S là vành con *sinh bởi* S.

(ii) Giao của tất cả các ideal của R có chứa S là *ideal sinh bởi* S, ký hiệu là $\langle S\rangle$.

Từ định nghĩa ta thấy vành con (tương ứng, ideal) của R sinh bởi tập hợp S chính là vành con (tương ứng, ideal) nhỏ nhất của R có chứa S. Đặc biệt $\{0\}$ là vành con và cũng là ideal sinh bởi tập rỗng. Mệnh đề sau đây mô tả vành con và ideal sinh bởi các tập hợp khác rỗng.

2.7. Định lý. *Cho S là một tập con khác rỗng của vành R. Khi đó*

(i) Vành con của R sinh bởi S là tập hợp

$$\Big\{ \sum_{\text{hữu hạn}} s_1 s_2 \cdots s_n | s_i \in S \text{ hay } -s_i \in S,\ n \in \mathbb{N}^* \Big\}.$$

(ii) Nếu R có đơn vị thì ideal sinh bởi S là tập hợp

$$\langle S\rangle = \Big\{ \sum_{i=1}^{n} x_i s_i y_i | x_i,\ y_i \in R, s_i \in S, n \in \mathbb{N}^* \Big\}.$$

(iii) Nếu R giao hoán có đơn vị thì

$$\langle S\rangle = \Big\{ \sum_{i=1}^{n} x_i s_i | x_i \in R,\ s_i \in S,\ n \in \mathbb{N}^* \Big\}.$$

Chứng minh. Ta chứng minh (ii). Các phần còn lại hoàn toàn tương tự và chúng tôi dành cho độc giả. Đặt

$$I = \left\{ \sum_{i=1}^{n} x_i s_i y_i | x_i,\ y_i \in R, s_i \in S, n \in \mathbb{N}^* \right\},$$

ta có $S \subset I$ vì mọi phần tử $s \in S$ đều được viết dưới dạng $s = ese \in I$. Hơn nữa, do cách đặt I, theo Định lý 2.3 ta có ngay I là ideal của R. Mặt khác, mọi ideal chứa S đều chứa tất cả các phần tử có dạng

$$\sum_{i=1}^{n} x_i s_i y_i \ (x_i,\ y_i \in R, s_i \in S)$$

nên phải chứa I. Điều này cho thấy I là ideal nhỏ nhất của R có chứa S, nghĩa là $I = \langle S \rangle$. ■

2.8. Định nghĩa

Cho S là một tập con của vành R và $I = \langle S \rangle$. Ta nói I *được sinh ra bởi* S và S là *tập sinh* của I. Nếu S hữu hạn thì ta nói I *hữu hạn sinh*. Đặc biệt, nếu $S = \{a\}$ thì ta viết $I = \langle a \rangle$, gọi là *ideal chính sinh bởi* a.

2.9. Nhận xét

Nếu vành R giao hoán, có đơn vị thì ideal chính sinh bởi a là:

$$\langle a \rangle = \{xa | x \in R\}.$$

Ta còn ký hiệu tập hợp trên là Ra.

Xét vành $(R, +, .)$ và I là một ideal tùy ý của R. Vì phép cộng giao hoán nên nhóm con $(I, +)$ chuẩn tắc trong $(R, +)$ và ta có thể lập được nhóm thương $(R/I, +)$. Định lý sau đây cho thấy ta có thể trang bị cho $(R, +)$ một phép toán nhân để nó trở thành một vành.

2.10. Định lý. *Giả sử I là một ideal của vành $(R, +, .)$. Trên nhóm thương $(R/I, +)$ ta định nghĩa phép toán nhân như sau:*

$$(x + I)(y + I) = xy + I.$$

Khi đó $(R/I, +, .)$ là một vành, gọi là vành thương của R trên ideal I.

Chứng minh. Trước hết ta chứng minh phép toán nhân được xác định. Thật vậy, giả sử $x + I = x' + I$ và $y + I = y' + I$, nghĩa là $x - x' \in I$ và $y - y' \in I$, hay $x = x' + a$ và $y = y' + b$ với $a, b \in I$ nào đó. Khi đó

$$xy = (x' + a)(y' + b) = x'y' + x'b + ay' + ab.$$

Chú ý rằng $x'b$, ay' và ab đều thuộc I vì I là ideal của vành R. Do đó $xy - x'y' \in I$ hay $xy + I = x'y' + I$. Như vậy phép nhân trên R/I được xác định. Do phép nhân trên R có tính kết hợp và phân phối đối với phép cộng nên dễ thấy phép nhân trên R/I được định nghĩa như trên cũng có tính chất kết hợp và phân phối đối với phép cộng. Điều này chứng tỏ $(R/I, +, .)$ là một vành. ■

2.11. Nhận xét

1) Nếu vành R giao hoán thì vành thương R/I cũng giao hoán. Chiều đảo lại không đúng.

2) Nếu vành R có đơn vị e thì vành thương R/I có đơn vị là $e + I$. Chiều đảo lại không đúng.

2.12. Ví dụ

Vành thương của vành các số nguyên $\mathbb{Z}$ trên ideal $n\mathbb{Z}$ chính là vành $\mathbb{Z}_n$ các số nguyên modulo n, trong đó ngoài phép cộng đã biết, ta có phép toán nhân định bởi

$$(x + n\mathbb{Z})(y + n\mathbb{Z}) = xy + n\mathbb{Z}.$$

Đây chính là vành mà ta đã xét trong ví dụ 1.3.

§3. Đồng cấu

3.1. Định nghĩa

Một ánh xạ f từ vành R vào vành R' được gọi là một *đồng cấu vành* nếu f bảo toàn các phép toán, nghĩa là với mọi $x, y \in R$,

$$f(x+y) = f(x) + f(y),$$

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

Một đồng cấu từ R vào R được gọi là một *tự đồng cấu* của R. Một đồng cấu đồng thời là đơn ánh, toàn ánh, song ánh được gọi lần lượt là *đơn cấu, toàn cấu, đẳng cấu*. Một tự đồng cấu song ánh được gọi là một *tự đẳng cấu*. Nếu tồn tại một đẳng cấu từ R vào R' thì ta nói R đẳng cấu với R', ký hiệu là $R \simeq R'$.

3.2. Ví dụ

1) Ánh xạ đồng nhất id_R của vành R là một tự đẳng cấu, gọi là *tự đẳng cấu đồng nhất* của R.

2) Giả sử A là một vành con của vành R. Khi đó ánh xạ bao hàm: $i_A : A \longrightarrow R$ định bởi $i_A(x) = x$ là một đơn cấu, gọi là *đơn cấu chính tắc*.

3) Giả sử I là một ideal của vành R. Khi đó ánh xạ $\pi : R \longrightarrow R/I$ định bởi $\pi(x) = x + I$ là một toàn cấu, gọi là *toàn cấu chính tắc*.

4) Giả sử R, R' là hai vành. Khi đó ánh xạ $f : R \longrightarrow R'$ định bởi $f(x) = 0_{R'}$ ($0_{R'}$ là phần tử không của vành R') là một đồng cấu, gọi là *đồng cấu tầm thường*.

5) Cho R là một vành có đơn vị và $a \in R$ khả nghịch. Khi đó ánh xạ $f : R \longrightarrow R$ định bởi $f(x) = axa^{-1}$ là một tự đẳng cấu của R. Thật vậy, dễ thấy f là một song ánh, hơn nữa f là đồng cấu vì

$$f(x+y) = a(x+y)a^{-1} = axa^{-1} + aya^{-1} = f(x) + f(y),$$

$$f(xy) = a(xy)a^{-1} = (axa^{-1})(aya^{-1}) = f(x)f(y);$$

vậy f là đẳng cấu.

6) Xét ánh xạ $f : \mathbb{Z}_6 \longrightarrow \mathbb{Z}_6$ định bởi $f(\overline{x}) = 4\overline{x}$. Khi đó f là đồng cấu vành vì

$$f(\overline{x} + \overline{y}) = f(\overline{x+y}) = 4(\overline{x+y}) = 4\overline{x} + 4\overline{y} = f(\overline{x}) + f(\overline{y}),$$

$$f(\overline{x}\ \overline{y}) = f(\overline{xy}) = 4\overline{xy} = 4\overline{x}\ \overline{y} + 12\overline{x}\ \overline{y} = 16\overline{x}\ \overline{y} = (4\overline{x})(4\overline{y}) = f(\overline{x})f(\overline{y}).$$

Từ Định nghĩa 3.1, lý luận tương tự như đối với đồng cấu nhóm ta thấy đồng cấu vành có các tính chất sau:

3.3. Mệnh đề. *Nếu $f : R \longrightarrow R'$ là một đồng cấu vành thì $f(0_R) = 0_{R'}$ và $f(-x) = -f(x)$ với mọi $x \in R$.*

3.4. Mệnh đề. *Tích của hai đồng cấu vành là một đồng cấu vành. Đặc biệt, tích của hai đơn cấu (tương ứng, toàn cấu, đẳng cấu) vành cũng là đơn cấu (tương ứng, toàn cấu, đẳng cấu) vành.*

3.5. Mệnh đề. *Ánh xạ ngược của một đẳng cấu vành cũng là đẳng cấu vành.*

3.6. Chú ý

Do các mệnh đề 3.4 và 3.5 ta thấy quan hệ đẳng cấu $\simeq$ giữa các vành là một quan hệ tương đương, nghĩa là thỏa ba tính chất: phản xạ, đối xứng và bắc cầu.

3.7. Định lý. *Cho đồng cấu vành $f : R \to R'$ và A là một vành con của R, A' là một vành con của R'. Khi đó*

(i) $f(A)$ là một vành con của R'.

(ii) $f^{-1}(A')$ là một vành con của R. Hơn nữa, nếu A' là một ideal của R' thì $f^{-1}(A')$ cũng là ideal của R.

Đặc biệt, $\mathrm{Im}f = f(R)$ là vành con của R' và $\mathrm{Ker}f = f^{-1}(0_{R'})$ là ideal của R. Ta gọi $\mathrm{Im}f$ là ảnh của f và $\mathrm{Ker}f$ là hạt nhân của f.

Chứng minh. (i) Vì $(A, +) \leq (R, +)$ nên theo Định lý 8.7, Chương I, $f(A)$ là nhóm con của nhóm cộng R'. Mặt khác, với mọi $x', y' \in f(A)$, tồn tại $x, y \in A$ sao cho $f(x) = x'$, $f(y) = y'$ nên $x'y' = f(x)f(y) = f(xy) \in f(A)$. Điều này chứng tỏ $f(A)$ là vành con của R'.

(ii) Vì $(A', +) \leq (R', +)$ nên theo Định lý 8.7, Chương I, $f^{-1}(A')$

là nhóm con của nhóm cộng R. Mặt khác, với mọi $x, y \in f^{-1}(A')$, $f(x),\ f(y) \in A'$ nên $f(xy) = f(x)f(y) \in A'$, nghĩa là $xy \in f^{-1}(A')$. Điều này chứng tỏ $f^{-1}(A')$ là vành con của R. Giả sử A' là một ideal của R'. Khi đó theo chứng minh trên $f^{-1}(A')$ là vành con của R; hơn nữa với mọi $r \in R$ và $x \in f^{-1}(A')$ ta có $f(rx) = f(r)f(x) \in A'$ (do $f(x) \in A'$ và A' là ideal của R'), nghĩa là $rx \in f^{-1}(A')$; tương tự $xr \in f^{-1}(A')$. Điều này chứng tỏ $f^{-1}(A')$ là ideal của R.

Cuối cùng, nhận xét rằng R là vành con của R và $\{0_{R'}\}$ là ideal của R' nên theo kết quả trên ta có khẳng định sau cùng trong định lý. ■

Theo lý thuyết ánh xạ, hiển nhiên một đồng cấu vành $f : R \longrightarrow R'$ là toàn cấu khi và chỉ khi $Imf = R'$. Mặt khác, do mọi đồng cấu vành đều thỏa tính chất của đồng cấu nhóm cộng nên từ Định lý 8.8, Chương I, ta có định lý sau:

3.8. Định lý. *Đồng cấu vành $f : R \longrightarrow R'$ là đơn cấu khi và chỉ khi* $\mathrm{Ker}f = \{0_R\}$.

Tương tự như trong lý thuyết nhóm ta cũng có các định lý đẳng cấu vành như sau:

3.9. Định lý đẳng cấu 1. *Cho đồng cấu vành $f : R \longrightarrow R'$. Khi đó ánh xạ $\overline{f} : R/\mathrm{Ker}f \longrightarrow R'$ định bởi $\overline{f}(x + \mathrm{Ker}f) = f(x)$ là đơn cấu vành. Đặc biệt,* $R/\mathrm{Ker}f \simeq \mathrm{Im}f$.

Chứng minh. Theo Định lý 3.7 $\mathrm{Ker}f$ là ideal của R nên ta lập được vành thương $R/\mathrm{Ker}f$. Theo Định lý 8.9, Chương I, $\overline{f}$ là đơn cấu nhóm cộng. Ta chỉ cần kiểm chứng $\overline{f}$ bảo toàn phép nhân. Thật vậy, đặt $I = kerf$, khi đó với mọi $x, y \in R$, ta có

$$\overline{f}((x+I)(y+I)) = \overline{f}(xy+I) = f(xy) = f(x)f(y) = \overline{f}(x+I)\overline{f}(y+I)$$

Điều này chứng tỏ $\overline{f}$ là đơn cấu vành. ■

3.10. Định lý đẳng cấu 2. *Cho R là một vành và I là một ideal, A là một vành con của R. Khi đó $I + A$ là vành con của R; I là ideal của $I + A$; $I \cap A$ là ideal của A và $A/I \cap A \simeq (I + A)/I$ qua đẳng cấu vành $x + I \cap A \mapsto x + I$.*

Chứng minh. Đối với phép cộng, I và A đều là các nhóm con của nhóm

R nên theo Định lý 8.10, Chương I, $I + A$ là nhóm con của nhóm R. Mặt khác, với mọi $x, x' \in I$ và $a, a' \in A$ ta có

$$(x + a)(x' + a') = (xx' + xa' + ax') + aa' \in I + A$$

nên $I + A$ là vành con của R. Khẳng định I là ideal của $I + A$ và $I \cap A$ là ideal của A được suy ra từ giả thiết I là một ideal của R. Theo Định lý 8.10, Chương I, ta đã biết, ánh xạ $f : A/I \cap A \longrightarrow (I + A)/I$ định bởi $f(x + I \cap A) = x + I$ là đẳng cấu nhóm cộng. Mặt khác, f cũng bảo toàn phép toán nhân vì với mọi $x, y \in A$, ta có

$$\begin{aligned} f((x + I \cap A)(y + I \cap A)) &= f(xy + I \cap A) \\ &= xy + I \\ &= (x + I)(y + I) \\ &= f(x + I \cap A)f(y + I \cap A). \end{aligned}$$

Điều này chứng tỏ f là đẳng cấu vành. ■

3.11. Định lý đẳng cấu 3. *Cho R là một vành và I là một ideal của R. Khi đó*

(i) $\mathcal{A}$ là một vành con của vành thương R/I khi và chỉ khi $\mathcal{A}$ có dạng A/I với A là một vành con của R và A chứa I.

(ii) $\mathcal{A}$ là một ideal của vành thươngR/I khi và chỉ khi $\mathcal{A}$ có dạng A/I với A là một ideal của R và A chứa I. Hơn nữa, ta có

$$(R/I)/(A/I) \simeq R/A$$

qua đẳng cấu

$$(x + I) + (A/I) \mapsto x + A.$$

Chứng minh. Vì mọi vành con của vành R đều là nhóm con của nhóm cộng R nên theo Định lý 8.11, Chương I, mọi vành con của $\mathcal{A}$ của R/I đều có dạng A/I với A là nhóm con của nhóm cộng R và A chứa I. Mặt khác, dễ kiểm chứng rằng $\mathcal{A}$ là vành (tương ứng, ideal) của R/I khi và chỉ khi A là vành con (tương ứng, ideal) của R. Như vậy, khi $\mathcal{A} = A/I$ là ideal của vành thương R/I, ta lập được các vành thương $(R/I)/(A/I)$ và R/A. Theo Định lý 8.11, Chương I, ánh xạ từ $(R/I)/(A/I)$ vào R/A được xác định bởi $(x + I) + (A/I) \mapsto x + A$ là đẳng cấu nhóm cộng.

Mặt khác, lý luận tương tự như trong chứng minh của các Định lý 3.9 và 3.10 ta thấy ánh xạ trên cũng bảo toàn phép nhân và do đó cũng là đẳng cấu vành. ■

3.12. Ví dụ

Xét đồng cấu vành $f : \mathbb{Z}_6 \longrightarrow \mathbb{Z}_6$ định bởi $f(\overline{x}) = 4\overline{x}$ (xem Ví dụ 3.2), ta có

$\mathrm{Im}f = 4\mathbb{Z}_6 = 2\mathbb{Z}_6 = \{2\overline{x} | \overline{x} \in \mathbb{Z}_6\}$;

$\mathrm{Ker}f = \{\overline{x} \in \mathbb{Z}_6 | 4\overline{x} = \overline{0}\} = \{\overline{x} \in \mathbb{Z}_6 | 4x \equiv 0(\mod 6)\} = \{\overline{x} \in \mathbb{Z}_6 | x \equiv 0(\mod 3)\} = 3\mathbb{Z}_6$. Theo Định lý đẳng cấu 3.9 ta có

$$\mathbb{Z}_6/3\mathbb{Z}_6 \simeq 2\mathbb{Z}_6.$$

3.13. Bổ đề *Cho R là một vành giao hoán có đơn vị và I, J là hai ideal của R sao cho $I+J = R$. Khi đó $I \cap J = IJ$ và $R/I \cap J \simeq (R/I) \times (R/J)$ qua đẳng cấu $x + I \cap J \mapsto (x + I, x + J)$.*

Chứng minh. Hiển nhiên ta có $IJ \subset I$ và $IJ \subset J$ nên $IJ \subset I \cap J$. Mặt khác, vì $I + J = R$ nên có $a \in I$, $b \in J$ sao cho $a + b = e$. Do đó với $x \in I \cap J$ bất kỳ ta có $x = ax + bx \in IJ$ vì ax và bx đều thuộc IJ. Điều này chứng tỏ $I \cap J = IJ$. Xét ánh xạ $f : R \longrightarrow (R/I) \times (R/J)$ định bởi $f(x) = (x + I, x + J)$. Dễ dàng kiểm chứng rằng f là đồng cấu vành và $kerf = I \cap J = IJ$. Hơn nữa, f là toàn ánh, thật vậy, xét $(y + I, z + J) \in (R/I) \times (R/J)$ bất kỳ. Theo như trên, ta có $e = a + b$ với $a \in I$, $b \in J$. Đặt $x = az + by$. Khi đó $x + I = az + by + I = by + I = (b + I)(y + I) = (a + b + I)(y + I) = (e + I)(y + I) = y + I$. Tương tự, $x + I = z + J$. Do đó $f(x) = (y + I, z + J)$. Vậy f là toàn ánh. Áp dụng Định lý 3.9 ta được đẳng cấu $\overline{f} : R/I \cap J \longrightarrow (R/I) \times (R/J)$ định bởi $\overline{f}(x + IJ) \mapsto (x + I, x + J)$. ■

Bổ đề 3.13 được mở rộng thành định lý sau:

3.14. Định lý Dư số Trung hoa. *Cho R là một vành giao hoán có đơn vị và $I_1, I_2, \cdots, I_n$ là các ideal của R sao cho $I_i + I_j = R$ với mọi $i \neq j$.*

Khi đó

$$R/I_1I_2\cdots I_n \simeq \prod_{i=1}^{n}(R/I_i)$$

qua đẳng cấu $x + I_1I_2\cdots I_n \mapsto (x + I_i)$.

Chứng minh. Bổ đề 3.13 là trường hợp $n = 2$ của định lý. Ta chứng minh định lý bằng qui nạp theo n. Đặt $J = I_2\cdots I_n$. Ta có $I_1 + J = R$. Thật vậy, với $j \geq 2$ ta có $I_1 + I_j = R$ nên tồn tại $a_j \in I_1$ và $b_j \in I_j$ sao cho $a_j + b_j = e$. Do đó

$$e = (a_2 + b_2)\cdots(a_n + b_n) = a + b_2\cdots b_n,$$

trong đó a là tổng của các hạng tử có chứa ít nhất một a_i làm nhân tử nên $a \in I_1$. Mặt khác $b_2\cdots b_n \in J$ nên $e \in I_1 + J$ và do đó $I_1 + J = R$. Áp dụng Bổ đề 3.13 cho vành R với các ideal I_1 và J ta có đẳng cấu $R/I_1J \simeq (R/I_1) \times (R/J)$. Giả thiết quy nạp cho ta đẳng cấu

$$R/J = R/I_2\cdots I_n \simeq \prod_{i=2}^{n}(R/I_i).$$

Kết hợp các đẳng cấu trên ta được đẳng cấu

$$R/I_1I_2\cdots I_n \simeq \prod_{i=1}^{n}(R/I_i).$$

định bởi $x + I_1I_2\cdots I_n \mapsto (x + I_i)$. ■

3.15. Áp dụng

Xét vành các số nguyên $\mathbb{Z}$. Mọi ideal của $\mathbb{Z}$ đều có dạng $n\mathbb{Z}$ với $n \in \mathbb{N}$. Hơn nữa $m\mathbb{Z} + n\mathbb{Z} = (m, n)\mathbb{Z}$ và $m\mathbb{Z} \cap n\mathbb{Z} = [m, n]\mathbb{Z}$. Do đó $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$ khi và chỉ khi m, n nguyên tố cùng nhau và khi đó ta có $m\mathbb{Z} \cap n\mathbb{Z} = (mn)\mathbb{Z}$. Áp dụng Định lý 3.14 ta suy ra:

1) Nếu m, n là các số nguyên tố cùng nhau thì ta có đẳng cấu vành

$$\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n.$$

Từ đó ta có đẳng cấu nhóm

$$\mathbb{Z}_{mn}^* \simeq \mathbb{Z}_m^* \times \mathbb{Z}_n^*.$$

2) Nếu $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ là sự phân tích chính tắc của n thành các thừa số nguyên tố thì ta có đẳng cấu vành

$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \mathbb{Z}_{p_k^{\alpha_k}}.$$

Từ đó ta có đẳng cấu nhóm

$$\mathbb{Z}_n^* \simeq \mathbb{Z}_{p_1^{\alpha_1}}^* \times \mathbb{Z}_{p_2^{\alpha_2}}^* \times \cdots \mathbb{Z}_{p_k^{\alpha_k}}^*.$$

Cấp của nhóm $\mathbb{Z}_n^*$ chính là số các phần tử khả nghịch trong $\mathbb{Z}_n$ và bằng $\varphi(n)$ với φ là hàm Euler ($\varphi(n)$ cũng là số các số nguyên dương $k \leq n$ thỏa k nguyên tố cùng nhau với n). Các kết quả trên cho thấy hàm φ-Euler có các tính chất sau:

a) $\varphi(mn) = \varphi(m)\varphi(n)$ với mọi m, n nguyên tố cùng nhau;

b) $\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k})$ nếu $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

Chú ý rằng với p nguyên tố ta có $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ (Bài tập 2.34), nên nhờ các tính chất trên ta có thể tìm được biểu thức của $\varphi(n)$.

§4. Miền nguyên và trường

4.1 Định nghĩa

(i) Cho R là một vành giao hoán. Phần tử $x \in R \setminus \{0\}$ được gọi là *ước của* 0 nếu tồn tại $y \in R \setminus \{0\}$ sao cho $xy = 0$.

(ii) Một vành giao hoán, có đơn vị, có nhiều hơn một phần tử và không có ước của không được gọi là *miền nguyên*.

(iii) Một vành giao hoán, có đơn vị, có nhiều hơn một phần tử trong đó mọi phần tử khác 0 đều khả nghịch được gọi là một *trường*.

4.2. Nhận xét

1) Trong miền nguyên R, phép nhân có tính giản ước cho các phần tử khác không nghĩa là nếu $xy = xz$ và $x \neq 0$ thì $y = z$.

Thật vậy, từ $xy = xz$ ta suy ra $x(y-z) = xy-xz = 0$ từ đó $y-z = 0$, nghĩa là $y = z$ (do $x \neq 0$ và R không có ước của không).

2) Mọi trường R chỉ có hai ideal là $\{0\}$ và R.

3) $(R, +, .)$ là một trường khi và chỉ khi các tính chất sau đây được thỏa:

i) $(R, +)$ là nhóm Abel;

ii) $R \setminus \{0\}$ là nhóm Abel;

iii) Phép nhân phân phối với phép cộng.

4.3. Ví dụ

1) Tập các số nguyên $\mathbb{Z}$ với phép cộng và nhân thông thường là miền nguyên nhưng không là trường.

2) Tập hợp các số hữu tỷ $\mathbb{Q}$ với phép cộng và nhân thông thường là trường. Ta gọi đó là *trường các số hữu tỷ* $\mathbb{Q}$. Tương tự, ta có *trường các số thực* $\mathbb{R}$ và *trường các số phức* $\mathbb{C}$.

3) Vành $\mathbb{Z}_n$ các số nguyên modulo n là trường khi và chỉ khi $n = p$ nguyên tố (Bài tập 2.25).

4.4. Định lý. *(i) Mọi trường đều là miền nguyên.*

(ii) Mọi miền nguyên hữu hạn đều là trường.

Chứng minh. (i) Ta chỉ cần chứng minh rằng mọi trường R đều không có ước của không. Thật vậy, giả sử $xy = 0$ và $x \neq 0$. Khi đó x khả nghịch nên tồn tại $x^{-1} \in R$ sao cho $x^{-1}x = e$. Do đó $y = ey = x^{-1}xy = x^{-1}0 = 0$. Điều này chứng tỏ R không có ước của không và do đó R là miền nguyên.

(ii) Giả sử R là một miền nguyên hữu hạn. Cho $a \in R \setminus \{0\}$ bất kỳ.

Ta chứng minh a khả nghịch. Thật vậy, xét ánh xạ

$$\begin{array}{rccc} f: & R\setminus\{0\} & \longrightarrow & R\setminus\{0\} \\ & x & \longmapsto & ax \end{array}$$

Vì trong miền nguyên R phép nhân có tính giản ước nên ta thấy ngay f là đơn ánh. Theo giả thiết $R\setminus\{0\}$ hữu hạn nên f phải là song ánh. Suy ra tồn tại $b \in R\setminus\{0\}$ sao cho $f(b) = e$, nghĩa là $ab = e$. Điều này chứng tỏ a khả nghịch, và do đó R là trường. ■

4.5. Nhận xét

Giả thiết hữu hạn trong (ii) của Định lý 4.4 không thể bỏ được. Chẳng hạn $\mathbb{Z}$ là miền nguyên vô hạn nhưng không phải là trường.

4.6. Định nghĩa

Cho R là một trường và I là một tập con khác rỗng của R ổn định đối với hai phép toán trong R. Ta nói I là một *trường con* của R nếu I với hai phép toán cảm sinh từ R cũng là một trường.

