XUÂN SÍNH

ĐẠI SỐ ĐẠI CƯƠNG

NHÀ XUẤT BẢN GIÁO DỤC VIỆT NAM

HOÀNG XUÂN SÍNH

ĐẠI SỐ ĐẠI CƯƠNG

(Tái bản lần thứ mười bốn)

NHÀ XUẤT BẢN GIÁO DỤC VIỆT NAM

Chịu trách nhiệm xuất bản:
Chủ tịch Hội đồng Thành viên kiêm Tổng Giám đốc NGÔ TRẦN ÁI
Phó Tổng Giám đốc kiêm Tổng biên tập VŨ VĂN HÙNG

Tổ chức bản thảo và chịu trách nhiệm nội dung:
Phó Tổng biên tập NGÔ ÁNH TUYẾT
Giám đốc Công ty CP Sách ĐH–DN NGÔ THỊ THANH BÌNH

Biên tập lần đầu và tái bản: TRẦN PHƯƠNG DUNG
Biên tập kĩ thuật: BÙI CHÍ HIẾU
Sửa bản in: HOÀNG DIỄM
Chế bản: PHÒNG CHẾ BẢN (NXB GIÁO DỤC VIỆT NAM)

LỜI NÓI ĐẦU

Cho xuất bản lần thứ nhất

Tập II hầu như độc lập đối với tập I, nếu không kể đến một số khái niệm như hoán vị, phép thế, ma trận..., mà một đôi khi đề cập đến. Tuy vậy, về mặt ngôn ngữ và kí hiệu của lí thuyết tập hợp, tập II trung thành với tập I.

Ở đây chúng tôi không làm việc thuyết minh từng chương, các bạn đọc có thể xem bản thuyết minh chương trình Đại số cao cấp của Bộ Giáo dục. Sau mỗi § của từng chương, bạn đọc có những bài tập để, hoặc hiểu sâu lí thuyết hơn và rèn luyện kĩ năng tính toán, hoặc hiểu rộng lí thuyết hơn, với một số khái niệm mới đưa vào trong bài tập. Mỗi vấn đề được nhắc lại thì được chú thích chương, tiết, mục của vấn đề đã được đưa vào, chẳng hạn ch V, §3, 2 có nghĩa là vấn đề đó đã nói đến ở chương V, tiết 3, mục 2. Nếu vấn đề được nhắc lại cùng chương với vấn đề đang xét thì chỉ chú thích tiết và mục ; nếu lại cùng tiết thì chỉ chú thích mục. Trong cùng một tiết, các định nghĩa, bổ đề, định lí được đánh số bằng 1, 2, 3...

Cuối cùng để xây dựng một giáo trình Đại số cao cấp càng ngày càng tốt hơn, chúng tôi rất mong bạn đọc vui lòng chỉ bảo những thiếu sót hẳn không tránh khỏi của cuốn sách này. Xin cảm ơn PTS Bùi Huy Hiền ở tổ Đại số của khoa Toán trường Đại học sư phạm Hà Nội 2 đã có nhiều đóng góp về phần Bài tập.

Hà Nội ngày 13-1-1972

HOÀNG XUÂN SÍNH

LỜI NÓI ĐẦU

Cho xuất bản lần thứ hai

Tuy nhiều lần Nhà xuất bản Giáo dục đề nghị chúng tôi cho tái bản cuốn sách Đại số cao cấp tập II, nhưng chúng tôi đã từ chối vì đã có cuốn Đại số và Số học của giáo sư Ngô Thúc Lanh. Nhưng trong quá trình dạy học, chúng tôi thấy cuốn Đại số cao cấp tập II được sinh viên các trường Đại học Sư phạm dùng để ôn thi, còn sinh viên các trường Cao đẳng Sư phạm lại dùng như tài liệu chính khóa, cho nên chúng tôi nhận lời với Nhà xuất bản Giáo dục cho in lại cuốn sách này.

Trong cuốn sách tái bản chúng tôi đã làm các việc sau :

1) Chữa lại một số chứng minh hay phát biểu định lí cho ngắn gọn hơn, hay không thừa.

2) Cho thêm §3 trong chương I, nói sơ lược về các tiên đề của lí thuyết tập hợp, một điều cần thiết cho người giảng và cũng cần thiết cho sinh viên có trí tò mò khoa học.

3) Thêm ví dụ, bài tập về vành chính và vành Oclit, hai loại vành đóng vai trò quan trọng trong Số học.

Chúng tôi trân trọng cám ơn các bạn đồng nghiệp đã có những ý kiến đóng góp và Nhà xuất bản Giáo dục đã nhiều lần đề nghị cho tái bản.

Hà Nội, ngày 21-12-1994

HOÀNG XUÂN SÍNH

CHƯƠNG I

TẬP HỢP VÀ QUAN HỆ

§1. TẬP HỢP VÀ ÁNH XẠ

1. Khái niệm tập hợp

Những vật, những đối tượng toán học... được tụ tập do một tính chất chung nào đó thành lập những *tập hợp*. Đây không phải là một định nghĩa mà là một hình ảnh trực quan của khái niệm tập hợp. Lí thuyết tập hợp trình bày ở đây là một lí thuyết sơ cấp theo quan điểm ngây thơ.

Người ta nói : Tập hợp các học sinh trong một lớp, tập hợp các lớp trong một trường, tập hợp **N** các số tự nhiên, tập hợp **Z** các số nguyên, tập hợp **Q** các số hữu tỉ, tập hợp **R** các số thực, tập hợp **C** các số phức...

Các vật trong tập hợp X gọi là các *phần tử* của X. Kí hiệu $x \in X$ đọc là "x là một phần tử của X" hoặc "x thuộc X". Phủ định của $x \in X$ kí hiệu là $x \notin X$.

Ta bảo *hai tập hợp A và B là bằng nhau* và viết là $A = B$ khi và chỉ khi mọi phần tử thuộc A thì thuộc B và đảo lại, nghĩa là các quan hệ $x \in A$ và $x \in B$ là tương đương. Như vậy $A = B$ khi và chỉ khi chúng chứa các phần tử y như nhau.

2. Bộ phận của một tập hợp

Định nghĩa 1. *Giả sử A và B là hai tập hợp. Ta kí hiệu $A \subset B$ quan hệ sau đây*

với mọi x, $x \in A$ kéo theo $x \in B$.

Nói một cách khác, quan hệ $A \subset B$ có nghĩa là mọi phần tử của A đều thuộc B.

Quan hệ $A \subset B$ là *quan hệ bao hàm*, đọc là "A chứa trong B", hoặc "B chứa A", hoặc "A là một bộ phận của B", hoặc "A là một tập hợp con của B" và người ta cũng viết $B \supset A$. Phủ định của $A \subset B$ viết là $A \not\subset B$ hay $B \not\supset A$.

Định lí 1. *Quan hệ bao hàm có các tính chất sau :*

(i) *Các quan hệ* $A \subset B$ *và* $B \subset C$ *kéo theo quan hệ* $A \subset C$.

(ii) *Muốn có* $A = B$ *cần và đủ có* $A \subset B$ *và* $B \subset A$.

Chứng minh. (i) Ta hãy lấy một phần tử tùy ý $x \in A$. Vì $A \subset B$ nên $x \in B$. Nhưng $B \subset C$ nên $x \in C$. Vậy với mọi x, $x \in A$ kéo theo $x \in C$, tức là $A \subset C$.

(ii) Hiển nhiên. ■

Thường một bộ phận A của một tập hợp B được xác định bởi một tính chất $\mathcal{C}$ nào đó, mà mọi phần tử của tập hợp B thỏa mãn tính chất $\mathcal{C}$ sẽ là phần tử của tập hợp A. Ta kí hiệu như sau

$$A = \{ x \in B \mid x \text{ có tính chất } \mathcal{C} \},$$

và đọc là : "A là tập hợp tất cả các phần tử $x \in B$ mà x có tính chất $\mathcal{C}$".

Ví dụ. – Xét tập hợp $\mathbf{Z}$ các số nguyên và bộ phận A các số nguyên chẵn, ta viết

$$A = \{ x \in \mathbf{Z} \mid x \text{ chia hết cho } 2 \}.$$

3. Hiệu của hai tập hợp

Định nghĩa 2. Cho hai tập hợp A và B tùy ý, tập hợp

$$A - B = \{ x \in A \mid x \notin B \}$$

gọi là *hiệu của tập hợp* A *và tập hợp* B. Nếu $B \subset A$ thì hiệu $A - B$ gọi là *phần bù của tập hợp* B *trong tập hợp* A và còn kí hiệu là $\mathbf{C}_A B$.

Định lí 2. *Giả sử A và B là những bộ phận của một tập hợp X, thế thì*

(i) $X - (X - A) = A$.

(ii) *Các quan hệ $A \subset B$ và $X - B \subset X - A$ là tương đương.*

Chứng minh. (i) Tập hợp $X - (X - A)$ gồm các phần tử $x \in X$ sao cho $x \notin X - A$, tức là gồm các phần tử $x \in X$ sao cho $x \in A$.

(ii) Giả sử $A \subset B$. Vì quan hệ $x \in A$ kéo theo quan hệ $x \in B$, nên quan hệ $x \notin B$ kéo theo $x \notin A$, tức là quan hệ $x \in X - B$ kéo theo quan hệ $x \in X - A$. Đảo lại giả sử $X - B \subset X - A$. Thế thì bằng lí luận tương tự như trên ta có $X - (X - A) \subset X - (X - B)$, tức là theo (i), $A \subset B$. ■

4. Tập hợp rỗng

Giả sử X là một tập hợp. X cũng là một bộ phận của X, điều đó cho phép ta xét tập hợp $\varnothing = X - X$ gọi là bộ phận rỗng của X. $x \in \varnothing$ có nghĩa là $x \in X$ và $x \notin X$. Rõ ràng không có một phần tử x nào của X lại có tính chất đó.

Tập hợp $X - X = \varnothing$ không phụ thuộc vào tập hợp X. Nói cách khác, ta có

$$X - X = Y - Y \text{ với mọi } X, Y$$

Thực vậy, ta có thể coi $X - X$ và $Y - Y$ chứa các phần tử y như nhau vì chúng chẳng có phần tử nào cả (xin đừng coi đây là một chứng minh).

Tập hợp $X - X = \varnothing$ không phụ thuộc vào tập hợp X, vì lí do đó, ta gọi nó là *tập hợp rỗng*. Tập hợp này không có một phần tử nào cả.

Rõ ràng ta có $\varnothing \subset X$ với mọi tập hợp X và tính chất này đặc trưng tập hợp rỗng.

5. Tập hợp một, hai phần tử

Giả sử x là một vật. Thế thì có một tập hợp kí hiệu (x) chỉ gồm có một phần tử là x. Một tập hợp thuộc loại đó gọi là *tập hợp một phần tử*.

Bây giờ giả sử x và y là hai vật phân biệt. Thế thì có một tập hợp kí hiệu (x, y) chỉ gồm có hai phần tử là x và y. Một tập hợp thuộc loại đó gọi là *tập hợp hai phần tử*.

Người ta cũng định nghĩa như vậy tập hợp ba bốn... phần tử. Các tập hợp đó cùng với tập hợp rỗng gọi là *các tập hợp hữu hạn*, còn các tập hợp khác gọi là *các tập hợp vô hạn*.

6. Tập hợp các bộ phận của một tập hợp

Giả sử X là một tập hợp, các bộ phận của X lập thành một tập hợp kí hiệu $\mathcal{P}(X)$ và gọi là *tập hợp các bộ phận của X*. Tập hợp này bao giờ cũng có ít nhất một phần tử, đó là X.

Ta có thể chứng minh được rằng, nếu X là một tập hợp hữu hạn gồm n phần tử thì $\mathcal{P}(X)$ là một tập hợp hữu hạn gồm 2^n phần tử. Như vậy các tập hợp $\varnothing$, $\mathcal{P}(\varnothing)$, $\mathcal{P}(\mathcal{P}(\varnothing))$, $\mathcal{P}(\mathcal{P}(\mathcal{P}(\varnothing)))$, $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathcal{P}(\varnothing))))$, $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathcal{P}(\varnothing)))))$... theo thứ tự có 0, 1, 2, $2^2 = 4$, $2^4 = 16$, $2^{16} = 65536$... phần tử. Từ tập hợp $\varnothing$ chúng ta đã thành lập những tập hợp có nhiều phần tử đến mức trong thực tế ta không đếm được.

7. Tích đề các của hai tập hợp

Giả sử x và y là hai vật, từ hai vật này ta thành lập một vật thứ ba kí hiệu (x, y) và gọi là *cặp* (x, y). Hai cặp (x, y) và (u, v) là bằng nhau khi và chỉ khi $x = u$ và $y = v$. Đặc biệt ta có $(x, y) = (y, x)$ khi và chỉ khi $x = y$, điều này nói lên thứ tự mà ta viết hai vật của một cặp là cần thiết.

Ta có thể mở rộng khái niệm cặp như sau. Giả sử cho ba vật x, y, z, ta đặt

$$(x, y, z) = ((x, y), z)$$

và gọi (x, y, z) là một *bộ ba* Muốn có

$$(x', y', z') = (x'', y'', z'')$$

cần và đủ là

$$x' = x'',\ y' = y'',\ z' = z''.$$

Thực vậy $((x', y'), z') = ((x'', y''), z'')$ tương đương với $(x', y') = (x'', y'')$ và $z' = z''$, vậy tương đương với $x' = x''$, $y' = y''$, $z' = z''$.

Cũng vậy, cho bốn vật x, y, z, t ta đặt

$$(x, y, z, t) = ((x, y), z), t)$$

và ta gọi (x, y, z, t) là một *bộ bốn*.

Định nghĩa 3. Cho hai tập hợp X và Y, tập hợp các cặp (x, y) với $x \in X$ và $y \in Y$ gọi là *tích đề các của X và Y* và kí hiệu bằng $X \times Y$.

Khái niệm tích đề các có thể mở rộng cho trường hợp nhiều tập hợp. Nếu X, Y, Z, T là những tập hợp, người ta định nghĩa

$$X \times Y \times Z = (X \times Y) \times Z$$

$$X \times Y \times Z \times T = (X \times Y \times Z) \times T...$$

Các phần tử của $X \times Y \times Z$ là các bộ ba (x, y, z) với $x \in X$, $y \in Y$, $z \in Z$. Cũng như vậy, các phần tử của $X \times Y \times Z \times T$ là các bộ bốn (x, y, z, t) với $x \in X$, $y \in Y$, $z \in Z$, $t \in T$. Cuối cùng nếu X là một tập hợp, ta đặt

$$X^2 = X \times X, X^3 = X \times X \times X, X^4 = X \times X \times X \times X...$$

8. Hợp và giao của hai tập hợp

Định nghĩa 4. Giả sử X và Y là hai tập hợp. Ta gọi là *hợp của X và Y* tập hợp kí hiệu $X \cup Y$ gồm các phần tử hoặc thuộc X hoặc thuộc Y, nghĩa là

$$z \in X \cup Y \text{ tương đương với } z \in X \text{ hoặc } z \in Y.$$

Ta còn có thể nói $X \cup Y$ gồm các phần tử thuộc ít nhất một trong hai tập hợp X và Y.

Định nghĩa 5. Giả sử X và Y là hai tập hợp. Ta gọi là *giao của X và Y* tập hợp kí hiệu $X \cap Y$ gồm các phần tử vừa thuộc X vừa thuộc Y, nghĩa là

$$z \in X \cap Y \text{ tương đương với } z \in X \text{ và } z \in Y.$$

Người ta bảo hai tập hợp X và Y là *không giao nhau* hay *rời nhau* khi $X \cap Y = \emptyset$, nghĩa là khi X và Y không có phần tử chung nào.

Rõ ràng ta có các quan hệ

$$X \cap Y \subset X \text{ và } Y,\ X \cup Y \supset X \text{ và } Y.$$

Ngoài ra, giả sử Z là một tập hợp tùy ý, muốn cho $Z \subset X$ và $Z \subset Y$, cần và đủ có $z \in X$ và $z \in Y$ với mọi $z \in Z$, nghĩa là $z \in X \cap Y$, tức là $Z \subset X \cap Y$. Như vậy $X \cap Y$ là tập hợp lớn nhất trong tất cả các tập hợp Z vừa chứa trong X vừa chứa trong Y. Cũng vậy, muốn Z chứa cả X và Y, cần và đủ là Z chứa $X \cup Y$; như thế $X \cup Y$ là tập hợp bé nhất chứa cả X lẫn Y.

Định lí 3. *Với các tập hợp A, B, C và X tùy ý, ta có :*

(i) *Tính chất giao hoán*

$$A \cap B = B \cap A,$$

$$A \cup B = B \cup A.$$

(ii) *Tính chất kết hợp*

$$A \cap (B \cap C) = (A \cap B) \cap C,$$

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

(iii) *Tính chất phân phối*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$

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

(iv) *Công thức Đờ Moóc-găng*

$$X - (A \cup B) = (X - A) \cap (X - B),$$
$$X - (A \cap B) = (X - A) \cup (X - B).$$

Chứng minh. (i) và (ii) hiển nhiên. Ta hãy chứng minh công thức thứ nhất của (iii). Giả sử $x \in A \cap (B \cup C)$, điều đó có nghĩa là $x \in A$ và x thuộc ít nhất một trong hai tập hợp B, C, chẳng hạn $x \in B$. Vậy $x \in A \cap B$, tức là $x \in (A \cap B) \cup (A \cap C)$. Đảo lại giả sử $x \in (A \cap B) \cup (A \cap C)$, điều đó có nghĩa là x thuộc ít nhất một trong hai tập hợp $A \cap B$, $A \cap C$, chẳng hạn $x \in A \cap B$, tức là $x \in A$ và $x \in B$, vậy $x \in A$ và $x \in (B \cup C)$ do đó $x \in A \cap (B \cup C)$.

Ta chứng minh công thức thứ hai của (iii). Giả sử $x \in A \cup (B \cap C)$, điều đó có nghĩa là x thuộc ít nhất một trong hai

tập hợp A, $B \cap C$, chẳng hạn $x \in A$. Vậy $x \in A \cup B$ và $x \in A \cup C$, tức là $x \in (A \cup B) \cap (A \cup C)$. Nếu $x \in B \cap C$ thì ta có $x \in B$ và $x \in C$, tức là $x \in A \cup B$ và $x \in A \cup C$, vậy $x \in (A \cup B) \cap (A \cup C)$. Đảo lại, giả sử $x \in (A \cup B) \cap (A \cup C)$, điều đó có nghĩa là $x \in A \cup B$ và $x \in A \cup C$. $x \in A \cup B$ có nghĩa là x thuộc ít nhất một trong hai tập hợp A, B. Nếu $x \in A$ thì $x \in A \cup (B \cap C)$. Nếu $x \notin A$ thì $x \in B$, và vì $x \in A \cup C$, nên $x \in C$. Vậy $x \in B \cap C$ và do đó $x \in A \cup (B \cap C)$.

(iv) Giả sử $x \in X - (A \cup B)$. Điều đó có nghĩa là $x \in X$ và $x \notin A \cup B$, tức là $x \in X$ và $x \notin A$ và $x \notin B$. Vậy $x \in X - A$ và $x \in X - B$, tức là $x \in (X - A) \cap (X - B)$. Đảo lại giả sử $x \in (X - A) \cap (X - B)$, điều đó có nghĩa là $x \in X - A$ và $x \in X - B$, tức là $x \in X$ và $x \notin A$ và $x \notin B$. Vậy $x \in X$ và $x \notin A \cup B$, tức là $x \in X - (A \cup B)$. Đối với công thức thứ hai của (iv) ta có thể chứng minh tương tự, hoặc áp dụng công thức thứ nhất của (iv) và định lí 2 (i) nếu A, $B \subset X$. Ta xét, với A, $B \subset X$

$$A \cap B = (X - (X - A)) \cap (X - (X - B)) =$$

$$= X - ((X - A) \cup (X - B))$$

Vậy $X - (A \cap B) = (X - A) \cup (X - B)$. ■

9. Ánh xạ

Định nghĩa 6. Giả sử X và Y là hai tập hợp đã cho. Một *ánh xạ* f *từ* X *đến* Y là một quy tắc cho tương ứng với mỗi phần tử x của X một phần tử xác định, kí hiệu $f(x)$ của Y. Ta viết

$$f : X \to Y \qquad \text{hay} \quad X \xrightarrow{f} Y$$
$$x \longmapsto f(x) \qquad\qquad x \longmapsto f(x)$$

Tập hợp X gọi là *nguồn* hay *miền xác định* và tập hợp Y gọi là *đích* hay *miền giá trị* của ánh xạ f.

Ví dụ. 1) Xét tập hợp $\mathbf{N}$ các số tự nhiên và tập hợp $\mathbf{Z}_m$ các số nguyên không âm nhỏ hơn một số nguyên dương đã cho m.

Với mọi $x \in \mathbf{N}$ ta hãy chia x cho m và được một số dư kí hiệu là $f(x)$. Số $f(x)$ thuộc $\mathbf{Z}_m$. Tương ứng

$$x \longmapsto f(x)$$

xác định một ánh xạ

$$f : \mathbf{N} \to \mathbf{Z}_m.$$

2) Xét tập hợp các số thực $\mathbf{R}$. Tương ứng

$$x \longmapsto x^2$$

xác định một ánh xạ từ $\mathbf{R}$ đến $\mathbf{R}$.

3) Giả sử $X = \{1, 2\}$, $Y = \{a, b, c\}$.

Tương ứng

$$1 \longmapsto c$$

$$2 \longmapsto a$$

xác định một ánh xạ từ X đến Y.

4) Giả sử $X = Y = \{1, 2, 3\}$.

Tương ứng

$$1 \longmapsto 3$$

$$2 \longmapsto 2$$

$$3 \longmapsto 1$$

xác định một ánh xạ từ X đến X.

Qua định nghĩa của ánh xạ, chúng ta thấy rằng khái niệm ánh xạ là khái niệm mở rộng của khái niệm hàm số mà ta gặp ở trường phổ thông. Các hàm số mà ta gặp ở trường phổ thông là những ánh xạ mà nguồn và đích là tập hợp các số thực $\mathbf{R}$ hoặc những bộ phận của $\mathbf{R}$, và số $f(x)$ tương ứng với số x là một biểu thức đại số hay một biểu thức lượng giác, chẳng hạn :

$$f(x) = 2x^2 - x + 3 \text{ hay } f(x) = 5\sin x.$$

Trong định nghĩa ánh xạ ta thấy các tập hợp nguồn và đích không nhất thiết là những tập hợp số và phần tử $f(x)$ tương ứng với x lại càng không phải là một biểu thức đại số hay lượng giác !

Trong Giải tích chúng ta thường có những bài toán về vẽ đồ thị của một hàm số. Ở đây chúng ta cũng hãy định nghĩa đồ thị của một ánh xạ.

Định nghĩa 7. Giả sử $f : X \to Y$. Bộ phận Γ của $X \times Y$ gồm các cặp $(x, f(x))$ với $x \in X$ gọi là *đồ thị của ánh xạ f*.

Như vậy, cho một ánh xạ $f : X \to Y$, ta được một bộ phận Γ của $X \times Y$ có tính chất : với mọi $x \in X$, có một và chỉ một cặp, có phần tử thứ nhất là x, thuộc Γ. Đảo lại, cho một bộ phận Γ của $X \times Y$ có tính chất đó, thì Γ cho ta một ánh xạ $f : X \to Y$ mà đồ thị là Γ. Cho nên người ta đồng nhất ánh xạ f với đồ thị của nó là một bộ phận của tích đề các $X \times Y$.

10. Ảnh và tạo ảnh

Định nghĩa 8. Giả sử $f : X \to Y$ là một ánh xạ đã cho, x là một phần tử tùy ý của X, A là một bộ phận tùy ý của X, B là một bộ phận tùy ý của Y. Thế thì người ta gọi :

- $f(x)$ là *ảnh của x bởi f* hay *giá trị của ánh xạ f tại điểm x*.

- $f(A) = \{ y \in Y \mid$ tồn tại $x \in A$ sao cho $f(x) = y \}$ là *ảnh của A bởi f*.

- $f^{-1}(B) = \{ x \in X \mid f(x) \in B \}$ là *tạo ảnh toàn phần của B bởi f*.

Đặc biệt với $b \in Y$, $f^{-1}(\{b\}) = \{ x \in X \mid f(x) = b \}$. Để đơn giản kí hiệu ta viết $f^{-1}(b)$ thay cho $f^{-1}(\{b\})$ và gọi là tạo ảnh toàn phần của b bởi f. Mỗi phần tử $x \in f^{-1}(b)$ gọi là một *tạo ảnh* của b bởi f.