4.7. Ví dụ

Trường các số hữu tỷ $\mathbb{Q}$ là trường con của trường các số thực $\mathbb{R}$. Tương tự, $\mathbb{R}$ là trường con của $\mathbb{C}$.

Từ Định nghĩa 4.6 ta suy ra ngay các tính chất đặc trưng của các trường con như sau:

4.8. Định lý (Đặc trưng của trường con). *Cho R là một trường và I là tập con của R có chứa ít nhất hai phần tử. Các mệnh đề sau tương đương:*

(i) I là một trường con của R;

(ii) Với mọi $x, y \in I$, $x + y \in I$, $xy \in I$, $-x \in I$ và hơn nữa, nếu $x \neq 0$ thì $x^{-1} \in I$;

(iii) Với mọi $x, y \in I$, $x - y \in I$ và hơn nữa, nếu $x \neq 0$ thì $x^{-1}y \in I$.

■

Xét R là một trường với phần tử đơn vị e. Trong nhóm cộng R,

phần tử đơn vị e hoặc có cấp hữu hạn hoặc có cấp vô hạn. Giả sử e có cấp hữu hạn là n. Khi đó n phải là số nguyên tố, vì nếu không thì có $1 < m,\ k < n$ sao cho $n = mk$ dẫn đến $0 = ne = (mk)e = (me)(ke)$, suy ra $me = 0$ hoặc $ke = 0$, mâu thuẫn với tính chất của cấp n. Vậy nếu e có cấp hữu hạn thì cấp đó phải là số nguyên tố. Trường hợp e có cấp vô hạn, ta nói R là trường có *đặc số* (hoặc *đặc trưng*) 0, ký hiệu là $\mathrm{char}R = 0$. Trường hợp e có cấp hữu hạn p, ta nói trường R có *đặc số* (hoặc *đặc trưng*) p, ký hiệu là $\mathrm{char}R = p$.

4.9. Ví dụ

1) Các trường số $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ đều có đặc số 0;

2) Với p nguyên tố, trường $\mathbb{Z}_p$ các số nguyên modulo p có đặc số p.

Các định lý sau nêu lên tính chất của đặc số của các trường:

4.10. Định lý. *Cho R là một trường. Các mệnh đề sau tương đương:*

(i) $\mathrm{char}R = 0$*;*

(ii) Với mọi $x \in R \setminus \{0\}$ *và* $n \in \mathbb{Z}$, *nếu* $nx = 0$ *thì* $n = 0$;

(iii) R *chứa một trường con đẳng cấu (vành) với* $\mathbb{Q}$.

Chứng minh. $(i) \Rightarrow (ii)$ Giả sử $\mathrm{char}R = 0$. Xét $x \in R \setminus \{0\}$ và $n \in \mathbb{Z}$ thỏa $nx = 0$. Khi đó $0 = nx = (ne)x$ và $x \neq 0$ nên $ne = 0$. Suy ra $n = 0$ (do $\mathrm{char}R = 0$).

$(ii) \Rightarrow (iii)$ Với giả thiết (ii), xét ánh xạ $f : \mathbb{Q} \longrightarrow R$ định bởi $f(mn^{-1}) = (me)(ne)^{-1}$. Ta thấy f được xác định và là đơn ánh vì

$$\begin{aligned} mn^{-1} = m'(n')^{-1} &\Leftrightarrow mn' - m'n = 0 \\ &\Leftrightarrow (mn' - m'n)e = 0 \text{ (do (ii))} \\ &\Leftrightarrow (me)(n'e) - (m'e)(ne) = 0 \\ &\Leftrightarrow (me)(ne)^{-1} - (m'e)(n'e)^{-1} = 0 \\ &\Leftrightarrow f(mn^{-1}) = f(m'(n')^{-1}). \end{aligned}$$

Hơn nữa, f bảo toàn các phép toán vì

$$\begin{aligned} f(mn^{-1}+m'(n')^{-1}) &= f((mn'+m'n)(nn')^{-1}) \\ &= [(mn'+m'n)e](nn'e)^{-1} \\ &= [(me)(n'e)+(m'e)(ne)](ne)^{-1}(n'e)^{-1} \\ &= (me)(ne)^{-1}+(m'e)(n'e)^{-1} \\ &= f(mn^{-1})+f(m'(n')^{-1}) \end{aligned}$$

và tương tự

$$f((mn^{-1})(m'(n')^{-1})) = f(mn^{-1})f(m'(n')^{-1}).$$

Vậy f là đơn cấu vành. Suy ra Imf là trường con của R đẳng cấu với $\mathbb{Q}$.

$(iii) \Rightarrow (i)$ Vì $\mathrm{char}\mathbb{Q} = 0$ nên trường con của R đẳng cấu với $\mathbb{Q}$ cũng có đặc số không. Do đó R cũng có đặc số không. ■

4.11. Định lý. *Cho R là một trường và p là một số nguyên tố. Các mệnh đề sau tương đương:*

(i) $\mathrm{char}R = p$;

(ii) Với mọi $x \in R \setminus \{0\}$ *và* $n \in \mathbb{Z}$, $nx = 0$ *khi và chỉ khi* $p|n$;

(iii) R *chứa một trường con đẳng cấu (vành) với* $\mathbb{Z}_p$.

Chứng minh. $(i) \Rightarrow (ii)$ Giả sử $\mathrm{char}R = p$. Xét $x \in R \setminus \{0\}$ và $n \in \mathbb{Z}$ thỏa $nx = 0$. Khi đó $0 = nx = (ne)x$ và $x \neq 0$ nên $ne = 0$. Từ đây do $\mathrm{char}R = p = |e|$ nên $p|n$. Đảo lại, nếu $p|n$ thì $nx = (ne)x = 0x = 0$.

$(ii) \Rightarrow (iii)$ Với giả thiết (ii), xét ánh xạ

$$f : \mathbb{Z} \longrightarrow R$$

định bởi $f(n) = ne$. Dễ thấy f là đồng cấu vành và $\mathrm{Ker}f = p\mathbb{Z}$. Do đó, theo Định lý 3.9 ta có

$$\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} \simeq \mathrm{Im}f$$

Chú ý rằng $\mathbb{Z}_p$ là trường do p nguyên tố (Bài tập 2.25), nên R chứa trường con $\mathrm{Im}f$ đẳng cấu với $\mathbb{Z}_p$.

$(iii) \Rightarrow (i)$ Vì $\mathrm{char}\mathbb{Z}_p = p$ nên trường con của R đẳng cấu với $\mathbb{Z}_p$ cũng có đặc trưng p. Do đó $\mathrm{char}R = p$. ■

4.12. Nhận xét

Cho R là một trường có đặc số p nguyên tố. Khi đó ánh xạ $\varphi : R \longrightarrow R$ định bởi $\varphi(x) = x^p$ là một tự đơn cấu của R. Thật vậy, với mọi $x,\ y \in R$ ta có

$$\varphi(xy) = (xy)^p = x^p y^p = \varphi(x)\varphi(y),$$

hơn nữa

$$\begin{aligned}
\varphi(x+y) &= (x+y)^p \\
&= x^p + \sum_{k=1}^{p-1} C_p^k x^{p-k} y^k + y^p \\
&= x^p + y^p \\
&= \varphi(x) + \varphi(y)
\end{aligned}$$

do $C_p^k = \dfrac{p!}{k!(p-k)!}$ là bội số của p (p nguyên tố) với mọi $1 \leq k \leq p-1$. Điều này chứng tỏ φ là đồng cấu. Mặt khác do $\mathrm{Ker}\varphi = 0$ nên φ là đơn cấu. ■

Xét R là một miền nguyên. Khi đó phép nhân trong R có tính giản ước cho các phần tử khác không. Tuy nhiên điều đó chưa đủ để khẳng định mọi phần tử khác không đều khả nghịch trong R. Ta sẽ xây dựng trường $\overline{R}$ nhỏ nhất có chứa R, trong đó mọi phần tử khác không của R đều khả nghịch trong $\overline{R}$. Ta gọi $\overline{R}$ là trường các thương của miền nguyên R.

4.13. Định nghĩa

Cho R là một miền nguyên và $\overline{R}$ là một trường. Ta nói $\overline{R}$ là *trường các thương* của miền nguyên R nếu tồn tại một đơn cấu (vành) $f : R \longrightarrow \overline{R}$ sao cho mọi phần tử của $\overline{R}$ đều có dạng $f(a)f(b)^{-1}$ với $a,\ b \in R,\ b \neq 0$.

4.14. Định lý. *Cho R là một miền nguyên. Khi đó trường các thương $\overline{R}$ của R luôn luôn tồn tại và duy nhất (sai khác một đẳng cấu).*

Chứng minh. *Sự tồn tại.* Đặt $D = R \setminus \{0\}$. Trên $R \times D$ xét quan hệ $(a,\, b) \sim (c,\, d) \Leftrightarrow ad = bc$. Khi đó, hiển nhiên $\sim$ có tính chất phản xạ và đối xứng. Ta chứng minh $\sim$ bắc cầu. Giả sử $(a,\, b) \sim (c,\, d)$ và $(c,\, d) \sim (u,\, v)$. Khi đó $ad = bc$ và $cv = du$ nên

$$d(av) = (bc)v = b(cv) = b(du) = d(bu).$$

Vì $d \neq 0$ nên $av = bu$, nghĩa là $(a,\, b) \sim (u,\, v)$. Vậy $\sim$ bắc cầu và do đó $\sim$ là quan hệ tương đương trên $R \times D$. Đặt $\overline{R} = (R \times D)/\sim$ là tập thương của $R \times D$ trên quan hệ $\sim$. Các phần tử của $\overline{R}$ là các lớp tương đương $\overline{(a,\, b)}$ mà ta ký hiệu là $\dfrac{a}{b}$. Trên $\overline{R}$ ta định nghĩa hai phép toán cộng và nhân như sau:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{và} \quad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

Ta chứng minh các phép toán trên được xác định. Thật vậy, giả sử $\dfrac{a}{b} = \dfrac{a'}{b'}$ và $\dfrac{c}{d} = \dfrac{c'}{d'}$. Khi đó $ab' = a'b$ và $cd' = c'd$ nên $(ad + bc)b'd' = ab'dd' + cd'bb' = a'bdd' + c'dbb' = (a'd' + b'c')bd$, hay $(ad + bc,\, bd) \sim (a'd' + b'c',\, b'd')$, nghĩa là $\dfrac{ad + bc}{bd} = \dfrac{a'd' + b'c'}{b'd'}$. Mặt khác, $(ac)(b'd') = (ab')(cd') = (a'b)(c'd) = (a'c')(bd)$ nên $(ac,\, bd) \sim (a'c',\, b'd')$, nghĩa là $\dfrac{ac}{bd} = \dfrac{a'c'}{b'd'}$. Vậy các phép toán cộng và nhân trên $\overline{R}$ được xác định. Dễ thấy rằng $(\overline{R},\, +)$ là nhóm Abel, trong đó phần tử không là $\dfrac{0}{e}$ và phần tử đối của $\dfrac{a}{b}$ là $\dfrac{-a}{b}$. Hơn nữa, $(\overline{R} \setminus \{0\}, .)$ là nhóm giao hoán với phần tử đơn vị là $\dfrac{e}{e}$ trong đó mọi phần tử $x = \dfrac{a}{b} \neq \dfrac{0}{e}$ đều có $a = ae - b0 \neq 0$ nên x có phần tử nghịch đảo $x^{-1} = \dfrac{b}{a}$.

Ngoài ra, bằng cách thử trực tiếp ta thấy phép nhân phân phối đối với phép cộng. Do đó $\overline{R}$ là trường. Xét ánh xạ $f : R \longrightarrow \overline{R}$ định bởi $f(a) = \dfrac{a}{e}$. Hiển nhiên f là đơn cấu vành. Với $x = \dfrac{a}{b} \in \overline{R}$ tùy ý ta có $x = \dfrac{a}{b} = \dfrac{a}{e}\dfrac{e}{b} = \dfrac{a}{e}\left(\dfrac{b}{e}\right)^{-1} = f(a)f(b)^{-1}$. Do đó $\overline{R}$ chính là trường các thươngcủa miền nguyên R.

Sự duy nhất. Giả sử ngoài $\overline{R}$ như đã xây dựng ở trên, R còn có trường các thương S với đơn cấu vành $g : R \longrightarrow S$ sao cho mọi phần tử trong S đều được viết dưới dạng $g(a)g(b)^{-1}$ với $a,\ b \in R,\ a \neq 0$. Xét ánh xạ $\varphi : \overline{R} \longrightarrow S$ định bởi

$$\varphi(f(a)f(b)^{-1}) = g(a)g(b)^{-1} \quad \text{với mọi } a,\ b \in R,\ b \neq 0.$$

Ta thấy φ được xác định và là đơn ánh vì $f(a)f(b)^{-1} = f(c)f(d)^{-1}$ $\Leftrightarrow f(a)f(d) = f(b)f(c) \Leftrightarrow f(ad) = f(bc) \Leftrightarrow ad = bc \Leftrightarrow g(ad) = g(bc)$ $\Leftrightarrow g(a)g(b)^{-1} = g(c)g(d)^{-1}$. Hiển nhiên φ là toàn ánh. Vậy φ là song ánh. Ta còn phải chứng minh φ là đồng cấu, nghĩa là bảo toàn các phép toán. Thật vậy, giả sử $x = f(a)f(b^{-1})$ và $y = f(c)f(d)^{-1}$, khi đó

$$\begin{aligned} x + y &= f(a)f(b^{-1}) + f(c)f(d)^{-1} \\ &= [f(a)f(d) + f(b)f(c)]f(b)^{-1}f(d)^{-1} \\ &= f(ad + bc)f(bd)^{-1}; \\ xy &= f(a)f(b)^{-1}f(c)f(d)^{-1} \\ &= f(ac)f(bd)^{-1} \end{aligned}$$

nên

$$\begin{aligned} \varphi(x + y) &= g(ad + bc)g(bd)^{-1} \\ &= [g(a)g(d) + g(b)g(c)]g(b)^{-1}g(d)^{-1} \\ &= g(a)g(b)^{-1} + g(c)g(d)^{-1} = \varphi(x) + \varphi(y); \\ \varphi(xy) &= g(ac)g(bd)^{-1} \\ &= g(a)g(c)g(b)^{-1}g(d)^{-1} \\ &= g(a)g(b)^{-1}g(c)g(d)^{-1} = \varphi(x)\varphi(y). \end{aligned}$$

Vậy φ là đồng cấu vành. Suy ra φ là đẳng cấu vành và $\overline{R} \simeq S$. Điều này chứng tỏ sự duy nhất (sai khác một đẳng cấu) của trường các thương của R.

4.15. Nhận xét

Vì ánh xạ $f : R \longrightarrow \overline{R}$ định bởi $f(a) = \dfrac{a}{e}$ là đơn cấu vành nên ta có thể đồng nhất $a \in R$ với $\dfrac{a}{e} \in \overline{R}$. Do đó có thể xem $\overline{R}$ như là một trường chứa miền nguyên R và mọi phần tử thuộc $\overline{R}$ đều có dạng $\dfrac{a}{b} = \dfrac{a}{e}(\dfrac{b}{e})^{-1} = ab^{-1}$ với $a,\ b \in R$ và $b \neq 0$. Rõ ràng mọi trường chứa miền nguyên R đều phải chứa các phần tử có dạng ab^{-1} như thế nên $\overline{R}$ là trường nhỏ nhất chứa R.

4.16. Ví dụ

Trường các số hữu tỷ $\mathbb{Q}$ chính là trường các thương của miền nguyên $\mathbb{Z}$ vì $\mathbb{Q} = \left\{\dfrac{a}{b} | a,\ b \in \mathbb{Z}\right\} = \{ab^{-1} | a, b \in \mathbb{Z}\}$.

Bài tập

Bài 2.1 Kiểm chứng các cấu trúc đại số sau có là vành; miền nguyên hay trường không:

a) $\mathcal{P}(X)$ với X là tập hợp khác rỗng, và hai phép toán tương ứng là Δ và $\cap$ (ở đây $A\Delta B = (A \setminus B) \cup (B \setminus A)$).

b) $\mathbb{Q}$ với hai phép toán $x \top y = x + y - 1$ và $x \perp y = x + y - xy$.

c) $\mathbb{R}^+$ với hai phép toán $x \top y = xy$ và $x \perp y = x^{lny}$.

d) $\mathbb{R}$ với hai phép toán $x \top y = \sqrt[n]{x^n + y^n}$ và $x \perp y = xy$ (n là một số nguyên dương lẻ) .

e) $\mathbb{R}$ với hai phép toán $x \top y = (\sqrt[n]{x} + \sqrt[n]{y})^n$ vài $x \perp y = xy$ (n là một số nguyên dương lẻ).

f) $\mathbb{Z}(\sqrt{2}) = \{a + b\sqrt{2} |\ a, b \in \mathbb{Z}$ với hai phép toán là phép cộng và nhân thông thường như trong $\mathbb{R}$.

g) $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} |\ a, b \in \mathbb{Q}\}$ với hai phép toán là phép cộng và nhân thông thường như trong $\mathbb{R}$.

h) $K = \left\{ \begin{pmatrix} a & b \\ 4b & a \end{pmatrix} |\ a, b \in \mathbb{Q} \right\}$ với hai phép toán là phép cộng và phép nhân ma trận thông thường.

i) Tập hợp A gồm tất cả các ma trận (tương ứng, ma trận chéo; ma trận tam giác trên; ma trận tam giác dưới; ma trận tam giác trên ngặt; ma trận tam giác dưới ngặt) vuông cấp $n \geq 2$ với hai phép toán là phép cộng và phép nhân ma trận thông thường.

j) $F = \left\{ \begin{pmatrix} a & b \\ 6b & a \end{pmatrix} |\ a, b \in \mathbb{Q} \right\}$ với hai phép toán là phép cộng và phép nhân ma trận thông thường.

k) $\mathbb{C} = \mathbb{R}^2$ với hai phép toán định bởi $(x, y) + (z, t) = (x + z, y + t)$ và $(x, y)(z, t) = (xz - yt, xt + yz)$.

Bài 2.2 Giả sử vành R có duy nhất một phần tử đơn vị trái. Chứng minh R có đơn vị.

Bài 2.3 Giải các phương trình

a) $21\overline{x} + \overline{24} = \overline{101}$ trong $\mathbb{Z}_{103}$.

b) $68(\overline{x} + \overline{24}) = \overline{102}$ trong $\mathbb{Z}_{492}$.

c) $78\overline{x} - \overline{13} = \overline{35}$ trong $\mathbb{Z}_{666}$.

Bài 2.4 Tìm tất cả các số nguyên n thỏa điều kiện trong mỗi trường hợp sau:

a) $27n - 18$ chia hết cho 133.

b) $92n + 18$ chia hết cho 100.

c) $95n - 15$ chia hết cho 335.

Bài 2.5 Cho R là một vành có tính chất sau:

$$x^2 = x \text{ với mọi } x \in R.$$

(Ta gọi R là *vành Bool*). Chứng minh rằng

a) $x = -x$ với mọi $x \in R$.

b) R là vành giao hoán.

c) Nếu R là vành không có ước của 0 và R có nhiều hơn một phần tử thì R là miền nguyên.

Bài 2.6 * Cho R là một vành có tính chất sau:

$$x^3 = x \text{ với mọi } x \in R.$$

Chứng minh rằng R là một vành giao hoán.

Bài 2.7 Cho R là một vành tùy ý.

a) Với $a \in R$, tập hợp $C(a) = \{x \in R | ax = xa\}$ được gọi là *tâm hoá tử của* a. Chứng minh rằng $C(a)$ là một vành con của R có chứa a.

b) Tập hợp $C(R) = \{x \in R | ax = xa, \forall a \in R\}$ được gọi là *tâm* của R. Chứng minh rằng $C(R)$ là một vành con giao hoán của R.

c) Tìm tâm của vành $M(n, \mathbb{R})$.

Bài 2.8 Cho R là một vành có đơn vị e và $x, y \in R$. Chứng minh rằng nếu $u = e + xy$ khả nghịch thì $e + yx$ cũng khả nghịch và $(e + yx)^{-1} = e - yu^{-1}x$.

Bài 2.9 Cho R là một vành có đơn vị e. Chứng minh rằng với I là một ideal của R ta có $I = R$ khi và chỉ khi I chứa đơn vị e. Kết qủa trên còn đúng cho các ideal trái, ideal phải hay các vành con của R hay không?

Bài 2.10 Cho R là một vành tùy ý, I và J là hai ideal của R. Đặt

$$I + J = \{x + y |\ x \in I,\ y \in J\}.$$

Chứng minh rằng $I + J$ là một ideal của R. Nếu R là vành các số nguyên và $I = m\mathbb{Z}$; $J = n\mathbb{Z}$ thì $I + J$ có dạng thế nào?

Bài 2.11 Cho R là một vành tùy ý, I và J là hai ideal của R. Đặt

$$IJ = \left\{ \sum_{i=1}^{n} x_i y_i \middle| \ n \in \mathbb{N},\ x_i \in I,\ y_i \in J \right\}.$$

Chứng minh rằng IJ là một ideal của R. Nếu R là vành các số nguyên và $I = m\mathbb{Z}$; $J = n\mathbb{Z}$ thì IJ có dạng thế nào?

Bài 2.12 Cho R là một vành tùy ý và n là một số nguyên cho trước. Chứng minh rằng tập hợp

$$I = \{x \in R | \ nx = 0\}$$

là một ideal của R.

Bài 2.13 Cho R là một vành tùy ý và $a \in R$. Chứng minh rằng tập hợp

$$aR = \{ax | \ x \in R\}$$

là một ideal phải của R, và tập hợp

$$Ra = \{xa | \ x \in R\}$$

là một ideal trái của R. Suy ra nếu R giao hoán thì $aR = Ra$ là ideal của R; hơn nữa, nếu giả thiết thêm R có đơn vị thì đây chính là ideal chính sinh bởi a.

Bài 2.14 Cho R là một vành có đơn vị và $a \in R$. Chứng minh rằng

a) a khả nghịch phải khi và chỉ khi $aR = R$.

b) a khả nghịch trái khi và chỉ khi $Ra = R$.

c) a khả nghịch khi và chỉ khi $aR = Ra = R$.

Bài 2.15 a) Cho R là một vành giao hoán và $a \in R$. Chứng minh rằng tập hợp con

$$Ann(a) = \{x \in R | ax = 0\}$$

là một ideal của R.

b) Tìm $Ann(\overline{4})$ trong vành $\mathbb{Z}_{32}$.

Bài 2.16 Cho R là một vành tùy ý . Một phần tử $x \in R$ được gọi là *lũy linh* nếu tồn tại một số n nguyên dương sao cho $x^n = 0$.

a) Chứng minh rằng nếu R có đơn vị là e và x lũy linh thì $e+x$ khả nghịch.

b) Giả sử R giao hoán, có đơn vị và $u \in R$ khả nghịch. Chứng minh rằng nếu x lũy linh thì $u+x$ khả nghịch.

c) Giả sử R giao hoán. Chứng minh rằng tập hợp $N(R)$ gồm tất cả các phần tử lũy linh của R là một ideal của R và trong vành thương $R/N(R)$ không có phần tử lũy linh nào khác không (Ta gọi $N(R)$ là *nil-căn* của R).

Bài 2.17 Xét R là một vành tùy ý và $\mathbb{Z}$ là vành các số nguyên. Trên tích Descartes $R \times \mathbb{Z}$ ta định nghĩa các phép toán như sau:

$$(x, m) + (y, n) = (x + y, m + n);$$

$$(x, m)(y, n) = (xy + my + nx, mn).$$

a) Chứng minh rằng $R \times \mathbb{Z}$ là một vành có đơn vị.

b) Chứng minh rằng ánh xạ $f : x \mapsto (x, 0)$ là một đơn cấu.

(Do các kết quả trên người ta nói rằng bao giờ cũng có thể nhúng một vành tùy ý vào một vành có đơn vị).

Bài 2.18 a) Chứng minh rằng mọi vành có đơn vị và có đúng p phần tử với p nguyên tố, đều đẳng cấu với vành $\mathbb{Z}_p$.

b) Khẳng định "Mọi vành có đơn vị và có đúng m phần tử với m nguyên dương đều đẳng cấu với $\mathbb{Z}_m$ " có đúng hay không?

Bài 2.19 Cho f là một tự đồng cấu của vành R. Chứng minh rằng tập hợp

$$I = \{x \in R | f(x) = x\}$$

là một vành con của R.

Bài 2.20 Cho R, S là hai vành. Xét tích Descartes $T = R \times S$ và các tập con $\overline{R} = R \times \{0\}$ và $\overline{S} = \{0\} \times S$. Trên T ta định nghĩa các phép toán như sau:

$$(x, y) + (z, t) = (x + z, y + t);$$

$$(x, y)(z, t) = (xz, yt).$$

Chứng minh rằng

a) T là một vành.

b) $\overline{R}$ và $\overline{S}$ lần lượt là các ideal của T đẳng cấu với R và S.

c) $\overline{R}$ và $\overline{S}$ là các ideal của T thỏa $\overline{R} \cap \overline{S} = \{(0, 0)\}$ và $\overline{R} + \overline{S} = T$.

d) Giả sử R, S là các vành có đơn vị. Hãy tìm các đơn vị của T, $\overline{R}$ và $\overline{S}$.

Bài 2.21 Cho R là một vành và $a \in R$. Chứng minh rằng:

a) Tập hợp E gồm tất cả các tự đồng cấu của nhóm cộng Abel R với các phép toán định bởi: Với mọi $f, g \in E$,

$$(f + g)(x) = f(x) + g(x) \quad \text{va} \quad (fg)(x) = f(g(x)), \quad \forall x \in R$$

là một vành.

b) Ánh xạ $h_a : x \mapsto ax$ là một tự đồng cấu của nhóm cộng Abel R.

c) Ánh xạ $h : b \mapsto h_b$ là một đồng cấu vành từ R đến E.

d) Tìm $\mathrm{Ker} h$. Chứng tỏ h là đơn cấu nếu R có đơn vị.

Bài 2.22 Cho R là một miền nguyên và n là cấp (trong nhóm $(R, +)$) của phần tử đơn vị e. Chứng minh rằng

a) n là một số nguyên tố.

b) Mọi phần tử khác không của R đều có cấp n.

c) Với mỗi số nguyên m cho trước, tập hợp

$$mR = \{mx | \ x \in R\}$$

là một ideal của R thỏa

$$R/mR \simeq \begin{cases} R & \text{nếu } m \text{ là bội số của } n; \\ \{0\} & \text{nếu } m \text{ không là bội số của } n. \end{cases}$$

Bài 2.23 Trong trường các số phức $\mathbb{C}$ xét

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} |\ a, b \in \mathbb{Q}\} \quad \text{và} \quad \mathbb{Q}(i) = \{a + bi |\ a, b \in \mathbb{Q}\}.$$

a) Chứng minh rằng $\mathbb{Q}(\sqrt{2})$ và $\mathbb{Q}(i)$ là các trường con của $\mathbb{C}$.

b) Chứng minh rằng $\mathbb{Q}(\sqrt{2})$ và $\mathbb{Q}(i)$ không đẳng cấu.

c) Tìm tất cả các trường con của $\mathbb{Q}(\sqrt{2})$; của $\mathbb{Q}(i)$.

d)* Chứng minh rằng tập hợp $A = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} |\ a, b, c \in \mathbb{Q}\}$ là một trường con của $\mathbb{C}$.