Kí hiệu $f(A)$ là một điều lạm dụng vì $f(A)$ chỉ có nghĩa khi $A \in X$. Rõ ràng ta có $f(\emptyset) = \emptyset$ với mọi f. Ta chứng minh dễ dàng các quan hệ :

- $A \subset f^{-1}(f(A))$ *với mọi bộ phận A của X*.

- $B \supset f(f^{-1}(B))$ *với mọi bộ phận B của Y*.

Nhưng ta không có quyền, trong các quan hệ ấy, thay các dấu bao hàm bằng dấu đẳng thức. Chẳng hạn, trong ví dụ 2)

của mục 9, nếu lấy $A = \{1\}$ thì ta có $f^{-1}(f(A)) = \{-1, 1\}$ và $B = \{-1, 1\}$ thì ta có $f(f^{-1}(B)) = \{1\}$.

11. Đơn ánh - Toàn ánh - Song ánh

Định nghĩa 9. Ánh xạ $f : X \to Y$ là một *đơn ánh* nếu với mọi $x, x' \in X$, quan hệ $f(x) = f(x')$ kéo theo quan hệ $x = x'$ hay $x \neq x'$ kéo theo $f(x) \neq f(x')$; hay với mọi $y \in Y$ có nhiều nhất một $x \in X$ sao cho $y = f(x)$. Người ta còn gọi một đơn ánh $f : X \to Y$ là một *ánh xạ một đối một*.

Ví dụ. 1) Xét ánh xạ

$$f : \mathbf{R} \to \mathbf{R}$$
$$x \mapsto x^3$$

Rõ ràng f là một đơn ánh, vì nếu x và y là những số thực thì quan hệ $x^3 = y^3$ kéo theo $x = y$.

Đáng lẽ lấy **R**, ta lấy **C** thì ánh xạ

$$f : \mathbf{C} \to \mathbf{C}$$
$$x \mapsto x^3$$

không phải là đơn ánh nữa, vì gọi ε_o, ε_1, ε_2 là ba giá trị của căn bậc ba của đơn vị, ta có

$$\varepsilon_o^3 = \varepsilon_1^3 = \varepsilon_2^3 = 1.$$

2) Giả sử X là một tập hợp, ánh xạ

$$X \to X$$
$$x \mapsto x$$

gọi là *ánh xạ đồng nhất* của X kí hiệu 1_X hoặc e_X. Hiển nhiên 1_X là đơn ánh.

3) Cho $X \subset Y$. Ánh xạ

$$j : X \to Y$$
$$x \mapsto j(x) = x$$

gọi là *đơn ánh chính tắc* từ X đến Y. Ta có thể có nhiều đơn ánh từ X đến Y, nhưng đơn ánh j gọi là chính tắc vì nó được xây dựng một cách tự nhiên.

Định nghĩa 10. Ta bảo một ánh xạ $f : X \to Y$ là một *toàn ánh* nếu $f(X) = Y$, nói một cách khác, nếu với mọi $y \in Y$ có ít nhất một $x \in X$ sao cho $y = f(x)$. Người ta còn gọi một toàn ánh $f : X \to Y$ là một *ánh xạ từ X lên Y*.

Các ánh xạ trong các ví dụ 1) và 2) là những toàn ánh.

Định nghĩa 11. Ta bảo một ánh xạ $f : X \to Y$ là một *song ánh* hay một *ánh xạ một đối một từ X lên Y*, nếu nó vừa là đơn ánh vừa là toàn ánh, nói một cách khác nếu với mọi $y \in Y$ có một và chỉ một $x \in X$ sao cho $y = f(x)$.

Chẳng hạn ánh xạ đồng nhất 1_X là một song ánh với mọi X.

12. Tích ánh xạ

Định nghĩa 12. Giả sử cho

$$f : X \to Y \text{ và } g : Y \to Z.$$

Ánh xạ

$$X \to Z$$
$$x \longmapsto g(f(x))$$

gọi là *tích của ánh xạ f và ánh xạ g*, kí hiệu gof, hay vắn tắt gf.

Định lí 4. *Giả sử cho*

$$f : X \to Y,\ g : Y \to Z,\ h : Z \to T$$

Thế thì :

$$h(gf) = (hg)f.$$

Ta bảo phép nhân các ánh xạ có tính chất kết hợp.

Chứng minh. Ta có với mọi $x \in X$:

$$(h(gf))(x) = h((gf)(x)) = h(g(f(x))) =$$
$$= (hg)(f(x)) = ((hg)f)(x). \blacksquare$$

Do đó ta kí hiệu $h(gf) = (hg)f$ bằng hgf và gọi là tích của ba ánh xạ f, g, h.

Chú ý rằng nếu $f : X \to Y$ là một ánh xạ bất kì thì ta có

$$f1_X = 1_Y f = f$$

Định nghĩa 13. Giả sử $f : X \to Y$ và $g : Y \to X$ là hai ánh xạ sao cho

$$gf = 1_X \text{ và } fg = 1_Y$$

Thế thì g gọi là một *ánh xạ ngược của* f.

Từ định nghĩa ta suy ra f cũng là một ánh xạ ngược của g.

Định lí sau đây cho ta biết khi nào một ánh xạ có ánh xạ ngược.

Định lí 5. *Ánh xạ $f : X \to Y$ có một ánh xạ ngược khi và chỉ khi f là một song ánh.*

Chứng minh. Giả sử f có một ánh xạ ngược $g : Y \to X$.

Theo định nghĩa 13, ta có

$$gf = 1_X \text{ và } fg = 1_Y.$$

tức là

$$g(f(x)) = x \text{ với mọi } x$$

Xét quan hệ

$$f(x) = f(x'),$$

ta suy ra $x = g(f(x)) = g(f(x')) = x'$.

Vậy f là một đơn ánh. Bây giờ giả sử y là một phần tử tùy ý của Y. Đặt $x = g(y) \in X$ trong đẳng thức $f(g(y)) = y$, ta được $y = f(x)$. Vậy f là một toàn ánh.

Đảo lại giả sử f là một song ánh. Quy tắc cho tương ứng với mỗi $y \in Y$ phần tử duy nhất của $f^{-1}(y)$ xác định một ánh xạ $g : Y \to X$ và ta thấy ngay

$$gf = 1_X \text{ và } fg = 1_Y. \blacksquare$$

Như vậy $f : X \to Y$ có một ánh xạ ngược khi và chỉ khi f là song ánh, và trong trường hợp đó ta có một ánh xạ ngược $g : Y \to X$ của f xác định bởi

$$y \longmapsto g(y) = x, \text{ sao cho } f(x) = y.$$

Ngoài ánh xạ ngược này, f còn có ánh xạ ngược nào khác không ? Ta có

Định lí 6. *Giả sử $g : Y \to X$ và $g' : Y \to X$ là hai ánh xạ ngược của $f : X \to Y$. Thế thì $g = g'$.*

Chứng minh. Ta có

$$gf = 1_X \text{ và } fg' = 1_Y.$$

Từ đó

$$g = g\,1_Y = g(fg') = (gf)g' = 1_X g' = g'. \blacksquare$$

Như vậy nếu $f : X \to Y$ có ánh xạ ngược thì ánh xạ ngược là duy nhất, xác định bởi

$$y \longmapsto x, \text{ với } x \text{ là phần tử duy nhất của } f^{-1}(y).$$

Do lạm dụng người ta cũng kí hiệu phần tử duy nhất x của $f^{-1}(y)$ bằng $f^{-1}(y)$ và do đó người ta kí hiệu ánh xạ

$$y \longmapsto f^{-1}(y),$$

là ánh xạ ngược của f, bằng f^{-1}. Vì f là ánh xạ ngược của f^{-1} nên $f = (f^{-1})^{-1}$. Ta có $1_X^{-1} = 1_X$.

Hệ quả. *Cho hai song ánh $f : X \to Y$ và $g : Y \to Z$. Thế thì $gf : X \to Z$ là một song ánh.*

Chứng minh. Ta có

$$(gf)(f^{-1}g^{-1}) = g(ff^{-1})g^{-1} = g1_Y g^{-1} = gg^{-1} = 1_Z$$
$$(f^{-1}g^{-1})(gf) = f^{-1}(g^{-1}g)f = f^{-1}1_Y f = f^{-1}f = 1_X.$$

Vậy $f^{-1}g^{-1} = (gf)^{-1}$. $\blacksquare$

13. Thu hẹp và mở rộng ánh xạ

Định nghĩa 14. Giả sử $f : X \to Y$ là một ánh xạ và A là một bộ phận của X. ánh xạ

$$g : A \to Y$$
$$x \longmapsto g(x) = fx$$

gọi là *cái thu hẹp của ánh xạ f vào bộ phận A* và kí hiệu là $g = f|_A$. còn ánh xạ f gọi là *cái mở rộng của g trên tập hợp X*.

14. Tập hợp chỉ số

Giả sử I là một tập hợp tùy ý khác rỗng mà các phần tử được kí hiệu là $\alpha, \beta, \gamma \ldots$ và f là một ánh xạ

$$f : I \to X$$

Ta kí hiệu

$$f(\alpha) = x_\alpha$$
$$f(\beta) = x_\beta$$
$$f(\gamma) = x_\gamma$$
$$\ldots\ldots$$

Ta bảo các phần tử $x_\alpha, x_\beta, x_\gamma \ldots$ thành lập *một họ những phần tử của X được đánh số bởi tập hợp I*, kí hiệu là $(x_\alpha)_{\alpha \in I}$, còn tập hợp I gọi là *tập hợp chỉ số*. Nếu các $x_\alpha, x_\beta, x_\gamma \ldots$ là những tập hợp thì ta gọi $(x_\alpha)_{\alpha \in I}$ là *một họ tập hợp đánh số bởi tập hợp I*. Nếu các phần tử của X là những bộ phận của một tập hợp E, tức là ta có $x_\alpha, x_\beta, x_\gamma \ldots \subset E$, thì ta gọi $(x_\alpha)_{\alpha \in I}$ là *một họ những bộ phận* của tập hợp E.

Thực ra chúng ta đã thấy việc đánh số trước đây rồi. Trong Giải tích chúng ta thường xét những dãy số thực $u_0, u_1, u_2, \ldots$ Điều đó có nghĩa là ta đã đánh số bằng các số tự nhiên 0, 1, 2, ...

Ví dụ. Giả sử $I = \{ 1, 2, 3 \}$, $X = \{ a, b \}$ và do đó $\mathcal{P}(X) = \{ \varnothing, \{ a \}, \{ b \}, \{ a, b \} \}$, và

$$f : I \to \mathcal{P}(X)$$
$$1 \mapsto A_1 = \{ b \}$$
$$2 \mapsto A_2 = \{ a, b \}$$
$$3 \mapsto A_3 = \{ a, b \}$$

Như vậy họ $(A_i)_{i \in I}$ gồm ba tập hợp A_1, A_2, A_3 trong đó $A_2 = A_3$.

15. Hợp, giao, tích để các một họ tập hợp

Ở đây, chúng ta hãy mở rộng các phép toán hợp, giao, tích ra một số tùy ý những tập hợp.

Định nghĩa 15. Giả sử $(X_\alpha)_{\alpha \in I}$ là một họ tập hợp. Ta gọi là *hợp của họ* đó, và kí hiệu bằng $\bigcup_{\alpha \in I} X_\alpha$ tập hợp các x sao cho x thuộc ít nhất một tập hợp của họ $(X_\alpha)_{\alpha \in I}$

Định nghĩa 16. Giả sử $(X_\alpha)_{\alpha \in I}$ là một họ tập hợp. Ta gọi là *giao của họ* đó, và kí hiệu bằng $\bigcap_{\alpha \in I} X_\alpha$, tập hợp các x sao cho x thuộc tất cả các tập hợp của họ $(X_\alpha)_{\alpha \in I}$.

Định nghĩa 17. Giả sử $(X_\alpha)_{\alpha \in I}$ là một họ tập hợp và $X = \bigcup_{\alpha \in I} X_\alpha$ là hợp của họ đó. Ta gọi là *tích đề các của họ* $(X_\alpha)_{\alpha \in I}$ và kí hiệu bằng $\prod_{\alpha \in I} X_\alpha$ tập hợp các họ $(x_\alpha)_{\alpha \in I}$ những phần tử của X sao cho $x_\alpha \in X_\alpha$ với mọi $\alpha \in I$. Nếu các tập hợp X_α đều bằng một tập hợp A, thì tích đề các của họ $(X_\alpha)_{\alpha \in I}$ gọi là *lũy thừa đề các bậc I của tập hợp A* và kí hiệu là A^I.

Trong trường hợp $I = \{1, 2\}$ ta lại tìm thấy hợp, giao, tích đề các của hai tập hợp.

Ví dụ. 1) Xét họ tập hợp $(I_n)_{n \in \mathbf{N}}$ đánh số bởi các số tự nhiên 0, 1, 2,... với

$$I_n = \{0, 1, \ldots, n\},$$

thế thì $$\bigcup_{n \in \mathbf{N}} I_n = \mathbf{N}$$

$$\bigcap_{n \in \mathbf{N}} I_n = I_0 = \{0\}.$$

2) Lũy thừa đề các $\mathbf{R}^{\mathbf{N}}$ là tập hợp các dãy số thực

$$(u_0, u_1, \ldots, u_n, \ldots).$$

BÀI TẬP

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

2. Chứng minh ta có $A - (A - B) = B$ khi và chỉ khi $B \subset A$.

3. Giả sử X là một tập hợp có n phần tử và r là một số tự nhiên, $0 \leqslant r \leqslant n$. Tính :

a) Số các bộ phận của X có r phần tử.

b) Số các phần tử của $\mathcal{P}(X)$.

4. Biểu diễn hình học các tập $A \times B$ với

a) $A = \{x \in R \mid 1 \leqslant x \leqslant 3\}$

$B = R$, tập hợp các số thực.

b) $A = B = Z$, tập hợp các số nguyên.

5. Biểu diễn hình học tập hợp X gồm các điểm (x, y) của mặt phẳng để các có dạng (x, x) với $0 \leqslant x \leqslant 1$ hoặc có dạng $(x, x + 1)$ với $x \geqslant 0$.

6. Chứng minh :

a) $A \cup B = A$ khi và chỉ khi $B \subset A$.

b) $A \cap B = A$ khi và chỉ khi $A \subset B$.

c) $A \cup \phi = A$.

d) $A \cap \phi = \phi$.

7. Tập hợp X ở bài tập 5) có phải là đồ thị của một ánh xạ từ R đến R ?

8. Tập hợp $G = \{(x, x) \mid x < 0\} \cup \{(x, 0) \mid x \geqslant 0\}$ có phải là đồ thị của một ánh xạ từ R đến R ? Biểu diễn hình học tập hợp đó.

9. Tập hợp

$$G = \left\{\left(x, \frac{1}{x-1}\right) \mid x \in R, x \neq 1\right\}$$

có thể coi như đồ thị của một ánh xạ thế nào ? Biểu diễn hình học tập hợp đó.

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

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

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

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

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

e) $f(X - A) \supset f(X) - f(A)$.

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

11. Giả sử n là một số tự nhiên cho trước, f là một ánh xạ từ tập hợp các số tự nhiên N đến chính nó được xác định bởi

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

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

12. Giả sử $f : X \to Y$ và $g : Y \to Z$ là hai ánh xạ và $h = gf$ là ánh xạ tích của f và g. Chứng minh :

a) Nếu h là đơn ánh thì f là đơn ánh, nếu thêm f là toàn ánh thì g là đơn ánh.

b) Nếu h là toàn ánh thì g là toàn ánh, nếu thêm g là đơn ánh thì f là toàn ánh.

13. Cho ánh xạ $f : X \to Y$. Chứng minh f là một đơn ánh khi và chỉ khi có một ánh xạ $g : Y \to X$ sao cho $gf = 1_X$. ($X \neq \emptyset$).

14. Cho ánh xạ $f : X \to Y$. Chứng minh f là một toàn ánh khi và chỉ khi có một ánh xạ $g : Y \to X$ sao cho $fg = 1_Y$.

15. Cho ba ánh xạ $f : X \to Y$ và $g, g' : U \to X$. Chứng minh : a) Nếu f là đơn ánh và $fg = fg'$, thì $g = g'$.

b) Nếu với mọi g, g' mà $fg = fg'$ kéo theo $g = g'$, thì f là một đơn ánh.

16. Cho ba ánh xạ $f : X \to Y$ và $h, h' : Y \to Z$. Chứng minh rằng nếu f là một toàn ánh và $hf = h'f$ thì $h = h'$. Ngược lại

nếu với mọi h, h' ta có $hf = h'f$ kéo theo $h = h'$ thì f là một toàn ánh.

17. Chứng minh nếu có một song ánh từ X đến Y và một song ánh từ X đến Z, thì có một song ánh từ Y đến Z.

18. Chứng minh rằng muốn cho một bộ phận G của tích để các $X \times Y$ là đồ thị của một ánh xạ từ X đến Y thì cần và đủ là ánh xạ (phép chiếu) :

$$\begin{aligned} G &\to X \\ (x, y) &\mapsto x \end{aligned}$$

là một song ánh.

19. Giả sử $(A_\alpha)_{\alpha \in I}$ là một họ những bộ phận của một tập hợp X, B là một tập hợp tùy ý. Chứng minh

a) $\bigcup_{\alpha \in I} A_\alpha \supset A_\alpha$ với mọi $\alpha \in I$.

b) $\bigcap_{\alpha \in I} A_\alpha \subset A_\alpha$ với mọi $\alpha \in I$.

c) $B \cap (\bigcup_{\alpha \in I} A_\alpha) = \bigcup_{\alpha \in I} (B \cap A_\alpha)$.

d) $B \cup (\bigcap_{\alpha \in I} A_\alpha) = \bigcap_{\alpha \in I} (B \cup A_\alpha)$.

e) $X - (\bigcup_{\alpha \in I} A_\alpha) = \bigcap_{\alpha \in I} (X - A_\alpha)$.

f) $X - (\bigcap_{\alpha \in I} A_\alpha) = \bigcup_{\alpha \in I} (X - A_\alpha)$.

20. Giả sử $f : X \to Y$ là một ánh xạ, $(A_\alpha)_{\alpha \in I}$ là một họ những bộ phận của X, $(B_\beta)_{\beta \in J}$ là một họ những bộ phận của Y. Chứng minh

a) $f(\bigcup_{\alpha \in I} A_\alpha) = \bigcup_{\alpha \in I} f(A_\alpha)$.

b) $f(\bigcap_{\alpha \in I} A_\alpha) \subset \bigcap_{\alpha \in I} f(A_\alpha)$.

c) $f^{-1}(\bigcup_{\beta\in J} B_\beta) = \bigcup_{\beta\in J} f^{-1}(B_\beta)$.

d) $f^{-1}(\bigcap_{\beta\in J} B_\beta) = \bigcap_{\beta\in J} f^{-1}(B_\beta)$.

21. Cho hai tập hợp X và Y. Ta kí hiệu bằng $\mathrm{Hom}(X, Y)$ tập hợp tất cả các ánh xạ từ X đến Y. Chứng minh

a) Có một song ánh từ $\mathrm{Hom}(X, Y)$ đến Y^X.

b) Nếu Y chỉ có hai phần tử thì có một song ánh từ $\mathrm{Hom}(X, Y)$ đến $\mathcal{P}(X)$.

c) Từ a) và b) hãy suy ra nếu X có n phần tử, thì $\mathcal{P}(X)$ có 2^n phần tử.

§2. QUAN HỆ

1. Quan hệ hai ngôi

Trong §1. 9 chúng ta đã đưa vào khái niệm ánh xạ. Một ánh xạ $f : X \to Y$ cho tương ứng với mỗi phần tử $x \in X$ một phần tử $y = fx \in Y$. Như vậy các phần tử x, y có một quan hệ với nhau, quan hệ đó là $y = fx$, hay nói một cách khác, quan hệ đó là $(x, y) \in G$, với G là đồ thị của f. Tổng quát hơn, người ta nghĩ đến một cách ghép cặp những phần tử của X với những phần tử của Y để thành lập một bộ phận của $X \times Y$, và gọi cách ghép cặp đó là một *quan hệ hai ngôi*.

Định nghĩa 1. Giả sử X và Y là những tập hợp. Một quan hệ hai ngôi từ X đến Y là một bộ phận S của tích đề các $X \times Y$. Ta bảo, với hai phần tử $a \in X$ và $b \in Y$, rằng a có quan hệ S với b nếu và chỉ nếu $(a, b) \in S$. Ta viết aSb.

Đồ thị G của một ánh xạ $f : X \to Y$ cho ta một ví dụ về quan hệ hai ngôi, và trong trường hợp này người ta viết $b = fa$ chứ không viết aGb. Một ánh xạ cho ta một quan hệ hai ngôi, nhưng đảo lại không đúng (§1, bài tập 5).

Như vậy, một ánh xạ cho ta một quan hệ hai ngôi đặc biệt. Ngoài quan hệ hai ngôi quan trọng này, toán học còn có hai loại quan hệ hai ngôi quan trọng nữa, đó là quan hệ tương đương và quan hệ thứ tự.

2. Quan hệ tương đương

Định nghĩa 2. Giả sử X là một tập hợp, S là một bộ phận của $X \times X$. Thế thì S gọi là một *quan hệ tương đương trong* X nếu và chỉ nếu các điều kiện sau đây thỏa mãn :

1. (Phản xạ) Với mọi $a \in X$; aSa.

2. (Đối xứng) Với mọi $a, b \in X$; nếu aSb, thì bSa.

3. (Bắc cầu) Với mọi $a, b, c \in X$; nếu aSb và bSc, thì aSc.

Nếu S là một quan hệ tương đương, thì người ta thường kí hiệu S bằng $\sim$ và thường đọc aSb ($a \sim b$) là "a tương đương với b".

Ví dụ. 1) Dấu bằng thường dùng trong số học thông thường các số thực là một ví dụ quen thuộc về quan hệ tương đương. Trong trường hợp đó tập hợp S là đường thẳng $y = x$ của mặt phẳng để các R^2.

2) Ta xét quan hệ đồng dư mod 5 chẳng hạn trong số học. Hai số nguyên m, n gọi là đồng dư mod 5 nếu $m - n$ chia hết cho 5. Rõ ràng quan hệ này là một quan hệ tương đương trong Z. Ta hãy kí hiệu bằng $C(i)$, $i = 0, 1, 2, 3, 4$ tập hợp các số nguyên tương đương với i

$$C(i) = \{5x + i \mid x \in Z\},$$

thế thì mọi số nguyên thuộc $\bigcup_{i=0}^{4} C(i)$ và $C(i) \cap C(j) = \varnothing$ với $i \neq j$, $i = 0, 1, \ldots, 4$; $j = 0, 1, \ldots, 4$, Ta sẽ thấy các điều kiện tương tự như vậy cho một quan hệ tương đương tùy ý.

3) Ta xét tập hợp X các vectơ trong không gian của Hình học giải tích. Ta bảo một vectơ α có quan hệ S với vectơ β khi và chỉ khi α cùng hướng, cùng chiều, cùng môđun với β. Quan hệ S rõ ràng là một quan hệ tương đương. Ta cũng kí hiệu

bằng $C(a)$ tập hợp các vectơ tương đương với a, thế thì $C(a)$ chẳng qua là một vectơ tự do.

Định nghĩa 3. Giả sử S là một quan hệ tương đương trong X và $a \in X$. Tập hợp

$$C(a) = \{x \in X \mid xSa\}$$

gọi là *lớp tương đương của a đối với quan hệ tương đương S.*

Vì S là phản xạ nên $a \in C(a)$.

Ta thấy tức khắc rằng $C(a)$ có các tính chất sau :

(i) $C(a) \neq \emptyset$.

(ii) $x, y \in C(a)$ kéo theo xSy.

(iii) $x \in C(a)$ và ySx kéo theo $y \in C(a)$.

Bổ đề 1. *Với hai phần tử bất kì a và b, ta đều có hoặc $C(a) \cap C(b) = \emptyset$ hoặc $C(a) = C(b)$.*

Chứng minh. Giả sử $C(a) \cap C(b) \neq \emptyset$. Ta sẽ chứng minh $C(a) = C(b)$. Gọi c là một điểm thuộc $C(a) \cap C(b)$. Ta có cSa và cSb, và do tính chất đối xứng và bắc cầu, nên $a \in C(b)$. Do đó với mọi $x \in C(a)$, tức là với mọi x tương đương với a, ta đều có $x \in C(b)$, tức là $C(a) \subset C(b)$. Tương tự, ta chứng minh $C(b) \subset C(a)$. Vậy, ta có $C(a) = C(b)$. ■

Từ bổ đề trên ta suy ra ngay $C(x) = C(a)$ với mọi $x \in C(a)$.