Bài 2.24 Chứng minh rằng

a) $K = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} :\ a, b \in \mathbb{Q} \right\}$ là một trường đẳng cấu với $\mathbb{Q}(i)$.

b) $F = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} :\ a, b \in \mathbb{Q} \right\}$ là một trường đẳng cấu với $\mathbb{Q}(\sqrt{2})$.

Bài 2.25 Cho n là một số nguyên dương. Chứng minh rằng các khẳng định sau tương đương:

a) $\mathbb{Z}_n$ là một miền nguyên;

b) $\mathbb{Z}_n$ là một trường;

c) n là một số nguyên tố.

Bài 2.26 Cho R là một vành giao hoán có đơn vị; I là một ideal của R và I khác R. Ta nói

i) I là *ideal tối đại* của R nếu chỉ có hai ideal chứa I là I và R.

ii) I là *ideal nguyên tố* của R nếu tính chất sau được thỏa: Với mọi $x, y \in R$, nếu $xy \in I$ thì $x \in I$ hay $y \in I$.

Chứng minh rằng

a) R/I là miền nguyên khi và chỉ khi I là ideal nguyên tố.

b) R/I là trường khi và chỉ khi I là ideal tối đại.

Bài 2.27 Cho R là một vành giao hoán có đơn vị và R có hơn một phần tử. Chứng minh rằng các khẳng định sau tương đương:

a) R là một trường;

b) R chỉ có hai ideal là $\{0\}$ và R.

c) Mọi đồng cấu vành từ R vào một vành bất kỳ hoặc là đồng cấu 0 hoặc là đơn cấu.

Bài 2.28 Cho trường F với phần tử đơn vị là 1.

a) Chứng minh rằng với $x \in F$, ta có $x^2 = 1$ khi và chỉ khi $x = \pm 1$.

b) Giả sử F có đúng p phần tử là $x_1, ..., x_{p-1}$ và $x_p = 0$. Chứng minh rằng $x_1...x_{p-1} = -1$ và $\forall x \in F^*, x^{p-1} = 1$.

c) Sử dụng kết quả b) để chứng minh rằng với mọi số nguyên tố dương p ta có (Định lý Wilson)

$$(p-1)! \equiv -1 \ (mod\ p) \quad \text{và} \quad k^p \equiv k \ (mod\ p), \quad \forall k \in \mathbb{Z}.$$

Bài 2.29 Cho F là một trường với phần tử đơn vị e. Xét tập hợp

$$A = \{ne | \ n \in \mathbb{Z}\}.$$

Chứng minh rằng:

a) A là một vành con của F; hỏi A có là miền nguyên không?

b) $A \simeq \begin{cases} \mathbb{Z} & \text{nếu } e \text{ có cấp vô hạn;} \\ \mathbb{Z}_p & \text{nếu } e \text{ có cấp } p. \end{cases}$

c) Nếu e có cấp p hữu hạn thì A là một trường.

Bài 2.30 Chứng minh rằng trường các số hữu tỉ $\mathbb{Q}$ không có trường con nào khác ngoài $\mathbb{Q}$.

Bài 2.31 Chứng minh rằng mọi trường đều có trường con bé nhất (theo quan hệ bao hàm) đẳng cấu hoặc với trường số hữu tỉ hoặc với trường $\mathbb{Z}_p$ với p nguyên tố.

Bài 2.32 Cho F là một trường và A là một vành con của F.

a) Chứng minh rằng nếu A có nhiều hơn một phần tử và A có đơn vị thì phần tử đơn vị của A trùng với phần tử đơn vị của F, và lúc đó A là một miền nguyên.

b) Giả sử A là một miền nguyên. Chứng minh rằng tập hợp

$$P = \{ab^{-1} |\ a, b \in A,\ b \neq 0\}$$

là một trường con của F và P là trường các thương của A.

c) Chứng minh rằng P là trường con bé nhất trong các trường con của F có chứa A.

Bài 2.33 Cho p là một số nguyên tố. Chứng minh rằng tập hợp tất cả các số hữu tỉ có dạng m/n, trong đó m, n là các số nguyên và n nguyên tố cùng nhau với p, là một miền nguyên. Tìm trường các thương của miền nguyên này.

Bài 2.34 Xét hàm φ-Euler.

a) Chứng minh rằng $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ với mọi p nguyên tố.

b) Xác định $\varphi(n)$ với $n \in \mathbb{N}^*$.

Bài 2.35 Tìm tất cả các tự đồng cấu của các trường sau:

a) Trường các số hữu tỉ $\mathbb{Q}$.

b) Trường $\mathbb{Q}(\sqrt{2})$.

c) Trường $\mathbb{Q}(i)$.

d) Trường các số thực $\mathbb{R}$.

e) Trường các số phức $\mathbb{C}$ sao cho các tự đồng cấu đó thu hẹp trên $\mathbb{R}$ là ánh xạ đồng nhất.

Chương III
VÀNH ĐA THỨC

§1. Vành đa thức một ẩn

1.1. Định nghĩa

Giả sử R là một vành giao hoán và có đơn vị 1. Gọi A là tập hợp tất cả các dãy

$$(a_0, a_1, ..., a_n, ...),$$

trong đó các $a_i \in R, \forall i \in \mathbb{N}$ và bằng 0 tất cả trừ một số hữu hạn. Như vậy A là một bộ phận của lũy thừa Descartes $R^{\mathbb{N}}$.

Ta định nghĩa phép cộng và nhân trong A như sau:

Giả sử $f = (a_0, a_1, ..., a_n, ...)$ và $g = (b_0, b_1, ..., b_n, ...)$ là các phần tử tùy ý của A. Khi đó

$$\begin{aligned} f + g &= (a_0 + b_0, a_1 + b_1, ..., a_n + b_n, ...), \\ fg &= (c_0, c_1, ..., c_n, ...), \end{aligned}$$

trong đó

$$c_k = \sum_{i+j=k} a_i b_j, \ k = 0, 1, 2, ...$$

Dễ dàng kiểm tra lại rằng A cùng với hai phép toán đó lập nên một vành giao hoán, có đơn vị là $(1, 0, 0, ...)$, phần tử không của vành này là $(0, 0, 0, ...)$. Ta sẽ ký hiệu phần tử đơn vị của A là 1 và phần tử không của A là 0.

Đặt $x = (0, 1, 0, 0, ...)$. Dễ thấy rằng

$$\begin{aligned} x^2 &= (0, 0, 1, 0, ...); \\ x^3 &= (0, 0, 0, 1, 0, ...); \\ x^n &= (\underbrace{0, 0, ..., 0}_{n \text{ phần tử } 0}, 1, 0, ...). \end{aligned}$$

Ta quy ước $x^0 = (1, 0, 0, ...)$ và mỗi phần tử $a \in R$ có thể đồng nhất với dãy $(a, 0, 0, ...)$ nhờ đơn cấu vành

$$\begin{aligned} R &\longrightarrow A \\ a &\longmapsto (a, 0, 0, ...). \end{aligned}$$

Như vậy

$$ax^n = (\underbrace{0, 0, ..., 0}_{n \text{ phần tử } 0}, a, 0, ...), \forall a \in R.$$

Do đó

$$f = (a_0, a_1, ..., a_n, 0, 0, ...) = a_0 + a_1 x + ... + a_n x^n,$$

và thường được viết là

$$f(x) = a_n x^n + ... + a_1 x + a_0.$$

Cách biểu thị như vậy là duy nhất đối với mỗi phần tử $f \in A$. Nói cách khác,

$$a_n x^n + ... + a_1 x + a_0 = b_n x^n + ... + b_1 x + b_0$$

khi và chỉ khi

$$a_n = b_n, \ldots, a_1 = b_1, \ a_0 = b_0.$$

Vành A nói trên được gọi là *vành đa thức* của ẩn x (hoặc biến x) với các hệ số trong R, và được ký hiệu là $R[x]$. Mỗi phần tử của $R[x]$ được gọi là một *đa thức của ẩn* x trên R. Đa thức dạng ax^n $(a \in R)$ được gọi là một *đơn thức*.

Giả sử

$$f(x) = a_n x^n + ... + a_1 x + a_0$$

với $a_n \neq 0$. Khi đó ta nói đa thức $f(x)$ có *bậc* là n và ký hiệu $\deg f = n$ hay $\deg f(x) = n$. Phần tử a_i được gọi là *hệ số thứ* i của $f(x)$, phần tử a_n được gọi là *hệ số cao nhất*, còn phần tử a_0 được gọi là *hệ số tự do*. Bậc của đa thức 0 được quy ước là $-\infty$.

Dễ dàng thấy rằng:

i) $\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}$

ii) $\deg(f(x)g(x)) \leq \deg f(x) + \deg g(x)$

với $f(x)$ và $g(x)$ là hai đa thức bất kỳ trên R.

1.2. Định lý. *Nếu D là một miền nguyên thì $D[x]$ cũng là một miền nguyên.*

Chứng minh. Giả sử $f(x), g(x) \in D[x]$ là các đa thức khác 0 có bậc tương ứng là m và n:

$$\begin{aligned} f(x) &= a_m x^m + ... + a_1 x + a_0,\ a_m \neq 0; \\ g(x) &= b_n x^n + ... + b_1 x + b_0,\ b_n \neq 0. \end{aligned}$$

Theo định nghĩa phép toán trên đa thức ta có

$$f(x)g(x) = a_m b_n x^{m+n} + ... + (a_0 b_1 + a_1 b_0)x + a_0 b_0.$$

Vì D là miền nguyên và $a_m, b_n \neq 0$ nên $a_m b_n \neq 0$, do đó $f(x)g(x) \neq 0$. ■

Cũng từ chứng minh trên ta suy ra

$$\deg(f(x)g(x)) = \deg f(x) + \deg g(x).$$

Tuy nhiên đẳng thức trên không còn đúng nữa khi R không phải là miền nguyên. Chẳng hạn, $\overline{2}x + \overline{1}$ và $\overline{3}x + \overline{1}$ là các đa thức bậc nhất trong $\mathbb{Z}_6[x]$ nhưng tích của chúng lại là một đa thức bậc nhất.

1.3. Định lý (Phép chia Euclide). *Giả sử K là một trường và $f(x), g(x) \in K[x], g(x) \neq 0$. Khi đó tồn tại duy nhất các đa thức $q(x), r(x) \in K[x]$ sao cho*

$$f(x) = g(x)q(x) + r(x),\ \textit{với}\ \deg r(x) < \deg g(x).$$

Các đa thức $q(x)$ và $r(x)$ được gọi tương ứng là *thương* và *dư* trong phép chia $f(x)$ cho $g(x)$.

Chứng minh. i) *Sự duy nhất.* Giả sử

$$f(x) = g(x)q(x) + r(x) = g(x)q'(x) + r'(x)$$

với $\deg r(x) < \deg g(x)$ và $\deg r'(x) < \deg g(x)$. Khi đó ta có

$$g(x)[q(x) - q'(x)] = r'(x) - r(x).$$

Nếu $q(x) \neq q'(x)$ thì

$$\deg[r'(x) - r(x)] = \deg g(x) + \deg[q(x) - q'(x)] \geq \deg g(x).$$

Điều này mâu thuẫn với giả thiết $\deg r(x) < \deg g(x)$ và $\deg r'(x) < \deg g(x)$. Do đó $q(x) = q'(x)$. Vì vậy $r(x) = r'(x)$.

ii) *Sự tồn tại.* Ta chứng minh sự tồn tại của $q(x)$ và $r(x)$ bằng phương pháp quy nạp theo bậc của $f(x)$. Giả sử

$$\begin{aligned} f(x) &= a_n x^n + ... + a_1 x + a_0,\ a_n \neq 0; \\ g(x) &= b_m x^m + ... + b_1 x + b_0,\ b_m \neq 0. \end{aligned}$$

Nếu $n = 0, m = 0$ thì đặt $r(x) = 0, q(x) = a_0 b_0^{-1}$, còn nếu $n = 0, m > 0$ thì đặt $q(x) = 0, r(x) = f(x)$. Giả sử định lý được chứng minh cho mọi đa thức f có bậc $< n$ với $n > 0$. Nếu $m > n$ thì ta chọn $q(x) = 0, r(x) = f(x)$. Nếu $m \leq n$ thì đặt

$$\overline{f}(x) = f(x) - (a_n b_m^{-1}) x^{n-m} g(x).$$

Khi đó $\overline{f}(x)$ là đa thức có bậc $< n$. Theo giả thiết quy nạp, tồn tại các đa thức $\overline{q}(x)$ và $r(x)$ sao cho

$$\overline{f}(x) = \overline{q}(x)g(x) + r(x),\ \deg r(x) < m.$$

Do đó

$$f(x) = (a_n b_m^{-1} x^{n-m} + \overline{q}(x))g(x) + r(x).$$

Đặt $q(x) = a_n b_m^{-1} x^{n-m} + \overline{q}(x)$, ta có các đa thức thương và dư cần tìm trong phép chia $f(x)$ cho $g(x)$. ■

1.4. Ví dụ

Trong thực hành, để thực hiện phép chia đa thức $f(x)$ cho đa thức $g(x)$ ta sắp đặt như việc chia số nguyên. Chẳng hạn trong $\mathbb{Z}_{11}[x]$, để tìm thương và dư trong phép chia đa thức

$$f(x) = -\overline{1}x^3 - \overline{7}x^2 + \overline{3}x - \overline{5}$$

cho

$$g(x) = -\overline{2}x^2 + \overline{2}x - \overline{1},$$

ta viết

$$\begin{array}{r|l} -\overline{1}x^3 - \overline{7}x^2 + \overline{3}x - \overline{5} & -\overline{2}x^2 + \overline{2}x - \overline{1} \\ \cline{2-2} -\overline{1}x^3 + \overline{1}x^2 - \overline{6}x & \\ \cline{1-1} & \overline{6}x + \overline{4} \\ -\overline{8}x^2 + \overline{9}x - \overline{5} & \\ -\overline{8}x^2 + \overline{8}x - \overline{4} & \\ \cline{1-1} & \\ \overline{1}x - \overline{1} & \end{array}$$

Vậy

$$-\overline{1}x^3 - \overline{7}x^2 + \overline{3}x - \overline{5} = (-\overline{2}x^2 + \overline{2}x - \overline{1})(\overline{6}x + \overline{4}) + \overline{1}x - \overline{1}.$$

1.5. Định nghĩa

Cho các đa thức $f(x), g(x) \in K[x]$, ở đây K là một trường và $g(x) \neq 0$. Nếu tồn tại $q(x) \in K[x]$ sao cho $f(x) = q(x)g(x)$ thì ta nói $f(x)$ *chia hết cho* $g(x)$ (hay $g(x)$ là *ước* của $f(x)$) trong $K[x]$. Một đa thức $d(x) \in K[x]$ là ước của hai đa thức $f(x)$ và $g(x)$ được gọi là *ước chung* của $f(x)$ và $g(x)$. Nếu $d(x)$ là ước chung của $f(x)$ và $g(x)$, đồng thời $d(x)$ chia hết cho mọi ước chung khác của $f(x)$ và $g(x)$ thì $d(x)$ được gọi là *ước chung lớn nhất* của $f(x)$ và $g(x)$, viết tắt là UCLN, ký hiệu là $d(x) = (f(x), g(x))$. Để đảm bảo tính duy nhất của UCLN, ta quy ước rằng hệ số cao nhất của UCLN bao giờ cũng lấy bằng 1.

1.6. Thuật chia Euclide

Để tìm UCLN của hai đa thức $f(x), g(x) \in K[x]$ ta dùng thuật chia Euclide bằng cách thực hiện một số hữu hạn phép chia liên tiếp như sau:

$$
\begin{aligned}
&f(x) = g(x)q(x) + r(x), && \deg r(x) < \deg g(x)\\
&g(x) = r(x)q_1(x) + r_1(x), && \deg r_1(x) < \deg r(x)\\
&\cdots\cdots\\
&r_{k-2}(x) = r_{k-1}(x)q_k(x) + r_k(x), && \deg r_k(x) < \deg r_{k-1}(x)\\
&r_{k-1}(x) = r_k(x)q_{k+1}(x).
\end{aligned}
$$

Đa thức dư cuối cùng khác 0 trong dãy phép chia nói trên chính là $r_k(x)$ và

$$UCLN = \frac{r_k(x)}{\text{hệ số cao nhất của } r_k(x)}.$$

Từ thuật toán Euclide ta thấy rằng nếu $d(x) = (f(x), g(x))$ thì ta có thể tìm được hai đa thức $u(x), v(x) \in K[x]$ sao cho

$$f(x)u(x) + g(x)v(x) = d(x).$$

1.7. Ví dụ

Trong $\mathbb{R}[x]$ cho các đa thức

$$f(x) = 4x^4 - 2x^3 - 16x^2 + 5x + 9$$

và

$$g(x) = 2x^3 - x^2 - 5x + 4.$$

Tìm $d(x) = (f(x), g(x))$ và tìm các đa thức $u(x), v(x) \in \mathbb{R}[x]$ sao cho

$$f(x)u(x) + g(x)v(x) = d(x).$$

Giải. Để tìm UCLN của $f(x)$ và $g(x)$, ta thực hiện dãy các phép chia liên tiếp

$$
\begin{array}{r|l}
4x^4 - 2x^3 - 16x^2 + 5x + 9 & 2x^3 - x^2 - 5x + 4\\
\cline{2-2}
4x^4 - 2x^3 - 10x^2 + 8x & 2x\\
\cline{1-1}
-6x^2 - 3x + 9 &
\end{array}
$$

$$f(x) = g(x)q(x) + r(x), r(x) = -6x^2 - 3x + 9, q(x) = 2x.$$

Nhân $g(x)$ với 3 rồi chia cho $r(x)$:

$$\begin{array}{r|l} 6x^3-3x^2-15x+12 & -6x^2-3x+9 \\ \hline 6x^3+3x^2-9x & -x+1 \\ \hline -6x^2-6x+12 & \\ -6x^2-3x+9 & \\ \hline -3x+3 & \end{array}$$

$$3g(x) = r(x)q_1(x) + r_1(x), q_1(x) = -x+1, r_1(x) = -3x+3.$$

Lấy $r(x)$ chia cho $r_1(x)$ ta có

$$\begin{array}{r|l} -6x^2-3x+9 & -3x+3 \\ \hline -6x^2+6x & 2x+3 \\ \hline -9x+9 & \\ -9x+9 & \\ \hline 0 & \end{array}$$

$$r(x) = (2x+3)r_1(x).$$

Do đó ta có $r_1(x) = -3x+3$ là dư cuối cùng khác 0. Theo quy ước, ta sẽ lấy

$$d(x) = (f(x), g(x)) = x-1.$$

Theo quá trình trên ta có

$$\begin{aligned} r_1(x) &= 3g(x) - r(x)q_1(x) \\ &= 3g(x) - q_1(x)(f(x) - g(x)q(x)) \\ &= (3 + q(x)q_1(x))g(x) - q_1(x)f(x). \end{aligned}$$

Suy ra

$$d(x) = \frac{-x+1}{3}f(x) + \frac{2x^2-2x-3}{3}g(x).$$

1.8. Đa thức bất khả quy trên miền nguyên

Nếu D là miền nguyên thì $D[x]$ cũng là miền nguyên (Định lý 1.2). Đa thức $f(x) \in D[x]$ khác không, không khả nghịch gọi là *bất khả quy*

trong $D[x]$ (hay còn gọi là bất khả quy trên D) nếu nó không có ước thực sự trong $D[x]$, tức là nếu $f(x) = g(x)h(x)$ $(g(x), h(x) \in D[x])$ thì $g(x)$ hay $h(x)$ phải là phần tử khả nghịch của D.

Nói riêng, nếu K là một trường thì các phần tử khả nghịch trong $K[x]$ chính là các phần tử khác không của K. Đa thức $f(x) \in K[x]$, khác không, không khả nghịch là bất khả quy trên K khi và chỉ khi nếu $f(x) = g(x)h(x), (g(x), h(x) \in K[x])$ thì $g(x)$ hay $h(x)$ là phần tử khác không của K. Số các đa thức bất khả quy trên một trường là vô hạn. Cụ thể ta có định lý sau:

1.9 Định lý. *Có vô số đa thức với hệ số cao nhất là* 1 *bất khả quy trên trường* K.

Chứng minh. Nếu K là trường vô hạn thì các đa thức dạng $x - a, a \in K$ là các đa thức với hệ số cao nhất là 1 bất khả quy trên K. Có vô số đa thức như vậy.

Trong trường hợp K là trường hữu hạn, giả sử chỉ có n đa thức bất khả quy $p_1(x), p_2(x), ..., p_n(x)$ với hệ số cao nhất là 1. Đa thức

$$f(x) = p_1(x)p_2(x)...p_n(x) + 1$$

có ít nhất một ước bất khả quy (với hệ số cao nhất là 1) vì $\deg f(x) \geq n$. Ước đó phải khác $p_1(x), p_2(x), ..., p_n(x)$ vì nếu không nó sẽ là ước của

$$f(x) - p_1(x)p_2(x)...p_n(x) = 1,$$

điều này vô lý. Vậy $K[x]$ phải có vô hạn đa thức bất khả quy với hệ số cao nhất là 1. ■

§2. Nghiệm của đa thức

2.1. Định nghĩa

Giả sử $c \in R$ và

$$f(x) = a_n x^n + ... + a_1 x + a_0 \in R[x].$$

Phần tử $f(c) = a_n c^n + ... + a_1 c + a_0$ được gọi là *giá trị* của $f(x)$ tại c. Nếu $f(c) = 0$ thì c được gọi là *nghiệm* của $f(x)$. Tìm nghiệm của $f(x)$ trong R là giải phương trình đại số $a_n x^n + ... + a_1 x + a_0 = 0$ trong R.

2.2. Định lý Bezout. *Phần tử c của trường K là nghiệm của đa thức $f(x) \in K[x]$ khi và chỉ khi $f(x)$ chia hết cho $x - c$.*

Chứng minh. Chia $f(x)$ cho $x - c$ ta được

$$f(x) = q(x)(x - c) + r(x)$$

với $\deg r(x) < \deg(x - c) = 1$. Vậy $r(x)$ là một phần tử của K. Thay $x = c$ ta được

$$f(c) = q(c).0 + r(c) = r(c).$$

Vậy ta có

$$f(x) = q(x)(x - c) + f(c).$$

Do đó dư của phép chia $f(x)$ cho $x - c$ là $f(c)$. Nói riêng, $f(x)$ chia hết cho $x - c$ khi và chỉ khi $f(c) = 0$. ■

2.3. Sơ đồ Horner

Cho $f(x) = a_n x^n + ... + a_1 x + a_0 \in K[x]$ và $c \in K$. Ta dùng sơ đồ Horner dưới đây để tìm $q(x) = b_{n-1}x^{n-1} + ... + b_1 x + b_0$ và $r = f(c)$ trong thuật chia Euclide $f(x) = (x - c)q(x) + r$.

	a_n	a_{n-1}	...	a_1	a_0
c	$b_{n-1} = a_n$	$b_{n-2} = a_{n-1} + cb_{n-1}$	...	$b_0 = a_1 + cb_1$	$r = a_0 + cb_0$

2.4. Ví dụ

a) Trong $\mathbb{Q}[x]$ cho

$$f(x) = 3x^5 + 4x^4 - 2x^3 + 5x^2 - x + 6$$

và $c = 4 \in \mathbb{Q}$. Ta có sơ đồ Horner như sau:

	3	4	−2	5	−1	6
4	3	16	62	253	1011	4050

Vậy

$$f(x) = (x - 4)q(x) + r$$

với

$$q(x) = 3x^4 + 16x^3 + 62x^2 + 253x + 1011 \text{ và } r = f(4) = 4050.$$

b) Trong $\mathbb{Z}_7[x]$ cho $f(x) = \overline{2}x^5 - x^3 + \overline{3}x^2 - \overline{2}$ và $c = -\overline{3} \in \mathbb{Z}_7$. Ta có sơ đồ Horner như sau:

	$\overline{2}$	$\overline{0}$	$-\overline{1}$	$\overline{3}$	$\overline{0}$	$-\overline{2}$
$-\overline{3}$	$\overline{2}$	$\overline{1}$	$\overline{3}$	$\overline{1}$	$-\overline{3}$	$\overline{0}$

Vậy $f(x) = (x + \overline{3})q(x)$ với $q(x) = \overline{2}x^4 + x^3 + \overline{3}x^2 + x - \overline{3}, r = 0$. Đa thức $f(x)$ chia hết cho $x + \overline{3}$ nên $c = -\overline{3}$ là một nghiệm của $f(x)$.

2.5. Định lý. *Cho đa thức $f(x)$ trên trường K, $\deg f(x) = n \geq 0$. Khi đó $f(x)$ có nhiều nhất n nghiệm trên K.*

Chứng minh. Ta chứng minh bằng phương pháp quy nạp theo n. Nếu $n = 0$ thì $f(x)$ là đa thức hằng khác không nên $f(x)$ vô nghiệm trên K.

Xét $n \geq 1$. Giả sử định lý đúng cho các đa thức $g(x) \in K[x]$ với $0 \leq \deg g(x) < n$. Nếu $f(x)$ vô nghiệm trên K thì định lý đúng cho $f(x)$. Nếu $f(x)$ có nghiệm $c \in K$ thì tồn tại $g(x) \in K[x], \deg g(x) = n - 1$ sao cho $f(x) = (x - c)g(x)$. Theo giả thiết quy nạp, $g(x)$ có không quá $n - 1$ nghiệm trên K, do đó $f(x)$ không có quá n nghiệm trên K. Định lý được chứng minh. ■

2.6. Hệ quả. *Nếu hai đa thức trên trường K có cùng bậc n và lấy những giá trị bằng nhau tại $n + 1$ phần tử khác nhau của K thì chúng bằng nhau.*

Chứng minh. Giả sử $f(x), g(x) \in K[x]$ có cùng bậc n và bằng nhau tại $n + 1$ phần tử khác nhau của K. Khi đó đa thức $h(x) = f(x) - g(x)$ có bậc không vượt quá n và có ít nhất $n + 1$ nghiệm. Như vậy $h(x)$ là đa thức không, và do đó $f(x) = g(x)$. ■

2.7. Nhận xét

Thực ra Hệ quả 2.6 vẫn còn đúng cho các đa thức trên miền nguyên R. Nếu R không phải là miền nguyên thì hệ quả trên không đúng.

2.8. Định nghĩa

Cho đa thức $f(x)$ trên trường K.

a) Nếu $f(x) = a_0 \in K$, đặt $f'(x) = 0$. Nếu $f(x) = \sum_{k=0}^{n} a_k x^k$ với $n \geq 1$, đặt $f'(x) = \sum_{k=1}^{n} k a_k x^{k-1}$. Ta gọi $f'(x)$ là *đạo hàm* của $f(x)$.

b) Đặt $f^{(0)}(x) = f(x)$, $f^{(1)}(x) = f'(x)$, $f^{(2)}(x) = (f^{(1)}(x))'$, ..., $f^{(k)}(x) = (f^{(k-1)}(x))', \forall k \in \mathbb{N}^*$. Ta nói $f^{(m)}(x)$ là *đạo hàm cấp* m của $f(x), \forall m \in \mathbb{N}$.

2.9. Khai triển Taylor

Cho đa thức $f(x)$ trên trường K và $\deg f(x) = n$. Khi đó với mỗi $c \in K$ đa thức $f(x)$ có thể khai triển duy nhất dưới dạng

$$f(x) = \sum_{k=0}^{n} c_k (x - c)^k.$$

Thật vậy, thực hiện phép chia $f(x)$ cho $x - c$ ta có

$$f(x) = (x - c)g(x) + c_0,$$

trong đó $c_0 \in K$ và $g(x) \in K[x]$ $(\deg g(x) = n - 1)$ xác định duy nhất theo Định lý 1.3. Lại tiếp tục thực hiện phép chia $g(x)$ cho $x - c$ ta có duy nhất $c_1 \in K$ và $g_1(x) \in K[x]$ sao cho

$$g(x) = (x - c)g_1(x) + c_1, \quad \deg g_1(x) = n - 2.$$

Khi đó ta có

$$f(x) = (x - c)^2 g_1(x) + c_1(x - c) + c_0.$$

Lặp lại quá trình trên, cuối cùng ta được

$$f(x) = c_n(x - c)^n + c_{n-1}(x - c)^{n-1} + \cdots + c_1(x - c) + c_0.$$

Nhờ sơ đồ Horner ta dễ dàng thu được các hệ số $c_0, ..., c_n$ như bảng sau:

	a_n	a_{n-1}	$\dots$	a_1	a_0
c	a_n	$*$	$\dots$	$*$	$\boxed{c_0}$
c	a_n	$*$	$\dots$	$\boxed{c_1}$	
$\vdots$	$\vdots$	$\vdots$	$\vdots$		
c	a_n	$\boxed{c_{n-1}}$			
c	$\boxed{c_n = a_n}$				

2.10. Ví dụ

Trong vành $\mathbb{Q}[x]$, để phân tích đa thức $f(x) = x^4 - x^3 + 1$ theo các lũy thừa của $x - 3$ ta lập sơ đồ Horner

	1	-1	0	0	1
3	1	2	6	18	$\boxed{55}$
3	1	5	21	$\boxed{81}$	
3	1	8	$\boxed{45}$		
3	1	$\boxed{11}$			
3	$\boxed{1}$				

Từ đó

$$f(x) = (x-3)^4 + 11(x-3)^3 + 45(x-3)^2 + 81(x-3) + 55.$$

2.11. Nhận xét

Trong trường hợp K là trường có đặc số 0 thì các hệ số c_k trong khai triển Taylor có thể tính theo các đạo hàm của đa thức $f(x)$ như sau:

$$c_k = \frac{f^{(k)}(c)}{k!},$$

nghĩa là

$$f(x) = \sum_{k=0}^{n} \frac{f^{(k)}(c)}{k!}(x-c)^k.$$

2.12. Định nghĩa

Giả sử k là một số tự nhiên khác không, R là miền nguyên. Phần tử $c \in R$ được gọi là *nghiệm bội* k của đa thức $f(x) \in R[x]$ nếu $f(x)$ chia hết cho $(x-c)^k$ nhưng không chia hết cho $(x-c)^{k+1}$, nghĩa là $f(x)$ có thể phân tích thành

$$f(x) = (x-c)^k g(x)$$

với $g(x) \in R[x]$ và $g(c) \neq 0$.

2.13. Nhận xét

i) Nếu $f(x) = \sum_{k=0}^{n} c_k(x-c)^k$ là khai triển Taylor của đa thức $f(x)$ thì

c là nghiệm bội m khi và chỉ khi $c_m \neq 0$ và $c_i = 0, \forall i < m$.

ii) Nói riêng, nếu $f(x) \in K[x]$ với $\mathrm{char}K = 0$ thì $c \in K$ là nghiệm bội m của $f(x)$ khi và chỉ khi $f^{(m)}(c) \neq 0$ và $f^{(i)}(c) = 0, \forall i < m$.

2.14. Ví dụ

Trong $\mathbb{Z}_7[x]$, cho $f(x) = \overline{2}x^4 - \overline{3}x^3 + \overline{2}x - \overline{3}$ và $c = -\overline{2} \in \mathbb{Z}_7$. Để kiểm tra xem c có là nghiệm của $f(x)$ hay không, nếu có thì là nghiệm bội bao nhiêu, ta sẽ dùng sơ đồ Horner một số lần liên tiếp như sau:

	$\overline{2}$	$-\overline{3}$	$\overline{0}$	$\overline{2}$	$-\overline{3}$
$-\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{0}$	$\overline{2}$	$\boxed{\overline{0}}$
$-\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{1}$	$\boxed{\overline{0}}$	
$-\overline{2}$	$\overline{2}$	$-\overline{1}$	$\boxed{\overline{3}}$		

Căn cứ vào sơ đồ Horner ta thấy $c = -\overline{2}$ là một nghiệm kép của $f(x)$.

2.15. Định nghĩa (Phần tử đại số và phần tử siêu việt)

Giả sử R là vành con chứa đơn vị của miền nguyên D. Phần tử $\alpha \in D$ được gọi là *đại số* trên R nếu α là nghiệm của một đa thức khác không với hệ số trong R. Nếu $\alpha \in D$ không đại số trên R thì α được gọi là phần tử *siêu việt*.

Một phần tử đại số (siêu việt) trên trường số hữu tỷ $\mathbb{Q}$ gọi tắt là phần tử đại số (siêu việt).

Với mỗi $\alpha \in D$, ký hiệu $R[\alpha] = \{f(\alpha) | f(x) \in R[x]\}$. Dễ dàng thấy rằng $R[\alpha]$ là vành con của vành D. Để đo *độ lệch* của vành $R[\alpha]$ so với vành $R[x]$ ta xét toàn cấu vành

$$\begin{array}{rccc} \varphi: & R[x] & \longrightarrow & R[\alpha] \\ & f(x) & \longmapsto & f(\alpha). \end{array}$$

Theo Định lý 3.9, chương II, ta có $R[x]/\mathrm{Ker}\varphi \simeq R[\alpha]$. Trong trường hợp α là phần tử siêu việt trên R thì $f(\alpha) = 0$ khi và chỉ khi $f(x)$ là đa thức không, tức là $\mathrm{Ker}\varphi = \{0\}$. Khi đó $R[\alpha] \simeq R[x]$.

2.16. Công thức Viète

Cho đa thức $f(x) \in K[x]$,

$$f(x) = a_n x^n + ... + a_1 x + a_0, a_n \neq 0.$$

Giả sử $f(x)$ có n nghiệm (kể cả số bội) là $\alpha_1, \alpha_2, ..., \alpha_n \in K$. Khi đó ta có

$$f(x) = a_n(x - \alpha_1)(x - \alpha_2)...(x - \alpha_n).$$

Khai triển vế phải và so sánh các hệ số của các lũy thừa giống nhau ta sẽ được công thức sau gọi là *công thức Viète*, chúng biểu thị các hệ số của đa thức theo các nghiệm của nó:

$$\begin{array}{rcl} \dfrac{a_{n-1}}{a_n} & = & -(\alpha_1 + \alpha_2 + ... + \alpha_n) = -\displaystyle\sum_{i=1}^{n} \alpha_i; \\ \dfrac{a_{n-2}}{a_n} & = & \displaystyle\sum_{1 \leq i < j \leq n} \alpha_i \alpha_j; \\ \vdots & & \vdots \\ \dfrac{a_{n-k}}{a_n} & = & (-1)^k \displaystyle\sum_{1 \leq i_1 < i_2 < ... < i_k \leq n} \alpha_{i_1} \alpha_{i_2} ... \alpha_{i_k}; \\ \vdots & & \vdots \\ \dfrac{a_0}{a_n} & = & (-1)^n \alpha_1 \alpha_2 ... \alpha_n. \end{array}$$

Ta thấy rằng các vế phải của công thức Viète không thay đổi nếu ta thực hiện phép hoán vị bất kỳ trên các nghiệm $\alpha_1, \alpha_2, ..., \alpha_n$. Đó là những đa thức đối xứng. Trong §7 ta sẽ khảo sát các đa thức này.

2.17. Ví dụ

a) Nếu x_1 và x_2 là các nghiệm của một phương trình bậc hai

$$ax^2 + bx + c = 0, a \neq 0$$

thì ta có

$$x_1 + x_2 = -\frac{b}{a}, x_1x_2 = \frac{c}{a}.$$

b) Nếu x_1, x_2 và x_3 là các nghiệm của một phương trình bậc ba

$$ax^3 + bx^2 + cx + d = 0, a \neq 0$$

thì ta có

$$\begin{aligned} x_1 + x_2 + x_3 &= -\frac{b}{a}, \\ x_1x_2 + x_2x_3 + x_3x_1 &= \frac{c}{a}, \\ x_1x_2x_3 &= -\frac{d}{a}. \end{aligned}$$

§3. Đa thức nội suy Lagrange

3.1. Bài toán

Cho x_1, x_2, ..., x_n, c_1, c_2, ..., c_n là các phần tử của trường K, trong đó $x_i \neq x_j, \forall i \neq j$. Tìm tất cả các đa thức $f(x) \in K[x]$ sao cho $f(x_i) = c_i, \forall i$.

Đặt

$$\varphi(x) = (x - x_1)(x - x_2)...(x - x_n) = \prod_{j=1}^{n}(x - x_j),$$

$$\varphi_i(x) = \frac{\varphi(x)}{(x - x_i)} = \prod_{j \neq i}(x - x_j),\ 1 \leq i \leq n,$$

$$\psi_i(x) = \frac{\varphi_i(x)}{\varphi_i(x_i)} = \prod_{j \neq i} \frac{(x - x_j)}{(x_i - x_j)},\ 1 \leq i \leq n,$$

$$f_0(x) = c_1\psi_1(x) + c_2\psi_2(x) + ... + c_n\psi_n(x) = \sum_{i=1}^{n} c_i\psi_i(x).$$

Khi đó ta có kết quả sau:

3.2. Mệnh đề. *Với giả thiết và ký hiệu như trên, đa thức* $f(x) \in K[x]$ *thỏa mãn điều kiện* $f(x_i) = c_i, i = 1, 2, ..., n$ *khi và chỉ khi* $f(x)$ *có dạng*

$$f(x) = f_0(x) + g(x)\varphi(x) \tag{1}$$

với $g(x)$ *là đa thức nào đó của* $K[x]$.

Chứng minh. Giả sử $f(x) = f_0(x) + g(x)\varphi(x)$ với $g(x) \in K[x]$. Đương nhiên $f(x) \in K[x]$. Ta có

$$\psi_i(x_j) = \delta_{ij} = \begin{cases} 1, & \text{nếu } i = j, \\ 0 & \text{nếu } i \neq j, \end{cases}\ 1 \leq i, j \leq n$$

nên $f_0(x_i) = c_i$, hơn nữa $\varphi(x_i) = 0, \forall i = 1, 2, ..., n$, do đó

$$f(x_i) = f_0(x_i) + g(x_i)\varphi(x_i) = c_i, \forall i = 1, 2, ..., n.$$

Ngược lại, giả sử $f(x) \in K[x]$ thỏa mãn điều kiện

$$f(x_i) = c_i, \forall i = 1, 2, ..., n.$$

Đặt

$$h(x) = f(x) - f_0(x) \in K[x].$$

Ta có $f_0(x_i) = c_i$ do đó

$$h(x_i) = 0, \forall i = 1, 2, ..., n.$$

Như vậy $h(x)$ chia hết cho $x - x_i (1 \leq i \leq n)$. Do đó $h(x)$ chia hết cho $\varphi(x)$, nghĩa là tồn tại $g(x) \in K[x]$ sao cho $h(x) = \varphi(x)g(x)$. Từ đó

$$f(x) = f_0(x) + h(x) = f_0(x) + \varphi(x)g(x).$$ ■

3.3. Nhận xét

Trong (1), lấy $g(x)$ là đa thức không thì ta có $f(x) = f_0(x)$ cũng là đa thức thỏa điều kiện $f(x_i) = c_i$, hơn nữa $\deg f(x) \leq n-1$.

3.4. Ví dụ

Tìm tất cả các đa thức $f(x) \in \mathbb{R}[x]$ sao cho $f(-4) = 2$, $f(-1) = 3, f(5) = -6$ và $f(7) = 9$.

Giải. Đặt

$$\begin{aligned}
\varphi(x) &= (x+4)(x+1)(x-5)(x-7),\\
\varphi_1(x) &= (x+1)(x-5)(x-7),\\
\varphi_2(x) &= (x+4)(x-5)(x-7),\\
\varphi_3(x) &= (x+4)(x+1)(x-7),\\
\varphi_4(x) &= (x+4)(x+1)(x-5).
\end{aligned}$$

Suy ra

$$\varphi_1(-4) = -297,\ \varphi_2(-1) = 144,\ \varphi_3(5) = -108,\ \varphi_4(7) = 176.$$

Đặt $\psi_1 = -\dfrac{1}{297}\varphi_1,\ \psi_2 = \dfrac{1}{144}\varphi_2,\ \psi_3 = -\dfrac{1}{108}\varphi_3,\ \psi_4 = \dfrac{1}{176}\varphi_4.$

Khi đó tất cả các đa thức cần tìm có dạng

$$f(x) = 2\psi_1(x) + 3\psi_2(x) - 6\psi_3(x) + 9\psi_4(x) + g(x)\varphi(x), g(x) \in \mathbb{R}[x].$$

§4. Đa thức trên trường số thực và phức

4.1. Định lý cơ bản của Đại số. *Mọi đa thức $f(x)$ bậc $n \geq 1$ trên trường số phức đều có n nghiệm phức (kể cả số bội).*

Định lý này có nhiều ứng dụng trong rất nhiều lĩnh vực khác nhau của toán học. Có nhiều cách chứng minh của Định lý này, tuy nhiên các chứng minh đều khá phức tạp, vả lại các chứng minh đã biết đều mang đặc thù tôpô, hình học hoặc giải tích. Do đó, chúng tôi không trình bày phép chứng minh của Định lý ở đây.

4.2. Hệ quả. *Các đa thức bất khả quy của vành $\mathbb{C}[x]$, $\mathbb{C}$ là trường số phức, là các đa thức bậc nhất.*

Chứng minh. Hiển nhiên các đa thức bậc nhất là các đa thức bất khả quy. Giả sử $f(x)$ là một đa thức của $\mathbb{C}[x]$ có bậc lớn hơn 1. Theo Định lý 4.1, $f(x)$ có nghiệm phức $c \in \mathbb{C}$. Vậy $f(x)$ chia hết cho $x - c$, do đó $f(x)$ không bất khả quy. ■

4.3. Mệnh đề. *Nếu một số phức α là nghiệm của đa thức $f(x)$ với hệ số thực thì số phức liên hợp $\overline{\alpha}$ cũng là một nghiệm của $f(x)$.*

Chứng minh. Giả sử

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$$

là một đa thức với hệ số thực và α là một nghiệm phức của $f(x)$. Khi đó

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0 = 0.$$

Lấy liên hợp hai vế của đẳng thức trên ta được

$$a_n\overline{\alpha}^n + a_{n-1}\overline{\alpha}^{n-1} + ... + a_1\overline{\alpha} + a_0 = 0.$$

Điều này chứng tỏ số phức liên hợp $\overline{\alpha}$ cũng là nghiệm của $f(x)$. ■

4.4. Định lý (Các đa thức bất khả quy trong $\mathbb{R}[x]$). *Các đa thức bất khả quy trong $\mathbb{R}[x]$ là các đa thức bậc nhất và các đa thức bậc hai $ax^2 + bx + c$ với biệt số $\Delta = b^2 - 4ac < 0$.*

Chứng minh. Dễ dàng thấy rằng các đa thức bậc nhất và đa thức bậc hai với biệt số $\Delta < 0$ là các đa thức bất khả quy trên $\mathbb{R}$. Ta chứng minh chiều ngược lại. Giả sử $f(x)$ là đa thức bất khả quy trên $\mathbb{R}$ và α là một nghiệm phức. Nếu $\alpha \in \mathbb{R}$ thì $f(x)$ chia hết cho $x - \alpha$, do $f(x)$ bất khả quy nên

$$f(x) = k(x - \alpha),\ k \in \mathbb{R}^*,$$

vậy $f(x)$ là đa thức bậc nhất. Nếu $\alpha \in \mathbb{C} \setminus \mathbb{R}$ thì $\overline{\alpha}$ cũng là nghiệm của $f(x)$, do đó $f(x)$ chia hết cho

$$p(x) = (x - \alpha)(x - \overline{\alpha}) = x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha}.$$

$p(x)$ là một tam thức bậc hai với hệ số thực và có biệt số $\Delta < 0$. Do $f(x)$ bất khả quy nên $f(x) = kp(x), k \in \mathbb{R}^*$. Vậy $f(x)$ là tam thức bậc hai với biệt số $\Delta < 0$. ■

§5. Đa thức trên trường số hữu tỷ

5.1. Nghiệm hữu tỷ của một đa thức với hệ số hữu tỷ

1°. Cho

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0, a_n \neq 0$$

là một đa thức với hệ số hữu tỷ. Khi đó $f(x)$ có thể được viết dưới dạng

$$f(x) = b^{-1}(b_n x^n + b_{n-1}x^{n-1} + ... + b_1 x + b_0) = b^{-1}g(x),$$

trong đó b là mẫu số chung của các phân số $a_i (i = 1, 2, ..., n)$ và b_i là những số nguyên. Tập nghiệm của $f(x)$ bằng tập nghiệm của $g(x)$. Vậy việc tìm nghiệm của một đa thức với hệ số hữu tỷ có thể đưa về việc tìm nghiệm của một đa thức với hệ số nguyên. Lại thấy, nếu α là nghiệm của đa thức $g(x)$ thì

$$b_n\alpha^n + b_{n-1}\alpha^{n-1} + ... + b_1\alpha + b_0 = 0.$$

Nhân hai vế với b_n^{n-1} ta có

$$(b_n\alpha)^n + b_{n-1}(b_n\alpha)^{n-1} + ... + b_1 b_n^{n-2}(b_n\alpha) + b_0 b_n^{n-1} = 0.$$

Do đó $\beta = b_n\alpha$ là nghiệm của đa thức

$$h(x) = x^n + b_{n-1}x^{n-1} + ... + b_1 b_n^{n-2}x + b_0 b_n^{n-1}$$

với hệ số nguyên và hệ số cao nhất bằng 1. Để tìm các nghiệm của $g(x)$ ta chỉ việc tìm các nghiệm của $h(x)$. Như vậy bài toán tìm nghiệm của đa thức với hệ số hữu tỷ được đưa về bài toán tìm nghiệm đa thức với hệ số nguyên mà hệ số cao nhất bằng 1.

2°. Để dễ dàng tìm nghiệm hữu tỷ của các đa thức với hệ số nguyên ta chú ý đến một số tính chất sau đây:

a) Giả sử $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0, n \geq 1$ là một đa thức với hệ số nguyên và $\alpha = \dfrac{p}{q}, (p, q) = 1$ là nghiệm hữu tỷ của $f(x)$. Khi đó p là ước của a_0 còn q là ước của a_n.

b) Mọi nghiệm hữu tỷ của đa thức với hệ số nguyên

$$g(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0, n \geq 1$$

đều là số nguyên và là ước của a_0. Nếu α là nghiệm nguyên của $g(x)$ thì $1 - \alpha$ là ước của $g(1)$, còn $1 + \alpha$ là ước của $g(-1)$.

Chứng minh. a) Nếu $\alpha = \frac{p}{q}, (p, q) = 1$ là nghiệm hữu tỷ của $f(x)$ thì

$$f(x) = a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + ... + a_1\left(\frac{p}{q}\right) + a_0 = 0.$$

Do đó

$$a_np^n + a_{n-1}p^{n-1}q + ... + a_1pq^{n-1} + a_0q^n = 0,$$

suy ra p là ước của a_0q^n và q là ước của a_np^n. Do $(p, q) = 1$ nên suy ra p là ước của a_0 còn q là ước của a_n.

b) Nếu $\alpha = \frac{p}{q}, (p, q) = 1$ là nghiệm hữu tỷ của $g(x)$ thì theo a) p là ước của a_0 còn q là ước của 1, do đó α nguyên và là ước của a_0.

Nếu α là một nghiệm nguyên của $g(x)$ thì $g(x) = (x - \alpha)q(x)$, với $q(x) \in \mathbb{Z}[x]$. Do đó

$$g(1) = (1 - \alpha)q(1) \quad \text{và} \quad g(-1) = -(1 + \alpha)q(-1).$$

Như thế $1 - \alpha$ là ước của $g(1)$, còn $1 + \alpha$ là ước của $g(-1)$. ■

Bây giờ ta sẽ sử dụng các tính chất trên trong ví dụ sau:

5.2. Ví dụ

Tìm nghiệm hữu tỷ của đa thức

$$f(x) = x^5 - 8x^4 + 20x^3 - 20x^2 + 19x - 12.$$

Vì tổng các hệ số của $f(x)$ bằng 0 nên 1 là một nghiệm của $f(x)$. Chia $f(x)$ cho $x - 1$ ta được đa thức thương là

$$g(x) = x^4 - 7x^3 + 13x^2 - 7x + 12.$$

Dễ thấy rằng $g(\alpha) > 0, \forall \alpha < 0$, do đó $g(x)$ không có nghiệm âm. Các nghiệm hữu tỷ của $g(x)$ đều nguyên và phải là các ước dương của 12. Ta lần lượt xét các ước dương của 12 là $2, 3, 4, 6, 12$ ta có $g(1) = 12$, $g(-1) = 40$,

$$\frac{g(-1)}{1+2} = \frac{40}{3}, \quad \frac{g(-1)}{1+6} = \frac{40}{7}, \quad \frac{g(-1)}{1+12} = \frac{40}{13}$$

không phải là các số nguyên nên các số $2, 6, 12$ không phải là nghiệm của $g(x)$ (theo tính chất 2b). Với $\alpha = 3$ và $\alpha = 4$ thì

$$\frac{g(1)}{1-\alpha}, \frac{g(-1)}{1+\alpha}$$

nguyên nên chúng có thể là nghiệm của $g(x)$. Ta lại sử dụng sơ đồ Horner để kiểm tra xem 3 và 4 có phải là nghiệm của $g(x)$ hay không.

	1	−7	13	−7	12
3	1	−4	1	−4	0
4	1	0	1	0	

Vậy ta có các nghiệm nguyên của $g(x)$ là 3 và 4. Do đó các nghiệm hữu tỷ của $f(x)$ là 1, 3 và 4.

5.3. Đa thức bất khả quy của vành $\mathbb{Q}[x]$

Trong §4 ta đã mô tả được tất cả các đa thức bất khả quy trên trường số thực và phức. Trong vành $\mathbb{Q}[x]$ các đa thức trên trường hữu tỷ thì vấn đề phức tạp hơn nhiều. Dưới đây ta sẽ trình bày tiêu chuẩn Eisenstein là một điều kiện đủ để nhận biết một đa thức là bất khả quy trên $\mathbb{Q}$. Để chuẩn bị chứng minh tiêu chuẩn ấy, ta cần một vài khái niệm và bổ đề sau:

5.4. Định nghĩa

Một đa thức với hệ số nguyên được gọi là *đa thức nguyên bản* nếu ước chung lớn nhất của các hệ số là 1.

5.5. Nhận xét

i) Nếu $f(x) \in \mathbb{Z}[x]$, ký hiệu a là ước chung lớn nhất của các hệ số thì $f(x) = af^*(x)$, với $f^*(x)$ là một đa thức nguyên bản.

ii) Nếu $f(x) \in \mathbb{Q}[x]$ thì $f(x)$ được viết dưới dạng

$$f(x) = \frac{a}{b} f^*(x),$$

trong đó $(a, b) = 1$ và $f^*(x)$ là một đa thức nguyên bản.

5.6. Bổ đề. *Tích của hai đa thức nguyên bản lại là một đa thức nguyên bản.*

Chứng minh. Cho hai đa thức nguyên bản

$$\begin{aligned} f(x) &= a_m x^m + a_{m-1} x^{m-1} + ... + a_1 x + a_0, \\ g(x) &= b_n x^n + b_{n-1} x^{n-1} + ... + b_1 x + b_0. \end{aligned}$$

Gọi p là số nguyên tố tùy ý, ta chứng minh rằng p không thể là ước của tất cả các hệ số của $f(x)g(x)$. Vì $f(x)$ và $g(x)$ là các đa thức nguyên bản nên tồn tại ít nhất một hệ số của $f(x)$ và $g(x)$ không chia hết cho p. Giả sử $a_0, ..., a_{r-1}, b_0, ..., b_{s-1}$ chia hết cho p nhưng a_r và b_s không chia hết cho p. Ta xét hệ số c_{r+s} của đa thức $f(x)g(x)$:

$$c_{r+s} = \sum_{i+j=r+s} a_i b_j,$$

ta thấy rằng tất cả các số hạng của c_{r+s}, trừ $a_r b_s$ đều chia hết cho p. Do đó c_{r+s} không chia hết cho p. Vậy $f(x)g(x)$ là đa thức nguyên bản. ■

5.7. Bổ đề. *Nếu $f(x)$ là đa thức với hệ số nguyên có bậc lớn hơn 0 và $f(x)$ không bất khả quy trong $\mathbb{Q}[x]$ thì $f(x)$ phân tích được thành tích những đa thức bậc lớn hơn 0 với hệ số nguyên.*

Chứng minh. Giả sử $f(x)$ là đa thức trong $\mathbb{Z}[x]$ không bất khả quy trên $\mathbb{Q}$. Khi đó $f(x)$ có thể phân tích thành

$$f(x) = \varphi(x)\psi(x),$$

trong đó $0 < \deg\varphi(x), \deg\psi(x) < \deg f(x), \varphi(x), \psi(x) \in \mathbb{Q}[x]$. Theo Nhận xét 5.5, $\varphi(x)$ và $\psi(x)$ có thể viết thành

$$\varphi(x) = \frac{a}{b}g(x),\ \psi(x)\frac{c}{d}h(x),$$

trong đó $g(x), h(x)$ là các đa thức nguyên bản, còn $(a, b) = (c, d) = 1$. Khi đó

$$f(x) = \frac{ac}{bd}g(x)h(x).$$

Gọi p, q là các số nguyên mà $\frac{p}{q} = \frac{ac}{bd}$ sao cho $(p, q) = 1$. Đặt các hệ số của đa thức tích $g(x)h(x)$ là c_i, khi đó các hệ số của $f(x)$ là $\frac{pc_i}{q}$ và là các số nguyên. Do $(p, q) = 1$ nên c_i chia hết cho q. Mà các hệ số của đa thức nguyên bản $g(x)h(x)$ nguyên tố cùng nhau nên $q = \pm 1$, vì vậy

$$f(x) = \pm pg(x)h(x).$$

Vì $0 < \deg\varphi(x), \deg\psi(x) < n$, suy ra $g(x)$ và $h(x)$ là những đa thức có bậc lớn hơn 0. ■

5.8. Tiêu chuẩn Eisenstein

Giả sử

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0\ (n > 1)$$

là đa thức với hệ số nguyên và giả sử tồn tại số nguyên tố p sao cho:

i) hệ số cao nhất a_n không chia hết cho p, tất cả các hệ số còn lại đều chia hết cho p;

ii) hệ số tự do a_0 không chia hết cho p^2.