Định nghĩa 4. Ta bảo ta thực hiện một *sự chia lớp trên một tập hợp X* khi ta chia nó thành những bộ phận $A, B, C, \ldots$ khác $\emptyset$, rời nhau từng đôi một, sao cho mọi phần tử của X thuộc một trong các bộ phận đó.

Định lí 1. *Giả sử X là một tập hợp, S là một quan hệ tương đương trong X. Thế thì các lớp tương đương phân biệt của X đối với S thành lập một sự chia lớp trên X.*

Chứng minh. Thật vậy, với mọi $x \in X$, ta có $x \in C(x)$. Còn hai lớp tương đương phân biệt là rời nhau thì do Bổ đề 1. ■

Như vậy cho một quan hệ tương đương S trong một tập hợp X, ta được một sự chia lớp trên X, đó là việc chia X thành các lớp tương đương. Định lí sau đây cho ta thấy điều ngược lại cũng đúng.

Định lí 2. *Giả sử ta có một sự chia lớp trên một tập hợp X và A, B, C,... là các bộ phận của X do sự chia lớp. Thế thì có một quan hệ tương đương duy nhất S trong X sao cho các lớp tương đương của X đối với S là các bộ phận A, B, C,...*

Việc chứng minh định lí trên, xin dành cho độc giả, xem như bài tập.

Định nghĩa 5. Giả sử X là một tập hợp, S là một quan hệ tương đương trong X. Tập hợp các lớp tương đương phân biệt của X đối với S gọi là *tập hợp thương của X trên quan hệ tương đương S* và được kí hiệu là X/S.

Ví dụ. Xét quan hệ đồng dư mod n trong Số học (n là một số nguyên dương cho trước). Hai số nguyên x, y gọi là đồng dư mod n nếu $x - y$ là bội của n. Rõ ràng quan hệ này là một quan hệ tương đương trong **Z**. Tập hợp thương của **Z** trên quan hệ đồng dư mod n có n lớp tương đương :

$$C(0),\ C(1),\ldots\ ,\ C(n-1)$$

với $$C(i) = \{nx + i \mid x \in \mathbf{Z}\}\ i = 0, 1, \ldots, n - 1.$$

3. Quan hệ thứ tự

Định nghĩa 6. Giả sử X là một tập hợp, S là một bộ phận của $X \times X$. Thế thì S được gọi là *một quan hệ thứ tự trong X* (hay người ta còn gọi S là một quan hệ thứ tự giữa các phần tử của X) nếu và chỉ nếu các điều kiện sau đây thỏa mãn :

1. (Phản xạ) Với mọi $a \in X$: aSa.

2. (Phản đối xứng) Với mọi $a, b \in X$: nếu aSb và bSa, thì $a = b$.

3. (Bắc cầu) Với mọi $a, b, c \in X$; nếu aSb và bSc, thì aSc.

Người ta bảo một tập hợp X là *sắp thứ tự* nếu trong X có một quan hệ thứ tự.

Ví dụ. 1) Quan hệ $\leqslant$ trong tập hợp các số tự nhiên **N** là một quan hệ thứ tự.

2) **Quan hệ chia hết trong N** : người ta kí hiệu $a|b$ và đọc "a chia hết b".

3) **Quan hệ bao hàm $\subset$ giữa các bộ phận của một tập hợp X.**

Trong ví dụ 1), với a và b tùy ý ta luôn có $a \leqslant b$ hoặc $b \leqslant a$. Người ta gọi một quan hệ thứ tự như vậy là *toàn phần*. Trong ví dụ 2) không phải ta luôn luôn có $a|b$ hoặc $b|a$ với a, b tùy ý, chẳng hạn với $a = 2$ và $b = 3$. Điều đó cũng xảy ra với ví dụ 3). Người ta bảo $|$ và $\subset$ là những quan hệ thứ tự *bộ phận*.

Nếu S là một quan hệ thứ tự trong X, thì người ta thường kí hiệu S bằng $\leqslant$ (bắt chước kí hiệu quan hệ thứ tự thông thường của số nguyên hay số thực) và đọc $a \leqslant b$ là "a bé hơn b". Người ta coi $b \geqslant a$ là đồng nghĩa với $a \leqslant b$ và đọc là "b lớn hơn a". Người ta còn viết $a < b$ (hay $b > a$) quan hệ "$a \leqslant b$ và $a \neq b$" và đọc là "a thực sự bé hơn b" hay "b thực sự lớn hơn a".

Định nghĩa 7. Giả sử X là một tập hợp sắp thứ tự. Một phần tử $a \in X$ gọi là *phần tử tối tiểu* (phần tử tối đại) của X nếu quan hệ $x \leqslant a$ ($x \geqslant a$) kéo theo $x = a$.

Ví dụ. 1) Trong tập hợp các số tự nhiên thực sự lớn hơn 1, sắp thứ tự theo quan hệ $|$ (quan hệ chia hết), các phần tử tối tiểu là các số nguyên tố.

2) Trong tập hợp các hệ vectơ độc lập tuyến tính của không gian vectơ $\mathbf{R}^n$ sắp thứ tự theo quan hệ bao hàm $\subset$, các hệ vectơ gồm n vectơ là tối đại.

3) Tập hợp các số thực, với quan hệ thứ tự thông thường, không có phần tử tối đại cũng không có phần tử tối tiểu.

Định nghĩa 8. Giả sử X là một tập hợp sắp thứ tự. Một phần tử $a \in X$ gọi là *phần tử bé nhất* (phần tử lớn nhất) của X nếu, với mọi $x \in X$, ta có $a \leqslant x$ ($x \leqslant a$).

Nếu một tập hợp X sắp thứ tự có một phần tử bé nhất a thì a là phần tử bé nhất duy nhất. Thật vậy giả sử có b là phần tử bé nhất, ta suy ra $a \leqslant b$ và $b \leqslant a$, tức là $a = b$. Cũng nhận xét như vậy đối với phần tử lớn nhất.

Ví dụ. 1) Tập hợp các số tự nhiên sắp thứ tự theo quan hệ | có phần tử bé nhất là 1 và phần tử lớn nhất là 0. Nếu sắp thứ tự theo quan hệ thứ tự thông thường, tập hợp các số tự nhiên có phần tử bé nhất là 0 và không có phần tử lớn nhất.

2) Giả sử X là một bộ phận khác rỗng của $\mathcal{P}(E)$, tập hợp các bộ phận của một tập hợp E. Nếu X có phần tử bé nhất A (lớn nhất) đối với quan hệ bao hàm, thì A chẳng qua là giao (hợp) của các tập hợp thuộc X. Đảo lại, nếu giao (hợp) các tập hợp của X lại thuộc X, thì đó là phần tử bé nhất (lớn nhất) của X. Đặc biệt, $\varnothing$ là phần tử bé nhất và E là phần tử lớn nhất của $\mathcal{P}(E)$.

3) Tập hợp các số thực, với quan hệ thứ tự thông thường, không có phần tử bé nhất cũng không có phần tử lớn nhất.

Định nghĩa 9. Ta bảo một tập hợp X là *sắp thứ tự tốt* nếu nó là sắp thứ tự và nếu mọi bộ phận khác rỗng của X có một phần tử bé nhất.

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

BÀI TẬP

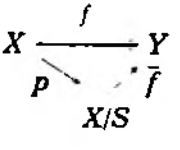
1. Giả sử $f : X \to Y$ là một ánh xạ, S là bộ phận của $X \times X$ gồm các cặp (x, x') sao cho $f(x) = f(x')$.

a) Chứng minh S là một quan hệ tương đương trong X.

b) Xét tập hợp thương X/S và ánh xạ

$$\begin{aligned} p : \ & X \to X/S \\ & x \mapsto C(x). \end{aligned}$$

Chứng minh có một ánh xạ duy nhất $\bar{f} : X/S \to Y$ sao cho biểu đồ sau là giao hoán



nghĩa là $f = \bar{f}p$.

c) Chứng minh $\bar{f}$ là đơn ánh và trong trường hợp f là toàn ánh thì $\bar{f}$ là song ánh.

2. Xét tập hợp các số nguyên $\mathbf{Z}$ và tập hợp $\mathbf{N}^*$ các số tự nhiên khác 0. Gọi S là quan hệ trong $\mathbf{Z} \times \mathbf{N}^*$ xác định bởi

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

Chứng minh S là một quan hệ tương đương.

3. Giả sử S là một quan hệ hai ngôi xác định trong tập hợp các số nguyên $\mathbf{Z}$ bởi các cặp (x, y) với x, y nguyên và $x + y$ lẻ.

Chứng minh :

a) S không phải là đồ thị của một ánh xạ từ $\mathbf{Z}$ đến $\mathbf{Z}$.

b) S không phải là một quan hệ tương đương.

c) S không phải là một quan hệ thứ tự.

d) Nếu đổi giả thiết một chút bằng cách cho $x + y$ chẵn, thì thế nào ?

4. Giả sử X là một tập hợp và T là một quan hệ hai ngôi phản xạ, đối xứng trong X. Ta hãy xác định một quan hệ hai ngôi S trong X như sau : xSy khi và chỉ khi có $x_1 = x, x_2, \ldots, x_n = y$ sao cho $x_1Tx_2, x_2Tx_3, \ldots, x_{n-1}Tx_n$. Chứng minh

a) S là một quan hệ tương đương và $T \subset S$.

b) Với mọi quan hệ tương đương H sao cho $T \subset H$ thì $S \subset H$.

5. Xét quan hệ hai ngôi trong tập hợp các số thực $\mathbf{R}$ xác định bởi tập hợp X (§1, bài tập 5).

a) Hãy bổ sung X để có một quan hệ hai ngôi phản xạ, đối xứng T (tất nhiên bổ sung ít nhất !). Biểu diễn hình học T.

b) Có T, hãy xây dựng quan hệ tương đương S như bài tập 4). Biểu diễn hình học S.

6. Giả sử X là tập hợp các hàm số khả vi xác định trên tập hợp các số thực $\mathbf{R}$. Giả sử S là quan hệ xác định bởi ySz khi và chỉ khi $dy\,dx = dz\,dx$ với mọi $x \in \mathbf{R}$. S có phải là quan hệ tương đương không ?

7. Cho X là không gian ba chiều thông thường và O là một điểm cố định của X. Trong X ta xác định quan hệ S như sau :

PSP' khi và chỉ khi O, P, P' thẳng hàng.

a) S có phải là quan hệ tương đương trong X không ?

b) S có phải là quan hệ tương đương trong $X - \{O\}$ không ? Nếu phải, xác định các lớp tương đương.

8. Giả sử X là một tập hợp và S là một quan hệ thứ tự trong X. Chứng minh rằng quan hệ T trong X xác định bởi aTb khi và chỉ khi bSa cũng là một quan hệ thứ tự trong X.

9. Giả sử X là một tập hợp và S là một quan hệ tương đương trong X. Chứng minh S không phải là một quan hệ thứ tự.

10. Xét tập hợp $X = \mathbf{N}^n$ $(n \geqslant 1)$, với $\mathbf{N}$ là tập hợp các số tự nhiên. Trong X ta xác định quan hệ S như sau :

$(a_1,..., a_n)S(b_1,..., b_n)$ khi và chỉ khi $(a_1, ..., a_n) = (b_1, ..., b_n)$ hoặc có một chỉ số i $(i = 1,2,... , n)$ sao cho $a_1 = b_1, ..., a_{i-1} = b_{i-1}, a_i < b_i$.

Chứng minh S là một quan hệ thứ tự toàn phần.

11. Giả sử f là một đơn ánh từ một tập hợp X đến tập hợp các số tự nhiên $\mathbf{N}$ và S là một quan hệ trong X xác định như sau :

$$xSx' \text{ khi và chỉ khi } f(x) \leqslant f(x').$$

Chứng minh S là một quan hệ thứ tự toàn phần.

12. Cho hai tập hợp X và Y. Gọi $\Phi(X, Y)$ là tập hợp các ánh xạ từ các bộ phận của X đến Y, nghĩa là nếu $f \in \Phi(X, Y)$ thì f là một ánh xạ có nguồn là một bộ phận của X và có đích là Y. Xét quan hệ S trong $\Phi(X, Y)$ xác định như sau :

fSg khi và chỉ khi g là mở rộng của ánh xạ f.

a) Chứng minh S là một quan hệ thứ tự.

b) Tìm các phần tử tối tiểu, tối đại, bé nhất, lớn nhất của $\Phi(X, Y)$ đối với S.

13. Chứng minh nếu a là phần tử bé nhất (lớn nhất) của một tập hợp X đối với một quan hệ thứ tự S, thì a là phần tử tối tiểu (tối đại) duy nhất của X.

14. Chứng minh nếu X sắp thứ tự tốt thì X sắp thứ tự toàn phần.

15. Chứng minh các tập hợp trong các bài tập 10) và 11) là sắp thứ tự tốt.

§3. SƠ LƯỢC VỀ CÁC TIÊN ĐỀ CỦA LÍ THUYẾT TẬP HỢP

1. Mở đầu

Như ta đã nói ở đầu chương, lí thuyết tập hợp mà ta đã trình bày là một lí thuyết sơ cấp theo quan điểm ngây thơ. Bây giờ chúng ta hãy giới thiệu sơ lược các tiên đề của lí thuyết tập hợp. Bạn đọc muốn tìm hiểu kĩ có thể tham khảo nhiều sách, chẳng hạn "Lí thuyết tập hợp" của Bourbaki.

2. Khái niệm nguyên thủy

Chúng ta không định nghĩa chữ tập hợp : ta gọi nó là khái niệm *nguyên thủy*. *Khái niệm thuộc vào*, được kí hiệu như ta đã biết bằng $\in$, cũng là một khái niệm *nguyên thủy*.

Tuy hai khái niệm tập hợp và thuộc vào không được định nghĩa, nhưng chúng ta lại tự ấn định các quy tắc : điều gì ta có thể làm được và điều gì ta không thể làm được với hai khái niệm đó. Đó là bảy tiên đề của *Zermelo - Fraenkel*, mà chúng ta thêm vào cái thứ tám, *tiên đề chọn*.

Theo truyền thống, các tiên đề đó được cho dưới tên và thứ tự sau : tiên đề *quảng tính*, tiên đề *tuyển lựa* (hay còn gọi tiên đề nói năm, hay tiên đề *chỉ rõ*, hay tiên đề *tách*), tiên đề cặp, tiên đề hợp, tiên đề *tập hợp các bộ phận*, tiên đề vô hạn

(hay *tiên đề các số tự nhiên*), tiên đề *chọn* và cuối cùng là tiên đề *thay thế*. Tiên đề cuối cùng còn gọi là tiên đề *thay chỗ* chỉ tham dự vào lí thuyết tập hợp khi đưa vào khái niệm quy nạp siêu hạn và số học thứ tự. Tiên đề đó được Fraenkel đưa vào năm 1922. Hệ thống tiên đề (không có tiên đề chọn) thành lập lí thuyết tập hợp của Zermelo - Fraenkel. Một vài trong các tiên đề đó nói lên những tính chất ít nhiều hiển nhiên khi ta phát biểu chúng trong ngôn ngữ thông thường.

Trước hết chúng ta hãy xác định thế nào là một văn bản toán học. Bằng các chữ (lớn, nhỏ, la tinh, hi lạp, v.v...), các kí hiệu của logic kinh điển, hai kí hiệu $\in$ và $=$, và các dấu ngoặc, chúng ta có thể viết bất kì văn bản toán học nào (mà chúng ta cũng gọi là *công thức, phát biểu, mệnh đề, khẳng định,* v.v...) của lí thuyết tập hợp.

Chúng ta sẽ gọi là phát biểu toán học hình thức cái mà ta được bằng cách áp dụng các quy tắc sau :

1°) $x \in y$, $A = B$, trong đó x, y, A, B là những chữ tùy ý, là những phát biểu. Các phát biểu đó gọi là những công thức *sơ cấp* hay *nguyên tử*.

2°) Nếu P và Q đã là những phát biểu, thế thì

$$(\neg P),\ (P \wedge Q),\ (P \vee Q),\ (P \to Q),\ (P \leftrightarrow Q)$$

là những phát biểu.

3°) Nếu P là một phát biểu, thế thì $(\exists x)\ (P(x))$, $(\forall x)\ (P(x))$ là những phát biểu.

3. Tiên đề quảng tính

$$(\forall A)(\forall B)[A = B \leftrightarrow (\forall x)(x \in A \leftrightarrow x \in B)]$$

Trực giác, điều đó muốn nói một tập hợp hoàn toàn được xác định bởi các phần tử của nó ; hai tập hợp A và B bằng nhau nếu và chỉ nếu mọi phần tử của A là phần tử của B và ngược lại.

Chú ý : - Giả sử X, A, B là những tập hợp. Chúng ta đã nói rằng quan hệ $X \in A$ đọc là X thuộc A, hay X là một phần tử của tập hợp A. Thông thường người ta hay viết quan hệ đó

dưới dạng $x \in A$, nhưng đó chỉ là một sự lạm dụng cách viết trong khi x là một tập hợp cũng như A.

4. Tiên đề tuyển lựa hay nội hàm

$$(\forall A)\ (\exists B)(\forall x)[x \in A \wedge P(x)) \leftrightarrow x \in B]$$

Trực giác, điều đó có nghĩa cho một công thức P(x) trên một tập hợp biến x, tồn tại một tập hợp B, mà các phần tử là các phần tử của A, có tính chất P(x) (nghĩa là làm cho công thức P(x) đúng). Tập hợp B lúc đó được xác định duy nhất bởi tiên đề quảng tính. Trước khi phát biểu tiên đề tuyển lựa dưới dạng đã cho, nhiều nhà toán học đã nghĩ rằng chỉ cần một công thức là đủ để xác định một tập hợp :

$$\{x \mid P(x)\} \qquad (4.1)$$

là tập hợp các vật làm cho công thức P(x) đúng.

Năm 1901 Bertrand Russel khám phá người ta có thể suy ra một mâu thuẫn từ (4.1) bằng cách xét các vật không thuộc chính nó. Thật vậy, xét công thức $x \notin x$. Khi đó chúng ta muốn xét tập hợp các tập hợp không thuộc chính nó. Giả sử tập hợp đó tồn tại. Vậy ta có thể viết

$$(\exists\ B)(\forall x)(x \in B \leftrightarrow x \notin x)$$

Lấy $x = B$, ta đi đến công thức :

$$B \in B \leftrightarrow B \notin B.$$

Về mặt lịch sử, chính nghịch lí đó đã dẫn tới công thức hiện nay của tiên đề tuyển lựa.

Nghịch lí B. Russel dựa trên công thức $x \notin x$, đưa chúng ta tới định lí sau đây

Định lí 1 - *Không tồn tại tập hợp mà các vật của nó là các tập hợp.*

Chứng minh. Thật vậy, giả sử một tập hợp A như vậy tồn tại. Theo tiên đề tuyển lựa, ta có thể xác định tập hợp B bởi :

$$B = \{x \in A \mid x \notin x\}$$

Theo định nghĩa của A, tập hợp B là một phần tử của A. Thế thì ta có $B \in B$ nếu và chỉ nếu $B \notin B$, điều này mâu

thuẫn vì P và ⌉P không thể đồng thời đúng (nguyên tắc không mâu thuẫn).■

Ta vừa thấy kí hiệu dạng (4.1) không nhất thiết chỉ ra một tập hợp. Nhưng kí hiệu đó lại rất tiện. Để sửa chữa bất tiện đó, ta đưa vào *một từ nguyên thủy mới*, đó là khái niệm *lớp*. Chúng ta sẽ bảo (4.1) kí hiệu lớp các tập hợp x thỏa mãn tính chất P(x). Ví dụ :

$$\{x \mid x = x\}$$

là *lớp tất cả các tập hợp*. Lúc đó ta sẽ nói đến *lớp các nhóm, lớp các không gian vecto trên một trường*.

5. Tiên đề cặp

$$(\forall a)\ (\forall b)\ (\exists\ c)\ (\forall x)\ [x \in c \leftrightarrow (x = a\ V\ x = b)]$$

Trực giác điều đó có nghĩa cho hai tập hợp a và b có một tập hợp c có phần tử là a và b và chỉ chúng. Tập hợp đó là duy nhất theo tiên đề quảng tính.

Định nghĩa 1 - Giả sử a và b là hai tập hợp. Ta gọi là *cặp* (không xếp thứ tự) thành lập bởi a và b, tập hợp kí hiệu {a, b} xác định bởi tiên đề cặp. Người ta gọi là *đơn tử* thành lập bởi tập hợp a, tập hợp {a, a} = {a} chỉ có tập hợp a là phần tử duy nhất.

Định nghĩa 2 - Giả sử a và b là hai tập hợp. Ta gọi là *cặp sắp thứ tự* của a (đứng thứ nhất) và của b (đứng thứ hai), cặp thành lập bởi đơn tử {a} và cặp {a, b}. Cặp đó kí hiệu :

$$(a, b) = \{\ \{a\}, \{a, b\}\ \}$$

6. Tiên đề hợp

$$(\forall A)\ (\exists\ B)\ (\forall x)[x \in B \leftrightarrow (\exists\ C)\ ((C \in A \wedge x \in C))]$$

Trực giác, điều có nghĩa cho một tập hợp A mà các phần tử gồm những tập hợp kí hiệu C, có một tập hợp B mà các phần tử là các tập hợp thuộc vào một trong các tập hợp C của bộ (= tập hợp) A. Tập hợp đó là duy nhất theo tiên đề quảng tính và gọi là *hợp* của các tập hợp của bộ A và kí hiệu

$$\bigcup_{C \in A} C \text{ hay } \bigcup A \text{ hay } \bigcup \{C \mid C \in A\}$$

7. Tiên đề tập hợp các bộ phận

$$(\forall A)\ (\exists\ B)(\forall X)(X \in B \leftrightarrow X \subset A)$$

Trực giác có nghĩa cho một tập hợp A, có một tập hợp B mà các phần tử là các bộ phận của A. Tập hợp đó là duy nhất theo tiên đề quảng tính và gọi là *tập hợp các bộ phận của tập hợp A*, kí hiệu $\mathcal{P}(A)$.

8. Tiên đề chọn

$$(\forall I)\ [(I \neq \emptyset), [(\forall i \in I,\ X_i \neq \emptyset\ ) \rightarrow \prod_{i \in I} X_i \neq \emptyset)]]$$

Trực giác điều đó có nghĩa nếu $(X_i)_{i \in I}$ là một họ *không rỗng* $(I \neq \emptyset)$ những tập hợp *không rỗng*, thế thì tích Descartes của họ đó là một tập hợp không rỗng.

Điều đó cũng có nghĩa rằng mọi họ *không rỗng* $(X_i)_{i \in I}$ những tập hợp *không rỗng* có một hàm chọn, nghĩa là một ánh xạ φ xác định trong I sao cho với mọi $i \in I$, $\varphi(i) \in X_i$.

Paul J. Cohen đã chứng minh rằng tiên đề chọn là độc lập đối với các tiên đề của lí thuyết Zermelo – Fraenkel. Trước đó Gödel đã chứng minh nếu lí thuyết tập hợp của Zermelo – Fraenkel là không mâu thuẫn, nó sẽ không mâu thuẫn nếu ta thêm vào tiên đề chọn.

Trong bài giảng Đại số, chúng ta hay dùng bổ đề Zorn và định lí Zermelo (thứ tự tốt). Tiên đề chọn tương đương với các phát biểu đó.

Bổ đề Zorn – *Mọi tập hợp E không rỗng sắp thứ tự quy nạp có ít nhất một phần tử tối đại.*

Định lí Zermelo – *Mọi tập hợp có thể sắp thứ tự tốt.*

9. Tiên đề vô hạn

Định nghĩa 3 – Với mọi tập hợp x, ta gọi là *cái kế tiếp* của x, tập hợp có các phần tử là các phần tử của x và tập

hợp x. Vậy đó là hợp của tập hợp x và đơn tử {x}. Nó được kí hiệu x^+ :

$$x^+ = x \cup \{x\}.$$

Với kí hiệu đó, ta có

$$1 = 0^+,\ 2 = 1^+,\ 3 = 2^+ \ldots$$

vì $0 = \varnothing,\ 1 = \{\varnothing\},\ 2 = \{\varnothing, \{\varnothing\}\} \ldots$

Theo cách xây dựng trên, mọi số tự nhiên đều có thể viết tường minh. Vấn đề đặt ra là có tồn tại một tập hợp chứa tất cả các số tự nhiên đó ? Tiên đề vô hạn sẽ trả lời câu hỏi đó.

Tiên đề vô hạn là như sau :

$$(\exists\ A)\ [\ \varnothing \in A \wedge (\forall x)\ (x \in A \Rightarrow x^+ \in A)]$$

Trực giác điều đó có nghĩa tồn tại một tập hợp chứa $\varnothing$ và chứa cái kế tiếp của mỗi phần tử của nó.