Khi đó $f(x)$ là một đa thức bất khả quy trong $\mathbb{Q}[x]$.

Chứng minh. Giả sử $f(x)$ không bất khả quy, khi đó theo Bổ đề 5.7, $f(x)$ có thể phân tích được thành tích của hai đa thức với hệ số nguyên và có bậc lớn hơn 0:

$$f(x) = (b_r x^r + b_{r-1}x^{r-1} + ... + b_1 x + b_0)(c_s x^s + c_{s-1}x^{s-1} + ... + c_1 x + c_0),$$

trong đó $0 < r, s < n$. Theo giả thiết, $a_0 = b_0c_0$ chia hết cho p mà p nguyên tố nên b_0 hay c_0 chia hết cho p. Giả sử b_0 chia hết cho p. Thế thì c_0 không chia hết cho p vì a_0 không chia hết cho p^2. Vì $a_n = b_rc_s$ không chia hết cho p nên b_r không chia hết cho p. Giả sử $b_0, ..., b_{k-1}$ chia hết cho p và b_k không chia hết cho p, $1 \leq k \leq r$. Ta có

$$a_k = b_kc_0 + b_{k-1}c_1 + ...,$$

mà $a_k, b_{k-1}, ...$ đều chia hết cho p, suy ra b_kc_0 phải chia hết cho p. Vì p nguyên tố và c_0 không chia hết cho p nên b_k phải chia hết cho p, mâu thuẫn với giả thiết về b_k. ■

5.9. Ví dụ

Dùng tiêu chuẩn Eisenstein để chứng minh các đa thức sau đây bất khả quy trong $\mathbb{Q}[x]$.

a) $x^4 - 8x^3 + 12x^2 - 6x + 2$;

b) $x^4 - x^3 + 2x + 1$.

Giải. a) Xét tiêu chuẩn Eisenstein với $p = 2$, ta thấy rằng hệ số cao nhất không chia hết cho 2, tất cả các hệ số còn lại chia hết cho 2, hệ số tự do không chia hết cho 2^2. Vậy đa thức đã cho bất khả quy trong $\mathbb{Q}[x]$.

b) Để đa thức đã cho như vậy ta không áp dụng được tiêu chuẩn Eisenstein nên ta phân tích đa thức theo lũy thừa của $x - 1$, ta có

$$x^4 - x^3 + 2x + 1 = (x-1)^4 + 3(x-1)^3 + 3(x-1)^2 + 3(x-1) + 3.$$

Đa thức $y^4 + 3y^3 + 3y^2 + 3y + 3$ là bất khả quy vì thỏa mãn tiêu chuẩn Eisenstein với $p = 3$. Do đó đa thức đã cho bất khả quy trong $\mathbb{Q}[x]$.

§6. Vành đa thức nhiều ẩn

6.1. Định nghĩa

Cho R là vành giao hoán có đơn vị, trong §1 ta đã xây dựng được vành $R[x]$ cũng là một vành giao hoán có đơn vị. Từ vành $R[x]$ ta lại

xây dựng được vành $(R[x])[y]$ là vành đa thức một ẩn y độc lập với x. Các phần tử của $(R[x])[y]$ được viết một cách duy nhất dưới dạng

$$\sum_{j=0}^{n} b_j y^j,\ b_j \in R[x], n \in \mathbb{N}.$$

Mỗi phần tử $b_j \in R[x]$ lại có thể được viết dưới dạng

$$b_j = \sum_{i=0}^{m} a_{ij} x^i,\ a_{ij} \in R, m \in \mathbb{N}.$$

Do đó mỗi phần tử của $(R[x])[y]$ đều có dạng

$$\sum_{j=0}^{n} \sum_{i=0}^{m} a_{ij} x^i y^j,\ a_{ij} \in R, m, n \in \mathbb{N}.$$

Đương nhiên, $(R[x])[y]$ cũng là một vành giao hoán có đơn vị, ta gọi nó là *vành đa thức hai ẩn* x, y trên R và ký hiệu là $R[x, y]$.

Vành đa thức n *ẩn* $x_1, x_2, ..., x_n$ được định nghĩa bằng quy nạp như sau:

$$R[x_1, x_2, ..., x_n] = (R[x_1, x_2, ..., x_{n-1}])[x_n].$$

Nói cách khác, $R[x_1, x_2, ..., x_n]$ là vành đa thức một ẩn x_n với các hệ số được lấy trong vành $R[x_1, x_2, ..., x_{n-1}]$. Mỗi phần tử của vành $R[x_1, x_2, ..., x_n]$ được gọi là một *đa thức* n *ẩn* $x_1, x_2, ..., x_n$ với các hệ số trong R, và ký hiệu là $f(x_1, ..., x_n)$, $g(x_1, ..., x_n)$, ... hoặc ngắn gọn là $f, g, ...$ Theo định nghĩa, mỗi phần tử của $R[x_1, ..., x_n]$ đều có dạng

$$f(x_1, ..., x_n) = \sum_{(i_1, ..., i_n)} a_{i_1, ..., i_n} x_1^{i_1} ... x_n^{i_n}, \qquad (1)$$

trong đó $(i_1, ..., i_n) \in \mathbb{N}^n$, các hệ số $a_{i_1, ..., i_n} \in R$ và chỉ có hữu hạn các hệ số khác không. Như thường lệ, ta vẫn gọi chúng là các *hệ số* của đa thức, còn các $a_{i_1, ..., i_n} x_1^{i_1} ... x_n^{i_n}$ gọi là các *số hạng* (hay *hạng tử*) của đa

thức. Từ Định nghĩa suy ra rằng các đa thức n ẩn bằng không khi và chỉ khi các hệ số của nó bằng không. Do đó mỗi đa thức n ẩn đều được viết một cách duy nhất dưới dạng (1).

6.2. Bậc

Cho đa thức $f \in R[x_1, ..., x_n]$ dưới dạng (1).

i) Bậc của f đối với x_i là số mũ cao nhất của x_i trong các hạng tử của f với hệ số khác không và được ký hiệu là $\deg_i f$.

ii) Bậc của hạng tử với hệ số khác không $a_{i_1,...,i_n}x_1^{i_1}...x_n^{i_n}$ là tổng các số mũ $i_1 + ... + i_n$ của các ẩn.

iii) Bậc của đa thức f là số lớn nhất trong các bậc của các hạng tử khác không của nó, ký hiệu là $\deg f$. Qui ước $\deg 0 = -\infty$.

iv) Nếu mọi hạng tử của f đều có bậc k thì f được gọi là một *đa thức đẳng cấp* bậc k hay một *dạng* bậc k. Nói riêng, một dạng bậc nhất được gọi là một *dạng tuyến tính*, một dạng bậc hai được gọi là một *dạng toàn phương*, một dạng bậc ba gọi là một *dạng lập phương*.

6.3. Thứ tự từ điển

Trên lũy thừa Descartes $\mathbb{N}^n$ $(n > 1)$ với $\mathbb{N}$ là tập các số tự nhiên, ta định nghĩa một quan hệ hai ngôi như sau:

$$(a_1, a_2, ..., a_n) \geq (b_1, b_2, ..., b_n)$$

khi và chỉ khi

$$(a_1, a_2, ..., a_n) = (b_1, b_2, ..., b_n)$$

hoặc tồn tại một chỉ số $i, 1 \leq i \leq n$, sao cho

$$a_1 = b_1, ..., a_{i-1} = b_{i-1} \text{ và } a_i > b_i.$$

Dễ dàng kiểm tra thấy rằng quan hệ hai ngôi trên là một quan hệ thứ tự toàn phần trên $\mathbb{N}^n$, ta gọi nó là quan hệ thứ tự từ điển. Bây giờ cho đa thức $f \in R[x_1, ..., x_n]$ có dạng (1). Ta nói hạng tử $ax_1^{i_1}x_2^{i_2}...x_n^{i_n}$ cao hơn hạng tử $bx_1^{j_1}x_2^{j_2}...x_n^{j_n}$ nếu

$$(i_1, i_2, ..., i_n) \geq (j_1, j_2, ..., j_n)$$

và

$$(i_1, i_2, ..., i_n) \neq (j_1, j_2, ..., j_n).$$

Lúc này ta cũng ký hiệu

$$(i_1, i_2, ..., i_n) > (j_1, j_2, ..., j_n).$$

Vì quan hệ thứ tự từ điển là quan hệ thứ tự toàn phần nên ta có thể sắp xếp các hạng tử của f theo thứ tự từ thấp đến cao. Ta gọi cách sắp xếp như vậy là sắp xếp theo thứ tự từ điển.

6.4. Định lý. *Giả sử* $f(x_1, ..., x_n)$ *và* $g(x_1, ..., x_n)$ *là hai đa thức khác không của vành* $R[x_1, ..., x_n]$ *có các hạng tử cao nhất lần lượt là* $ax_1^{i_1}x_2^{i_2}...x_n^{i_n}$ *và* $bx_1^{j_1}x_2^{j_2}...x_n^{j_n}$. *Nếu* $ab \neq 0$ *thì hạng tử cao nhất của đa thức tích* $f(x_1, ..., x_n)g(x_1, ..., x_n)$ *là*

$$abx_1^{i_1+j_1}x_2^{i_2+j_2}...x_n^{i_n+j_n}.$$

Chứng minh. Ta có nhận xét sau:

Nếu $(a_1, ..., a_n), (b_1, ..., b_n), (c_1, ..., c_n), (d_1, ..., d_n) \in \mathbb{N}^n$ thỏa mãn điều kiện

$$(a_1, ..., a_n) > (b_1, ..., b_n), \text{ và } (c_1, ..., c_n) > (d_1, ..., d_n)$$

thì

$$(a_1 + c_1, ..., a_n + c_n) > (b_1 + d_1, ..., b_n + d_n).$$

Thật vậy, vì

$$(a_1, ..., a_n) > (b_1, ..., b_n)$$

nên tồn tại một chỉ số $i, 1 \leq i \leq n$, sao cho

$$a_1 = b_1, ..., a_{i-1} = b_{i-1} \text{ và } a_i > b_i.$$

Do đó

$$a_1 + c_1 = b_1 + c_1, ..., a_{i-1} + c_{i-1} = b_{i-1} + c_{i-1} \text{ và } a_i + c_i > b_i + c_i$$

với mọi $(c_1, ..., c_n) \in \mathbb{N}^n$. Do đó

$$(a_1 + c_1, ..., a_n + c_n) > (b_1 + c_1, ..., b_n + c_n).$$

Tương tự ta có

$$(b_1 + c_1, ..., b_n + c_n) > (b_1 + d_1, ..., b_n + d_n).$$

Suy ra

$$(a_1 + c_1, ...a_n + c_n) > (b_1 + d_1, ..., b_n + d_n).$$

Bây giờ ta chú ý rằng mọi hạng tử của đa thức

$$f(x_1, ..., x_n)g(x_1, ..., x_n)$$

đều có dạng

$$cdx_1^{k_1+l_1}x_2^{k_2+l_2}...x_n^{k_n+l_n},$$

trong đó

$$(i_1, i_2, ..., i_n) \geq (k_1, k_2, ..., k_n)$$

và

$$(j_1, j_2, ..., j_n) \geq (l_1, l_2, ..., l_n).$$

Áp dụng nhận xét ở trên ta có

$$(i_1 + j_1, i_2 + j_2, ..., i_n + j_n) \geq (k_1 + l_1, k_2 + l_2, ..., k_n + l_n).$$

Từ đây ta suy ra khẳng định trong Định lý. ■

§7. Đa thức đối xứng

7.1. Định nghĩa

Giả sử R là một vành giao hoán có đơn vị và $f(x_1, x_2, ..., x_n)$ là một đa thức trong vành $R[x_1, x_2, ..., x_n]$. Ta nói $f(x_1, x_2, ..., x_n)$ là một *đa thức đối xứng* n ẩn nếu

$$f(x_1, x_2, ..., x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)})$$

với mọi hoán vị $\sigma \in S_n$. Trong đó $f(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)})$ được suy ra từ $f(x_1, x_2, ..., x_n)$ bằng cách thay x_i bởi $x_{\sigma(i)}, i = 1, 2, ..., n$.

7.2. Mệnh đề. *Tập hợp tất cả các đa thức đối xứng của vành* $R[x_1, x_2, ..., x_n]$ *lập thành một vành con của vành* $R[x_1, x_2, ..., x_n]$.

Chứng minh. Giả sử $f(x_1, x_2, ..., x_n)$ và $g(x_1, x_2, ..., x_n)$ là hai đa thức đối xứng n ẩn $x_1, x_2, ..., x_n$. Khi đó với mọi hoán vị $\sigma \in S_n$ ta có

$$f(x_1, x_2, ..., x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)})$$

và

$$g(x_1, x_2, ..., x_n) = g(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)}).$$

Do đó

$$f(x_1, x_2, ..., x_n) - g(x_1, x_2, ..., x_n) =$$

$$= f(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)}) - g(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)})$$

và

$$f(x_1, x_2, ..., x_n)g(x_1, x_2, ..., x_n) =$$

$$= f(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)})g(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)}).$$

Vì vậy, theo Định lý 2.2, chương II, ta có điều phải chứng minh. ■

7.3. Đa thức đối xứng cơ bản

Trong lý thuyết các đa thức đối xứng n ẩn $x_1, x_2, ..., x_n$, các đa thức sau đây đóng vai trò quan trọng:

$$\begin{aligned}
\sigma_1 &= x_1 + x_2 + ... + x_n;\\
\sigma_2 &= x_1x_2 + x_1x_3 + ... + x_1x_n + x_2x_3 + ... + x_{n-1}x_n;\\
\sigma_3 &= x_1x_2x_3 + ... + x_1x_2x_n + x_2x_3x_4 + ... + x_{n-2}x_{n-1}x_n;\\
&\cdots\cdots\\
\sigma_n &= x_1x_2...x_n.
\end{aligned}$$

Ta chứng tỏ rằng các đa thức $\sigma_1, \sigma_2, ..., \sigma_n$ là các đa thức đối xứng. Thật vậy, ta gọi z là ẩn mới và xét đa thức

$$f(z) = (z - x_1)...(z - x_n) = z^n - \sigma_1 z^{n-1} + ... + (-1)^n\sigma_n.$$

Dễ thấy $f(z)$ không thay đổi với mọi hoán vị của các ẩn, do đó $\sigma_1, \sigma_2, ..., \sigma_n$ cũng vậy. Như vậy, $\sigma_1, \sigma_2, ..., \sigma_n$ là đa thức đối xứng n ẩn. Ta gọi chúng là các *đa thức đối xứng cơ bản.*

7.4. Định lý cơ bản về đa thức đối xứng. *Mọi đa thức đối xứng $f(x_1, x_2, ..., x_n)$ trong vành $R[x_1, x_2, ..., x_n]$ đều có thể biểu diễn một cách duy nhất dưới dạng một đa thức của các đa thức đối xứng cơ bản với các hệ số trong R.*

Chứng minh. Ta hãy sắp xếp các hạng tử của đa thức đối xứng $f(x_1, ..., x_n)$ theo thứ tự từ điển. Giả sử hạng tử cao nhất của nó là

$$ax_1^{\alpha_1}x_2^{\alpha_2}...x_n^{\alpha_n}. \qquad (1)$$

Vì $f(x_1, ..., x_n)$ là đa thức đối xứng nên $f(x_1, ..., x_n)$ phải chứa các số hạng suy từ (1) bằng cách hoán vị tùy ý các ẩn trong số đó có hạng tử

$$ax_1^{\alpha_1}x_2^{\alpha_2}...x_n^{\alpha_n} = ax_1^{\alpha_2}x_2^{\alpha_1}...x_n^{\alpha_n}.$$

Đương nhiên $(\alpha_1, \alpha_2, ..., \alpha_n) \geq (\alpha_2, \alpha_1, ..., \alpha_n)$ do đó $\alpha_1 \geq \alpha_2$. Lập luận tương tự, ta có $\alpha_2 \geq \alpha_3, ...$ Như vậy $\alpha_1 \geq \alpha_2 \geq ... \geq \alpha_n$. Xét đa thức

$$a{\sigma_1}^{\alpha_1-\alpha_2}{\sigma_2}^{\alpha_2-\alpha_3}...{\sigma_n}^{\alpha_n}. \qquad (2)$$

Ta biết hạng tử cao nhất của $\sigma_1, \sigma_2, ..., \sigma_n$ lần lượt là x_1, x_1x_2, ..., $x_1...x_n$ nên hạng tử cao nhất của (2) là $ax_1^{\alpha_1}x_2^{\alpha_2}...x_n^{\alpha_n}$ (xem Định lý 6.4). Lập

hiệu

$$f(x_1, x_2, ..., x_n) - a{\sigma_1}^{\alpha_1-\alpha_2}{\sigma_2}^{\alpha_2-\alpha_3}...{\sigma_n}^{\alpha_n}$$

thì hạng tử (2) bị mất đi và ta nhận được một đa thức đối xứng $f_1(x_1, ..., x_n)$ bao gồm các hạng tử thấp hơn $ax_1^{\alpha_1}x_2^{\alpha_2}...x_n^{\alpha_n}$.

Giả sử $b_1{x_1}^{\beta_1}x_2^{\beta_2}...x_n^{\beta_n}$ là hạng tử cao nhất của $f_1(x_1, ..., x_n)$. Lại lập hiệu

$$f_2(x_1, ..., x_n) = f_1(x_1, ..., x_n) - b_1{\sigma_1}^{\beta_1-\beta_2}\sigma_2^{\beta_2-\beta_3}...\sigma_n^{\beta_n}$$

là đa thức đối xứng bao gồm các hạng tử thấp hơn $b_1{x_1}^{\beta_1}x_2^{\beta_2}...x_n^{\beta_n}$. Quá trình này không thể kéo dài ra vô tận được vì chỉ có hữu hạn phần tử $(\delta_1, \delta_2, ..., \delta_n) \in \mathbb{N}^n$ thỏa điều kiện $\alpha_1 \geq \delta_1 \geq \delta_2 \geq ... \geq \delta_n$.

Vậy sau một số hữu hạn bước ta sẽ có

$$f_k(x_1, ..., x_n) - b_k{\sigma_1}^{\nu_1-\nu_2}\sigma_2^{\nu_2-\nu_3}...\sigma_n^{\nu_n} = 0.$$

Từ đẳng thức trên ta có

$$f(x_1, x_2, ..., x_n) = a{\sigma_1}^{\alpha_1-\alpha_2}{\sigma_2}^{\alpha_2-\alpha_3}...{\sigma_n}^{\alpha_n} -$$

$$-b_1{\sigma_1}^{\beta_1-\beta_2}\sigma_2^{\beta_2-\beta_3}...\sigma_n^{\beta_n} - ... - b_k{\sigma_1}^{\nu_1-\nu_2}\sigma_2^{\nu_2-\nu_3}...\sigma_n^{\nu_n}.$$

Như vậy ta đã viết được đa thức đối xứng $f(x_1, ..., x_n)$ thành một đa thức trên R của $\sigma_1, ..., \sigma_n$.

Bây giờ ta chứng minh sự biểu diễn như vậy là duy nhất, bằng phương pháp quy nạp theo số ẩn n của đa thức. Định lý hiển nhiên đúng khi $n = 1$. Giả sử định lý đã được chứng minh cho các đa thức bậc $n - 1$, ta chứng minh định lý đúng cho các đa thức n ẩn. Giả sử $h_1, h_2 \in R[x_1, ..., x_n]$ sao cho

$$f(x_1, ..., x_n) = h_1(\sigma_1, ..., \sigma_n) = h_2(\sigma_1, ..., \sigma_n).$$

Ta cần chứng minh $h_1 = h_2$. Giả sử ngược lại $h_1 \neq h_2$. Vì

$$(h_1 - h_2)(\sigma_1, ..., \sigma_n) = h_1(\sigma_1, ..., \sigma_n) - h_2(\sigma_1, ..., \sigma_n) = 0$$

nên tồn tại đa thức $\varphi \in R[x_1, ..., x_n]$ là đa thức khác không bậc thấp nhất sao cho $\varphi(\sigma_1, ..., \sigma_n) = 0$. Ta viết φ như đa thức ẩn x_n với các hệ tử lấy trong vành $R[x_1, ..., x_{n-1}]$:

$$\varphi(x_1, x_2, ..., x_n) = \varphi_0(x_1, ..., x_{n-1}) + \varphi_1(x_1, ..., x_{n-1})x_n + ...$$

$$... + \varphi_k(x_1, ..., x_{n-1})x_n^k. \qquad (*)$$

Ta nhận thấy rằng $\varphi_0(x_1, ..., x_{n-1}) \neq 0$ vì nếu trái lại thì

$$\begin{aligned}\varphi(x_1, x_2, ..., x_n) &= \varphi_1(x_1, ..., x_{n-1})x_n + ... + \varphi_k(x_1, ..., x_{n-1})x_n^k \\ &= x_n(\varphi_1(x_1, ..., x_{n-1}) + ... + \varphi_k(x_1, ..., x_{n-1})x_n^{k-1}) \\ &= x_n\psi(x_1, ..., x_n)\end{aligned}$$

với $\psi(x_1, ..., x_n)$ là đa thức thuộc $R[x_1, ..., x_n]$. Khi đó

$$\varphi(\sigma_1, ..., \sigma_n) = \sigma_n\psi(\sigma_1, ..., \sigma_n) = 0,$$

suy ra $\psi(\sigma_1, ..., \sigma_n) = 0$, mà ψ có bậc bé hơn bậc của φ nên ta có điều mâu thuẫn.

Thay x_i bởi σ_i trong đẳng thức $(*)$ ta có

$$\varphi(\sigma_1, \sigma_2, ..., \sigma_n) = \varphi_0(\sigma_1, ..., \sigma_{n-1}) + \varphi_1(\sigma_1, ..., \sigma_{n-1})\sigma_n + ...$$

$$... + \varphi_k(\sigma_1, ..., \sigma_{n-1})\sigma_n^k. \qquad (**)$$

Trong $(**)$ cho $x_n = 0$ và chú ý rằng khi đó $\sigma_n = 0$, ta có

$$\varphi_0(\sigma_1, \sigma_2, ..., \sigma_{n-1}) = \varphi(\sigma_1, \sigma_2, ..., \sigma_n) = 0.$$

Mặt khác từ $\varphi_0(x_1, ..., x_{n-1}) \neq 0$ ta suy ra $\varphi_0(\sigma_1, \sigma_2, ..., \sigma_{n-1}) \neq 0$ (do giả thiết quy nạp). Điều mâu thuẫn này kết thúc phép chứng minh định lý. ■

7.5. Phương pháp biểu diễn đa thức đối xứng qua các đa thức đối xứng cơ bản

Từ phép chứng minh của Định lý cơ bản về đa thức đối xứng ta suy ra thuật toán biểu diễn một đa thức đối xứng qua các đa thức đối xứng cơ bản như sau:

Giả sử đã cho đa thức đối xứng n ẩn

$$f(x_1, ..., x_n) \in R[x_1, ..., x_n]$$

với hạng tử cao nhất (theo thứ tự từ điển) là

$$ax_1^{\alpha_1}x_2^{\alpha_2}...x_n^{\alpha_n}(\alpha_1 \geq \alpha_2 \geq ... \geq \alpha_n).$$

Ta tiến hành như sau:

Bước 1. Chọn hệ thống số mũ, mỗi hệ thống gồm n số tự nhiên thỏa mãn các điều kiện: tổng các số của hệ thống đều bằng bậc của đa thức, tức là bằng $\alpha_1 + \alpha_2 + ... + \alpha_n$; các số trong mỗi hệ thống, số đứng sau bé hơn hoặc bằng số đứng trước nó, hệ thống sau bé hơn hệ thống trước theo thứ tự từ điển.

Bước 2. Với mỗi hệ thống số mũ $(\beta_1, \beta_2, ..., \beta_n)$ lập tích các đa thức đối xứng cơ bản

$$a_i{\sigma_1}^{\beta_1-\beta_2}...\sigma_{n-1}^{\beta_{n-1}-\beta_n}\sigma_n^{\beta_n},$$

trong đó hệ số a_i được xác định sau. Lấy tổng các tích nói trên

$$\sum_i a_i{\sigma_1}^{\beta_1-\beta_2}...\sigma_{n-1}^{\beta_{n-1}-\beta_n}\sigma_n^{\beta_n}. \tag{3}$$

Bước 3. Bằng phương pháp hệ số bất định, so sánh hệ số của $f(x_1, ..., x_n)$ và hệ số của (3) để tính các hệ số a_i chưa biết của (3).

7.6. Ví dụ

Biểu diễn đa thức đối xứng sau đây qua các đa thức đối xứng cơ bản:

$$f(x_1,x_2,x_3)=x_1^3x_2^2x_3+x_1^3x_2x_3^2+x_1^2x_2x_3^3+x_1x_2^2x_3^3+$$

$$+x_1^2x_2^3x_3^2+x_1x_2^3x_3^2+x_1^3+x_2^3+x_3^3\in\mathbb{Z}[x_1,x_2,x_3].$$

Giải. Trước hết ta nhận thấy rằng đa thức $f(x_1,x_2,x_3)$ là tổng hai đa thức thuần nhất

$$f(x_1,x_2,x_3)=\varphi(x_1,x_2,x_3)+\psi(x_1,x_2,x_3),$$

trong đó $\varphi(x_1,x_2,x_3)$ gồm các hạng tử có bậc bằng 6, còn $\psi(x_1,x_2,x_3)$ là các hạng tử còn lại của $f(x_1,x_2,x_3)$.

Ta sẽ áp dụng thuật toán trên để biểu diễn các đa thức φ và ψ qua các đa thức đối xứng cơ bản.

a) Biểu diễn φ qua các đa thức đối xứng cơ bản.

• Hệ thống số mũ: $(3,2,1)$, $(2,2,2)$.

• $\varphi(x_1,x_2,x_3)=\sigma_1\sigma_2\sigma_3+a\sigma_3^2$.

• Cho $x_1=x_2=1,x_3=-2$ thì

$$\varphi(x_1,x_2,x_3)=-12,\sigma_1=0,\sigma_2=-5,\sigma_3=-2.$$

Do đó $-12=4a$. Vậy $a=-3$. Suy ra

$$\varphi(x_1,x_2,x_3)=\sigma_1\sigma_2\sigma_3-3\sigma_3^2.$$

b) Biểu diễn ψ qua các đa thức đối xứng cơ bản.

• Hệ thống số mũ: $(3,0,0)$, $(2,1,0)$, $(1,1,1)$.

• $\psi(x_1,x_2,x_3)=\sigma_1^3+a\sigma_1\sigma_2+b\sigma_3$.