Ta có thể dễ dàng chứng minh định lí sau đây :

Định lí 2 – *Có một tập hợp bé nhất, kí hiệu* **N**, *có các tính chất sau*

(i) $\varnothing \in \mathbf{N}$,

(ii) Với mọi $x \in \mathbf{N}$, $x^+ \in \mathbf{N}$.

Tập hợp **N** gọi là *tập hợp các số tự nhiên*.

10. Tiên đề thay thế

$$[(\forall x)\ \exists Y)\ (\forall y)\ ((x \in A) \wedge S(x, y) \Rightarrow y \in Y)]$$

$$\Rightarrow [(\exists\ B)(\forall y)(y \in B \Leftrightarrow (\exists\ x)(x \in A \wedge S(x, y))]$$

Nói một cách khác, giả sử S(x, y) là một phát biểu phụ thuộc hai biến x và y và A là một tập hợp. Ta giả sử với mọi $x \in A$, lớp $\{y \mid S(x, y)\}$ là một tập hợp. Thế thì tồn tại một tập hợp chứa đúng các phần tử y sao cho S(x, y) là đúng với ít nhất một $x \in A$.

Tiên đề này được sử dụng khi ta đưa vào khái niệm quy nạp siêu hạn và số thứ tự.

CHƯƠNG II

NỬA NHÓM VÀ NHÓM

§1. NỬA NHÓM

1. Phép toán hai ngôi

Làm Đại số, chủ yếu là *tính toán* mà ví dụ điển hình là bốn phép toán của Số học sơ cấp. Thực chất mà nói, làm một phép toán đại số trên hai phần tử a, b của cùng một tập hợp X là cho tương ứng với cặp (a, b) một phần tử xác định của tập hợp X. Nói một cách khác, cho một phép toán đại số là cho một ánh xạ từ $X \times X$ đến X.

Định nghĩa 1. Ta gọi là *phép toán hai ngôi* (hay còn gọi tắt là phép toán) trong một tập hợp X một ánh xạ f từ $X \times X$ đến X. Giá trị $f(x, y)$ của f tại (x, y) gọi là *cái hợp thành của* x *và* y.

Cái hợp thành của x và y thường được kí hiệu bằng cách viết x và y theo một thứ tự nhất định với một dấu đặc trưng cho phép toán đặt giữa x, y. Trong các dấu mà người ta hay dùng tới nhiều nhất, là các dấu + và . ; đối với dấu . người ta thường quy ước bỏ đi ; với các dấu đó, cái hợp thành của x và y được viết $x + y$, $x . y$ hay xy. Một phép toán hai ngôi kí hiệu bằng dấu + gọi là *phép cộng*, cái hợp thành $x + y$ lúc đó gọi là *tổng* của x và y ; một phép toán hai ngôi kí hiệu bằng dấu . gọi là *phép nhân*, cái hợp thành $x . y$ hay xy lúc đó gọi là *tích* của x và y. Người ta còn dùng các kí hiệu $x \circ y$, $x * y$, $x \top y$, $x \perp y$... để chỉ cái hợp thành của x và y.

Ví dụ : 1) Trong tập hợp **N** các số tự nhiên, phép cộng, phép nhân là những phép toán hai ngôi ; cái hợp thành của $x \in \mathbf{N}$ và $y \in \mathbf{N}$ bởi các phép toán đó kí hiệu theo thứ tự bằng $x + y$, xy. Phép hợp thành x^y, là một phép toán 2 ngôi trong tập $\mathbf{N}^* = \mathbf{N}-\{0\}$.

2) Phép trừ không phải là một phép toán hai ngôi trong **N**, nhưng là một phép toán hai ngôi trong tập hợp **Z** các số nguyên.

3) Tích ánh xạ là một phép toán hai ngôi trong tập hợp các ánh xạ từ một tập hợp X đến chính nó.

4) Tích ngoại các vectơ $\alpha \wedge \beta$ của Hình học giải tích là một phép toán hai ngôi trong tập hợp các vectơ có cùng một điểm gốc O của không gian 3 chiều thông thường.

5) Tích ma trận là một phép toán hai ngôi trong tập hợp các ma trận vuông cấp n.

Sau đây, trong các lí luận tổng quát, ta sẽ viết cái hợp thành của x và y là xy, nếu không có lí do nào khiến ta phải viết khác.

Định nghĩa 2. Một bộ phận A của X gọi là *ổn định* (đối với phép toán hai ngôi trong X) nếu và chỉ nếu $xy \in A$ với mọi $x, y \in A$.

Phép toán hai ngôi $*$ xác định trong bộ phận ổn định A bởi quan hệ $x * y = xy$ với mọi $x, y \in A$ gọi là cái *thu hẹp* vào A của phép toán hai ngôi trong X. Người ta còn nói rằng $*$ là *phép toán cảm sinh* trên A bởi phép toán . của X. Người ta thường kí hiệu phép toán cảm sinh như phép toán của X.

Định nghĩa 3. Một phép toán hai ngôi trong một tập hợp X gọi là *kết hợp* nếu và chỉ nếu ta có

$$(x\ y)\ z = x\ (y\ z)$$

với mọi $x, y, z \in X$; là *giao hoán* nếu và chỉ nếu ta có

$$xy = yx$$

với mọi $x, y \in X$.

Phép cộng và phép nhân trong tập hợp các số tự nhiên **N** là kết hợp, giao hoán ; nhưng phép mũ hóa không kết hợp :

$(2^1)^2 \neq 2^{(1^2)}$, cũng không giao hoán : $2^1 \neq 1^2$. Tích ánh xạ trong ví dụ 3) là kết hợp, không giao hoán (nếu X có nhiều hơn một phần tử).

Định nghĩa 4. Giả sử đã cho một phép toán hai ngôi trong một tập hợp X. Một phần tử e của X gọi là một *đơn vị trái* của phép toán hai ngôi nếu và chỉ nếu

$$ex = x$$

với mọi $x \in X$. Tương tự, một phần tử e của X gọi là một *đơn vị phải* của phép toán hai ngôi nếu và chỉ nếu

$$xe = x$$

với mọi $x \in X$. Trong trường hợp một phần tử e của X vừa là một đơn vị trái vừa là một đơn vị phải, thì e gọi là một *đơn vị*, hoặc một phần tử *trung lập* của phép toán hai ngôi.

Trong ví dụ 1) số 0 là phần tử trung lập của phép cộng, số 1 là phần tử trung lập của phép nhân và là đơn vị phải của phép mũ hóa. Trong ví dụ 3), ánh xạ đồng nhất là phần tử trung lập. Tích ngoại các vectơ trong ví dụ 4) không có đơn vị trái cũng không có đơn vị phải.

Định lí 1. *Nếu một phép toán hai ngôi trong một tập hợp X có một đơn vị trái e' và một đơn vị phải e'', thì $e' = e''$.*

Chứng minh. Xét tích $e'e''$ trong X. Vì e' là đơn vị trái nên $e'e'' = e''$. Mặt khác, vì e'' là đơn vị phải nên $e'e'' = e'$. Ta suy ra $e' = e''$.

Một hệ quả tức khắc là

Hệ quả. *Một phép toán hai ngôi có nhiều nhất một phần tử trung lập.*

2. Nửa nhóm

Định nghĩa 5. Ta gọi là *nửa nhóm* một tập hợp X cùng với một phép toán hai ngôi kết hợp đã cho trong X. Một nửa nhóm có phần tử trung lập gọi là một *vị nhóm*. Một nửa nhóm là *giao hoán* nếu phép toán của nó là giao hoán.

Các ví dụ 1) (trừ phép mũ hóa), 3), 5) trong 1 là những ví dụ về nửa nhóm, và hơn nữa vị nhóm. Mọi bộ phận ổn định

A của một nửa nhóm X cùng với phép toán cảm sinh trên A là một nửa nhóm gọi là *nửa nhóm con* của nửa nhóm X.

Trong một nửa nhóm X, người ta kí hiệu giá trị chung của hai vế của đẳng thức

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

bằng kí hiệu duy nhất xyz, gọi là tích của ba phần tử x, y, z lấy theo thứ tự đó. Cũng như vậy, ta đặt

$$xyzt = (xyz)t$$

và gọi là tích của bốn phần tử x, y, z, t lấy theo thứ tự đó. Một cách tổng quát

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

và gọi là tích của n phần tử $x_1, \dots, x_n$.

Tính chất chính của các phép toán hai ngôi kết hợp là định lí sau đây :

Định lí 2 (định lí kết hợp). *Giả sử $x_1, x_2, \dots, x_n$ là n ($n \geqslant 3$) phần tử (phân biệt hay không) của một nửa nhóm X, thế thì*

$$x_1x_2 \dots x_n = (x_1 \dots x_i)(x_{i+1} \dots x_j) \dots (x_{m+1} \dots x_n) .$$

Chứng minh. Vì X là một nửa nhóm nên mệnh đề là đúng với $n = 3$. Ta giả sử mệnh đề là đúng cho k nhân tử, với mọi $3 \leqslant k < n$. Ta có, theo định nghĩa tích của nhiều phần tử và theo giả thiết quy nạp

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

$$= [(x_1 \dots x_i) \dots (x_{e+1} \dots x_m)] (x_{m+1} \dots x_n) =$$

$$= (x_1 \dots x_m)(x_{m+1} \dots x_n) = (x_1 \dots x_m)[(x_{m+1} \dots x_{n-1})x_n] =$$

$$[(x_1 \dots x_m)(x_{m+1} \dots x_{n-1})]x_n = (x_1 \dots x_{n-1})x_n = x_1x_2 \dots x_n.$$

Định nghĩa 6. Trong một nửa nhóm X, *lũy thừa n* (n là một tự nhiên khác 0) của một phần tử $a \in X$ là tích của n phần tử đều bằng a, kí hiệu a^n. Ta có các quy tắc (do định lí 2)

$$a^m . a^n = a^{m+n}, \quad (a^m)^n = a^{mn} .$$

Trong trường hợp phép toán hai ngôi của X kí hiệu bằng dấu cộng +, thì tổng của n phần tử đều bằng a gọi là bội n của a, kí hiệu na. Quy tắc trên lúc đó viết

$$ma + na = (m + n)a, \quad n(ma) = mna .$$

Trong một nửa nhóm giao hoán, tích của ba phần tử không phụ thuộc vào thứ tự các nhân tử, cụ thể

$$x_1x_2x_3 = x_1x_3x_2 = x_2x_1x_3 = x_2x_3x_1 = x_3x_1x_2 = x_3x_2x_1.$$

Tổng quát hơn ta có định lí

Định lí 3. *Trong một nửa nhóm giao hoán X, tích*

$$x_1x_2 \dots x_n$$

không phụ thuộc vào thứ tự các nhân tử.

Chứng minh. Vì X là giao hoán nên mệnh đề là đúng với $n = 2$. Ta giả sử mệnh đề là đúng cho k nhân tử, với mọi $k < n$. Ta hãy chứng minh

$$x_1x_2 \dots x_n = x_{i_1}x_{i_2} \dots x_{i_n}$$

trong đó $(i_1, i_2, \dots, i_n)$ là một hoán vị của $\{1, 2, \dots, n\}$. Nếu $x_n = x_{i_k}$, ta có thể viết vế hai của đẳng thức trên như sau theo Định lí 2 và tính giao hoán của X :

$$x_{i_1} \dots x_{i_{k-1}} x_{i_k} x_{i_{k+1}} \dots x_{i_n} =$$

$$= (x_{i_1} \dots x_{i_{k-1}})(x_{i_k}(x_{i_{k+1}} \dots x_{i_n})) =$$

$$= (x_{i_1} \dots x_{i_{k-1}})((x_{i_{k+1}} \dots x_{i_n})x_{i_k})$$

$$= ((x_{i_1} \dots x_{i_{k-1}})(x_{i_{k+1}} \dots x_{i_n}))x_{i_k}$$

$$= (x_{i_1} \dots x_{i_{k-1}}x_{i_{k+1}} \dots x_{i_n})x_{i_k} \text{ theo Định lí 2}$$

$$= (x_1x_2 \dots x_{n-1})x_n \text{ theo giả thiết quy nạp}$$

hay

$$= x_1x_2 \dots x_n. \blacksquare$$

Ví dụ. 1) Tập hợp các số tự nhiên **N** với một trong các phép toán hai ngôi sau đây

phép cộng,

phép nhân,

phép lấy ƯCLN (ước chung lớn nhất),

phép lấy BCNN (bội chung nhỏ nhất),

là một nửa nhóm giao hoán. Đối với phép cộng, **N** còn là một vị nhóm gọi là vị nhóm cộng các số tự nhiên. (Điều đó có đúng với các phép toán còn lại không ?)

2) Tập hợp $\mathcal{P}(X)$ các bộ phận của một tập hợp X là một vị nhóm giao hoán đối với mỗi phép toán hai ngôi giao và hợp.

BÀI TẬP

1. Giả sử a và b là hai phần tử của một nửa nhóm X sao cho $ab = ba$. Chứng minh $(ab)^n = a^n b^n$ với mọi số tự nhiên $n > 1$. Nếu a và b là hai phần tử sao cho $(ab)^2 = a^2b^2$ thì ta có suy ra được $ab = ba$ không ?

2. Gọi X là tập hợp thương của **Z** trên quan hệ đồng dư mod n (ch I, §2, 2, ví dụ).

a) Với mỗi cặp $(C(a), C(b))$ ta cho tương ứng lớp tương đương $C(a + b)$. Chứng minh như vậy ta có một ánh xạ từ $X \times X$ đến X.

b) Chứng minh X là một vị nhóm giao hoán đối với phép toán hai ngôi xác định ở a).

c) Nếu với mỗi cặp $(C(a), C(b))$ ta cho tương ứng lớp $C(ab)$, chứng minh lúc đó X cũng là một vị nhóm giao hoán.

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

$$X \times X \to X$$
$$(x, y) \mapsto x.$$

Chứng minh X là một nửa nhóm đối với phép toán hai ngôi trên. Nửa nhóm đó có giao hoán không ? có phần tử đơn vị không ?

4. Gọi X là tập hợp thương của $\mathbf{Z} \times \mathbf{N}^*$ trên quan hệ tương đương S xác định bởi

$(a, b)\ S\ (c, d)$ khi và chỉ khi $ad = bc$ (ch I, §2, bài tập 2). Ta kí hiệu các phần tử $C(a, b)$ của X bằng $\frac{a}{b}$. $(a, b) \in \mathbf{Z} \times \mathbf{N}^*$.

a) Với mỗi cặp $(\frac{a}{b}, \frac{c}{d})$ ta cho tương ứng lớp tương đương $\frac{ad + bc}{bd}$. Chứng minh như vậy ta có một ánh xạ từ $X \times X$ đến X.

b) Chứng minh X là một vị nhóm giao hoán đối với phép toán hai ngôi ở a).

c) Nếu với mỗi cặp $(\frac{a}{b}, \frac{c}{d})$ ta cho tương ứng lớp tương đương $\frac{ac}{bd}$. Chứng minh lúc đó X cũng là một vị nhóm giao hoán.

5. Xét tích đề các $\mathbf{N}^n$ $(n \geq 1)$ với $\mathbf{N}$ là vị nhóm cộng giao hoán các số tự nhiên.

a) Chứng minh $\mathbf{N}^n$ cùng với phép toán
$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$ là một vị nhóm giao hoán.

b) Trong $\mathbf{N}^n$ ta đã xác định một quan hệ thứ tự (ch I, § 2, bài tập 10). Chứng minh nếu $\alpha, \beta \in \mathbf{N}^n$ sao cho $\alpha < \beta$ thì $\alpha + \gamma < \beta + \gamma$ với mọi $\gamma \in \mathbf{N}^n$.

§2. NHÓM

1. Nhóm

Định nghĩa 1. Ta gọi là nhóm một nửa nhóm X có các tính chất sau : 1° có phần tử trung lập e ; 2° với mọi $x \in X$ có một $x' \in X$ sao cho $x'x = xx' = e$ (phần tử x' gọi là một phần tử đối xứng hay nghịch đảo của x). Như vậy, một nhóm là một vị nhóm mà mỗi phần tử đều có nghịch đảo.

Nếu tập hợp X là hữu hạn thì ta bảo ta có một *nhóm hữu hạn* và số phần tử của X gọi là *cấp* của nhóm. Nếu phép toán hai ngôi trong X là giao hoán thì ta bảo ta có một *nhóm giao hoán* hay *nhóm aben*.

Ví dụ. 1) Tập hợp các số nguyên **Z** cùng với phép cộng thông thường là một nhóm giao hoán mà ta gọi là nhóm cộng các số nguyên. Cũng vậy, ta có nhóm cộng các số hữu tỉ, nhóm cộng các số thực, nhóm cộng các số phức.

2) Tập hợp các số hữu tỉ khác 0 cùng với phép nhân thông thường là một nhóm giao hoán mà ta gọi là nhóm nhân các số hữu tỉ khác 0. Cũng vậy, ta có nhóm nhân các số thực khác 0, nhóm nhân các số phức khác 0.

3) Tập hợp S_n các phép thế của {1, 2, ..., n} cùng với tích các phép thế là một nhóm hữu hạn, không giao hoán với mọi $n \geqslant 3$.

4) Nửa nhóm cộng các số tự nhiên **N** không phải là một nhóm (tại sao ?).

Ngoài các tính chất của một vị nhóm, một nhóm còn có một số tính chất cơ bản sau đây.

Định lí 1. *Mỗi phần tử của một nhóm chỉ có một phần tử đối xứng.*

Chứng minh. Giả sử x', x'' là hai phần tử đối xứng của x. Ta có

$$xx'' = e$$

Nhân hai vế về bên trái với x', ta được

$$x'(xx'') = x'e, \text{ vậy } (x'x)x'' = x'e.$$

hay

$$ex'' = x'e$$

tức là $$x'' = x'. \blacksquare$$

Trong trường hợp phép toán hai ngôi của nhóm kí hiệu bằng dấu . (dấu cộng +), thì phần tử đối xứng duy nhất của x kí hiệu là x^{-1} ($-x$) và còn gọi là *nghịch đảo* của x (*đối* của x). Từ định nghĩa của phần tử nghịch đảo (phần tử đối) ta có nghịch

$(x^{-1})^{-1} = x$, $(-(-x) = x)$. Nếu nhóm là aben và phép toán của nhóm kí hiệu bằng dấu . (dấu +) thì phần tử $xy^{-1} = y^{-1}x$ $(x + (-y) = (-y) + x)$ kí hiệu là x/y $(x - y)$ và gọi là *thương của x trên y* (*hiệu của x và y*).

Định lí 2 (luật giản ước). *Trong một nhóm, đẳng thức* $xy = xz$ $(yx = zx)$ *kéo theo đẳng thức* $y = z$.

Như vậy, ta bảo trong một nhóm luật giản ước thực hiện được với mọi phần tử.

Chứng minh. Nhân bên trái hai vế của đẳng thức $xy = xz$ với x^{-1}, ta có

$$x^{-1}(xy) = x^{-1}(xz)$$

hay $$(x^{-1}x)y = (x^{-1}x)z$$

hay $$ey = ez$$

tức là $$y = z.$$ ■

Định lí 3. *Trong một nhóm, phương trình* $ax = b$ $(xa = b)$ *có nghiệm duy nhất* $x = a^{-1}b$ $(x = ba^{-1})$.

Chứng minh. Ta thấy ngay giá trị $x = a^{-1}b$ là nghiệm của phương trình vì $a(a^{-1}b) = (aa^{-1})b = eb = b$. Đó là nghiệm duy nhất, vì nếu c là một nghiệm của phương trình nghĩa là $ac = ax = b$, ta suy ra $c = x$ theo luật giản ước. Chứng minh tương tự cho phương trình $xa = b$. ■

Định lí 4. *Trong một nhóm ta có*

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

với x, y là hai phần tử bất kì của nhóm.

Chứng minh. Ta có

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

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

tức là

$$(xy)^{-1} = y^{-1}x^{-1}.$$ ■

Định lí này mở rộng tức khắc cho tích một số n tùy ý nhân tử $(x_1x_2 \ldots x_n)^{-1} = x_n^{-1} \ldots x_2^{-1} x_1^{-1}$. Đặc biệt

$$(a^n)^{-1} = (a^{-1})^n$$

với mọi số tự nhiên khác 0 ; người ta quy ước viết phần tử đó dưới dạng a^{-n}, và mặt khác đặt $a^0 = e$, như vậy ta đã hoàn thành việc xác định a^λ cho mọi số nguyên λ. Ta vẫn có (độc giả hãy chứng minh điều đó)

$$a^\lambda a^\mu = a^{\lambda+\mu}, \ (a^\lambda)^\mu = a^{\lambda\mu}$$

với mọi $\lambda, \mu \in \mathbf{Z}$. Chú ý : kí hiệu a^λ dùng cho phép nhân, trong trường hợp phép cộng ta viết λa.

Dưới đây ta hãy đưa ra một số định nghĩa tương đương của nhóm.

Định lí 5. *Một nửa nhóm* X *là một nhóm nếu và chỉ nếu hai điều kiện sau được thỏa mãn :*

1°. *X có một đơn vị trái e.*

2°. *Với mọi* $x \in X$, *có một* $x' \in X$ *sao cho* $x'x = e$.

Chứng minh. Hiển nhiên hai điều kiện trên là cần, ta hãy chứng minh chúng là đủ. Giả sử có các điều kiện 1° và 2°. Lấy một phần tử tùy ý $x \in X$. Theo 2° có một $x' \in X$ sao cho $x'x = e$. Vẫn theo 2° có một $x'' \in X$ sao cho $x''x' = e$. Ta có

$$xx' = exx' = x''x'xx' = x''ex' = x''x' = e.$$

Mặt khác, ta lại có

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

Kết luận e là đơn vị của X và x' là nghịch đảo của x. Vậy X là một nhóm. ■

Ta cũng được một định lí tương tự nếu ta thay thế đơn vị trái bằng đơn vị phải và phần tử x' trong điều kiện 2° đáng lẽ ở bên trái của x thì viết ở bên phải của x.

Định lí 6. *Một nửa nhóm khác rỗng X là một nhóm nếu và chỉ nếu các phương trình $ax = b$ và $ya = b$ có nghiệm trong X với mọi $a, b \in X$.*

Chứng minh. Định lí 3 cho ta biết điều kiện là cần, ta hãy chứng minh nó là đủ. Vì X là khác rỗng nên có một phần tử $a \in X$. Giả sử e là một nghiệm của phương trình $ya = a$. Ta hãy chứng minh e là đơn vị trái của X. Giả sử b là một phần tử tùy ý của X. Gọi c là một nghiệm của phương trình $ax = b$. Ta có

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

Vậy e là một đơn vị trái của X. Bây giờ ta hãy chứng minh với mọi $b \in X$, có $b' \in X$ sao cho $b'b = e$. Muốn vậy ta xét phương trình $yb = e$. Sự tồn tại nghiệm của phương trình này cho ta b'. Như vậy các điều kiện 1° và 2° của định lí 5 được thỏa mãn, ta có X là một nhóm. ■

2. Nhóm con

Giả sử A là một bộ phận của một nhóm X, ta có thể có $xy \in A$ với mọi $x, y \in A$, tức là A là một bộ phận ổn định của X (§1, 1, định nghĩa 2). Như vậy phép toán hai ngôi trong X cảm sinh một phép toán hai ngôi trong A. Nếu A cùng với phép toán cảm sinh là một nhóm, thì ta bảo A là một *nhóm con* của nhóm X. Chẳng hạn ta có bộ phận các số nguyên $\mathbf{Z}$ là một nhóm con của nhóm cộng các số hữu tỉ $\mathbf{Q}$. Ta chú ý bộ phận $\{-1, 1\}$ tuy lập thành một nhóm đối với phép nhân, nhưng không phải là một nhóm con của nhóm cộng các số nguyên $\mathbf{Z}$.

Định nghĩa 2. Một bộ phận ổn định A của một nhóm X là một *nhóm con* của X nếu A cùng với phép toán cảm sinh là một nhóm.

Định lí 7. *Một bộ phận A của một nhóm X là một nhóm con của X nếu và chỉ nếu các điều kiện sau đây thỏa mãn :*

1) Với mọi $x, y \in A$, $xy \in A$.

2) $e \in A$, với e là phần tử trung lập của X.

3) Với mọi $x \in A$, $x^{-1} \in A$.

Chứng minh. Ắt có. Giả sử A là một nhóm con của X. Theo định nghĩa nhóm con, ta có ngay 1^o. Gọi e' là phần tử trung lập của nhóm A. Ta có

$$e'a = a \text{ với mọi } a \in A$$

Mặt khác ta cũng có

$$ea = a$$

vì e là phần tử trung lập của X.