• Bằng cách gán cho x_1,x_2,x_3 những giá trị thích hợp ta sẽ thu được $a=-3,b=3$. Do đó ta có

$$\psi(x_1,x_2,x_3)=\sigma_1^3-3\sigma_1\sigma_2+3\sigma_3.$$

Như vậy

$$f(x_1, x_2, x_3) = \sigma_1^3 - 3\sigma_3^2 - 3\sigma_1\sigma_2 + \sigma_1\sigma_2\sigma_3 + 3\sigma_3.$$

7.7. Ứng dụng đa thức đối xứng vào đại số sơ cấp

Nhiều bài toán trong đại số sơ cấp mà giả thiết của bài toán có tính đối xứng, chẳng hạn giải hệ phương trình đối xứng nhiều ẩn số, chứng minh hằng đẳng thức, bất đẳng thức,... có thể giải được bằng cách phân tích các đa thức xuất hiện trong bài toán qua các đa thức đối xứng cơ bản. Khi đó bài toán có thể trở nên dễ dàng hơn. Để minh họa, ta xét ví dụ:

7.8. Ví dụ

Tìm nghiệm nguyên của hệ phương trình

$$\begin{cases} x_1 + x_2 + x_3 &= 6 \\ x_1^3 + x_2^3 + x_3^3 &= 36 \\ x_1x_2x_3 &= 6 \end{cases}$$

Giải. Theo Ví dụ 7.6, ta có $x_1^3 + x_2^3 + x_3^3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$, ở đây $\sigma_1, \sigma_2, \sigma_3$ là các đa thức đối xứng cơ bản của vành $\mathbb{Z}[x_1, x_2, x_3]$. Hệ phương trình trở thành

$$\begin{cases} \sigma_1 &= 6 \\ \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 &= 36 \\ \sigma_3 &= 6 \end{cases}, \text{ suy ra } \begin{cases} \sigma_1 &= 6 \\ \sigma_2 &= 11 \\ \sigma_3 &= 6 \end{cases}$$

Như vậy x_1, x_2, x_3 phải là nghiệm của đa thức bậc ba

$$f(x) = x^3 - \sigma_1x^2 + \sigma_2x - \sigma_3 = x^3 - 6x^2 + 11x - 6 = (x-1)(x^2 - 5x + 6).$$

Dễ thấy các nghiệm nguyên của $f(x)$ là $1, 2, 3$. Do đó các nghiệm nguyên của hệ phương trình đã cho là $(1, 2, 3)$, $(1, 3, 2)$, $(2, 1, 3)$, $(2, 3, 1)$, $(3, 1, 2)$, $(3, 2, 1)$.

§8. Kết thức, biệt thức

Trong suốt mục này ta giả thiết K là trường có đặc số 0.

8.1. Định nghĩa

Cho

$$f(x) = a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n(a_0 \neq 0)$$

và

$$g(x) = b_0x^s + b_1x^{s-1} + ... + b_{s-1}x + b_s(b_0 \neq 0) \quad (1)$$

là các đa thức thuộc $K[x]$. Giả sử $f(x)$ có n nghiệm $\alpha_1, \alpha_2, ..., \alpha_n$ và $g(x)$ có s nghiệm $\beta_1, \beta_2, ..., \beta_s$ trong $\overline{K}$. Phần tử

$$R(f,g) = a_0^s b_0^n \prod_{i=1}^{n} \prod_{j=1}^{s} (\alpha_i - \beta_j) \quad (2)$$

của trường $\overline{K}$ được gọi là *kết thức* của đa thức $f(x)$ và $g(x)$.

8.2. Nhận xét

i) Từ (2) ta nhận thấy rằng các đa thức $f(x)$ và $g(x)$ có nghiệm chung trong $\overline{K}$ khi và chỉ khi $R(f,g) = 0$.

ii) Vì $g(x)$ có s nghiệm trong $\overline{K}$ là $\beta_1, \beta_2, ..., \beta_s$ nên $g(x)$ có thể phân tích thành tích của các nhân tử tuyến tính

$$g(x) = b_0 \prod_{j=1}^{s} (x - \beta_j)$$

do đó

$$g(\alpha_i) = b_0 \prod_{j=1}^{s} (\alpha_i - \beta_j), 1 \leq i \leq n.$$

Như vậy kết thức $R(f,g)$ có thể được viết dưới dạng

$$R(f,g) = a_0^s \prod_{i=1}^{n} g(\alpha_i). \quad (3)$$

Tương tự, cũng có

$$R(g,f) = b_0^n \prod_{j=1}^{s} f(\beta_j). \tag{4}$$

iii) $$R(g,f) = b_0^n a_0^s \prod_{j=1}^{s}\prod_{i=1}^{n}(\beta_j - \alpha_i) = (-1)^{ns} R(f,g). \tag{5}$$

Từ (3), (4) hay (5) chúng ta đều nhận thấy kết thức $R(f,g)$ không có tính chất đối xứng đối với $f(x)$ và $g(x)$.

iv) Định nghĩa kết thức của hai đa thức $f(x)$ và $g(x)$ bởi công thức (2) bất lợi ở chỗ phải biết tất cả các nghiệm của $f(x)$ và $g(x)$. Vì vậy, dưới đây ta sẽ tìm cách tính kết thức của $f(x)$ và $g(x)$ thông qua các hệ số của chúng.

8.3. Định lý. *Cho các đa thức $f(x)$ và $g(x)$ như (1). Khi đó kết thức $R(f,g)$ bằng định thức cấp $n+s$ sau đây:*

$$D = \left|\begin{array}{cccccc}
a_0 & a_1 & \ldots & a_n & & \\
 & a_0 & a_1 & \ldots & a_n & \\
 & & \ldots & & & \\
 & & & a_0 & a_1 & \ldots\ a_n \\
b_0 & b_1 & \ldots & b_s & & \\
 & b_0 & b_1 & \ldots & b_s & \\
 & & \ldots & & & \\
 & & & b_0 & b_1 & \ldots\ b_s
\end{array}\right| \begin{array}{l} \left.\vphantom{\begin{array}{c}a\\a\\a\end{array}}\right\} s \text{ dòng} \\ \left.\vphantom{\begin{array}{c}a\\a\\a\end{array}}\right\} n \text{ dòng} \end{array}$$

(Các chỗ trống trong định thức đều bằng 0).

Chứng minh. Gọi

$$\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_s \tag{6}$$

lần lượt là n nghiệm của $f(x)$ và s nghiệm của $g(x)$ trong $\overline{K}$. Để chứng minh định lý, ta sẽ tính tích $a_0^s b_0^n DM$ bằng hai cách, trong đó M là

định thức Vandermonde cấp $n+s$ xác định như sau

$$M = \begin{vmatrix} \beta_1^{n+s-1} & \dots & \beta_s^{n+s-1} & \alpha_1^{n+s-1} & \dots & \alpha_n^{n+s-1} \\ \beta_1^{n+s-2} & \dots & \beta_s^{n+s-2} & \alpha_1^{n+s-2} & \dots & \alpha_n^{n+s-2} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \beta_1 & \dots & \beta_s & \alpha_1 & \dots & \alpha_n \\ 1 & \dots & 1 & 1 & \dots & 1 \end{vmatrix}$$

Trước hết, theo công thức tính định thức Vandermonde ta có ngay

$$M = \prod_{1\le i<j\le s}(\beta_i - \beta_j)\prod_{j=1}^{s}\prod_{i=1}^{n}(\beta_j - \alpha_i)\prod_{1\le i<j\le n}(\alpha_i - \alpha_j). \tag{7}$$

Theo (5) ta có

$$a_0^s b_0^n DM = DR(g,f)\prod_{1\le i<j\le s}(\beta_i - \beta_j)\prod_{1\le i<j\le n}(\alpha_i - \alpha_j). \tag{8}$$

Mặt khác, ta sẽ tính DM như là định thức của tích hai ma trận. Thực hiện phép nhân hai ma trận mà các dòng và các cột của nó lần lượt chính là các dòng và cột của hai định thức D và M, chú ý rằng $f(\alpha_i) = 0, g(\beta_j) = 0$ với $1 \le i \le n, 1 \le j \le s$. Ta thu được

$$M = \begin{vmatrix} \beta_1^{s-1}f(\beta_1) & \dots & \beta_s^{s-1}f(\beta_s) & 0 & \dots & 0 \\ \beta_1^{s-2}f(\beta_1) & \dots & \beta_s^{s-2}f(\beta_s) & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \beta_1 f(\beta_1) & \dots & \beta_s f(\beta_s) & 0 & \dots & 0 \\ f(\beta_1) & \dots & f(\beta_s) & 0 & \dots & 0 \\ 0 & \dots & 0 & \alpha_1^{n-1}g(\alpha_1) & \dots & \alpha_n^{n-1}g(\alpha_n) \\ 0 & \dots & 0 & \alpha_1^{n-2}g(\alpha_1) & \dots & \alpha_n^{n-2}g(\alpha_n) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \alpha_1 g(\alpha_1) & \dots & \alpha_n g(\alpha_n) \\ 0 & \dots & 0 & g(\alpha_1) & \dots & g(\alpha_n) \end{vmatrix}$$

Áp dụng khai triển Laplace, rồi sau đó trong mỗi định thức thu được đưa các nhân tử chung của mỗi cột ra ngoài ta thu được hai định thức

Vandermonde cấp s và cấp n. Do đó

$$a_0^s b_0^n DM = a_0^s b_0^n \prod_{j=1}^{s} f(\beta_j) \prod_{1\le i<j\le s} (\beta_i - \beta_j) \prod_{i=1}^{n} g(\alpha_i) \prod_{1\le i<j\le n} (\alpha_i - \alpha_j).$$

Sử dụng công thức (3) và (4) ta nhận được

$$a_0^s b_0^n DM = R(f,g)R(g,f) \prod_{1\le i<j\le s} (\beta_i - \beta_j) \prod_{1\le i<j\le n} (\alpha_i - \alpha_j). \qquad (9)$$

Bằng cách xem (6) như là một hệ gồm $n+s$ biến độc lập, khi đó từ (8) và (9) ta suy ra $D = R(f,g)$. ■

8.4. Ví dụ

Cho các đa thức trong $\mathbb{C}[x]$: $f(x) = x^3 - 3x^2 + 1$, $g(x) = x^3 + 3x - 2$. Các đa thức $f(x)$ và $g(x)$ có nghiệm chung trên $\mathbb{C}$ hay không?

Giải. Ta có $R(f,g) = \begin{vmatrix} 1 & -3 & 0 & 1 & 0 & 0 \\ 0 & 1 & -3 & 0 & 1 & 0 \\ 0 & 0 & 1 & -3 & 0 & 1 \\ 1 & 0 & 3 & -2 & 0 & 0 \\ 0 & 1 & 0 & 3 & -2 & 0 \\ 0 & 0 & 1 & 0 & 3 & -2 \end{vmatrix} = -3 \neq 0.$ Vậy đa thức $f(x)$ và $g(x)$ không có nghiệm chung.

8.5. Định nghĩa

Cho đa thức $f(x) \in K[x]$.

$$f(x) = a_0 x^n + a_1 x^{n-1} + ... + a_{n-1}x + a_n (a_0 \neq 0)$$

và gọi $f'(x)$ là đạo hàm của $f(x)$. Biểu thức

$$D = (-1)^{\frac{n(n-1)}{2}} a_0^{-1} R(f, f')$$

được gọi là *biệt thức* của đa thức f.

Từ Định lý 8.3 ta có ngay kết quả sau:

8.6. Mệnh đề. *Đa thức $f(x) \in K[x]$ có nghiệm bội khi và chỉ khi $R(f, f') = 0$, tức là $D = 0$.*

8.7. Ví dụ

Chứng tỏ rằng đa thức $f(x) = x^3 - x^2 - 2x + 1$ không có nghiệm bội trong $\mathbb{C}$.

Giải. Ta có $f'(x) = 3x^2 - 2x - 2$. Do đó

$$R(f, f') = \begin{vmatrix} 1 & -1 & 2 & 1 & 0 \\ 0 & 1 & -1 & 2 & 1 \\ 3 & -2 & -2 & 0 & 0 \\ 0 & 3 & -2 & -2 & 0 \\ 0 & 0 & 3 & -2 & -2 \end{vmatrix} = -49 \neq 0.$$

Vậy đa thức $f(x)$ không có nghiệm bội.

Bài tập

Bài 3.1 Chứng minh rằng đa thức $x^2 + 14 \in \mathbb{Z}_{15}[x]$ có bốn nghiệm phân biệt trong $\mathbb{Z}_{15}$.

Bài 3.2 Xác định các số thực a, b, c sao cho đa thức $f(x) = 2x^4 + ax^2 + bx + c$ chia hết cho $x + 2$ và chia cho $x^2 - 1$ thì dư x.

Bài 3.3 Cho $f \in \mathbb{R}[x]$ và $m, n \in \mathbb{N}^*$.

a) Chứng minh rằng nếu $(x - 1)|f(x^n)$ thì $(x^n - 1)|f(x^n)$.

b) Chứng minh rằng nếu $a \in \mathbb{R}^*$ thỏa $(x - a)^m|f(x^n)$ thì $(x^n - a^n)^m|f(x^n)$.

c) Giả sử $(x^2 + x + 1)|f(x)$ và có $g, h \in \mathbb{R}[x]$ thỏa $f(x) = g(x^3) + xh(x^3)$. Chứng minh rằng $(x - 1)|g(x)$ và $(x - 1)|h(x)$.

Bài 3.4 Cho F là một trường và K là một trường con của F. Chứng minh rằng với $f, g \in K[x]$, f là ước của g trong $K[x]$ khi và chỉ khi f là ước của g trong $F[x]$.

Bài 3.5 Chứng minh rằng trong vành $\mathbb{C}[x]$, $f(x)|g(x)$ khi và chỉ khi mọi nghiệm của $f(x)$ đều là nghiệm của $g(x)$ và mọi nghiệm bội cấp k của $f(x)$ đều là nghiệm bội cấp l với $l \geq k$ của $g(x)$.

Bài 3.6 Trong các trường hợp sau hãy chứng minh $f|g$ trong $\mathbb{Q}[x]$.

a) $f(x) = x(x+1)(2x+1)$ và $g(x) = (x+1)^{2n} - x^{2n} - 2x - 1$.

b) $f(x) = x^2 - x + 1$ và $g(x) = (x-1)^{n+2} + x^{2n+1}$.

c) $f(x) = x^2 + x + 1$ và $g(x) = x^{3k} + x^{3m+1} + x^{3n+2}$.

trong đó k, m, n là các số nguyên dương.

Bài 3.7 Tìm điều kiện của $k, m, n \in \mathbb{N}$ để $f|g$ trong $\mathbb{Q}[x]$ cho mỗi trường hợp sau:

a) $f(x) = x^2 + x + 1$ và $g(x) = x^{2n} + x^n + 1$.

b) $f(x) = x^2 + x + 1$ và $g(x) = (x+1)^n + x^n + 1$.

c) $f(x) = x^2 - x + 1$ và $g(x) = (x-1)^n + x^n + 1$.

d) $f(x) = x^2 - x + 1$ và $g(x) = x^{3k} - x^{3m+1} + x^{3n+2}$.

Bài 3.8 * Với mỗi số nguyên dương k, đặt $f_k(x) = x^k - 1$ là đa thức với hệ số hữu tỉ. Chứng minh rằng với mọi $m, n \in \mathbb{N}^*$,

a) $f_m|f_n$ khi và chỉ khi $m|n$.

b) $(f_m, f_n) = f_d$ với $d = (m, n)$.

Bài 3.9 Cho F là trường $\mathbb{Q}$ hay trường $\mathbb{Z}_5$ và $f, g \in F[x]$. Tìm $h = (f, g)$; $k = [f, g]$ và $u, v \in F[x]$ thỏa $h = uf + vg$ trong các trường hợp sau:

a) $f(x) = 4x^4 - 2x^3 - 16x^2 + 5x + 9$ và $g(x) = 2x^3 - x^2 - 5x + 4$.

b) $f(x) = x^5 + 3x^4 + x^3 + x^2 + 3x + 1$ và $g(x) = x^4 + 2x^3 + x + 2$.

c) $f(x) = 4x^4 - 8x^3 + 9x^2 - 5x + 1$ và $g(x) = 4x^4 + x^2 + 3x + 1$.

Bài 3.10 Trong các trường hợp sau hãy tìm khai triển Taylor của đa thức $f \in \mathbb{R}[x]$ tại x_0. Xét xem x_0 là nghiệm bội cấp mấy của f và tìm các đạo hàm $f^{(i)}(x_0)$ với $1 \leq i \leq 6$.

a) $f(x) = x^5 - 2x^4 - 5x^3 + 15x^2 - 16x + 12$ và $x_0 = 2$.

b) $f(x) = x^5 - 5x^4 + 4x^3 + 4x^2 + 3x + 9$ và $x_0 = 3$.

c) $f(x) = x^6 - 6x^5 + 13x^4 - 15x^3 + 18x^2 - 20x + 8$ và $x_0 = 2$.

d) $f(x) = 8x^6 - 12x^5 + 6x^4 + 7x^3 - 12x^2 + 6x - 1$ và $x_0 = 1/2$.

Bài 3.11 Trong các trường hợp sau hãy tìm tất cả các đa thức f thỏa điều kiện đã cho:

a) $f \in \mathbb{R}[x]$ thỏa $f(2) = 4;\ f(3) = 6;\ f(4) = 8$.

b) $f \in \mathbb{Z}_5[x]$ thỏa $f(\overline{2}) = \overline{1};\ f(-\overline{1}) = \overline{3};\ f(\overline{3}) = \overline{2}$.

c) $f \in \mathbb{Z}_{101}[x]$ thỏa $f(\overline{2}) = \overline{30};\ f(\overline{5}) = \overline{21};\ f(\overline{3}) = \overline{-13}$.

Bài 3.12 Cho F là một trường và $a, b \in F;\ a \neq 0$. Chứng minh rằng $f(x) \in F[x]$ bất khả qui khi và chỉ khi $f(ax + b)$ bất khả qui.

Bài 3.13 * Cho $a_1, ..., a_n$ là các số nguyên phân biệt. Chứng minh rằng các đa thức sau bất khả qui trên $\mathbb{Q}$.

a) $f(x) = (x - a_1)...(x - a_n) - 1$.

b) $g(x) = (x - a_1)^2...(x - a_n)^2 + 1$.

Bài 3.14 Trong các trường hợp sau hãy phân tích f thành tích các đa thức bất khả qui trên $\mathbb{Q}$, trên $\mathbb{R}$ và trên $\mathbb{C}$:

a) $f(x) = x^5 + 2x^4 - 2x^3 - 15x - 18$.

b) $f(x) = x^5 + 2x^4 - 7x^3 - 14x^2 - 18x - 36$.

c) $f(x) = x^5 - 2x^4 - 4x^3 + 4x^2 - 5x + 6$.

d) $f(x) = 16x^6 - 36x^5 - 84x^4 + 99x^3 + 201x^2 + 45x - 25$.

e) $f(x) = 9x^6 - 30x^5 + 49x^4 - 28x^3 - 4x^2 + 16x + 4$.

f) $f(x) = -4x^6 - 23x^5 - 63x^4 - 85x^3 - 57x^2 - 8x - 16$.

Bài 3.15 Chứng minh rằng các đa thức sau bất khả qui trên $\mathbb{Q}$.

a) $x^4 - 8x^3 + 12x^2 - 6x + 3$.

b) $x^4 - x^3 + 2x + 1$.

c) $x^{p-1} + ... + x + 1$ với p là số nguyên tố dương.

d) $5x^3 + 6x^2 + 5x + 25$.

e) $7x^3 + 6x^2 + 11x + 11$.

f) $x^3 - 3n^2x + n^3$ với n nguyên dương.

g) $3x^4 + 5x^3 - 4x + 1$.

h) $x^4 - 9x^3 + 6x - 1$.

i) $x^4 + 8x^3 + x^2 + 2x + 5$.

Bài 3.16 Giải các phương trình bậc 3 sau trong $\mathbb{C}$:

a) $4x^3 - 36x^2 + 84x - 20 = 0$.

b) $x^3 - x - 6 = 0$.

c) $x^3 + 18x + 15 = 0$.

d) $x^3 + 3x^2 - 6x + 4 = 0$.

Bài 3.17 Chứng minh rằng nếu $x_1,\ x_2,\ x_3$ là các nghiệm phức của phương trình $x^3 + px + q = 0$ thì

$$(x_2 - x_1)^2(x_3 - x_2)^2(x_1 - x_3)^2 = -4p^3 - 27q^2.$$

Bài 3.18 Giải các phương trình bậc 4 sau trong $\mathbb{C}$:

a) $x^4 - 3x^3 + x^2 + 4x - 6 = 0$.

b) $x^4 - 4x^3 + 3x^2 + 2x - 1 = 0$.

c) $x^4 + 2x^3 + 8x^2 + 2x + 7 = 0$.

d) $x^4 + 6x^3 + 6x^2 - 8 = 0$.

Bài 3.19 * Cho $f(x)$ là một đa thức với hệ số nguyên có $f(0)$ và $f(1)$ đều lẻ. Chứng minh rằng $f(x)$ không có nghiệm nguyên.

Bài 3.20 Chứng minh rằng đa thức $x^4 + px^2 + q$ bất khả qui trên $\mathbb{Q}$ khi và chỉ khi các số $p^2 - 4q;\ 2\sqrt{q} - p$ không là bình phương của các số hữu tỉ.

Bài 3.21 Biểu thị các đa thức đối xứng sau đây qua các đa thức đối xứng cơ bản:

a) ${x_1}^3 + {x_2}^3 + {x_3}^3 - 3x_1x_2x_3$.

b) ${x_1}^2x_2 + x_1{x_2}^2 + x_1{x_3}^2 + {x_2}^2x_3 + x_2{x_3}^2$.

c) ${x_1}^4 + {x_2}^4 + {x_3}^4 - 2{x_1}^2{x_2}^2 - 2{x_2}^2{x_3}^2 - 2{x_3}^2{x_1}^2$.

d) ${x_1}^5{x_2}^2 + {x_1}^2{x_2}^5 + {x_1}^5{x_3}^2 + {x_1}^2{x_3}^5 + {x_2}^5{x_3}^2 + {x_2}^2{x_3}^5$.

e) $(x_1 + x_2)(x_1 + x_3)(x_2 + x_3)$.

f) $(2x_1 - x_2 - x_3)(2x_2 - x_1 - x_3)(2x_3 - x_1 - x_2)$.

g) $(x_1x_2 + x_3x_4)(x_1x_3 + x_2x_4)(x_1x_4 + x_2x_3)$.

h) $(x_1 + x_2 - x_3 - x_4)(x_1 - x_2 + x_3 - x_4)(x_1 - x_2 - x_3 + x_4)$.

Bài 3.22 a) Tính tổng bình phương các nghiệm của phương trình

$$x^3 + 2x - 3 = 0.$$

b) Tính

$${x_1}^3x_2 + x_1{x_2}^3 + {x_2}^3x_3 + x_2{x_3}^3 + {x_3}^3x_1 + x_3{x_1}^3$$

trong đó x_1, x_2, x_3 là các nghiệm của phương trình

$$x^3 - x^2 - 4x + 1 = 0.$$

c) Giả sử x_1, x_2, x_3 là các nghiệm của phương trình

$$x^3 + px + q = 0.$$

Tính

$$\frac{x_1}{x_2} + \frac{x_2}{x_3} + \frac{x_3}{x_1} + \frac{x_2}{x_1} + \frac{x_3}{x_2} + \frac{x_1}{x_3}.$$

Bài 3.23 Cho phương trình

$$x^3 + a_1x^2 + a_2x + a_3 = 0.$$

Biểu thị các đa thức đối xứng sau đây qua các hệ số của phương trình đó.

a) $({x_1}^2 - x_2x_3)({x_2}^2 - x_3x_1)({x_3}^2 - x_1x_2)$.

b) $({x_1}^2 + x_1x_2 + {x_2}^2)({x_2}^2 + x_2x_3 + {x_3}^2)({x_3}^2 + x_3x_1 + {x_1}^2)$.

Bài 3.24 Dùng đa thức đối xứng, giải các hệ phương trình sau:

a) $\begin{cases} x + y + z = 2 \\ x^2 + y^2 + z^2 = 14 \\ \dfrac{1}{x} + \dfrac{1}{y} + \dfrac{1}{z} = \dfrac{5}{6} \end{cases}$

b) $\begin{cases} x + y + z = -2 \\ x^2 + y^2 + z^2 = -8 \\ xyz = 2 \end{cases}$

c) $\begin{cases} x^2 + y^2 + z^2 = 7 \\ x^3 + y^3 + z^3 = 27 \\ \dfrac{1}{x} + \dfrac{1}{y} + \dfrac{1}{z} = \dfrac{1}{9} \end{cases}$

Chương IV

MÔĐUN VÀ ĐẠI SỐ

§1. Khái niệm về môđun

Khái niệm về môđun là sự tổng quát hóa của không gian vectơ trên một trường. Trong chương này chúng tôi chỉ xét trường hợp vành hệ tử R là giao hoán. Nếu vành hệ tử R không giao hoán thì ta cần phân biệt môđun phải, môđun trái trên R. Đó là một trong những chú ý khá tinh tế. Độc giả quan tâm nhiều hơn về lý thuyết môđun có thể tham khảo trong sách [1].

1.1. Định nghĩa

Cho R là vành giao hoán có đơn vị , đơn vị của R ký hiệu là 1. Một *môđun* trên vành R là một nhóm Abel X (viết theo lối cộng) cùng với một ánh xạ

$$\begin{aligned} R \times X &\longrightarrow X \\ (r, x) &\longmapsto rx, \end{aligned}$$

(ánh xạ này thường được gọi là phép nhân với vô hướng trong R) sao cho các tiên đề sau đây cần được thỏa mãn:

(M1) $\forall x \in X, 1x = x$,

(M2) $\forall r, s \in R, \forall x \in X, (rs)x = r(sx)$,

(M3) $\forall r \in R, \forall x, y \in X, r(x+y) = rx + ry$,

(M4) $\forall r, s \in R, \forall x \in X, (r+s)x = rx + sx$.

Phép nhân với vô hướng trong R cũng còn được gọi là *phép nhân ngoài* từ R vào X. Vành R được gọi là *vành hệ tử* hay *vành các vô hướng*. Các môđun trên R cũng được gọi là các *R-môđun*. Hơn nữa, khi vành hệ tử R đã xác định, để đơn giản, ta sẽ gọi các R-môđun là các *môđun*.

1.2. Các ví dụ

a) Rõ ràng mỗi không gian vectơ trên trường F đều là các F-môđun.

b) Cho X là vành bất kỳ có đơn vị 1 và R là một vành con giao hoán của X chứa 1. Ánh xạ

$$\begin{aligned} R \times X &\longrightarrow X \\ (r, x) &\longmapsto rx \end{aligned}$$

(ở đây rx là tích của các phần tử r và x trong vành X) thỏa mãn các điều kiện (M1)-(M4). Do đó mọi vành X với đơn vị 1 đều là môđun trên bất kỳ vành con giao hoán nào đó của nó chứa 1. Nói riêng, mọi vành giao hoán với đơn vị đều có thể xem là môđun trên chính nó. Như vậy các nghiên cứu về môđun cho chúng ta biết tính chất của vành giao hoán có đơn vị.

c) Một nhóm cộng Abel A có thể xem là môđun trên vành số nguyên $\mathbb{Z}$, trong đó tích của $n \in \mathbb{Z}$ với $a \in A$ là bội nguyên n của a, mà ta vẫn ký hiệu là na như thông thường.

d) Nhóm cộng chỉ gồm một phần tử 0 là một môđun trên vành bất kỳ, được gọi là *môđun không* và ký hiệu là 0.

f) Tập hợp $X = R^S$ tất cả các ánh xạ $f : S \longrightarrow R$ từ một tập hợp S vào vành giao hoán có đơn vị R lập thành nhóm như với phép cộng định nghĩa bởi

$$(f+g)(s) = f(s) + g(s)$$

với f, g tùy ý thuộc X và s tùy ý thuộc S . Phép nhân với vô hướng trong R xác định bởi

$$rf(s) = r(f(s))$$

với f tùy ý thuộc X và s tùy ý thuộc S, thỏa mãn các điều kiện (M1)-(M4) . Do đó X là R-môđun .

1.3. Vài tính chất đơn giản của môđun

Cho X là R - môđun

Tính chất 1. $\forall x \in X, \forall r \in R,\ 0x = 0,\ r0 = 0$.

Thật vậy, $0x = (0+0)x = 0x + 0x$ và $r0 = r(0+0) = r0 + r0$. Do đó $0x = 0$ và $r0 = 0$.

Tính chất 2. $\forall r \in R, \forall x \in X,\ (-r)x = r(-x) = -rx$.

Thật vậy, $(-r)x + rx = (-r+r)x = 0x = 0$ và $r(-x) + rx = r(-x+x) = r0 = 0$, do đó $(-r)x = -rx$ và $r(-x) = -rx$.

Tính chất 3. $\forall x, y \in X, \forall r, s \in R,\ (r-s)x = rx - sx$ và $r(x-y) = rx - ry$.

Thật vậy, $(r-s)x = (r+(-s))x = rx + (-s)x = rx + (-sx) = rx - sx$. Tương tự, $r(x-y) = rx - ry$.

1.4. Môđun con

Cho X là một môđun bất kỳ trên R. Tập con không rỗng A của X được gọi là *môđun con* của X nếu A là một nhóm con của nhóm cộng X và A khép kín đối với phép nhân với vô hướng, tức là $rx \in A$ với mọi $r \in R$, với mọi $x \in A$. Chúng ta dễ dàng thấy rằng:

1) Mọi nhóm con A của nhóm Abel cộng X đều là $\mathbb{Z}$-môđun con của A.

2) Mọi không gian vectơ con A của không gian vectơ X trên trường $\mathbb{F}$ đều là các $\mathbb{F}$-môđun con của X.

3) Xét môđun $X = R^S$ trong Ví dụ 1.2f. Gọi A là tập con của X gồm tất cả các ánh xạ $f : S \longrightarrow R$ sao cho $f(s) = 0$ với tất cả trừ một số hữu hạn những phần tử $s \in S$. Khi đó, A là một R-môđun con của X .

1.5. Định lý. *Mỗi tập hợp con không rỗng A của một môđun X trên R là một môđun con của X nếu và chỉ nếu với mọi $x, y \in A$ và với mọi*

$r \in R$ ta có $x + y \in A$ và $rx \in A$.

Chứng minh. Điều kiện cần là hiển nhiên. Ta chỉ còn phải chứng minh điều kiện đủ. Muốn vậy ta chỉ cần chứng minh rằng $-x \in A$ với mọi $x \in A$. Nhưng điều này hiển nhiên vì

$$-x = (-1)x \in A. \qquad \blacksquare$$

1.6. Định lý. *Giao của họ khác rỗng các môđun con tùy ý của môđun X lại là môđun con của X.*

Chứng minh. Cho $\{A_i | i \in I\}$ là một họ khác rỗng các môđun con của X trên R và giả sử

$$A = \bigcap_{i \in I} A_i.$$

Xét các phần tử x, y tùy ý thuộc A và r tùy ý thuộc R. Với mỗi chỉ số i tùy ý thuộc I ta đều có $x, y \in A_i$, do $A \subset A_i$. Mà A_i là R-môđun con nên suy ra $x + y \in A_i$ và $rx \in A_i$. Do đó $x + y \in A$ và $rx \in A$. Vậy A là R-môđun con của X. $\blacksquare$

1.7. Môđun con sinh bởi một tập hợp

Cho X là một môđun và S là một tập con nào đó của X. Xét họ $\mathcal{T}$ tất cả các môđun con của X chứa S. Đương nhiên $\mathcal{T} \neq \emptyset$ vì $X \in \mathcal{T}$. Theo Định lý 1.6, giao của họ $\mathcal{T}$ là môđun con của X chứa S. Ta gọi môđun con đó là *môđun con sinh bởi tập* S và ký hiệu nó là $\langle S \rangle$. Tập S được gọi là tập sinh (hay hệ sinh) của môđun $\langle S \rangle$. Dễ dàng thấy rằng $\langle S \rangle$ là môđun con nhỏ nhất (theo quan hệ bao hàm) của môđun X chứa S. Chúng ta sẽ mô tả một cách tường minh môđun con sinh bởi tập $S \neq \emptyset$. Trước hết chúng ta cũng có khái niệm tổ hợp tuyến tính tương tự như trong không gian vectơ. Phần tử x của một môđun X trên R được gọi là một tổ hợp tuyến tính của các phần tử trong tập con S của X nếu tồn tại hữu hạn các phần tử $x_1, x_2, ..., x_n \in S$ và $r_1, r_2, ..., r_n \in R$ sao cho

$$x = r_1x_1 + r_2x_2 + \ldots + r_nx_n.$$

Khi đó ta cũng gọi đơn giản x là *tổ hợp tuyến tính* của S. Dễ dàng thấy rằng tổng của hai tổ hợp tuyến tính của S, tích của một hệ tử thuộc R

với một tổ hợp tuyến tính của S cũng là một tổ hợp tuyến tính của S. Như vậy tập hợp A các tổ hợp tuyến tính của S là một môđun con của X. Rõ ràng $S \subset A$ vì mỗi phần tử $x \in S$ cũng là một tổ hợp tuyến tính của S. Hơn nữa, nếu B là một môđun con nào đó của X chứa S thì B chứa A. Vậy $A = \langle S \rangle$. Ta đã chứng minh được định lý sau:

1.8. Định lý. *Môđun con sinh bởi tập $S \subset X$ là môđun con gồm tất cả các tổ hợp tuyến tính của S.*

1.9. Tổng của các môđun con

Cho $\{A_i | i \in I\}$ là họ khác rỗng các môđun con của môđun X. Ta gọi môđun con sinh bởi tập $\bigcup_{i \in I} A_i$ là môđun con tổng của họ các môđun con $\{A_i | i \in I\}$ và ký hiệu là $\sum_{i \in I} A_i$. Như vậy

$$\sum_{i \in I} A_i = \langle \bigcup_{i \in I} A_i \rangle.$$

Theo Định lý 1.8 ta thấy rằng các phần tử của $\sum_{i \in I} A_i$ là các tổ hợp tuyến tính của $\bigcup_{i \in I} A_i$. Nói riêng, nếu A và B là các môđun con của môđun X thì môđun con tổng $A + B$ gồm tất cả các phần tử $x \in X$ có dạng $x = a + b$ với $a \in A, b \in B$.

1.10. Môđun thương

Cho X là một R-môđun và A là môđun con của X. Khi đó $(A, +)$ là nhóm con chuẩn tắc của nhóm $(X, +)$. Do đó ta có nhóm thương X/A hoàn toàn được xác định như trong chương 1. Do X giao hoán nên X/A cũng là nhóm cộng giao hoán. Để biến X/A thành R-môđun ta xác định phép nhân với vô hướng trong R như sau:

$$\begin{array}{rcl} R \times X/A & \longrightarrow & X/A \\ (r, x + A) & \longmapsto & r(x + A) = rx + A. \end{array}$$

Dễ dàng thấy rằng tương ứng nói trên là ánh xạ, nói cách khác, nó xác định phép nhân với vô hướng trong R. Thật vậy, nếu $x + A = x' + A$ thì $x' = x + a$ với $a \in A$. Do đó

$$r(x' + A) = rx' + A = r(x + a) + A = rx + ra + A = rx + A.$$

Có thể kiểm tra một cách đơn giản phép nhân với vô hướng được xác định như trên thỏa mãn các tiên đề (M1)-(M4). Do đó nhóm thương X/A trở thành R-môđun. Ta gọi đó là *môđun thương* của môđun X theo môđun con A của X.

§2. Đồng cấu môđun

2.1. Định nghĩa

Cho X và Y là các R-môđun. Ánh xạ $f : X \longrightarrow Y$ được gọi là *đồng cấu R-môđun* nếu

$$\begin{aligned} f(x+y) &= f(x)+f(y), \\ f(rx) &= rf(x) \end{aligned}$$

với mọi $x, y \in X$ và với mọi $r \in R$. Các đồng cấu R-môđun đôi khi cũng được gọi là các ánh xạ *R-tuyến tính* và để đơn giản ta cũng sẽ gọi là các *đồng cấu* khi vành R đã được chỉ rõ.

Nhận xét. Ánh xạ $f : X \longrightarrow Y$ là đồng cấu R-môđun khi và chỉ khi

$$f(rx+sy) = rf(x)+sf(y), \forall x, y \in X,\ \forall r, s \in R.$$

2.2. Các ví dụ về đồng cấu

a) Ánh xạ nhúng $i : A \longrightarrow X$ từ môđun con A của X vào X xác định bởi $i(x) = x, \forall x \in A$ là một đồng cấu. Thật vậy, với mọi $x, y \in A$ và mọi $r, s \in R$ ta có

$$i(rx+sy) = rx+sy = ri(x)+si(y).$$

Nói riêng, ánh xạ đồng nhất trên một môđun X tùy ý là một đồng cấu, được gọi là *đồng cấu đồng nhất* trên X và thường được ký hiệu là 1_X.

b) Cho A là một môđun con của X, và X/A là môđun thương của môđun X theo A. Ánh xạ chiếu $p : X \longrightarrow X/A$ xác định bởi $p(x) = x+A, \forall x \in X$ cũng là đồng cấu, gọi là *phép chiếu tự nhiên* của môđun X lên môđun thương X/A.

c) Ánh xạ $0 : X \longrightarrow Y$ biến tất cả các phần tử của X thành phần tử 0 của Y là đồng cấu môđun với mọi môđun X, Y. Ta gọi nó là *đồng cấu không*.

d) Đồng cấu $\mathbb{Z}$-môđun chính là đồng cấu của các nhóm Abel.

e) Nếu R là một trường thì R-đồng cấu môđun chính là ánh xạ tuyến tính của các không gian vectơ.

2.3. Tính chất của đồng cấu

a) Vì đồng cấu môđun $f : X \longrightarrow Y$ là đồng cấu của nhóm $f : (X,+) \longrightarrow (Y,+)$ nên f có các tính chất của đồng cấu nhóm Abel. Nói riêng, ta có $f(0) = 0$ và $f(-x) = -f(x), \forall x \in X$.

b) Đồng cấu R-môđun $f : X \longrightarrow Y$ chuyển môđun con của X thành môđun con của Y và nghịch ảnh qua f của một môđun con của Y lại là môđun con của X. Nghĩa là,

i) Nếu A là môđun con của X thì $f(A)$ là môđun con của Y.

ii) Nếu B là môđun con của Y thì $f^{-1}(B)$ là môđun con của X.

Thật vậy, nếu A là môđun con của X và x, y là các phần tử tùy ý của A, r là phần tử tùy ý của R thì $x+y$ và rx cũng là các phần tử của A. Do đó

$$\begin{aligned} f(x)+f(y) &= f(x+y) \in f(A), \\ rf(x) &= f(rx) \in f(A). \end{aligned}$$

Vì vậy $f(A)$ là môđun con của Y.

Nếu B là môđun con của Y thì với mọi x, y thuộc $f^{-1}(B)$ và r tùy ý thuộc R, theo định nghĩa nghịch ảnh, ta có $f(x), f(y)$ và $rf(x) \in B$, suy ra

$$\begin{aligned} f(x+y) &= f(x)+f(y) \in B, \\ f(rx) &= rf(x) \in B. \end{aligned}$$

Do đó $x+y$ và $rx \in f^{-1}(B)$. Vậy $f^{-1}(B)$ là môđun con của X.

Trường hợp riêng, khi chọn $A = X$ ta có $\mathrm{Im}f = f(X)$ là môđun con của Y và khi chọn $B = 0$ thì $\mathrm{Ker}f = f^{-1}(0)$ là môđun con của X.

c) Tích của hai đồng cấu R-môđun là một đồng cấu R-môđun.

Thật vậy, cho $f : X \longrightarrow Y$ và $g : Y \longrightarrow Z$ là các đồng cấu R-môđun. Khi đó gf là đồng cấu từ nhóm Abel X vào Z, do đó

$$gf(x+y) = gf(x) + gf(y), \forall x, y \in X.$$

Bây giờ với x tùy ý thuộc X và r tùy ý thuộc R ta có

$$gf(rx) = g[f(rx)] = g[rf(x)] = rg[f(x)] = rgf(x).$$

Suy ra gf là đồng cấu R-môđun.

2.4. Định nghĩa đơn cấu, toàn cấu, đẳng cấu

Cho đồng cấu R-môđun $f : X \longrightarrow Y$.

i) Nếu f đồng thời là một đơn ánh thì f được gọi là một *đơn cấu môđun.*

ii) Nếu f đồng thời là một toàn ánh thì f được gọi là một *toàn cấu môđun.*

iii) Nếu f đồng thời là một song ánh thì f được gọi là một *đẳng cấu môđun.*

Nếu có đẳng cấu môđun $f : X \longrightarrow Y$ thì ta nói môđun X đẳng cấu với môđun Y và ký hiệu là $X \simeq Y$. Quan hệ đẳng cấu giữa các môđun là quan hệ tương đương.

2.5. Định lý. *Cho đồng cấu $f : X \longrightarrow Y$.*

i) Đồng cấu f là đơn cấu khi và chỉ khi $\mathrm{Ker}f = 0$.

ii) Đồng cấu f là toàn cấu khi và chỉ khi $\mathrm{Coker}f = 0$, *trong đó* $\mathrm{Coker}f$ *là ký hiệu của môđun thương* $Y/\mathrm{Im}f$ *và được gọi là đối hạt nhân của môđun* Y.

Chứng minh. i) Nếu f là đơn cấu thì f là đồng cấu, do đó $f(0) = 0$, hay $0 \in \mathrm{Ker}f = f^{-1}(0)$. Vì f là đơn ánh nên $f^{-1}(0)$ có không quá một phần tử. Suy ra $\mathrm{Ker}f = 0$.

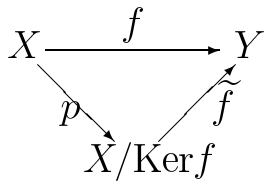
Nếu $\mathrm{Ker}f = 0$ và x, y là hai phần tử tùy ý của X mà $f(x) = f(y)$ thì $f(x - y) = f(x) - f(y) = 0$ nên $x - y \in \mathrm{Ker}f$, do đó $x - y = 0$, hay $x = y$. Vậy f là đơn cấu.

ii) Nếu f là một toàn cấu thì f là toàn ánh, do đó $\mathrm{Im}f = f(X) = Y$. Suy ra $\mathrm{Coker}f = Y/\mathrm{Im}f = 0$.

Nếu $\mathrm{Coker}f = 0$ thì $f(X) = Y$. Do đó f là toàn cấu.

2.6. Định lý về đồng cấu môđun. *Đối với mọi đồng cấu môđun $f : X \longrightarrow Y$, tồn tại duy nhất đẳng cấu môđun*

$\widetilde{f} : X/\mathrm{Ker}f \longrightarrow \mathrm{Im}f$ *làm cho biểu đồ sau đây giao hoán:*



nghĩa là $f = \widetilde{f}p$, *trong đó* $p : X \longrightarrow X/\mathrm{Ker}f$ *là phép chiếu chính tắc.*

Chứng minh. Vì $f : X \longrightarrow Y$ cũng là đồng cấu của các nhóm cộng Abel nên theo Định lý đồng cấu nhóm, tồn tại duy nhất đẳng cấu nhóm

$$\begin{array}{rccc} \widetilde{f}: & X/\mathrm{Ker}f & \longrightarrow & \mathrm{Im}f \\ & x + \mathrm{Ker}f & \longmapsto & f(x) \end{array}$$

thỏa mãn điều kiện $f = \widetilde{f}p$. Ta chỉ còn phải chứng minh $\widetilde{f}$ cũng là đồng cấu môđun. Thật vậy,

$$\widetilde{f}(r(x + \mathrm{Ker}f)) = \widetilde{f}(rx + \mathrm{Ker}f) = f(rx) = rf(x) = r\widetilde{f}(x + \mathrm{Ker}f)$$

với mọi $r \in R$ và với mọi $x \in X$. Do đó $\widetilde{f}$ là đồng cấu môđun.

Chú ý. Trong lý thuyết về môđun đôi khi người ta còn gọi $X/\mathrm{Ker}f$ là đối ảnh của f và ký hiệu là $\mathrm{Coim}f$. Như vậy, theo Định lý 2.6 thì $\mathrm{Coim}f \simeq \mathrm{Im}f$ với mọi đồng cấu f. Từ Định lý 2.6 ta suy ra hệ quả sau đây:

2.7. Hệ quả. *Đối với mọi đồng cấu môđun* $f : X \longrightarrow Y$, *tồn tại và duy nhất đơn cấu* $\widetilde{f} : X/\mathrm{Ker}f \longrightarrow Y$ *sao cho* $f = \widetilde{f}p$.

Chứng minh. Thật vậy, ta phân tích $f = if'$, trong đó $f' : X \longrightarrow \mathrm{Im}f$ xác định bởi $f'(x) = f(x), \forall x \in X$, còn $i : \mathrm{Im}f \longrightarrow X$ là đơn cấu nhúng. Theo Định lý 2.6 tồn tại và duy nhất đẳng cấu $\widetilde{f'} : X/\mathrm{Ker}f = X/\mathrm{Ker}f' \longrightarrow \mathrm{Im}f$ sao cho $f' = \widetilde{f'}p$. Đặt $\widetilde{f} = i\widetilde{f'}$ thì $f = if' = i\widetilde{f'}p = \widetilde{f}p$. Vậy $\widetilde{f}$ là đơn cấu duy nhất cần tìm.

2.8. Định nghĩa dãy khớp

Dãy các môđun và các đồng cấu môđun

$$\cdots \longrightarrow X_{n-1} \xrightarrow{f_{n-1}} X_n \xrightarrow{f_n} X_{n+1} \longrightarrow \cdots$$

được gọi là một *dãy khớp* nếu ảnh của đồng cấu vào bằng hạt nhân của đồng cấu ra tại mọi môđun khác với hai đầu (nếu có) của dãy, tức là $\mathrm{Im}f_{n-1} = \mathrm{Ker}f_n$ với mọi n.

Một dãy khớp bất kỳ dạng

$$0 \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow 0,$$

trong đó môđun đầu tiên và môđun cuối cùng trong dãy đều là các môđun không, được gọi là *dãy khớp ngắn*. Dễ dàng thấy rằng, dãy

$$0 \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow 0$$

là dãy khớp ngắn khi và chỉ khi các điều kiện sau đây được thỏa mãn:

i) f là một đơn cấu,

ii) $\mathrm{Im}f = \mathrm{Ker}g$,

iii) g là một toàn cấu.

Chúng ta xét các ví dụ sau đây về dãy khớp ngắn.

a) Cho A là môđun con của môđun X. Khi đó dãy

$$0 \longrightarrow A \xrightarrow{i} X \xrightarrow{p} X/A \longrightarrow 0,$$

trong đó i là phép nhúng còn p là phép chiếu tự nhiên, tạo thành dãy khớp ngắn.

b) Cho $f : X \longrightarrow Y$ là đơn cấu mà không là toàn cấu. Khi đó ta có dãy

$$0 \longrightarrow X \xrightarrow{f} Y \xrightarrow{p} Y/\mathrm{Im}f \longrightarrow 0,$$

trong đó p là phép chiếu tự nhiên, là dãy khớp ngắn. Tương tự, nếu f là toàn cấu nhưng không phải là đơn cấu thì ta cũng có dãy khớp ngắn:

$$0 \longrightarrow \mathrm{Ker}f \xrightarrow{i} X \xrightarrow{f} Y \longrightarrow 0,$$

trong đó i là phép nhúng. Các dãy khớp ngắn này đôi khi được gọi là *dãy khớp của đồng cấu* f.

2.9. Định nghĩa dãy khớp chẻ ra

Dãy khớp các đồng cấu

$$\cdots \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow \cdots$$

được gọi là *dãy khớp chẻ ra* tại môđun B nếu ảnh của đồng cấu vào $\mathrm{Im}f$ là hạng tử trực tiếp của B, tức là tồn tại môđun con B' của B sao cho $B = \mathrm{Im}f + B'$ và $\mathrm{Im}f \cap B' = 0$. Ta sử dụng ký hiệu $B = \mathrm{Im}f \oplus B'$ khi $\mathrm{Im}f$ là một hạng tử trực tiếp của B. Lúc đó ta cũng nói B' là hạng tử trực tiếp của B. Tổng quát, nếu B_1 và B_2 là hai môđun con tùy ý của B thỏa mãn

$$B = B_1 + B_2 \quad \text{và} \quad B_1 \cap B_2 = 0$$

thì ta nói B_1 và B_2 là các hạng tử trực tiếp của B và ký hiệu $B = B_1 \oplus B_2$.

Trong phần còn lại của mục này ta sẽ chỉ ra các điều kiện cần và đủ để dãy khớp ngắn là chẻ ra. Trước hết ta cần đến bổ đề sau:

2.10. Bổ đề. *Cho các đồng cấu $f : X \longrightarrow Y$ và $g : Y \longrightarrow Z$ sao cho gf là đẳng cấu. Khi đó ta có sự phân tích $Y = \mathrm{Im}f \oplus \mathrm{Ker}g$.*

Chứng minh. Giả sử y là phần tử tùy ý của Y. Ta có sự phân tích

$$y = f[(gf)^{-1}g(y)] + y - f[(gf)^{-1}g(y)],$$

trong đó, hiển nhiên $f[(gf)^{-1}g(y)] \in \mathrm{Im}f$, còn

$$g(y - f[(gf)^{-1}g(y)]) = g(y) - gf(gf)^{-1}g(y) = g(y) - g(y) = 0,$$

nên $y - f[(gf)^{-1}g(y)] \in \mathrm{Ker}g$. Vì vậy $Y = \mathrm{Im}f + \mathrm{Ker}g$.

Bây giờ nếu y là phần tử tùy ý của $\mathrm{Im}f \cap \mathrm{Ker}g$ thì do $y \in \mathrm{Im}f$ nên $y = f(x)$ với x nào đó thuộc X, mà $y \in \mathrm{Ker}g$ nên $g(y) = gf(x) = 0$. Do giả thiết gf là đẳng cấu suy ra $x = 0$. Vậy $y = f(0) = 0$. Do đó $\mathrm{Im}f \cap \mathrm{Ker}g = 0$. Từ các khẳng định trên ta có $Y = \mathrm{Im}f \oplus \mathrm{Ker}g$. ■

2.11. Định lý. *Đối với mỗi dãy khớp ngắn*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0,$$

ba mệnh đề sau đây là tương đương:

i) Dãy khớp ngắn đó chẻ ra;

ii) Đồng cấu f có nghịch đảo trái;

iii) Đồng cấu g có nghịch đảo phải.

Chứng minh. Nếu đồng cấu f có nghịch đảo trái, tức là tồn tại đồng cấu $f' : B \longrightarrow A$ sao cho $f'f = 1_A$. Do $f'f$ là đẳng cấu nên theo Bổ đề 2.10. Suy ra $B = \mathrm{Im}f \oplus \mathrm{Ker}f'$. Do đó dãy khớp chẻ ra. Lập luận hoàn toàn tương tự ta cũng thấy nếu đồng cấu g có nghịch đảo phải thì dãy khớp là chẻ ra. Như vậy từ (ii) suy ra (i) và từ (iii) suy ra (i).

Bây giờ giả sử dãy khớp đã cho chẻ ra. Đặt $D = \mathrm{Im}f = \mathrm{Ker}g$. Theo định nghĩa, tồn tại môđun con E của B sao cho $B = D \oplus E$. Vì f là đơn cấu nên nó xác định đẳng cấu

$$\begin{array}{rccc} i: & A & \longrightarrow & D = \mathrm{Im}f \\ & \alpha & \longmapsto & f(\alpha). \end{array}$$

Với mỗi $x \in B$, tồn tại duy nhất các phần tử $u \in D, v \in E$ sao cho $x = u + v$. Ta dễ dàng kiểm tra rằng tương ứng

$$\begin{array}{rccc} f': & B & \longrightarrow & A \\ & x & \longmapsto & f'(x) = i^{-1}(u) \end{array}$$

là một đồng cấu và f' là một nghịch đảo trái của f. Vậy (i) suy ra (ii).

Vì g là toàn cấu và $D = \mathrm{Ker}g$, $D \cap E = 0$ nên suy ra đồng cấu thu hẹp

$$j = g|_E : E \longrightarrow C$$

là đẳng cấu. Do đó tương ứng

$$\begin{array}{rccc} g': & C & \longrightarrow & B \\ & x & \longmapsto & g'(x) = j^{-1}(x) \end{array}$$

là đồng cấu và là nghịch đảo phải của g. Vậy (i) suy ra (iii). ■

2.12. Hệ quả. *Nếu dãy khớp*

$$\cdots \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow \cdots$$

chẻ ra tại B *thì ta có*

$$B \simeq \mathrm{Im}f \oplus \mathrm{Im}g.$$

Chứng minh. Từ tính chất khớp và chẻ ra tại B ta lập được dãy khớp ngắn chẻ ra sau đây:

$$0 \longrightarrow \mathrm{Im}f \xrightarrow{i} B \xrightarrow{g'} \mathrm{Im}g \longrightarrow 0,$$

trong đó i là phép nhúng và $g'(x) = g(x), \forall x \in B$. Vì i là đơn cấu, g' là toàn cấu và $\mathrm{Ker}g' = \mathrm{Ker}g = \mathrm{Im}f = \mathrm{Im}i$ nên dãy là khớp. Lại có $\mathrm{Im}f$ là hạng tử trực tiếp của B nên dãy là chẻ ra. Do đó $B = \mathrm{Im}f \oplus B'$, trong đó $B' \simeq \mathrm{Im}g$. Vậy $B \simeq \mathrm{Im}f \oplus \mathrm{Im}g$. ■

2.13. Định nghĩa môđun các đồng cấu

Cho A và B là các môđun tùy ý trên vành R. Ta ký hiệu $Hom_R(A, B)$ (hay đơn giản hơn, $Hom(A, B)$ khi vành R đã được chỉ rõ) là tập hợp tất cả các đồng cấu của môđun A vào môđun B. Với f, g là các đồng cấu tùy ý thuộc $Hom(A, B)$ và r tùy ý thuộc R, ta định nghĩa các ánh xạ $f + g$ và rf từ A vào B xác định như sau:

$$\begin{aligned} (f+g)(x) &= f(x) + g(x), \forall x \in A, \\ (rf)(x) &= r(f(x)), \forall x \in A. \end{aligned}$$

Dễ dàng kiểm tra thấy rằng $f + g$ cũng là đồng cấu từ A vào B. Phép cộng này biến $Hom(A, B)$ thành nhóm Abel. Bây giờ, với mọi $x, y \in A$ và $s \in R$ ta có

$$(rf)(x+y) = r(f(x) + f(y)) = r(f(x)) + r(f(y)) = (rf)(x) + (rf)(y)$$

và

$$\begin{aligned} (rf)(sx) &= r[f(sx)] = r[sf(x)] = (rs)f(x) \\ &= (sr)f(x) = s(rf(x)) = s(rf)(x) \end{aligned}$$

(do tính giao hoán của R). Vậy rf là đồng cấu từ A vào B. Kiểm tra dễ dàng thấy rằng $Hom(A,B)$ cùng với phép cộng và phép nhân với vô hướng xác định như trên thỏa mãn các tiên đề (M1)-(M4). Do đó ta gọi $Hom(A,B)$ là môđun các đồng cấu của môđun A vào môđun B. Phần tử không của $Hom(A,B)$ là đồng cấu 0 biến mọi phần tử của A thành phần tử 0 của B. Bây giờ cho $f : A' \longrightarrow A$ và $g : B \longrightarrow B'$. Ta định nghĩa ánh xạ

$$\begin{array}{rccc} Hom(f,g): & Hom(A,B) & \longrightarrow & Hom(A',B') \\ & \varphi & \longmapsto & g\varphi f. \end{array}$$

Rõ ràng $Hom(f,g)$ là một đồng cấu của môđun $Hom(A,B)$ vào môđun $Hom(A',B')$.