Do đó

$$e'a = ea$$

hay

$$e' = e$$

vì luật giản ước thực hiện được với mọi phần tử của nhóm X. Vậy ta có 2^o. Cuối cùng gọi x' là nghịch đảo trong nhóm A của một phần tử $x \in A$. Vậy ta có

$$x'x = e = x^{-1}x.$$

Thực hiện luật giản ước, ta được $x' = x^{-1}$. Điều này chứng minh 3^o.

Đủ. Giả sử A là một bộ phận của X thỏa mãn các điều kiện đã cho. Với 1^o, A là một nửa nhóm, vì phép toán hai ngôi đã cho trong X là kết hợp. 2^o và 3^o nói lên nửa nhóm A có phần tử trung lập và mọi phần tử của A có nghịch đảo trong A. Vậy A là một nhóm, do đó A là một nhóm con của X. ■

Hệ quả. *Giả sử A là một bộ phận khác rỗng của một nhóm X. Các điều kiện sau đây là tương đương :*

a) A là một nhóm con của X.

b) Với mọi $x, y \in A$, $xy \in A$ và $x^{-1} \in A$.

c) Với mọi $x, y \in A$, $xy^{-1} \in A$.

Chứng minh. Theo định lí 7 ta có ngay a) kéo theo b). Hiển nhiên b) kéo theo c). Ta chứng minh c) kéo theo a). Vì $A \neq \emptyset$ nên có một $x \in A$. Theo c) ta có $e = xx^{-1} \in A$. Vậy điều kiện 2^o của định lí 7 thỏa mãn. Giả sử $x \in A$. Vẫn theo c) ta có

$x^{-1} = ex^{-1} \in A$. Ta được điều kiện 3° của định lí 7. Cuối cùng, giả sử $x, y \in A$. Vì $y^{-1} \in A$, nên c) cho $x(y^{-1})^{-1} = xy \in A$. Như vậy điều kiện 1° của định lí 7 thỏa mãn. Do đó A là một nhóm con của X. ■

Ví dụ. 1) Bộ phận $m\mathbb{Z}$ gồm các số nguyên là bội của một số nguyên m cho trước là một nhóm con của nhóm cộng các số nguyên $\mathbb{Z}$. Thật vậy, áp dụng điều kiện c) của hệ quả trên, ta có $m\mathbb{Z}$ là nhóm con vì $mx - my = m(x - y) \in m\mathbb{Z}$, tức là hiệu của hai phần tử thuộc $m\mathbb{Z}$ lại thuộc $m\mathbb{Z}$.

2) Trong một nhóm X, bộ phận A gồm các lũy thừa a^λ của một phần tử $a \in X$ là một nhóm con của X. Thật vậy, $a^\lambda (a^\mu)^{-1} = a^\lambda a^{-\mu} = a^{\lambda - \mu} \in A$. Đặc biệt các bội của một số nguyên là một nhóm con của nhóm cộng các số nguyên $\mathbb{Z}$. Như vậy, ví dụ 1) chỉ là một trường hợp đặc biệt của ví dụ 2).

3) Bộ phận $\{ e \}$ chỉ gồm có phần tử trung lập và bộ phận X là hai nhóm con của một nhóm X. Người ta gọi chúng là *các nhóm con tầm thường* của X.

Định lí 8. *Giao của một họ bất kì những nhóm con của một nhóm X là một nhóm con của X.*

Chứng minh. Xét một họ bất kì $(A_\alpha)_{\alpha \in I}$ những nhóm con của X và gọi A là giao của chúng. Trước hết ta có $A \neq \emptyset$, vì phần tử trung lập e của X thuộc A_α với mọi $\alpha \in I$, do đó $e \in A$. Bây giờ ta lấy hai phần tử bất kì $x, y \in A$. Vì $x, y \in A$, nên $x, y \in A_\alpha$ với mọi $\alpha \in I$. Vì các A_α là những nhóm con nên $xy^{-1} \in A_\alpha$ với mọi $\alpha \in I$, do đó $xy^{-1} \in A$. Hệ quả của định lí 7 cho ta biết A là nhóm con của X. ■

Giả sử U là một bộ phận của một nhóm X. Thế thì U chứa trong ít nhất một nhóm con của X, cụ thể X. Theo định lí 8, giao A của tất cả các nhóm con của X chứa U là một nhóm con của X chứa U. Đó là nhóm con bé nhất của X chứa U (quan hệ thứ tự là quan hệ bao hàm).

Định nghĩa 3. Giả sử U là một bộ phận của một nhóm X. Nhóm con A bé nhất của X chứa U gọi là *nhóm con sinh ra*

bởi U. Trong trường hợp $A = X$, ta nói rằng U là một *hệ sinh* của X và X *được sinh ra bởi* U.

Nếu $U = \{ a \}$, $a \in X$, thì dễ dàng thấy rằng nhóm con A sinh ra bởi U có các phần tử là các lũy thừa a^λ, $\lambda \in \mathbf{Z}$. Thật vậy, theo ví dụ 2) bộ phận gồm các lũy thừa a^λ là một nhóm con của X. Hơn nữa, đó là nhóm con bé nhất của X chứa $\{a\}$ vì mọi nhóm con của X chứa $\{ a \}$ thì đều chứa các lũy thừa của a. Người ta gọi A là nhóm con sinh ra bởi a.

Định nghĩa 4. Một nhóm X gọi là *xyclic* nếu và chỉ nếu X được sinh ra bởi một phần tử $a \in X$. Phần tử a gọi là một *phần tử sinh* của X.

Như vậy một nhóm X là xyclic nếu và chỉ nếu các phần tử của nó là các lũy thừa a^λ , $\lambda \in \mathbf{Z}$, của một phần tử $a \in X$.

Ví dụ. 1) Xét nhóm các phép thế S_3 mà các phần tử là

$$e = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}, f_1 = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, f_2 = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}, f_3 = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$$

$$f_4 = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}, f_5 = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}.$$

Ta hãy nghiên cứu các phần tử của nhóm con sinh ra bởi f_1. Ta có

$$f_1^2 = f_2, f_1^3 = e$$

Ta hãy chứng minh rằng các lũy thừa f_1^λ khi λ chạy khắp $\mathbf{Z}$ chỉ cho ta ba phần tử phân biệt là e, f_1, f_2. Thật vậy ta hãy lấy một lũy thừa tùy ý f_1^λ . Chia λ cho 3 ta được

$$\lambda = 3q + r, \ 0 \leqslant r < 3$$

r là dư của phép chia λ cho 3. Ta xét

$$f_1^\lambda = f_1^{3q+r} = f_1^{3q} \cdot f_1^r = (f_1^3)^q f_1^r .$$

Nhưng $f_1^3 = e$, nên

$$f_1^\lambda = (f_1^3)^q f_1^r = e^q f_1^r = e f_1^r = f_1^r .$$

Vì r lấy một trong ba giá trị 0, 1, 2, nên f_1^i là một trong ba phần tử $f_1^0 = e$, $f_1^1 = f_1$, $f_1^2 = f_2$. Như vậy nhóm con A_3 sinh ra bởi f_1 gồm ba phần tử, đó là e, f_1 và f_2. Nghiên cứu f_2, ta có

$$f_2^2 = f_1, f_2^3 = e.$$

Bằng lí luận tương tự, ta cũng có nhóm con sinh ra bởi f_2 gồm ba phần tử e, f_1, f_2. Vậy nhóm con sinh ra bởi f_2 trùng với nhóm con sinh ra bởi f_1.

Còn f_3, f_4, f_5 là những chuyển trí nên ta có ngay

$$f_3^2 = f_4^2 = f_5^2 = e.$$

Cũng lí luận như trên ta được $\{e, f_3\}$ là nhóm con sinh ra bởi f_3, $\{e, f_4\}$ là nhóm con sinh ra bởi f_4, $\{e, f_5\}$ là nhóm con sinh ra bởi f_5.

Cuối cùng, vì $e^k = e$ với mọi $k \in \mathbf{Z}$ nên nhóm con sinh ra bởi e là nhóm con tầm thường $\{e\}$.

Nhóm S_3 không được sinh ra bởi một phần tử nào của nó cả, vậy S_3 không phải là xyclic. Còn các nhóm con kể trên của S_3 đều là xyclic.

2) Nhóm cộng các số nguyên $\mathbf{Z}$ là xyclic vì các phần tử của nó là các bội của 1, vậy 1 là một phần tử sinh của $\mathbf{Z}$. Ta cũng có thể coi các phần tử của $\mathbf{Z}$ là các bội của -1, cho nên -1 cũng là một phần tử sinh của $\mathbf{Z}$.

Ngoài 1 và -1 ra, $\mathbf{Z}$ không còn phần tử sinh nào khác. $\mathbf{Z}$ là một nhóm xyclic vô hạn, còn các nhóm xyclic trong ví dụ 1) là hữu hạn.

Giả sử X là một nhóm, e là phần tử trung lập của X và a là một phần tử của X. Nếu không có một số nguyên dương n nào sao cho $a^n = e$ thì nhóm con sinh ra bởi a là vô hạn, vì $a^k \neq a^h$ với $k \neq h$. Trong trường hợp trái lại, gọi m là số nguyên dương bé nhất sao cho $a^m = e$, thế thì nhóm con sinh ra bởi a có m phần tử : $a^0 = e$, $a^1 = a$, $a^2, \ldots, a^{m-1}$ (chứng minh tương tự như trong ví dụ 1)).

Định nghĩa 5. Giả sử a là một phần tử bất kì của một nhóm X và A là nhóm con sinh ra bởi a. Phần tử a gọi là có *cấp vô hạn* nếu A vô hạn ; trong trường hợp này không có một số nguyên dương n nào sao cho $a^n = e$. Phần tử a gọi là có *cấp* m nếu A có cấp m ; trong trường hợp này m là số nguyên dương bé nhất sao cho $a^m = e$.

Một phần tử $a \in X$ có cấp 1 khi và chỉ khi $a = e$.

3. Nhóm con chuẩn tắc và nhóm thương

Giả sử A là một nhóm con của một nhóm X, ta hãy định nghĩa quan hệ $\sim$ trong tập hợp X như sau : với mọi $x, y \in A$, $x \sim y$ nếu và chỉ nếu $x^{-1}y \in A$.

Bổ đề 1. *Quan hệ $\sim$ trong X là một quan hệ tương đương.*

Chứng minh. $\sim$ là phản xạ vì $x^{-1}x = e \in A$. $\sim$ là đối xứng vì nếu $x^{-1}y \in A$ thì $y^{-1}x = (x^{-1}y)^{-1} \in A$. Cuối cùng $\sim$ là bắc cầu vì nếu $x^{-1}y$ và $y^{-1}z \in A$ thì $x^{-1}z = (x^{-1}y)(y^{-1}z) \in A$. ■

Với mỗi phần tử $x \in X$, ta kí hiệu lớp tương đương chứa x là $\bar{x}$ và kí hiệu bộ phận của X gồm các phần tử có dạng xa với a chạy khắp A là xA, tức là $xA = \{ xa \mid a \in A \}$.

Bổ đề 2. $\bar{x} = xA$.

Chứng minh. Trước hết ta hãy chứng minh $\bar{x} \subset xA$. Giả sử $y \in \bar{x}$. Vậy $x \sim y$, tức là $x^{-1}y$ là một phần tử a nào đó của A, do đó $y = xa \in xA$. Bây giờ ta chứng minh bao hàm ngược lại : $xA \subset \bar{x}$. Muốn vậy ta lấy một phần tử y tùy ý của xA. y có dạng xa với a là một phần tử nào đó của A. Từ $y = xa$, ta suy ra $x^{-1}y \in A$, vậy $x \sim y$, tức là $y \in \bar{x}$. ■

Định nghĩa 6. Các bộ phận xA gọi là *các lớp trái* của nhóm con A trong X. Tương tự, *các lớp phải* Ax của A trong X là các bộ phận mà các phần tử có dạng là ax với $a \in A$.

Cũng như đối với các lớp trái, ta có thể chứng minh các lớp phải của A là các lớp tương đương theo quan hệ tương đương : $x \sim y$ nếu và chỉ nếu $xy^{-1} \in A$.

Từ các bổ đề 1 và 2 ta suy ra

Hệ quả. *Giả sử x và y là hai phần tử tùy ý của nhóm X, thế thì :*

(i) $xA = yA$ nếu và chỉ nếu $x^{-1}y \in A$.

(ii) $xA \cap yA = \emptyset$ nếu và chỉ nếu $x^{-1}y \notin A$.

Tập hợp thương của X trên quan hệ tương đương $\sim$ gọi là tập hợp thương của nhóm X trên nhóm con A, kí hiệu là X/A. Các phần tử của X/A là các lớp trái xA.

Bây giờ ta hãy áp dụng các kết quả trên để nghiên cứu quan hệ giữa cấp của một nhóm hữu hạn và cấp của một nhóm con của nó. Ta có :

Định lí 9 (Định lí Lagrăngiơ). *Cấp của một nhóm X hữu hạn là bội của cấp của mọi nhóm con của nó.*

Chứng minh. Giả sử X có cấp là n và A, một nhóm con bất kì của nó, có cấp là m. Trước hết ta hãy chứng minh mọi lớp trái xA, $x \in X$, đều có số phần tử là m. Muốn vậy ta hãy xét

$$A = \{x_1, x_2, \ldots, x_m\}$$

và các phần tử

$$xx_1, xx_2, \ldots, xx_m .$$

Các phần tử này là phân biệt, vì nếu có $xx_1 = xx_2$ chẳng hạn, thì $x_1 = x_2$. Đó là tất cả các phần tử của lớp trái xA. Như vậy xA có m phần tử. Vì X là hữu hạn nên số các lớp trái xA là hữu hạn, gọi l là số các lớp trái xA. Do các lớp trái là rời nhau nên ta có $n = ml$.

Tương tự ta cũng có l là số các lớp phải Ax. ■

Số l các lớp trái xA (hay lớp phải Ax) gọi là *chỉ số của nhóm con A trong X*.

Vì mọi phần tử x của một nhóm X sinh ra một nhóm con có cấp bằng cấp của x, nên :

Hệ quả 1. *Cấp của một phần tử tùy ý của một nhóm hữu hạn X là ước của cấp của X.*

Vì mọi phần tử $x \neq e$ của một nhóm X đều sinh ra một nhóm con có cấp không nhỏ hơn 2, nên :

Hệ quả 2. *Mọi nhóm hữu hạn có cấp nguyên tố đều là xyclic và được sinh ra bởi một phần tử bất kì, khác phần tử trung lập, của nhóm.*

Ví dụ. Ta hãy lấy nhóm các phép thế S_3 có cấp 6. Ví dụ ở mục 2 cho ta biết các phần tử của nó có cấp hoặc là 1, hoặc là 2, hoặc là 3, đó là những ước của 6. Bây giờ ta hãy lấy một nhóm con của S_3, chẳng hạn nhóm con $A = \{e, f_3\}$. Định lí Lagrăngiơ cho ta biết số các lớp trái của A là 3. Ta hãy thành lập các lớp trái đó. Ta có

$$eA = \{ee = e,\ ef_3 = f_3\}$$

$$f_1A = \{f_1e = f_1,\ f_1f_3 = f_4\}$$

$$f_2A = \{f_2e = f_2,\ f_2f_3 = f_5\}$$

$$f_3A = eA, \text{ vì } f_3 \in eA$$

$$f_4A = f_1A, \text{ vì } f_4 \in f_1A.$$

$$f_5A = f_2A, \text{ vì } f_5 \in f_2A.$$

Bây giờ ta hãy xét các lớp phải của A :

$$Ae = \{ee = e,\ f_3e = f_3\} = Af_3$$

$$Af_1 = \{ef_1 = f_1,\ f_3f_1 = f_5\} = Af_5$$

$$Af_2 = \{ef_2 = f_2,\ f_3f_2 = f_4\} = Af_4.$$

Chú ý ta có

$$f_1A \neq Af_1,\ f_2A \neq Af_2.$$

Trở về trường hợp tổng quát, giả sử X là một nhóm và A là một nhóm con của nó. Ta được tập hợp thương X/A mà các phần tử là các lớp trái xA, $x \in X$. Ta muốn trang bị cho X/A một phép toán để nó trở thành một nhóm. Nhưng ta lại muốn phép toán đó không phải là tùy ý mà suy ra từ phép toán của X, cụ thể ta muốn cho tương ứng với cặp (xA, yA) lớp trái xyA, thế thì tương ứng đó có phải là một ánh xạ từ $X/A \times X/A$ đến X/A không ? Để trả lời câu hỏi đó, ta xét ví dụ trên. Chẳng

hạn ta cho tương ứng với cặp (f_1A, f_1A) lớp f_1^2A. Vì $f_1^2 = f_2$, nên $f_1^2A = f_2A$. Mặt khác vì $f_1A = f_4A$, nên cũng với quy tắc tương ứng ấy, ta có lớp trái $eA = f_4^2A$ tương ứng với cặp $(f_4A, f_4A) = (f_1A, f_1A)$. Nhưng $f_2A \neq eA$, vậy quy tắc trên không cho ta một ánh xạ. Muốn quy tắc đó cho ta một ánh xạ, ta cần ấn định cho nhóm con A của X một điều kiện, mà ta gọi là điều kiện chuẩn tắc.

Định nghĩa 7. Một nhóm con A của một nhóm X gọi là *chuẩn tắc* nếu và chỉ nếu $x^{-1}ax \in A$ với mọi $a \in A$ và $x \in X$.

Định lí 10. *Nếu A là một nhóm con chuẩn tắc của một nhóm X, thì :*

(i) *Quy tắc cho tương ứng với cặp (xA, yA) lớp trái xyA là một ánh xạ từ $X/A \times X/A$ đến X/A*

(ii) *X/A cùng với phép toán hai ngôi*

$$(xA, yA) \longmapsto xyA$$

là một nhóm, gọi là nhóm thương của X trên A.

Chứng minh. (i) Để chứng minh quy tắc đó là một ánh xạ thì ta phải chứng minh rằng nếu $x_1A = xA$ và $y_1A = yA$ thì $x_1y_1A = xyA$, hay theo hệ quả của bổ đề 2, nếu $x^{-1}x_1 \in A$ và $y^{-1}y_1 \in A$ thì $(xy)^{-1}(x_1y_1) = y^{-1}x^{-1}x_1y_1 \in A$. Đặt $x^{-1}x_1 = a$, ta có $a \in A$ theo giả thiết. Xét tích $y^{-1}x^{-1}x_1y_1 = y^{-1}ay_1$. Ta có thể viết : $y^{-1}ay_1 = (y^{-1}ay)(y^{-1}y_1)$. Nhưng $y^{-1}ay \in A$ vì A là chuẩn tắc, và $y^{-1}y_1 \in A$ theo giả thiết, vậy $(y^{-1}ay)(y^{-1}y_1) \in A$, tức là $(xy)^{-1}(x_1y_1) \in A$. Ta kí hiệu cái hợp thành của xA và yA là $xA.yA$.

(ii) Để thử nghiệm tính chất kết hợp của phép toán hai ngôi trong X/A, ta hãy lấy ba phần tử tùy ý x, y, z của X. Thế thì

$$xA.yA.zA = xyzA = xA.yA.zA.$$

Do đó phép toán hai ngôi đã cho là kết hợp

Để thử nghiệm sự tồn tại của một đơn vị trái, ta hãy xét lớp trái $eA = A$, trong đó e là phần tử trung lập. Ta có

$$eA.xA = exA = xA$$

với mọi lớp trái $xA \in X/A$. Vậy $eA = A$ là một đơn vị trái.

Cuối cùng với mọi $xA \in X/A$, ta có

$$x^{-1}A\,.xA = x^{-1}xA = eA.$$

Theo định lí 5, X/A cùng với phép toán hai ngôi đã cho trong X/A là một nhóm, với eA là phần tử trung lập và $x^{-1}A$ là nghịch đảo của xA. ■

Định lí sau đây cho ta biết một định nghĩa tương đương của nhóm con chuẩn tắc.

Định lí 11. *Giả sử A là một nhóm con của một nhóm X. Các điều kiện sau đây là tương đương :*

a) *A là chuẩn tắc.*

b) *$xA = Ax$ với mọi $x \in X$.*

Chứng minh. Ta hãy chứng minh a) kéo theo b). Giả sử xa, $a \in A$, là một phần tử tùy ý của xA. Vì A là chuẩn tắc nên $y^{-1}ay \in A$ với mọi $y \in X$. Lấy $y = x^{-1}$, ta có $xax^{-1} \in A$. Đặt $xax^{-1} = a' \in A$, ta có $xa = a'x \in Ax$. Vậy $xA \subset Ax$. Đảo lại giả sử ax, $a \in A$, là một phần tử tùy ý của Ax. Vì A là chuẩn tắc nên $x^{-1}ax \in A$. Đặt $x^{-1}ax = a' \in A$, ta có $ax = xa' \in xA$. Vậy $Ax \subset xA$. Kết luận $xA = Ax$.

Bây giờ ta chứng minh b) kéo theo a). Giả sử a và x là hai phần tử tùy ý theo thứ tự của A và X. Ta có $ax \in Ax$. Theo giả thiết $Ax = xA$, nên $ax \in xA$, tức là $ax = xa'$ với a' là một phần tử nào đó của A. Ta suy ra $x^{-1}ax = a' \in A$. Theo định nghĩa 7, A là chuẩn tắc. ■

Do định lí trên, từ giờ nếu A là chuẩn tắc thì ta không phân biệt lớp trái, lớp phải của A và gọi một lớp trái (hay một lớp phải) của A là một *lớp* của A.

Ví dụ. 1) Trong một nhóm X, các nhóm con tầm thường $\{e\}$ và X là chuẩn tắc.

2) Trong một nhóm aben mọi nhóm con là chuẩn tắc.

3) Trong nhóm các phép thế S_3 ta hãy xét nhóm con A_3 gồm các phép thế chẵn (2, ví dụ 1) Ta có

$$eA_3 = A_3 = \{e, f_1, f_2\}$$

Vì $f_1, f_2 \in eA_3$, nên

$$eA_3 = f_1A_3 = f_2A_3 .$$

Vì các lớp trái của A_3 là các lớp tương đương, nên chúng thành lập một sự chia lớp của S_3, vậy ngoài lớp trái eA_3 ra ta chỉ còn một lớp trái gồm các phần tử còn lại f_3, f_4, f_5. Ta suy ra

$$f_3A_3 = f_4A_3 = f_5A_3 = \{f_3, f_4, f_5\}.$$

Cũng bằng lí luận tương tự, ta được

$$A_3 = A_3e = A_3f_1 = A_3f_2 = \{e, f_1, f_2\}$$

$$A_3f_3 = A_3f_4 = A_3f_5 = \{f_3, f_4, f_5\}$$

Do đó, A_3 là chuẩn tắc theo định lí 11.

4) Xét nhóm cộng các số nguyên $\mathbf{Z}$ và nhóm con $n\mathbf{Z}$ của $\mathbf{Z}$ gồm các số nguyên là bội của một số nguyên n đã cho. Vì nhóm cộng các số nguyên là aben, nên $n\mathbf{Z}$ là chuẩn tắc, và do đó các lớp trái, phải của $n\mathbf{Z}$ bằng nhau. Các lớp của $n\mathbf{Z}$ được kí hiệu là $x + n\mathbf{Z}$, $x \in \mathbf{Z}$, vì phép toán ở đây là phép cộng $+$. Quan hệ tương đương xác định bởi $n\mathbf{Z}$ là : $x \sim y$ nếu và chỉ nếu $x - y \in n\mathbf{Z}$, tức là hiệu $x - y$ là một bội của n. Quan hệ này chẳng qua là quan hệ đồng dư mod n. Vậy $\mathbf{Z}/n\mathbf{Z}$ gồm n lớp, đó là $0 + n\mathbf{Z}$, $1 + n\mathbf{Z}$, ..., $(n - 1) + n\mathbf{Z}$ (Chương I, §2, 2, Ví dụ) Tập hợp thương $\mathbf{Z}/n\mathbf{Z}$ cùng với phép toán

$$(x + n\mathbf{Z}) + (y + n\mathbf{Z}) = (x + y) + n\mathbf{Z}$$

gọi là nhóm cộng các số nguyên mod n. Kí hiệu $x + n\mathbf{Z}$ bằng $\bar{x}$ và lấy $n = 4$ ta có bảng cộng của $\mathbf{Z}/4\mathbf{Z}$ như sau

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	0	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

4. Đồng cấu

Định nghĩa 8. Một *đồng cấu* (nhóm) là một ánh xạ f từ một nhóm X đến một nhóm Y sao cho

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

với mọi $a, b \in X$. Nếu $X = Y$ thì đồng cấu f gọi là một *tự đồng cấu* của X.