2.14. Định lý. *Nếu M là một môđun tùy ý trên R và*

$$A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

là một dãy khớp những môđun trên R thì dãy

$$0 \longrightarrow Hom(C,M) \xrightarrow{g^*} Hom(B,M) \xrightarrow{f^*} Hom(A,M)$$

(với $f^* = Hom(f,i)$, $g^* = Hom(g,i)$, trong đó $i : M \longrightarrow M$ là tự đồng cấu đồng nhất của môđun M) cũng là khớp.

Chứng minh. 1°. Khớp tại $Hom(C,M)$:

Giả sử $\varphi \in Hom(C,M)$ mà $g^*(\varphi) = 0$. Ta có $g^*(\varphi) = i\varphi g = \varphi g = 0$, vì g là toàn ánh nên từ $\varphi g = 0$ suy ra $\varphi = 0$. Vậy g^* là đơn cấu, nghĩa là dãy khớp tại $Hom(C,M)$.

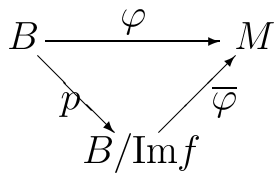
2°. Khớp tại $Hom(B,M)$:

Với φ tùy ý thuộc $Hom(B,M)$ ta có

$$f^*g^*(\varphi) = f^*(\varphi g) = \varphi gf = \varphi 0 = 0.$$

Do đó $\mathrm{Im}g^* \subset \mathrm{Ker}f^*$.

Đảo lại, với $\varphi \in \mathrm{Ker}f^*$, tức là $\varphi \in Hom(B,M)$ mà $f^*(\varphi) = 0$, hay $\varphi f = 0$, suy ra $\varphi(y) = 0, \forall y \in \mathrm{Im}f$. Ta phân tích φ như biểu đồ sau:



Do tính chất khớp của dãy

$$A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

suy ra $B/\mathrm{Ker}g \simeq C$ hay $B/\mathrm{Im}f \simeq C$. Ta đồng nhất $B/\mathrm{Im}f$ với C thì p đồng nhất với g và $\overline{\varphi}$ là đồng cấu từ C vào M. Như vậy, $g^*(\overline{\varphi}) = \overline{\varphi}g = \overline{\varphi}p = \varphi$. Do đó $\varphi \in \mathrm{Im}g^*$. Vậy $\mathrm{Ker}f^* \subset \mathrm{Im}g^*$. Tổng kết lại ta có $\mathrm{Ker}f^* = \mathrm{Im}g^*$, hay dãy khớp tại $Hom(B, M)$.

Định lý được chứng minh. ■

Bằng cách lập luận tương tự ta chứng minh được định lý sau đây:

2.15. Định lý. *Nếu M là một môđun tùy ý trên R và*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C$$

là một dãy khớp những môđun trên R thì dãy

$$0 \longrightarrow Hom(M, A) \xrightarrow{f_*} Hom(M, B) \xrightarrow{g_*} Hom(M, C)$$

(với $f_* = Hom(i, f)$, $g_* = Hom(i, g)$, trong đó $i : M \longrightarrow M$ là tự đồng cấu đồng nhất của môđun M) cũng là khớp.

Nhận xét. Từ Định lý 2.14 và 2.15 chúng ta thấy rằng cả hai loại đồng cấu Hom đều không chuyển một dãy khớp ngắn thành dãy khớp ngắn mà chỉ bảo đảm tính khớp bên trái. Để đo độ lệch của tính khớp bên phải ta xây dựng một loại hàm tử mà gọi là hàm tử mở rộng. Đó là một trong bốn trụ cột của Đại số đồng điều.

§3. Môđun tự do

3.1. Định nghĩa

i) Tập con S của R-môđun X được gọi là *độc lập tuyến tính* nếu phần tử 0 của X chỉ có một cách biểu thị tuyến tính duy nhất qua các phần tử của S, đó là tổ hợp tuyến tính mà tất cả các hệ tử đều bằng 0.

Tập con S của R-môđun X không độc lập tuyến tính thì được gọi là *phụ thuộc tuyến tính*. Như thế, tập con S của X là phụ thuộc tuyến tính khi và chỉ khi tồn tại các phần tử $x_1, x_2, ..., x_n$ thuộc S và các hệ tử không đồng thời bằng không $r_1, r_2, ..., r_n$ thuộc R sao cho

$$r_1x_1 + r_2x_2 + \ldots + r_nx_n = 0.$$

ii) Một hệ sinh độc lập tuyến tính của một môđun X được gọi là *cơ sở* của X.

iii) Môđun X có cơ sở được gọi là *môđun tự do*.

Kết quả sau đây tương tự như kết quả trong không gian vectơ.

3.2. Định lý. *Tập con $S = \{x_i\}_{i\in I}$ của môđun X là cơ sở của môđun X khi và chỉ khi mỗi phần tử x thuộc X chỉ có một cách biểu thị tuyến tính duy nhất qua S.*

Chứng minh. *Điều kiện cần.* Giả sử $S = \{x_i\}_{i\in I} \subset X$ là một cơ sở của X. Vì S là một tập sinh nên mọi phần tử của X đều là tổ hợp tuyến tính của các phần tử của S. Nếu $x = \sum\limits_{i\in I} r_ix_i$ và $x = \sum\limits_{i\in I} r'_ix_i$, trong đó

chỉ có một số hữu hạn các hệ tử r_i, r'_i khác không, là các biểu thị tuyến tính của phần tử $x \in X$ qua S, thì

$$0 = \sum_{i\in I} r_ix_i - \sum_{i\in I} r'_ix_i = \sum_{i\in I}(r_i - r'_i)x_i.$$

Suy ra $r_i - r'_i = 0$ với mọi $i \in I$ do S độc lập tuyến tính. Như vậy mọi phần tử của x đều chỉ có một cách biểu thị tuyến tính duy nhất qua S.

Điều kiện đủ. Nếu S là một tập con của X mà mọi phần tử của X đều chỉ có một cách biểu thị tuyến tính qua S thì suy ra S là một tập sinh và phần tử 0 của X cũng chỉ có một cách biểu thị tuyến tính duy nhất qua S, tức là S là một tập sinh độc lập tuyến tính, do đó S là một cơ sở của X. ■

3.3. Môđun tự do sinh bởi một tập hợp

Cho S là một tập hợp khác $\emptyset$ tùy ý. Gọi $F(S)$ là tập hợp các tổng hình thức $\sum_{s\in S} a_s s$, trong đó $a_s \in R$ và $a_s \neq 0$ chỉ với một số hữu hạn $s \in S$. Tập hợp $F(S)$ trở thành R-môđun với các phép toán xác định như sau:

$$\sum_{s\in S} a_s s + \sum_{s\in S} b_s s = \sum_{s\in S} (a_s + b_s)s,$$

$$a\left(\sum_{s\in S} a_s s\right) = \sum_{s\in S} (aa_s)s,$$

trong đó a, a_s, b_s là các phần tử của R. Ta đồng nhất S với tập con của $F(S)$ gồm các phần tử có dạng $1.s$. Dễ dàng kiểm tra rằng $F(S)$ là một R-môđun tự do với cơ sở S. $F(S)$ được gọi là *môđun tự do sinh bởi tập* S.

Định lý sau đây xác định tính chất đặc trưng của cơ sở môđun.

3.4. Định lý. *Tập con S khác rỗng của môđun X là cơ sở của S khi và chỉ khi với mọi môđun Y, mỗi ánh xạ $f : S \longrightarrow Y$ đều có thể mở rộng tới một đồng cấu duy nhất $\widetilde{f} : X \longrightarrow Y$.*

Chứng minh. Nếu $S = \{x_i\}_{i\in I}$ là cơ sở của môđun tự do X thì mỗi phần tử $x \in X$ đều biểu diễn được một cách duy nhất dưới dạng $x = \sum_{i\in I} r_i x_i$.

Do đó mỗi ánh xạ $f : S \longrightarrow Y$ có thể mở rộng tới đồng cấu duy nhất $\widetilde{f} : X \longrightarrow Y$ xác định bởi

$$\widetilde{f}(x) = \widetilde{f}(\sum_{i\in I} r_i x_i) = \sum_{i\in I} r_i f(x_i).$$

Đảo lại, nếu S là tập con của môđun X có tính chất mỗi ánh xạ $f : S \longrightarrow Y$ đều có thể mở rộng tới đồng cấu duy nhất $\widetilde{f} : X \longrightarrow Y$,

ta cần chứng minh S là cơ sở của X. Thật vậy, gọi $F(S)$ là môđun tự do sinh bởi tập hợp S. Xét ánh xạ nhúng

$$\begin{array}{rccc} j_S: & S & \longrightarrow & F(S) \\ & s & \longmapsto & 1.s. \end{array}$$

Theo giả thiết, j_S có thể mở rộng tới đồng cấu duy nhất $j : X \longrightarrow F(S)$. Để chứng tỏ rằng X có cơ sở ta chỉ cần chứng minh j là đẳng cấu. Đặt $S' = j_S(S)$ thì ta có song ánh $j_S : S \longrightarrow S'$. S' là cơ sở của $F(S)$, j là mở rộng của j_S nên j là toàn ánh.

Xét $g : S' \longrightarrow S$ là ánh xạ ngược của j_S. Vì S' là cơ sở của $F(S)$ nên g có thể mở rộng tới đồng cấu duy nhất $\widetilde{g} : F(S) \longrightarrow X$. Khi đó tích các đồng cấu $\widetilde{g}j : X \longrightarrow X$ thực hiện sự đồng nhất trên tập S, do đó nó là mở rộng của phép nhúng $i : S \longrightarrow X$. Mà 1_X là một mở rộng của phép nhúng i nên từ tính duy nhất của mở rộng ta có $\widetilde{g}j = 1_X$. Vì 1_X là đơn cấu suy ra j cũng là đơn cấu. Vậy j là đẳng cấu. ■

Cuối cùng, để kết thúc mục này ta đưa ra một kết quả mà thường được gọi là "tính đủ nhiều của các môđun tự do", được sử dụng trong đại số đồng điều.

3.5. Định lý. *Mỗi môđun X đều đẳng cấu với môđun thương của một môđun tự do nào đó.*

Chứng minh. Xét môđun tự do $F(X)$ sinh bởi tập X. Khi đó ánh xạ đồng nhất $1_X : X \longrightarrow X$ có thể mở rộng duy nhất tới đồng cấu $\varphi : F(X) \longrightarrow X$. Vì φ là toàn cấu nên theo Định lý đồng cấu môđun ta có $X \simeq F(X)/\mathrm{Ker}\varphi$. Như vậy X đẳng cấu với môđun thương của môđun tự do sinh bởi tập X. ■

§4. Đại số

Trong mục này chúng tôi giới thiệu sơ lược về đại số trên một trường. Khái niệm đại số ở đây được hiểu là đại số kết hợp, tức là phép nhân có tính chất kết hợp, các đại số mà phép nhân không có tính chất kết hợp sẽ không được đề cập đến.

4.1. Định nghĩa

Một *đại số* trên trường K là một tập hợp A khác rỗng cùng với ba phép toán:

- Phép cộng:

$$\begin{array}{ccc} A \times A & \longrightarrow & A \\ (x, y) & \longmapsto & x + y. \end{array}$$

- Phép nhân:

$$\begin{array}{ccc} A \times A & \longrightarrow & A \\ (x, y) & \longmapsto & xy. \end{array}$$

- Phép nhân với vô hướng trong K:

$$\begin{array}{ccc} K \times A & \longrightarrow & A \\ (k, x) & \longmapsto & kx \end{array}$$

sao cho các phép toán này phải thỏa mãn ba tiên đề sau đây:

(A1) Tập A cùng với các phép toán cộng và nhân lập thành một vành.

(A2) Tập A cùng với phép cộng và phép nhân với vô hướng lập thành một không gian vectơ trên trường K.

(A3) Phép nhân của vành A và phép nhân với vô hướng của môđun A thỏa mãn điều kiện

$$\forall k \in K, \forall x, y \in A, k(xy) = (kx)y = x(ky).$$

Số chiều của không gian vectơ A trên K được gọi là *số chiều* của đại số A và vẫn ký hiệu là $\dim_K A$, hay đơn giản là $\dim A$ khi không sợ nhầm lẫn.

4.2. Ví dụ

a) Gọi $K[x]$ là vành đa thức của một ẩn x trên trường K. Ta định nghĩa phép nhân với vô hướng như sau:

$$\begin{array}{ccc} K \times K[x] & \longrightarrow & K[x] \\ (k, a_0 + a_1x + ... + a_nx^n) & \longmapsto & ka_0 + ka_1x + ... + ka_nx^n. \end{array}$$

$K[x]$ với phép cộng đa thức và phép nhân với vô hướng xác định như trên lập thành một không gian vectơ trên K. Hơn nữa tiên đề (A3) được thỏa mãn. Vì vậy $K[x]$ là một đại số, ta gọi là đại số của đa thức trên K của ẩn x.

b) Tập hợp $M(n, K)$ các ma trận vuông cấp n với các phần tử trên K lập nên một đại số với các phép toán thông thường trên ma trận: phép cộng ma trận, phép nhân ma trận, phép nhân một vô hướng với một ma trận. Ta gọi $M(n, K)$ là đại số ma trận.

c) Xét không gian vectơ thực bốn chiều $H = R \oplus Ri \oplus Rj \oplus Rk$ với cơ sở $\{1, i, j, k\}$. Phép toán nhân trên H được định nghĩa thông qua các phần tử sinh như sau:

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

Kiểm tra thấy rằng H cùng với phép cộng vectơ và phép nhân xác định như trên là một vành, phép nhân trên H và phép nhân với vô hướng trong $\mathbb{R}$ thỏa mãn tiên đề (A3). Do đó H lập thành một đại số trên trường số thực $\mathbb{R}$, được gọi là đại số Quaternion.

4.3. Đại số con

Tập con khác rỗng B của đại số A trên trường K được gọi là *đại số con* của A nếu B vừa là một vành con của vành A vừa là một không gian vectơ con của không gian vectơ A. Như vậy tập con khác rỗng B của A là đại số con khi và chỉ khi nó thỏa mãn các điều kiện sau đây:

i) $\forall x, y \in B, xy \in B$ và $x + y \in B$,

ii) $\forall x \in B, \forall k \in K, kx \in B$.

Cho S là tập con của A. Giao của tất cả các đại số con của A chứa S cũng là đại số con của A chứa S, và là đại số con nhỏ nhất (theo quan hệ bao hàm) của A chứa S, ta gọi nó là *đại số con sinh bởi tập* S.

4.4. Iđeal và đại số thương

Tập con I của đại số A được gọi là một ideal của đại số A nếu I vừa là ideal của vành A vừa là không gian vectơ con của không gian vectơ

A. Khi đó A/I là vành thương của A với các phép toán

$$\begin{aligned}(x+I)+(y+I) &= (x+y)+I,\\ (x+I)(y+I) &= (xy)+I\end{aligned}$$

với mọi $x, y \in A$.

Ta cũng có A/I là không gian thương của không gian vectơ A theo không gian con I với phép cộng xác định như trên, còn phép nhân với vô hướng như sau:

$$k(x+I) = (kx)+I, \forall x \in A,\ \forall k \in K.$$

Vì phép nhân trên A/I và phép nhân với vô hướng trong K được định nghĩa qua các phần tử đại diện nên chúng thỏa mãn tiên đề (A3) bởi A thỏa mãn tiên đề ấy. Vậy A/I cũng lập thành đại số và được gọi là đại số thương của đại số A theo đại số con I.

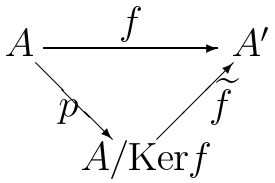
4.5. Đồng cấu

i) Cho ánh xạ $f : A \longrightarrow A'$ từ đại số A vào đại số A' trên trường K. Nếu f vừa là đồng cấu vành vừa là đồng cấu của các K-không gian vectơ thì f được gọi là *đồng cấu đại số*.

ii) Đồng cấu $f : A \longrightarrow A'$ từ đại số A vào đại số A' được gọi là *đơn cấu* (tương ứng, *toàn cấu, đẳng cấu*) nếu nó đồng thời là đơn ánh (tương ứng, toàn ánh, song ánh).

Từ Định lý 8.9, chương 1 và Định lý 2.6, ta dễ dàng suy ra định lý sau đây:

4.6. Định lý đồng cấu đại số. *Đối với mọi đồng cấu đại số $f : A \longrightarrow A'$, tồn tại duy nhất đẳng cấu đại số $\widetilde{f} : A/\mathrm{Ker}f \longrightarrow \mathrm{Im}f$ sao cho biểu đồ sau đây giao hoán*



trong đó p là phép chiếu chính tắc

$$p(x) = x + \mathrm{Ker}f, \forall x \in A.$$

Bài tập

Bài 4.1 Cho I là một idealcủa vành giao hoán có đơn vị R và x là một phần tử tùy ý của R-môđun X. Chứng minh rằng

$$Ix = \{rx | r \in I\}$$

là môđun con của X.

Bài 4.2 Cho R là miền nguyên và X là R-môđun. Phần tử $x \in X$ được gọi là phần tử xoắn nếu tồn tại $r \in R \setminus \{0\}$ sao cho $rx = 0$. Đặt $\tau(X)$ là tập hợp tất cả các phần tử xoắn của X. Nếu $\tau(X) = 0$ thì X được gọi là môđun không xoắn, nếu $\tau(X) = X$ thì X được gọi là môđun xoắn.

Chứng minh rằng:

a) $\tau(X)$ là môđun con của X.

b) Mọi môđun con của môđun xoắn trên R đều là môđun xoắn trên R.

c) Mọi môđun con của môđun không xoắn trên R cũng là môđun không xoắn trên R.

d) Môđun thương $X/\tau(X)$ có phải là môđun không xoắn hay không?

e) $\mathbb{Z}$-môđun $\mathbb{Q}/\mathbb{Z}$ có phải là môđun xoắn không ?

Bài 4.3 Cho R là miền nguyên và X là R-môđun. Phần tử $x \in X$ gọi là chia được nếu với mọi $\lambda \in R \setminus \{0\}$, tồn tại phần tử $y \in X$ sao cho $x = \lambda y$. Đặt $\delta(X)$ là tập hợp tất cả các phần tử chia được của X. Nếu $\delta(X) = X$ thì X được gọi là môđun chia được. Chứng minh rằng:

a) $\delta(X)$ là môđun con của X.

b) Môđun thương của môđun chia được là môđun chia được.

c) Các $\mathbb{Z}$-môđun $\mathbb{Q}$ và $\mathbb{Q}/\mathbb{Z}$ đều là các môđun chia được.

Bài 4.4 Cho $f, g \in Hom_R(X, Y)$. Gọi

$$A = \{x \in X | f(x) = g(x)\}.$$

Chứng minh rằng A là môđun con của X.

Bài 4.5 Môđun X được gọi là môđun đơn nếu X chỉ có hai môđun con là 0 và X. Cho ánh xạ $f : X \longrightarrow Y$ với X là môđun đơn. Chứng minh rằng:

a) Imf là môđun con đơn của Y.

b) Nếu $Imf \neq 0$ thì f là một đơn cấu.

Bài 4.6 Chứng minh rằng:

a) $Hom_{\mathbb{Z}}(\mathbb{Z}, G) \simeq G$.

b) $Hom_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \simeq \mathbb{Z}$.

c) $Hom_{\mathbb{Z}}(G, \mathbb{Z}) = 0$.

Trong đó G là một $\mathbb{Z}$-môđun hữu hạn bất kỳ.

Bài 4.7 Chứng minh rằng nếu p và q là các số nguyên tố cùng nhau thì

$$Hom_{\mathbb{Z}}(\mathbb{Z}_p, \mathbb{Z}_q) = 0.$$

Bài 4.8 Cho A và B là các môđun con của môđun X. Chứng minh rằng:

$$(A + B)/A \simeq B/(A \cap B).$$

Bài 4.9 Cho môđun X và các môđun con M, N mà $N \subset M$. Chứng minh rằng:

$$(X/N)/(M/N) \simeq X/M.$$

Bài 4.10 Cho $f : X \longrightarrow X$ là tự đồng cấu của môđun X thỏa mãn điều kiện $f^2 = f$. Chứng minh rằng

$$X = \mathrm{Im}f \oplus \mathrm{Ker}f.$$

Bài 4.11 Cho biểu đồ các đồng cấu

$$\begin{array}{ccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow h & & & & \\ & & X & & & & \end{array}$$

trong đó $hf = 0$, dòng là khớp. Hãy chứng minh rằng tồn tại và duy nhất đồng cấu $k : C \longrightarrow X$ sao cho $h = kg$.

Bài 4.12 Cho biểu đồ các đồng cấu

$$\begin{array}{ccccccc} & & & & X & & \\ & & & & \downarrow h & & \\ 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C, \end{array}$$

trong đó dòng là khớp và $gh = 0$. Hãy chứng minh rằng tồn tại và duy nhất đồng cấu $k : X \longrightarrow A$ sao cho $fk = h$.

Bài 4.13 Cho dãy khớp $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$, trong đó A và C là các môđun hữu hạn sinh. Chứng minh rằng B cũng là môđun hữu hạn sinh.

Bài 4.14 Cho X là môđun và X_1, X_2 là các môđun con của X mà $X_1 + X_2$, $X_1 \cap X_2$ là các môđun con hữu hạn sinh. Chứng minh rằng X_1, X_2 cũng là các môđun con hữu hạn sinh.

Bài 4.15 Môđun X được gọi là môđun nửa đơn nếu mỗi môđun con của X đều là hạng tử trực tiếp. Chứng minh rằng:

a) Mỗi không gian vectơ trên trường K đều là môđun nửa đơn trên K.

b) Mọi môđun con của môđun nửa đơn là môđun nửa đơn.

c) Mỗi môđun con khác 0 của một môđun đơn đều chứa một môđun con đơn.

Bài 4.16 Cho X là một môđun trên vành R. Chứng minh rằng các điều kiện sau đây tương đương:

a) Mọi môđun con của môđun X đều hữu hạn sinh.

b) Nếu X_1, $X_2, \ldots$ là các môđun con của X sao cho $X_1 \subset X_2 \subset \ldots$ thì tồn tại một chỉ số n sao cho $X_n = X_{n+1} = \ldots$

c) Mọi tập con $S \neq \emptyset$ các môđun con của X đều chứa một phần tử tối đại (tức là chứa một môđun con X_0 sao cho mọi Y thuộc S mà $X_0 \subset Y$ suy ra $X_0 = Y$).

Bài 4.17 Cho biểu đồ

$$\begin{array}{ccccccc} & & & & 0 & & \\ & & & & \downarrow & & \\ & & & & Y & & \\ & & & & \downarrow\beta & & \\ 0 & \longrightarrow & X & \xrightarrow[\alpha]{} & A & \xrightarrow{\alpha'} & X' \\ & & & & \downarrow\beta' & & \\ & & & & Y' & & \end{array}$$

trong đó dòng và cột là khớp. Chứng minh rằng $\beta'\alpha$ là đơn cấu khi và chỉ khi $\alpha'\beta$ là đơn cấu.

Bài 4.18 Cho biểu đồ

$$\begin{array}{ccccccc} & & & & Y & & \\ & & & & \downarrow\beta & & \\ X & \xrightarrow{\alpha} & A & \xrightarrow{\alpha'} & X' & \longrightarrow & 0 \\ & & & & \downarrow\beta' & & \\ & & & & Y' & & \\ & & & & \downarrow & & \\ & & & & 0 & & \end{array}$$

trong đó dòng và cột là khớp. Chứng minh rằng $\beta'\alpha$ toàn cấu khi và chỉ khi $\alpha'\beta$ là toàn cấu.

Bài 4.19 Chứng minh rằng môđun con A của môđun X là hạng tử trực tiếp nếu môđun thương X/A là tự do.

Bài 4.20 Cho X, Y là các môđun trên vành chính, hơn nữa Y là môđun tự do. Chứng minh rằng $X \simeq \mathrm{Ker}f \oplus \mathrm{Im}f$ với mọi đồng cấu $f : X \longrightarrow Y$.

Bài 4.21 Chứng minh rằng mọi môđun tự do trên miền nguyên đều là môđun không xoắn.

TÀI LIỆU THAM KHẢO

[1] Nguyễn Viết Đông, Trần Huyên, *Đại số đồng điều*, NXB Đại học quốc gia TP Hồ Chí Minh, 2002.

[2] Lê Thanh Hà, *Các cấu trúc đại số cơ bản*, NXB Giáo dục, 2000.

[3] Đặng Xuân Hồng, *Giáo trình Đại số I*, Đại học Tổng hợp TP Hồ Chí Minh, 1977.

[4] Nguyễn Hữu Việt Hưng, *Đại số đại cương*, NXB Giáo dục, 1998.

[5] Mỵ Vinh Quang, *Đại số đại cương*, NXB Giáo dục, 1998.

[6] Hoàng Xuân Sính, *Đại số đại cương*, NXB Giáo dục, 1997.

[7] M. I. Kargapolov & Ju. I. Merzljakov, *Fundamentals of the Theory of Groups*, English translation, Springer-Verlag, 1979.

[8] A. Kurosh, *Giáo trình Đại số cao cấp*, Nauka, Moskva, 1975 (Tiếng Nga)

[9] Joseph J. Rotman, *An Introduction to the Theory of Groups*, 4th edition, , Springer-Verlag, 1995.