Một đồng cấu mà là một đơn ánh thì gọi là một *đơn cấu*, một đồng cấu toàn ánh gọi là một *toàn cấu*, một đồng cấu song ánh gọi là một *đẳng cấu*, một tự đồng cấu song ánh gọi là một *tự đẳng cấu*. Nếu $f : X \to Y$ là một đẳng cấu từ nhóm X đến nhóm Y thì người ta viết $f : X \xrightarrow{\sim} Y$. (Trong trường hợp X và Y là những nửa nhóm, ta cũng định nghĩa đồng cấu (nửa nhóm) như trên và cũng có các khái niệm tương tự).

Ví dụ. 1) Giả sử A là một nhóm con của một nhóm X. Đơn ánh chính tắc

$$\begin{aligned} A &\to X \\ a &\mapsto a \end{aligned}$$

là một đồng cấu gọi là *đơn cấu chính tắc*.

2) Ánh xạ đồng nhất của một nhóm X là một đồng cấu gọi là *tự đẳng cấu đồng nhất* của X.

3) Xét ánh xạ từ nhóm nhân các số thực dương $\mathbf{R}^+$ đến nhóm cộng các số thực $\mathbf{R}$

$$\begin{aligned} \log : \mathbf{R}^+ &\to \mathbf{R} \\ x &\mapsto \log x \end{aligned}$$

trong đó log x là logarit cơ số 10 của x. Vì $\log(xy) = \log x + \log y$, nên log là một đồng cấu. Đồng cấu này còn là một song ánh nên là một đẳng cấu.

4) Giả sử A là một nhóm con chuẩn tắc của một nhóm X. Ánh xạ

$$h : X \to X/A$$
$$x \mapsto h(x) = xA$$

là một đồng cấu từ nhóm X đến nhóm thương X/A. Thật vậy, $h(xy) = xyA = xA.yA = h(x)\,h(y)$. Đồng cấu này còn là một toàn cấu, gọi là *toàn cấu chính tắc*.

5) Giả sử X và Y là hai nhóm tùy ý, ánh xạ

$$X \to Y$$
$$x \mapsto e,$$

với e là phần tử trung lập của Y, là một đồng cấu gọi là *đồng cấu tầm thường*.

6) Nếu $f : X \to Y$ là một đẳng cấu từ nhóm X đến nhóm Y thì ánh xạ ngược $f^{-1} : Y \to X$ cũng là một đẳng cấu. Thật vậy, ta có f^{-1} là một song ánh, ta chỉ còn chứng minh f^{-1} là một đồng cấu. Giả sử y, y' là hai phần tử tùy ý của Y. Đặt $x = f^{-1}(y)$, $x' = f^{-1}(y')$, ta có $f(x) = y$ và $f(x') = y'$. Vì f là một đồng cấu nên $f(xx') = f(x)\,f(x') = yy'$. Do đó $f^{-1}(yy') = xx' = f^{-1}(y)f^{-1}(y')$. Vậy f^{-1} là một đồng cấu. Ta bảo hai nhóm X và Y là đẳng cấu với nhau, và ta viết $X \simeq Y$, nếu có một đẳng cấu từ nhóm này đến nhóm kia.

Định nghĩa 9. Giả sử $f : X \to Y$ là một đồng cấu từ nhóm X đến nhóm Y. các phần tử trung lập của X và Y được kí hiệu theo thứ tự là e_X và e_Y. Ta kí hiệu

$$Imf = f(X)$$
$$Kerf = \{\, x \in X \mid f(x) = e_Y \,\} = f^{-1}(e_Y)$$

và gọi Imf là *ảnh* của đồng cấu f, $Kerf$ là *hạt nhân* của đồng cấu f.

Sau đây, ta sẽ đưa ra một số tính chất của đồng cấu.

Định lí 12. *Giả sử X, Y, Z là những nhóm và* $f : X \to Y$ *và* $g : Y \to Z$ *là những đồng cấu. Thế thì ánh xạ tích*

$$gf : X \to Z$$

cũng là một đồng cấu. Đặc biệt tích của hai đẳng cấu là một đẳng cấu.

Chứng minh. Giả sử a, b là hai phần tử tùy ý của nhóm X. Ta có, do f và g là những đồng cấu, $gf(ab) = g(f(ab)) = g(f(a)\,f(b)) = g(f(a))\,g(f(b)) = gf(a)g\,f(b)$. ■

Định lí 13. *Giả sử* $f : X \to Y$ *là một đồng cấu từ một nhóm X đến một nhóm Y. Thế thì :*

(i) $f(e_X) = e_Y$

(ii) $f(x^{-1}) = [f(x)]^{-1}$ *với mọi* $x \in X$.

Chứng minh. (i) Giả sử x là một phần tử tùy ý của X.

Ta có $f(e_X)f(x) = f(e_X x) = f(x) = e_Y f(x)$

Vậy $f(e_X)f(x) = e_Y f(x)$ hay $f(e_X) = e_Y$ sau khi thực hiện luật giản ước.

(ii) Ta có

$$f(x^{-1})f(x) = f(x^{-1}x) = f(e_X) = e_Y = [f(x)]^{-1}f(x).$$

suy ra

$$f(x^{-1}) = [f(x)]^{-1}\ .\ \blacksquare$$

Định lí 14. *Giả sử* $f : X \to Y$ *là một đồng cấu từ một nhóm X đến một nhóm Y, A là một nhóm con của X và B là một nhóm con chuẩn tắc của Y. Thế thì :*

(i) $f(A)$ *là một nhóm con của Y.*

(ii) $f^{-1}(B)$ *là một nhóm con chuẩn tắc của X.*

Chứng minh. (i) Trước hết $f(A) \neq \Phi$ vì A là một nhóm con nên $e_X \in A$, do đó $e_Y = f(e_X) \in f(A)$. Ta hãy lấy hai phần tử tùy ý : $y, y_1 \in f(A)$. Vì $y, y_1 \in f(A)$, nên có $x, x_1 \in A$ sao cho $y = f(x)$ và $y_1 = f(x_1)$. Xét tích yy_1^{-1}. Ta có $yy_1^{-1} = f(x)\,f(x_1)^{-1} =$

$= f(x)f(x_1^{-1}) = f(xx_1^{-1})$. Vì A là nhóm con nên $xx_1^{-1} \in A$, do đó $yy_1^{-1} = f(xx_1^{-1}) \in f(A)$. Ta suy ra $f(A)$ là nhóm con của Y.

(ii) $f_1^{-1}(B) \neq \emptyset$, vì B là nhóm con nên $e_Y \in B$, do đó $f(e_X) = e_Y \in B$, ta suy ra $e_X \in f^{-1}(B)$. Bây giờ ta lấy hai phần tử tùy ý $x, x_1 \in f^{-1}(B)$, ta chứng minh $xx_1^{-1} \in f^{-1}(B)$. Muốn vậy ta xét $f(xx_1^{-1})$. Ta có $f(xx_1^{-1}) = f(x)f(x_1^{-1}) = f(x)f(x_1)^{-1}$. Nhưng $f(x), f(x_1) \in B$ và $f(x)f(x_1)^{-1} \in B$ vì B là nhóm con. Vậy $f(xx_1^{-1}) \in B$, tức là $xx_1^{-1} \in f^{-1}(B)$, do đó $f^{-1}(B)$ là nhóm con của X. Cuối cùng ta chứng minh nó là chuẩn tắc. Muốn vậy giả sử $a \in f^{-1}(B)$ và $x \in X$. Xét
$f(x^{-1}ax) = f(x^{-1})f(a)f(x) = f(x)^{-1}f(a)f(x) \in B$ vì $f(a) \in B$ và B là chuẩn tắc. Do đó $x^{-1}ax \in f^{-1}(B)$ với mọi $a \in f^{-1}(B)$ và mọi $x \in X$. Vậy $f^{-1}(B)$ chuẩn tắc. ■

Từ định lí 14 ta có hệ quả tức khắc

Hệ quả. *Giả sử $f : X \to Y$ là một đồng cấu từ một nhóm X đến một nhóm Y. Thế thì Imf là một nhóm con của Y và $Kerf$ là một nhóm con chuẩn tắc của X.*

Định lí 15. *Giả sử $f : X \to Y$ là một đồng cấu từ một nhóm X đến một nhóm Y. Thế thì :*

(i) *f là một toàn ánh nếu và chỉ nếu $Imf = Y$.*

(ii) *f là một đơn ánh nếu và chỉ nếu $Kerf = \{e_X\}$.*

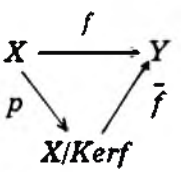
Chứng minh. (i) Suy ra từ định nghĩa của toàn ánh.

(ii) Giả sử f là một đơn ánh. Với mỗi phần tử $y \in Y$ có nhiều nhất một phần tử x sao cho $f(x) = y$. Vậy $Kerf = \{e_X\}$. Đảo lại giả sử $Kerf = \{e_X\}$. Xét hai phần tử $x, x_1 \in X$ sao cho $f(x) = f(x_1)$. Ta suy ra $f(x)f(x_1)^{-1} = e_Y$. Nhưng $f(x)f(x_1)^{-1} = f(x)f(x_1)^{-1} = f(xx_1^{-1})$. Vậy $f(xx_1^{-1}) = e_Y$, tức là

$xx_1^{-1} \in \text{Ker}f = \{e_x\}$. Do đó $xx_1^{-1} = e_x$ hay $x = x_1$. Như vậy f là đơn ánh. ■

Định lí 16. *Giả sử $f : X \to Y$ là một đồng cấu từ một nhóm X đến một nhóm Y, $p : X \to X/\text{Ker}f$ là toàn cấu chính tắc* (Ví dụ 4) *từ nhóm X đến nhóm thương của X trên hạt nhân của f. Thế thì :*

(i) *Có một đồng cấu duy nhất $\bar{f} : X/\text{Ker}f \to Y$ sao cho tam giác sau*



là giao hoán, tức là $f = \bar{f}p$

(ii) *Đồng cấu $\bar{f}$ là một đơn cấu và* $\text{Im}\bar{f} = f(X)$.

Chứng minh. (i) Đặt $\text{Ker}f = A$ và cho tương ứng với mỗi phần tử xA của X/A phần tử $f(x)$ của Y. Quy tắc cho tương ứng như vậy là một ánh xạ. Thật vậy, giả sử $xA = x_1A$, thế thì ta có $x^{-1}x_1 \in A$ (hệ quả của bổ đề 2). Nhưng A là hạt nhân của f, nên $f(x^{-1}x_1) = f(x^{-1})f(x_1) = f(x)^{-1}f(x_1) = e_Y$, tức là $f(x) = f(x_1)$. Ta đặt

$$\bar{f} : X/A \to Y$$
$$xA \mapsto \bar{f}(xA) = f(x).$$

Ta chứng minh $\bar{f}$ là một đồng cấu. Ta có, với xA và yA là hai phần tử tùy ý của X/A,

$$\bar{f}(xA.yA) = \bar{f}(xyA) = f(xy).$$

Nhưng f là một đồng cấu nên $f(xy) = f(x)f(y)$, do đó

$$\bar{f}(xA.yA) = f(x)f(y) = \bar{f}(xA)\bar{f}(yA)$$

theo định nghĩa của $\bar{f}$. Vậy $\bar{f}$ là một đồng cấu. Từ đẳng thức $\bar{f}(xA) = f(x)$ với mọi $x \in X$, ta có thể viết

$$f(x) = \bar{f}(xA) = \bar{f}(p(x)) = \bar{f}p(x)$$

với mọi $x \in X$. Vậy $f = \bar{f}p$. Cuối cùng giả sử có một đồng cấu $\varphi : X/A \to Y$ sao cho $f = \varphi p$. Vậy, với mọi $xA \in X/A$, ta có

$$\varphi(xA) = \varphi(p(x)) = \varphi p(x) = f(x) = \bar{f}(xA),$$

do đó $\varphi = \bar{f}$.

(ii) Giả sử $xA \in X_A$ sao cho $\bar{f}(xA) = e_Y$. Theo định nghĩa của $\bar{f}$, $\bar{f}(xA) = f(x)$, vậy $f(x) = e_Y$. Do đó $x \in A = eA$, tức là $xA = eA$. Ta suy ra $\mathrm{Ker}\bar{f} = \{ eA \}$, vậy $\bar{f}$ là một đơn cấu (định lí 15). Vì p là toàn cấu và vì $f = \bar{f}p$ nên ta suy ra $Im\bar{f} = Imf = f(X)$. ■

Hệ quả. *Với mọi đồng cấu $f : X \to Y$ từ một nhóm X đến một nhóm Y, ta có*

$$f(X) = X/\mathrm{Ker}f.$$

Ví dụ. 1) Giả sử A là một nhóm con chuẩn tắc của X, h là toàn cấu chính tắc từ X đến X/A. Ta có $\mathrm{Ker}\, h = A$. Thật vậy, ta có $h(x) = xA = eA$ nếu và chỉ nếu $x \in A$ (hệ quả của bổ đề 2). Trong trường hợp $A = \{e\}$ thì toàn cấu h còn là đơn ánh, do đó h là một đẳng cấu, vậy $X = X/\{e\}$ (điều này ta có thể chứng minh trực tiếp). Trong trường hợp $A = X$ thì nhóm thương X/X là nhóm chỉ có một phần tử, đó là lớp eX, vì ta có $xX = eX$ với mọi $x \in X$. Toàn cấu chính tắc h lúc đó là tầm thường vì "biến" mọi phần tử của X thành phần tử trung lập.

2) Giả sử f là một ánh xạ từ nhóm cộng $\mathbf{Z}$ các số nguyên đến nhóm nhân $\mathbf{C}^*$ các số phức khác 0 xác định như sau

$$f : \mathbf{Z} \to \mathbf{C}^*$$

$$k \longmapsto \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$$

trong đó n là một số nguyên dương cho trước. Rõ ràng f là một đồng cấu vì

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

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

Mặt khác vì

$$\left(\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}\right)^n = \cos 2k\pi + i\sin 2k\pi = 1$$

nên các phần tử của $f(Z)$ là các căn bậc n của đơn vị. Ta suy ra tập hợp các căn bậc n của đơn vị cùng với phép nhân các số phức là một nhóm. Bây giờ ta xét tới Ker$f$. Đó là bộ phận của $\mathbf{Z}$ gồm các số nguyên k sao cho

$$\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} = 1.$$

Vậy k là bội của n, do đó Ker$f$ = $n\mathbf{Z}$. Theo hệ quả của định lí 16 ta có

$$f(Z) \simeq \mathbf{Z}/n\mathbf{Z},$$

tức là nhóm nhân các căn bậc n của đơn vị đẳng cấu với nhóm cộng các số nguyên mod n.

5. Đối xứng hóa

Ta đã biết rằng trong một nhóm, đẳng thức $ab = ac$ (hay $ba = ca$) kéo theo đẳng thức $b = c$. Điều này do sự tồn tại của đối xứng a^{-1} của a. Nhưng nếu ta xét một nửa nhóm, thì $ab = ac$ chưa chắc đã kéo theo $b = c$; chẳng hạn trong nửa nhóm nhân các số tự nhiên $\mathbf{N}$ ta có đẳng thức $0.2 = 0.3$, nhưng $2 \neq 3$. Từ đây ta có khái niệm :

Định nghĩa 10. Cho một tập hợp X cùng với một phép toán hai ngôi trong X. Một phần tử $a \in X$ gọi là *chính quy bên trái (bên phải)* nếu với mọi $b, c \in X$ sao cho $ab = ac$ $(ba = ca)$ thì $b = c$, a gọi là *chính quy* nếu nó là chính quy bên trái và bên phải.

Như vậy, trong một vị nhóm, mọi phần tử có đối xứng đều là chính quy, nhưng ngược lại không đúng (xét vị nhóm nhân $\mathbf{N}$ các số tự nhiên). Điều kiện chính quy chỉ là điều kiện cần để có đối xứng.

Bây giờ ta hãy xét vấn đề sau đây : "nhúng" một vị nhóm giao hoán X vào một vị nhóm $\overline{X}$ "rộng" hơn sao cho mọi phần tử chính quy của X có đối xứng trong $\overline{X}$.

Bổ đề 3. *Giả sử X là một nửa nhóm giao hoán có phần tử trung lập e và X^* là bộ phận của X gồm các phần tử chính quy của X. Thế thì*

(i) $e \in X^*$.

(ii) X^* *là ổn định.*

Chứng minh. (i) Vì $ex = x$ với mọi $x \in X$, nên từ $ea = eb$ ta có $a = b$.

(ii) Giả sử $a, b \in X^*$. Từ $abx = aby$ ta suy ra $bx = by$ vì a là chính quy. Nhưng b cũng chính quy nên $bx = by$ kéo theo $x = y$. Vậy ab là chính quy, tức là $ab \in X^*$. ■

Định lí 17. *Giả sử X là một vị nhóm giao hoán, X^* là bộ phận của X gồm các phần tử chính quy của X. Có một vị nhóm giao hoán $\overline{X}$ và một đơn cấu f từ X đến $\overline{X}$ có các tính chất sau :*

1°. *Các phần tử của $f(X^*)$ có đối xứng trong $\overline{X}$.*

2°. *Các phần tử của $\overline{X}$ có dạng $f(a)\ f(b)^{-1}$ với $a \in X$, $b \in X^*$.*

Chứng minh. Ta hãy xét quan hệ S sau đây trong tập hợp $X \times X^*$:

$(a, b)\ S\ (a', b')$ nếu và chỉ nếu $ab' = a'b$.

Quan hệ S là một quan hệ tương đương : thật vậy, rõ ràng nó là phản xạ và đối xứng ; nó là bắc cầu, vì nếu ta có $ab' = a'b$ và $a'b'' = a''b'$, ta suy ra $ab'b'' = a'bb'' = a''bb'$ nhưng b' là chính quy, nên $ab'' = a''b$. Giả sử $\overline{X}$ là tập hợp thương của $X \times X^*$ trên quan hệ tương đương S. Các phần tử của $\overline{X}$ là các lớp tương đương $C(a, b)$ mà ta kí hiệu là $\overline{(a, b)}$. Ta đặt $f(a) = \overline{(a, e)}$ với mọi $a \in X$, e là phần tử trung lập của X. Ta hãy trang bị cho $\overline{X}$ một phép toán để $\overline{X}$ là một vị nhóm giao hoán và ta sẽ thấy rằng cặp $(\overline{X}, f)$ thỏa mãn bài toán đặt ra.

Giả sử $x = \overline{(a, b)}$ và $y = \overline{(c, d)}$ là hai phần tử của $\overline{X}$. Phần tử $\overline{(ac, bd)}$ chỉ phụ thuộc vào x và y ; thật vậy giả sử $x = \overline{(a', b')}$, vậy $ab' = a'b$ hay nhân hai vế với cd, $ab'cd = a'bcd$, ta suy ra $\overline{(ac, bd)} = \overline{(a'c, b'd)}$. *Ta thấy ngay rằng* $\overline{X}$ *cùng với phép toán* $(x, y) \mapsto xy = \overline{(ac, bd)}$ là một vị nhóm giao hoán với phần tử đơn vị là $\overline{(e, e)}$. Ta chú ý là ta có $\overline{(e, e)} = \overline{(a, a)}$ với mọi $a \in X^*$. Ngoài ra ta có ngay f là một đơn cấu và, với mọi $a \in X^*$, đối xứng của $f(a) = \overline{(a, e)}$ trong $\overline{X}$ là $\overline{(e, a)}$. Cuối cùng mọi phần tử $x = \overline{(a, b)} \in X$ có thể viết

$$x = \overline{(a, b)} = \overline{(a, e)}\,\overline{(e, b)} = \overline{(a, e)}\,\overline{(b, e)}^{-1} = f(a)\,f(b)^{-1}. \blacksquare$$

Cặp $(\overline{X}, f)$ của định lí 17 là duy nhất (sai kém một đẳng cấu) nghĩa là nếu có một cặp (Y, g) khác thỏa mãn bài toán thì có một đẳng cấu $\varphi : \overline{X} \to Y$ và $g = \varphi f$. Thật vậy, ứng với mỗi phần tử $x = f(a)\,f(b)^{-1}$, ta xét phần tử $g(a)\,g(b)^{-1}$. Phần tử $g(a)\,g(b)^{-1}$ chỉ phụ thuộc vào phần tử x, vì nếu có $f(a)\,f(b)^{-1} = f(a')\,f(b')^{-1}$ tức là $f(a)\,f(b') = f(a')\,f(b)$ hay $f(ab') = f(a'b)$ (f là đồng cấu), ta suy ra $ab' = a'b$ (f *là đơn ánh*), *do đó* $g(ab') = g(a'b)$, hay $g(a)g(b') = g(a')\,g(b)$ (g là đồng cấu), tức là $g(a)\,g(b)^{-1} = g(a')\,g(b')^{-1}$; vậy ta có ánh xạ φ :

$$f(a)\,f(b)^{-1} \longmapsto g(a)\,g(b)^{-1}$$

từ $\overline{X}$ đến Y. Dễ dàng chứng minh rằng đó là một đẳng cấu và $g = \varphi f$.

Trong định lí 17, vì f là một đơn cấu nên ta hãy đồng nhất a và $f(a)$ với mọi $a \in X$. Do đó các phần tử của $\overline{X}$ viết dưới dạng ab^{-1} với $a \in X$, $b \in X^*$.

Hệ quả. *Nếu tất cả các phần tử của* X *đều là chính quy thì tất cả các phần tử của* $\overline{X}$ *đều có đối xứng, do đó* $\overline{X}$ *là một nhóm.*

Ứng dụng. 1) *Số nguyên.* Ta hãy lấy X là vị nhóm các số tự nhiên N, phép toán là phép cộng thông thường ; mọi phần tử của N là chính quy nên $\overline{X}$ là một nhóm. Ta kí hiệu $\overline{X}$ bằng

$\mathbf{Z}$; các phần tử của $\mathbf{Z}$ gọi là các *số nguyên* ; phép toán trong $\mathbf{Z}$ xây dựng như trong định lí 17 gọi là phép cộng các số nguyên và cũng kí hiệu bằng dấu + như phép cộng các số tự nhiên. Mỗi phần tử của $\mathbf{Z}$ viết dưới dạng $m - n$ với $m, n \in \mathbf{N}$. Nếu $m \geqslant n$ ta có $m - n = p$, p là số tự nhiên sao cho $m = n + p$. Nếu $m < n$, ta có $m - n = -p$, p là số tự nhiên sao cho $m + p = n$. Vậy các phần tử của $\mathbf{Z}$ là... $-3, -2, -1, 0, 1, 2, 3, ...$

2) *Số hữu tỉ dương*. Lấy $\mathbf{N}^*$ tập hợp các số tự nhiên khác 0 làm X, phép toán lần này là phép nhân thông thường các số tự nhiên ; mọi phần tử của $\mathbf{N}^*$ là chính quy nên $\overline{X}$ là một nhóm. Trong trường hợp này $\overline{X}$ kí hiệu là $\mathbf{Q}^+$ và các phần tử của nó gọi là các số *hữu tỉ dương* ; phép toán trong $\mathbf{Q}^+$ xây dựng như trong định lí 17 gọi là phép nhân các số hữu tỉ dương và kí hiệu bằng $x.y$ hay xy cái hợp thành của hai số hữu tỉ dương x và y. Mỗi phần tử của $\mathbf{Q}^+$ viết dưới dạng pq^{-1} với $p, q \in \mathbf{N}^*$, ta còn quy ước viết phần tử pq^{-1} của $\mathbf{Q}^+$ là p/q hay $\frac{p}{q}$; tích của $\frac{p_1}{q_1}$ và $\frac{p_2}{q_2}$ như vậy là $\frac{p_1p_2}{q_1q_2}$; số tự nhiên m được đồng nhất với $m/1 = m.n/n$ $(n \in \mathbf{N}^*)$.

Chú ý. Tại sao với $\mathbf{Z}$, ta có

$$\mathbf{Z} = \mathbf{N} \cup \{-1, -2, -3, ..., -n, ...\}$$

(xem Ứng dụng 1)), trong khi đối với $\mathbf{Q}^+$ ta không có

$$\mathbf{Q}^+ = \mathbf{N}^* \cup \left\{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, ..., \frac{1}{n}, ...\right\}$$

(xem Ứng dụng 2)) ? Để tìm hiểu ta xét các định lí sau đây.

X trong hai định lí sau chỉ một vị nhóm nhân giao hoán (tất nhiên ta cũng có thể lấy một vị nhóm cộng), và X^* là bộ phận các phần tử chính quy của X mà ta giả thiết $X^* = X$. Theo Hệ quả của Định lí 17, $\overline{X}$ là một nhóm, mà các phần tử có dạng ab^{-1} với $a, b \in X$ (Định lí 17).

Định lí 18. Nếu với mọi $a, b \in X$, hoặc phương trình $ax = b$ có nghiệm trong X, hoặc phương trình $bx = a$ có nghiệm trong X ; thế thì :

$$\overline{X} = X \cup \{c^{-1} \mid c \in X\}$$

Chứng minh. Giả sử $ab^{-1} \in \overline{X}$. Nếu phương trình $ax = b$ có nghiệm trong X, nghiệm đó phải có dạng $ba^{-1} \in X$, vậy $ab^{-1} \in \{ c^{-1} / c \in X \}$. Nếu phương trình bx = a có nghiệm trong X, nghiệm đó phải có dạng $ab^{-1} \in X$. Vậy $\overline{X} \subset X \cup \{c^{-1} \mid c \in X\}$.

Bao hàm thức ngược lại là hiển nhiên. Vậy ta có

$$\overline{X} = X \cup \{c^{-1} \mid c \in X\}. \blacksquare$$

Định lí 19. Đảo lại, giả sử

$$\overline{X} = X \cup \{c^{-1} \mid c \in X\}.$$

Thế thì với mọi $a, b \in X$, hoặc phương trình $ax = b$ có nghiệm trong X, hoặc phương trình $bx = a$ có nghiệm trong X.

Chứng minh. Giả sử $a, b \in X$. Xét phương trình $ax = b$. Phương trình này có nghiệm trong $\overline{X}$, đó là $x = ba^{-1}$. Theo giả thiết về $\overline{X}$, $ba^{-1} \in X$ hoặc $ba^{-1} \in \{ c^{-1} / c \in X \}$. Nếu $ba^{-1} \in X$, điều đó có nghĩa phương trình có nghiệm trong X ; nếu $ba^{-1} \in \{ c^{-1} / c \in X \}$, ta có $ba^{-1} = c^{-1}$, $c \in X$, hay $ab^{-1} = c$, hay phương trình $bx = a$ có nghiệm trong X. $\blacksquare$

Từ hai định lí trên, ta thấy rằng : "Với mọi $a, b \in \mathbf{N}$, hoặc phương trình $a + x = b$ có nghiệm trong N hoặc $b + x = a$ có nghiệm trong N". Cho nên

$$\mathbf{Z} = \mathbf{N} \cup \{-1, -2, -3, ...\}.$$

Trong khi đó, với mọi $a, b \in \mathbf{N}^*$, không phải bao giờ ta cũng có $ax = b$ có nghiệm trong $\mathbf{N}^*$ hay $bx = a$ có nghiệm trong $\mathbf{N}^*$.

Chẳng hạn $a = 2$, $b = 3$, cả $2x = 3$ và $3x = 2$ đều không có nghiệm trong $\mathbf{N}^*$.

BÀI TẬP

1. Lập các bảng toán cho các tập hợp gồm hai phần tử, ba phần tử để được những nhóm.

2. Thử xem các tập hợp sau đây với phép toán đã cho có lập thành một nhóm :

1) **Tập hợp các số nguyên với phép cộng.**

2) **Tập hợp các số hữu tỉ với phép cộng.**

3) **Tập hợp các số thực với phép cộng.**

4) **Tập hợp các số phức với phép cộng.**

5) **Tập hợp các số nguyên là bội của một số nguyên m với phép cộng.**

6) **Tập hợp các số thực dương với phép nhân.**

7) **Tập hợp các số thực khác 0 với phép nhân.**

8) **Tập hợp các số phức có môđun bằng 1 với phép nhân.**

9) **Tập hợp các số phức khác 0 với phép nhân.**

10) **Tập hợp các số hữu tỉ có dạng 2^n, $n \in \mathbf{Z}$, với phép nhân.**

11) **Tập hợp các căn phức bậc n của 1 với phép nhân.**

12) **$M = \{1, -1\}$ với phép nhân.**

13) **Tập hợp các số thực dương với phép toán T xác định như sau : $aTb = a^2b^2$ với mọi số thực a, $b > 0$.**

14) **Tập hợp các số thực có dạng $a + b\sqrt{3}$ (a, $b \in \mathbf{Z}$) với phép cộng.**

15) **Tập hợp các số thực có dạng $a + b\sqrt{3}$ (a, $b \in \mathbf{Q}$ và $a^2 + b^2 \neq 0$) với phép nhân.**

16) **Tập hợp các số phức có dạng $a + bi$ (a, $b \in \mathbf{Z}$) với phép cộng.**

17) Tập hợp các vectơ n chiều của không gian $\mathbf{R}^n$ với phép cộng vectơ.

18) Tập hợp các ma trận vuông cấp n với phép cộng ma trận.

19) Tập hợp các ma trận vuông cấp n không suy biến với phép nhân ma trận.

20) Tập hợp các ma trận vuông cấp n có định thức bằng 1 với phép nhân ma trận.

21) Tập hợp các ma trận vuông cấp n có định thức bằng ± 1 với phép nhân ma trận.

22) Tập hợp các đa thức (có hệ số thực) với phép cộng các đa thức.

23) Tập hợp gồm đa thức 0 và các đa thức có bậc không quá n (n là một số nguyên, $n \geq 0$, cho trước) với phép cộng các đa thức.

3. Chứng minh rằng mọi nửa nhóm khác rỗng hữu hạn X là một nhóm nếu và chỉ nếu luật giản ước thực hiện được với mọi phần tử của X.

4. Cho X là một tập hợp tùy ý. Kí hiệu Hom (X, X) là tập hợp các ánh xạ từ X đến X. Với phép nhân ánh xạ Hom (X, X) có lập thành một nhóm hay không ? Chứng minh rằng bộ phận $S(X)$ của Hom (X, X) gồm các song ánh từ X đến X là một nhóm với phép nhân ánh xạ. Hãy tìm cấp của S(X) trong trường hợp X có n phần tử.

5. Cho X là một nhóm với đơn vị là e. Chứng minh rằng nếu với mọi $a \in X$ ta có $a^2 = e$, thì X là aben.

6. Cho một họ những nhóm $(X_\alpha)_{\alpha \in I}$ mà các phép toán đều kí hiệu bằng dấu nhân. Chứng minh rằng tập hợp tích đề các $\prod_{\alpha \in I} X_\alpha$ với phép toán xác định như sau :

$$(x_\alpha)_{\alpha \in I} \cdot (y_\alpha)_{\alpha \in I} = (x_\alpha y_\alpha)_{\alpha \in I}$$

là một nhóm (gọi là *tích* các nhóm X_α).

7. Cho X là một tập hợp khác rỗng cùng với một phép toán hai ngôi kết hợp trong X, a là một phần tử của X. Kí hiệu

$$aX = \{ ax \mid x \in X \},$$

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

Chứng minh X là một nhóm khi và chỉ khi với mọi $a \in X$ ta có $aX = Xa = X$.

8. Chứng minh rằng mọi bộ phận khác rỗng ổn định của một nhóm hữu hạn X là một nhóm con của X.

9. Trong các nhóm ở 2) nhóm nào là nhóm con của nhóm nào ?

10. Chứng minh rằng trong nhóm cộng các số nguyên $\mathbf{Z}$, một bộ phận A của $\mathbf{Z}$ là một nhóm con của $\mathbf{Z}$ nếu và chỉ nếu A có dạng $m\mathbf{Z}$, $m \in \mathbf{Z}$.

11. Trong nhóm các phép thế S_4, chứng minh rằng các phép thế sau : e, $a = (12)\ (34)$, $b = (1\ 3)\ (2\ 4)$ và $c = (1\ 4)\ (2\ 3)$ thành lập một nhóm con của S_4. Nhóm con đó có aben không ?

12. Cho Y là một bộ phận của một tập hợp X. Chứng minh rằng bộ phận $S(X, Y)$ của $S(X)$ gồm các song ánh $f : X \to X$

sao cho $f(Y) = Y$ là một nhóm con của $S(X)$ (bài tập 4). Tìm số phần tử của $S(X, Y)$ trong trường hợp X có n phần tử và Y có một phần tử.

13. Cho A và B là hai bộ phận của một nhóm X. Ta định nghĩa

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

$$A^{-1} = \{ a^{-1} \mid a \in A \}$$

Chứng minh các đẳng thức sau đây :

a) $(AB)\,C = A(BC)$.

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

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

d) Nếu A là một nhóm con của X thì $A^{-1} = A$.

14. Cho X là một nhóm và A là một bộ phận khác rỗng của X. Chứng minh A là nhóm con của X khi và chỉ khi $AA^{-1} = A$.

15. Cho A là một nhóm con của nhóm X và $a \in X$. Chứng minh aA là nhóm con của X khi và chỉ khi $a \in A$.

16. Trong một nhóm X chứng minh rằng nhóm con sinh ra bởi bộ phận $\varnothing$ là nhóm con tầm thường $\{e\}$, e là phần tử trung lập của X.

17. Giả sử S là một bộ phận khác rỗng của một nhóm X. Chứng minh rằng các phần tử của nhóm con sinh ra bởi S là các phần tử có dạng $x_1 x_2 \ldots x_n$ với các $x_1, \ldots, x_n$ thuộc S hoặc S^{-1}. Tìm nhóm con của nhóm nhân các số hữu tỉ dương sinh ra bởi bộ phận các số nguyên tố.

18. Chứng minh rằng mọi nhóm con của một nhóm xyclic là một nhóm xyclic

19. Cho X là một nhóm với phần tử đơn vị là e, $a \in X$ có cấp là n. Chứng minh rằng $a^k = e$ khi và chỉ khi k chia hết cho n.

20. Cho a, b là hai phần tử tùy ý của một nhóm. Chứng minh ab và ba có cùng cấp

21. Giả sử X là một nhóm xyclic cấp n và $a \in X$ là một phần tử sinh của nó. Xét phần tử $b = a^k$. Chứng minh rằng :

a) Cấp của b bằng n/d, ở đây d là UCLN của k và n.

b) b là phần tử sinh của X khi và chỉ khi k nguyên tố với n (từ đó suy ra số phần tử sinh của X).

22. Giả sử a, b là hai phần tử của một nhóm, và giả sử ta có cấp của a bằng r, cấp của b bằng s, với r, s nguyên tố cùng nhau, và thêm nữa $ab = ba$. Chứng minh cấp của ab bằng rs.

23. Chứng minh rằng mọi nhóm cấp vô hạn đều có vô hạn nhóm con.

24. Cho X và Y là những nhóm xyclic có cấp là m và n. Chứng minh rằng $X \times Y$ là một nhóm xyclic khi và chỉ khi m và n nguyên tố cùng nhau.

25. Cho A là một nhóm con của một nhóm X. Giả sử tập hợp thương X/A có hai phần tử. Chứng minh A là chuẩn tắc.

26. Trong nhóm các phép thế S_n, bộ phận A_n gồm các phép thế chẵn là nhóm con chuẩn tắc của S_n.

27. Giả sử X là một nhóm xyclic vô hạn, và $a \in X$ là một phần tử sinh. Gọi A là nhóm con của X sinh ra bởi a^3. Chứng minh rằng các lớp trái của A bằng các lớp phải của A và số các lớp đó bằng 3.

28. Giả sử X là một nhóm, ta gọi là *tâm* của X bộ phận

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

Chứng minh rằng $C(X)$ là một nhóm con giao hoán của X và mọi nhóm con của $C(X)$ là một nhóm con chuẩn tắc của X.

29. Tìm tất cả các nhóm con và nhóm con chuẩn tắc của nhóm các phép thế S_3.

30. Giả sử X là một nhóm, x và y là hai phần tử của X. Ta gọi là *hoán tử* của x và y phần tử $xyx^{-1}y^{-1}$. Chứng minh rằng nhóm con A sinh ra bởi tập hợp các hoán tử của tất cả các cặp phần tử x, y của X là một nhóm con chuẩn tắc của X gọi là nhóm các hoán tử, và nhóm thương X/A là aben.

31. Chứng minh rằng muốn cho một nhóm thương X/H của một nhóm X là aben, ắt có và đủ là nhóm con chuẩn tắc H chứa nhóm các hoán tử của X.

32. Tìm nhóm các hoán tử của S_3.

33. Chứng minh rằng mọi nhóm có cấp bé hơn hoặc bằng 5 là aben.

34. Hãy tìm các nhóm thương của

a) Nhóm cộng các số nguyên là bội của 3 trên nhóm con các số nguyên là bội của 15.

b) Nhóm cộng các số nguyên là bội của 4 trên nhóm con các số nguyên là bội của 24.

c) Nhóm nhân các số thực khác 0 trên nhóm con các số thực dương.

35. Cho D là tập hợp các đường thẳng Δ trong mặt phẳng có phương trình là $y = ax + b$ ($a \neq 0$, b là những số thực). Ánh xạ

$$D \times D \to D$$

$$(\Delta_1, \Delta_2) \mapsto \Delta_3$$

trong đó Δ_1, Δ_2, Δ_3 lần lượt có các phương trình là $y = a_1x + b_1$, $y = a_2x + b_2$, $y = a_1a_2x + (b_1 + b_2)$ xác định một phép toán hai ngôi trong D.

a) Chứng minh D là một nhóm với phép toán trên.

b Ánh xạ

$$\varphi : D \to \mathbf{R}^*$$

$$\Delta \mapsto a$$

trong đó $\mathbf{R}^*$ là nhóm nhân các số thực khác 0 và Δ là đường thẳng có phương trình $y = ax + b$ là một đồng cấu.

c) Xác định $\mathrm{Ker}\varphi$.

36. Cho G_1, G_2 là những nhóm với đơn vị theo thứ tự là e_1, e_2 và G là nhóm tích $G_1 \times G_2$ (bài tập 6). A và B là các bộ phận $G_1 \times \{e_2\}$, $\{e_1\} \times G_2$ của G. Xét các ánh xạ

$$p_1 : G \to G_1$$
$$(x_1, x_2) \mapsto x_1$$
$$p_2 : G \to G_2$$
$$(x_1, x_2) \mapsto x_2$$
$$q_1 : G_1 \to G$$
$$x_1 \mapsto (x_1, e_2)$$
$$q_2 : G_2 \to G$$
$$x_2 \mapsto (e_1, x_2)$$

a) Chứng minh p_1, p_2 là những toàn cấu. Xác định Ker p_1 và Ker p_2.

b) Chứng minh q_1, q_2 là những đơn cấu. Xác định $\mathrm{Im}q_1$ và $\mathrm{Im}q_2$. Từ đó suy ra G_1 đẳng cấu với A, và G_2 đẳng cấu với B.

c) Chứng minh A và B là những nhóm con chuẩn tắc và $AB = BA = G$.

37. Chứng minh rằng mọi nhóm xyclic hữu hạn cấp n đều đẳng cấu với nhau (đẳng cấu với nhóm cộng các số nguyên mod n).

38. Chứng minh rằng mọi nhóm xyclic vô hạn đều đẳng cấu với nhau (đẳng cấu với nhóm cộng các số nguyên $\mathbf{Z}$).

39. Giả sử X là một nhóm và Y là một tập hợp được trang bị một phép toán. Giả sử có một song ánh

$$f : X \to Y$$

thỏa mãn tính chất $f(ab) = f(a)f(b)$ với mọi $a, b \in X$. Chứng minh Y cùng với phép toán đã cho trong Y là một nhóm ; thêm nữa là aben nếu X aben, là xyclic nếu X xyclic.

40. Cho X và Y là hai nhóm xyclic có các phần tử sinh theo thứ tự là x và y và có cấp là s và t.

a) Chứng minh rằng quy tắc φ cho tương ứng với phần tử $x^a \in X$ phần tử $(y^k)^a \in Y$, trong đó k là một số tự nhiên khác 0 cho trước, là một đồng cấu khi và chỉ khi sk là bội của t.

b) Nếu $sk = mt$ và φ là đẳng cấu thì $(s, m) = 1$.

41. Cho X là một nhóm giao hoán. Chứng minh rằng ánh xạ

$$\varphi : X \to X$$
$$a \mapsto a^k$$

với k là một số nguyên cho trước, là một đồng cấu.

Xác định Ker φ.

42. Cho X là một nhóm. Ánh xạ

$$\varphi : X \to X$$
$$a \mapsto a^{-1}$$

là một tự đẳng cấu của nhóm X khi và chỉ khi X là aben.

43. Cho X là một nhóm. Chứng minh rằng tập hợp các tự đẳng cấu của X cùng với phép nhân ánh xạ là một nhóm.

44. Giả sử X, G_1, G_2 là những nhóm, $G = G_1 \times G_2$ và $f : X \to G_1$ $g : X \to G_2$ *là những ánh xạ. Xét ánh xạ*

$$h : X \to G$$
$$x \mapsto h(x) = (f(x), g(x)).$$

Chứng minh rằng h là một đồng cấu khi và chỉ khi f và g là những đồng cấu.

45. Trong tập hợp $X = \mathbf{Z}^3$, với $\mathbf{Z}$ là tập hợp các số nguyên, ta xác định một phép toán hai ngôi như sau :

$$(k_1, k_2, k_3)(l_1, l_2, l_3) = (k_1 + (-1)^{k_3} l_1, k_2 + l_2, k_3 + l_3)$$

a) Chứng minh rằng X cùng với phép toán đó là một nhóm.

b) Chứng minh rằng nhóm con A sinh ra bởi phần tử $(1, 0, 0)$ là chuẩn tắc

c) Chứng minh rằng nhóm thương X/A đẳng cấu với nhóm cộng các số phức có dạng $a + bi$ với $a, b \in \mathbf{Z}$

46. Chứng minh rằng :

a) Nhóm cộng các số thực đẳng cấu với nhóm nhân các số thực dương.

b) Nhóm cộng các số phức có dạng $a + bi$ với a, b nguyên đẳng cấu với nhóm tích $\mathbf{Z} \times \mathbf{Z}$ trong đó $\mathbf{Z}$ là nhóm cộng các số nguyên.

47. Cho X là một nhóm. Với mỗi phần tử $a \in X$ ta xét ánh xạ

$$f_a : X \to X$$

$$x \mapsto a^{-1}xa.$$

a) Chứng minh f_a là một tự đẳng cấu của X, gọi là *tự đẳng cấu trong* xác định bởi phần tử a.

b) Chứng minh các tự đẳng cấu trong lập thành một nhóm con của nhóm các tự đẳng cấu của X (bài tập 43).

c) Chứng minh một nhóm con H của X là chuẩn tắc nếu và chỉ nếu $f_a(H) = H$ với mọi tự đẳng cấu trong f_a của X. Vì lí do đó, các nhóm con chuẩn tắc cũng còn gọi là các *nhóm con bất biến*.

d) Chứng minh ánh xạ $a \mapsto f_a$ là một đồng cấu từ nhóm X đến nhóm các tự đẳng cấu trong của X và hạt nhân của đẳng cấu đó là tâm $C(X)$ (bài tập 28) của X.

c) Chứng minh $X/C(X)$ đẳng cấu với nhóm các tự đẳng cấu trong của X.

48. Chứng minh rằng nếu $f : X \to Y$ là một đồng cấu từ một nhóm hữu hạn X đến một nhóm Y thì

a) Cấp của $a \in X$ chia hết cho cấp của $f(a)$

b) Cấp của X chia hết cho cấp của $f(X)$.

49. Chứng minh rằng nhóm Y là ảnh đồng cấu của một nhóm xyclic hữu hạn X khi và chỉ khi Y là nhóm *xyclic và cấp của nó chia hết cấp của* X.

50. Hãy tìm tất cả các đồng cấu từ

a) Một nhóm xyclic cấp n đến chính nó.

b) Một nhóm xyclic cấp 6 đến một nhóm xyclic cấp 18.

c) Một nhóm xyclic cấp 18 đến một nhóm xyclic cấp 6.

51. Chứng minh rằng ngoài đồng cấu tầm thường ra thì không có một đồng cấu nào từ nhóm cộng các số hữu tỉ đến nhóm cộng các số nguyên.

52. Giả sử $\mathbf{C}^*$ là nhóm nhân các số phức khác 0, H là tập hợp các số phức của $\mathbf{C}^*$ nằm trên trục thực và trục ảo. Chứng minh rằng H là một nhóm con của $\mathbf{C}^*$ và nhóm thương $\mathbf{C}^*/H$ đẳng cấu với nhóm nhân U các số phức có môđun bằng 1.

53. Chứng minh rằng nhóm thương $\mathbf{R}/\mathbf{Z}$ ($\mathbf{R}$ là nhóm cộng các số thực, $\mathbf{Z}$ là nhóm cộng các số nguyên) đẳng cấu với nhóm U (bài tập 52).

54. Gọi X là nhóm nhân các ma trận vuông cấp n không suy biến mà các phần tử là thực. Hãy chứng minh

a) Nhóm thương của X trên nhóm con các ma trận có định thức bằng 1 đẳng cấu với nhóm nhân các số thực khác 0.

b) Nhóm thương của X trên nhóm con các ma trận có định thức bằng ± 1 đẳng cấu với nhóm nhân các số thực dương.

c) Nhóm thương của X trên nhóm con các ma trận có định thức dương là một nhóm xyclic cấp hai.

55. Giả sử X là một vị nhóm (nhân) sinh bởi một phần tử a có cấp vô hạn, nghĩa là :

$$X = \{a^n \mid n \in N\}$$

Chứng minh vị nhóm $\overline{X}$ (Định lí 17) là nhóm và các phần tử của $\overline{X}$ là $\ldots a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, a^3 \ldots$ nghĩa là

$$\overline{X} = X \cup \{a^{-1}, a^{-2}, a^{-3}, \ldots\}$$

CHƯƠNG III

VÀNH VÀ TRƯỜNG

§1. VÀNH VÀ MIỀN NGUYÊN

1. Vành

Định nghĩa 1. Ta gọi là *vành* một tập hợp X cùng với hai phép toán hai ngôi đã cho trong X kí hiệu theo thứ tự bằng các dấu + và . *(người ta thường kí hiệu như vậy)* và gọi là phép cộng và phép nhân sao cho các điều kiện sau thỏa mãn :

1) X cùng với phép cộng là một nhóm aben.

2) X cùng với phép nhân là một nửa nhóm.

3) Phép nhân phân phối đối với phép cộng : với các phần tử tùy ý $x, y, z \in X$ ta có

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

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

Phần tử trung lập của phép cộng thì kí hiệu là 0 và gọi là phần tử *không*. Phần tử đối xứng (đối với phép cộng) của một phần tử x thì kí hiệu là $-x$ và gọi là *đối* của x. Nếu phép nhân là giao hoán thì ta bảo *vành X là giao hoán*. Nếu phép nhân có phần tử trung lập thì phần tử đó gọi là *phần tử đơn vị* của X và thường kí hiệu là e hay 1 (nếu không có sự nhầm lẫn).

Ví dụ. 1) Tập hợp $\mathbf{Z}$ các số nguyên cùng với phép cộng và phép nhân thông thường là một vành giao hoán có đơn vị gọi

là vành các số nguyên. Ta cũng có vành các số hữu tỉ, các số thực, các số phức (các phép toán vẫn là phép cộng và phép nhân thông thường)

2) Tập hợp $\mathbf{Z}/n\mathbf{Z}$ các số nguyên mod n cùng với phép cộng và phép nhân các số nguyên mod n (ch II, §1, bài tập 2) và ch II, §2, 3, ví dụ) là một vành giao hoán có đơn vị, gọi là *vành các số nguyên mod n*.

3) Tập hợp các ma trận vuông cấp $n, n > 1$, (với các phần tử là thực chẳng hạn) cùng với phép cộng và phép nhân ma trận là một vành có đơn vị. Vành này không giao hoán.

4) Tập hợp các số nguyên là bội của một số nguyên $n > 1$ cho trước là một vành với phép cộng và phép nhân thông thường. Vành này là giao hoán, nhưng không có đơn vị.

5) Tập hợp các ma trận vuông cấp $n > 1$ có dạng

$$\begin{bmatrix} a_1 & a_2 & \dots & a_n \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{bmatrix}$$

trong đó các a_i là những số thực, cùng với phép cộng và phép nhân ma trận là một vành. Vành này không giao hoán, không có đơn vị.

6) Giả sử X là một nhóm giao hoán mà phép toán kí hiệu bằng dấu cộng $+$. Tập hợp E các tự đồng cấu từ X đến X được trang bị hai phép toán kết hợp : một mặt, phép toán cộng $f, g \longrightarrow f + g$, $f + g\,(x) = f(x) + g(x)$ với mọi $x \in X$, khiến cho E là một nhóm cộng giao hoán (phần tử không là ánh xạ 0 xác định bởi $0(x) = 0$ với mọi $x \in X$, phần tử đối của f là ánh xạ $-f$ xác định bởi $(-f)(x) = -f(x)$ với mọi $x \in X$) ; mặt khác, phép toán nhân $(f, g) \longrightarrow fg$. Ta có $(g + h)f = gf + hf$ và $f(g + h) = fg + fh$. Thật vậy, $(g + h)f(x) = g(f(x)) + h(f(x)) = gf(x) + hf(x) = (gf + hf)(x)$, và $f(g + h)(x) = f(g(x) + h(x)) = f(g(x)) + f(h(x)) = (fg)(x) + (fh)(x) = (fg + fh)(x)$. Vậy E cùng với hai phép toán đó là một vành, gọi là *vành các tự đồng cấu của nhóm* X. Vành này có đơn vị,

đó là ánh xạ đồng nhất của X, nhưng không giao hoán nếu X có quá 2 phần tử.

Ngoài các tính chất là một nhóm cộng giao hoán và một nửa nhóm nhân, một vành còn có *một số tính chất suy ra từ luật phân phối*.

Định lí 1. *Cho X là một vành. Với mọi $x, y, z \in X$ ta có :*

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

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

(iii) $x(-y) = (-x)y = -xy$, $(-x)(-y) = xy$.

Chứng minh. (i) Theo luật phân phối ta có $xy = x((y - z) + z) = x(y - z) + xz$. Ta suy ra $x(y - z) = xy - xz$. Đẳng thức thứ hai chứng minh cũng tương tự.

(ii) Theo (i) ta có $0x = (y - y)x = yx - yx = 0 = xy - xy = x(y - y) = x0$.

(iii) Từ (i) và (ii) ta được $x(-y) = x(0 - y) = x0 - xy = 0 - xy = -xy = 0y - xy = (0 - x)y = (-x)y$; ta suy ra $(-x)(-y) = xy$. Đặc biệt, với mọi số nguyên $n > 0$, ta được $(-x)^n = x^n$ nếu n chẵn, và $(-x)^n = -x^n$ nếu n lẻ. ■

Từ (ii) ta suy ra nếu vành X có đơn vị và có nhiều hơn một phần tử thì $e \neq 0$.

2. Ước của không. Miền nguyên.

Ở đây ta hãy tổng quát hóa khái niệm ước và bội ở trong vành các số nguyên.

Định nghĩa 2. Giả sử X là một vành giao hoán. Ta bảo một phần tử $a \in X$ là *bội* của một phần tử $b \in X$ hay a chia hết cho b, kí hiệu $a \vdots b$, nếu có $c \in X$ sao cho $a = bc$; ta còn nói rằng b là *ước* của a hay b chia hết a, kí hiệu $b \mid a$.

Như vậy theo định lí 1 (ii), mọi phần tử $x \in X$ là ước của 0 ; nhưng do lạm dụng ngôn ngữ, người ta định nghĩa :

Định nghĩa 3. Ta gọi là *ước của 0* mọi phần tử $a \neq 0$ sao cho có $b \neq 0$ thỏa mãn quan hệ $ab = 0$.

Ta suy ra ngay từ định nghĩa rằng phần tử 0 và các ước của 0 không phải là chính quy. Trong một vành không có ước của 0, mọi phần tử khác 0 đều là chính quy. Thật vậy, quan hệ $ab = ac$ tương đương với quan hệ $a(b - c) = 0$.

Định nghĩa 4. Ta gọi là *miền nguyên* một vành có nhiều hơn một phần tử, giao hoán, có đơn vị, không có ước của *0*.

Ví dụ : Vành các số nguyên **Z** là một miền nguyên.

3. Vành con

Định nghĩa 5. Giả sử X là một vành, A là một bộ phận của X ổn định đối với hai phép toán trong X nghĩa là $x + y \in A$ và $xy \in A$ với mọi $x, y \in A$. A là một *vành con* của vành X nếu A cùng với hai phép toán cảm sinh trên A là một vành.

Định lí 2. *Giả sử A là một bộ phận khác rỗng của một vành X. Các điều kiện sau đây là tương đương :*

a) A là một vành con của X.

b) Với mọi $x, y \in A$, $x + y \in A$, $xy \in A$, $-x \in A$.

c) Với mọi $x, y \in A$, $x - y \in A$, $xy \in A$.

Chứng minh. a) kéo theo b). Vì A là một vành con cho nên ta có ngay $x + y$ và xy thuộc A với mọi $x, y \in A$. Mặt khác vì A là một vành nên nó là một nhóm đối với phép cộng, ta suy ra $-x \in A$ với mọi $x \in A$ (ch II, §2,2, định lí 7).

b) kéo theo c) theo (ch II, §2, 2, hệ quả của định lí 7).

c) kéo theo a). Trước hết ta chú ý rằng các phép toán cảm sinh trên A cũng có tính chất kết hợp và phân phối. Do đó cùng với hệ quả của định lí 7 (ch II, §2, 2) ta có A là một vành con của X. ■

Ví dụ. 1) Bộ phận {0} chỉ gồm có phần tử không và bộ phận X là hai vành con của vành X.

2) Bộ phận $m\mathbf{Z}$ gồm các số nguyên là bội của một số nguyên m cho trước là một vành con của vành các số nguyên **Z**.

Định lí 3. *Giao của một họ bất kì những vành con của một vành X là một vành con của X.*

Chứng minh tương tự như trong nhóm.

Giả sử U là một bộ phận của một vành X. Thế thì U chứa trong ít nhất một vành con của X, cụ thể X. Theo định lí 3, giao A của tất cả các vành con của X chứa U là một vành con của X chứa U, vành con này gọi là *vành con của X sinh ra bởi U.*

4. Iđêan và vành thương

Định nghĩa 6. Ta gọi là *iđêan trái (iđêan phải)* của một vành X, một vành con A của X thỏa mãn điều kiện $xa \in A$ ($ax \in A$) với mọi $a \in A$ và mọi $x \in X$. Một vành con A của một vành X gọi là một *iđêan* của X nếu và chỉ nếu A vừa là iđêan trái vừa là iđêan phải của X.

Từ định nghĩa ta suy ra ngay tức khắc

Định lí 4. Một bộ phận A khác rỗng của một vành X là một iđêan của X nếu và chỉ nếu các điều kiện sau thỏa mãn :

1) $a - b \in A$ với mọi $a, b \in A$.

2) $xa \in A$ và $ax \in A$ với mọi $a \in A$ và mọi $x \in X$.

Ví dụ. 1) Bộ phận {0} và bộ phận X là hai iđêan của vành X.

2) Bộ phận $m\mathbf{Z}$ gồm các số nguyên là bội của một số nguyên m cho trước là một iđêan của vành các số nguyên $\mathbf{Z}$.

Định lí 5. *Giao của một họ bất kì những iđêan của một vành X là một iđêan của X.*

Chứng minh tương tự như định lí 3.

Giả sử U là một bộ phận của một vành X. Thế thì U chứa trong nó ít nhất một iđêan của X, cụ thể X. Theo định lí 5, giao A của tất cả các iđêan của X chứa U là một iđêan của X chứa U, iđêan này gọi là *iđêan sinh ra bởi U* ; nếu $U = \{a_1, a_2, ..., a_n\}$ thì A gọi là iđêan sinh ra bởi các phần tử $a_1, a_2, ..., a_n$. Iđêan sinh ra bởi một phần tử gọi là *iđêan chính.*

Định lí 6. *Giả sử X là một vành giao hoán có đơn vị và $a_1, a_2, ..., a_n \in X$. Bộ phận A của X gồm các phần tử có dạng $x_1a_1 + x_2a_2 + ... + x_na_n$ với $x_1, x_2, ..., x_n \in X$ là iđêan của X sinh ra bởi $a_1, a_2, ..., a_n$.*

Chứng minh. Giả sử $a = x_1a_1 + ... + x_na_n, b = y_1a_1 + ... + y_na_n$ là hai phần tử tùy ý thuộc A và x là một phần tử tùy ý thuộc X. Ta có

$$a - b = (x_1a_1 + ... + x_na_n) - (y_1a_1 + ... + y_na_n) =$$

$$(x_1a_1 - y_1a_1) + ... + (x_na_n - y_na_n) =$$

$$(x_1 - y_1)a_1 + ... + (x_n - y_n)a_n \in A ;$$

$$xa = ax = x(x_1a_1 + ... + x_na_n) = xx_1a_1 + ... + xx_na_n \in A.$$

Vậy A là một iđêan của X. A chứa các a_i với $i = 1, 2, ..., n.$,

vì $a_i = 0a_1 + ... + 1a_i + ... + 0a_n$, $i = 1, 2, ..., n.$

Cuối cùng mọi iđêan chứa $a_1, ..., a_n$ thì cũng chứa $x_1a_1, ..., x_na_n$ với $x_1, ..., x_n \in X$ và do đó chứa $x_1a_1 + ... + x_na_n$. Kết luận A là giao của tất cả các iđêan chứa $\{a_1, ..., a_n\}$ tức là iđêan sinh ra bởi $a_1, a_2, ..., a_n$. ■

Từ định nghĩa ta cũng suy ra ngay

Định lí 7. *Nếu X là một vành có đơn vị và nếu A là một iđêan của X chứa đơn vị của X thì ta có $A = X$.*

Bây giờ ta hãy xét một iđêan A tùy ý của một vành đã cho X. Vì A là một nhóm con của nhóm aben cộng của X, nhóm thương X/A là một nhóm aben hoàn toàn xác định theo (ch II, §2, 3). Các phần tử của X/A là các lớp khác nhau $x + A$ của A trong X. Ta hãy trang bị cho X/A một phép toán nhân để nó trở thành một vành.

Định lí 8. *Nếu A là một iđêan của vành X, thì :*

(i) *Lớp $xy + A$ chỉ phụ thuộc vào các lớp $x + A$ và $y + A$ mà không phụ thuộc vào sự lựa chọn của các phần tử x, y từ các lớp đó.*

(ii) *X/A cùng với hai phép toán*

$$(x + A, y + A) \longmapsto x + y + A$$

$$(x + A, y + A) \longmapsto xy + A$$

là một vành gọi là vành thương của X trên A.

Chứng minh. (i) Giả sử $x' + A = x + A$ và $y' + A = y + A$.

Vậy $x' - x = a \in A$ và $y' - y = b \in A$, hay $x' = x + a$ và $y' = y + b$.

Do đó $x'y' = (x + a)(y + b) = xy + ay + xb + ab$. Vì A là một iđêan, nên từ $a, b \in A$ ta suy ra $ay, xb, ab \in A$ vậy $x'y' + A = xy + A$. Ta kí hiệu $(x + A)(y + A) = xy + A$. Như vậy ngoài phép cộng $(x + A) + (y + A) = x + y + A$ trong X/A, ta có phép nhân xác định bởi $(x + A)(y + A) = xy + A$.

(ii) Phép nhân trong X/A rõ ràng là kết hợp do tính kết hợp của phép nhân trong X. Ngoài ra ta cũng có luật phân phối. Vậy X/A là một vành. Nếu X là giao hoán thì X/A cũng giao hoán. Nếu X có đơn vị 1 thì $1 + A$ là đơn vị của X/A. ■

Ví dụ. Vành thương của $\mathbf{Z}$ trên iđêan $n\mathbf{Z}$ gọi là vành các số nguyên mod n. Phép cộng và phép nhân trong $\mathbf{Z}/n\mathbf{Z}$ xác định bởi

$$(x + n\mathbf{Z}) + (y + n\mathbf{Z}) = x + y + n\mathbf{Z}$$

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

Kí hiệu $x + n\mathbf{Z}$ bằng $\bar{x}$ và lấy $n = 4$ ta có bảng cộng và bảng nhân của $\mathbf{Z}/4\mathbf{Z}$ như sau

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

5. Đồng cấu

Định nghĩa 7. Một *đồng cấu (vành)* là một ánh xạ từ một vành X đến một vành Y sao cho

$$f(a + b) = f(a) + f(b)$$

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

với mọi $a, b \in X$. Nếu $X = Y$ thì đồng cấu f gọi là một tự đồng cấu của X.

Ta cũng định nghĩa đơn cấu, toàn cấu, đẳng cấu tương tự như đã định nghĩa trong nhóm.

Ví dụ. 1) Giả sử A là một vành con của một vành X. Đơn ánh chính tắc

$$A \to X$$

$$a \mapsto a$$

là một đồng cấu gọi là đơn cấu chính tắc.

2) Ánh xạ đồng nhất của một vành X là một đồng cấu gọi là tự đẳng cấu đồng nhất của X.

3) Giả sử A là một iđêan của một vành X. Ánh xạ

$$h : X \to X/A$$
$$x \mapsto x + A$$

là một đồng cấu từ vành X đến vành thương X/A. Đồng cấu này còn là toàn cấu, gọi là toàn cấu chính tắc.

4) Giả sử X và Y là hai vành, ánh xạ

$$X \to Y$$
$$x \mapsto 0$$

với 0 là phần tử không của Y là một đồng cấu gọi là *đồng cấu không*.

Dưới đây chúng ta hãy đưa ra các định lí tương tự như trong nhóm mà việc chứng minh, hoặc tương tự hoặc áp dụng các kết quả trong nhóm, xin nhường cho độc giả.

Định lí 9. *Giả sử X, Y, Z là những vành, $f : X \to Y$ và $g : Y \to Z$ là những đồng cấu. Thế thì tích ánh xạ*

$$gf : X \to Z$$

cũng là một đồng cấu. Đặc biệt tích của hai đẳng cấu là một đẳng cấu.

Định lí 10. *Giả sử $f : X \to Y$ là một đồng cấu từ một vành X đến một vành Y. Thế thì :*

(i) $f(0) = 0$

(ii) $f(-x) = -f(x)$ *với mọi* $x \in X$.

Định lí 11. *Giả sử $f : X \to Y$ là một đồng cấu từ một vành X đến một vành Y, A là một vành con của X và B là một iđêan của Y. Thế thì :*

(i) $f(A)$ *là một vành con của Y.*

(ii) $f^{-1}(B)$ *là một iđêan của X.*

Hệ quả. *Giả sử $f : X \to Y$ là một đồng cấu từ một vành X đến một vành Y. Thế thì* Imf *là một vành con của Y và* Ker$f$ *là một iđêan của X.*

Định lí 12. *Giả sử $f : X \to Y$ là một đồng cấu từ một vành X đến một vành Y. Thế thì :*

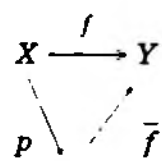
(i) f *là một toàn ánh nếu và chỉ nếu* Im$f = Y$.

(ii) f *là một đơn ánh nếu và chỉ nếu* Ker$f = \{0\}$.

Định lí 13. *Giả sử $f : X \to Y$ là một đồng cấu từ một vành X đến một vành Y, $p : X \to X/\text{Ker}f$ là toàn cấu chính tắc (ví dụ 3). từ vành X đến vành thương của X trên* Ker$f$.

Thế thì :

(i) *Có một đồng cấu duy nhất* $\bar{f} : X/\text{Ker}f \to Y$ *sao cho tam giác*



$X/\text{Ker}f$

là giao hoán.

(ii) *Đồng cấu* $\bar{f}$ *là một đơn cấu và* Im $\bar{f} = f(X)$.

Hệ quả. *Với mọi đồng cấu $f : X \to Y$ từ một vành X đến một vành Y, ta có*

$$f(X) = X/\mathrm{Ker} f$$

BÀI TẬP

1. Chứng minh các tập hợp sau đây với phép cộng và phép nhân các số lập thành một vành :

a) Tập hợp các số có dạng $a + b\sqrt{2}$ với $a, b \in \mathbf{Z}$.

b) Tập hợp các số phức có dạng $a + bi$ với $a, b \in \mathbf{Z}$.

Chứng minh các vành đó giao hoán có đơn vị.

2. Chứng minh tập hợp các ma trận vuông cấp n với các phần tử là những số nguyên làm thành một vành với phép cộng và phép nhân ma trận.

3. Chứng minh tập hợp các đa thức của x với hệ số nguyên làm thành một vành với phép cộng và phép nhân đa thức.

4. Giả sử đã cho trong một tập hợp X hai phép toán cộng và nhân sao cho : 1) X cùng với phép cộng là một nhóm ; 2) X cùng với phép nhân là một vị nhóm ; 3) phép nhân phân phối đối với phép cộng. Chứng minh X là một vành.

5. Tìm các ước của không trong vành $\mathbf{Z}/6\mathbf{Z}$.

6. Chứng minh $\mathbf{Z}/n\mathbf{Z}$ $(n \neq 0)$ là một miền nguyên khi và chỉ khi n là nguyên tố.

7. Chứng minh tập hợp $X = \mathbf{Z} \times \mathbf{Z}$ cùng với hai phép toán

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

$$(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$$

là một vành giao hoán, có đơn vị. Hãy tìm tất cả các ước của không của vành này.

8. Giả sử X là một vành có tính chất sau đây :

$$x^2 = x \text{ với mọi } x \in X$$

Chứng minh rằng

a) $x = -x$ với mọi $x \in X$.

b) X là vành giao hoán.

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

9. Các vành ở các bài tập 1), 2), 3) là những vành con của những vành nào ?

10. Cho X là một vành tùy ý, A và B là hai iđêan của X. Chứng minh rằng bộ phận

$$A + B = \{a + b \mid a \in A,\ b \in B\}$$

là một iđêan của X.

11. Cho X là một vành tùy ý, n là một số nguyên cho trước.

Chứng minh bộ phận

$$A = \{x \in X \mid nx = 0\}$$

là một iđêan của X.

12. Cho X là một vành tùy ý, $a \in X$. Chứng minh rằng bộ phận

$$aX = \{ax \mid x \in X\}$$

là một iđêan phải của X, và bộ phận

$$Xa = \{xa \mid x \in X\}$$

là một iđêan trái của X.

13. Giả sử X là một miền nguyên và n là cấp (ch II, § 2, 2, định nghĩa 5) của phần tử đơn vị e. Chứng minh

a) n là một số nguyên tố.

b) Mọi phần tử khác không $x \in X$ có cấp n.

c) Bộ phận

$$mX = \{mx \mid x \in X\},$$

với m là một số nguyên cho trước, là một iđêan của X.

d) $X/mX = X$ nếu m là bội của n,

$X/mX = \{0\}$ nếu m không phải là bội của n.

14. Giả sử X là một vành giao hoán, có đơn vị. Một iđêan $A \neq X$ của X gọi là *iđêan tối đại* nếu và chỉ nếu các iđêan của X chứa A chính là X và bản thân A. Một iđêan $P \neq X$ của X gọi là *iđêan nguyên tố* nếu và chỉ nếu với $u, v \in X$ tích $uv \in P$ thì $u \in P$ hoặc $v \in P$. Chứng minh rằng :

a) X/P là miền nguyên khi và chỉ khi P là iđêan nguyên tố.

b) X/A là trường (§2) khi và chỉ khi A là tối đại.

15. Giả sử A là một vành, B là một tập hợp có hai phép toán cộng và nhân, và $f : A \to B$ là một song ánh thỏa mãn

$$f(a + b) = f(a) + f(b)$$

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

với mọi $a, b \in A$.

Chứng minh : a) B là một vành.

b) Nếu A là vành giao hoán thì B cũng là vành giao hoán.

c) Nếu A là vành có đơn vị thì B cũng là vành có đơn vị.

d) Nếu A là miền nguyên thì B cũng là miền nguyên.

16. Hãy tìm tất cả các tự đồng cấu của vành các số nguyên.

17. Giả sử $f : X \to X$ là một tự đồng cấu của vành X. Chứng minh rằng tập hợp

$$A = \{x \in X \mid f(x) = x\}$$

là một vành con của X.

18. Giả sử X là một vành tùy ý. $\mathbf{Z}$ là vành các số nguyên. Xét tập hợp tích $X \times \mathbf{Z}$. Trong $X \times \mathbf{Z}$ ta định nghĩa các phép toán như sau :

$$(x_1, n_1) + (x_2, n_2) = (x_1 + x_2, n_1 + n_2)$$

$$(x_1, n_1)(x_2, n_2) = (x_1 x_2 + n_1 x_2 + n_2 x_1, n_1 n_2)$$

a) Chứng minh rằng $X \times \mathbf{Z}$ là một vành có đơn vị.

b) Ánh xạ

$$f : X \to X \times \mathbf{Z}$$
$$x \mapsto (x, 0)$$

là một đơn cấu.

19. Cho A và B là hai vành tùy ý. Xét tập hợp tích đề các $X = A \times B$. Trong X ta định nghĩa các phép toán

$$(a, b) + (c, d) = (a + c, b + d)$$
$$(a, b)(c, d) = (ac, bd)$$

Chứng minh :

a) X là một vành.

b) Các bộ phận $\overline{A} = \{(a, 0) \mid a \in A\}$ và $\overline{B} = \{(0, b) \mid b \in B\}$ là những vành con của X đẳng cấu theo thứ tự với A và B.

c) $\overline{A}$ và $\overline{B}$ là hai iđêan của x sao cho $\overline{A} \cap \overline{B} = \{(0, 0)\}$ và $X = \overline{A} + \overline{B}$ (bài tập 10).

d) Giả sử A và B là những vành có đơn vị, hãy tìm các đơn vị của X, $\overline{A}$ và $\overline{B}$.

20. Giả sử X là một vành và $a \in X$. Chứng minh rằng :

a) Ánh xạ

$$h_a : X \to X$$
$$x \mapsto ax$$

là một đồng cấu (nhóm) từ nhóm cộng aben X đến nhóm cộng aben X.

b) Ánh xạ

$$h : X \to E$$
$$a \mapsto h(a) = h_a$$

là một đồng cấu từ vành X đến vành E các tự đồng cấu của nhóm cộng aben X (1, ví dụ 6).

c) Tìm Ker$h$. Chứng minh rằng h là đơn cấu khi X có đơn vị.

21. Giả sử X và Y là hai vành, $f : X \to Y$ là một đồng cấu từ vành X đến vành Y, A và B theo thứ tự là hai iđêan của

X và Y sao cho $f(A) \subset B$, $p : X \to X/A$ và $p' : Y \to Y/B$ là các toàn cấu chính tắc (5, ví dụ 3). Chứng minh rằng tồn tại một đồng cấu duy nhất $\bar{f}$ từ X/A đến Y/B sao cho hình vuông

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle p'} \\ X/A & \xrightarrow{\bar{f}} & Y/B \end{array}$$

là giao hoán, tức là $\bar{f}p = p'f$

Nếu f là một toàn cấu thì $\bar{f}$ có phải là một toàn cấu hay không ?

§2. TRƯỜNG

1. Trường

Định nghĩa 1. Ta gọi là *trường* một miền nguyên X trong đó mọi phần tử khác không đều có một nghịch đảo trong vị nhóm nhân X. Vậy một vành X giao hoán, có đơn vị, có nhiều hơn một phần tử là một trường nếu và chỉ nếu $X - \{0\}$ là một nhóm đối với phép nhân của X.

Ví dụ. Tập hợp $\mathbf{Q}$ các số hữu tỉ cùng với phép cộng và phép nhân các số là một trường. Ta cũng có trường số thực $\mathbf{R}$ và trường số phức $\mathbf{C}$.

2. Trường con

Định nghĩa 2. Giả sử X là một trường; A là một bộ phận của X ổn định đối với hai phép toán trong X. A là một *trường con* của trường X nếu A cùng với hai phép toán cảm sinh trên A là một trường.

Từ định nghĩa 2 và áp dụng hệ quả của định lí 7 trong (ch II, §2) cùng với định lí 2 (§1, 3) ta được

Định lí 1. *Giả sử A là một bộ phận có nhiều hơn một phần tử của một trường X. Các điều kiện sau đây là tương đương :*

a) *A là một trường con của X.*

b) *Với mọi* $x, y \in A$, $x + y \in A$, $xy \in A$, $-x \in A$, $x^{-1} \in A$ *nếu* $x \neq 0$.

c) *Với mọi* $x, y \in A$, $x - y \in A$, $xy^{-1} \in A$ *nếu* $y \neq 0$.

Ví dụ. 1) X là trường con của trường X. Bộ phận $\{0\}$ không phải là một trường con của X, vì theo định nghĩa một trường có ít nhất hai phần tử.

2) Trường số hữu tỉ $\mathbf{Q}$ là trường con của trường số thực $\mathbf{R}$, bản thân $\mathbf{R}$ lại là trường con của trường số phức $\mathbf{C}$.

Coi một trường X như một vành, ta có thể đặt vấn đề xét các iđêan của X. Mặc dù một trường X có thể có nhiều trường con, nó lại chỉ có hai iđêan tầm thường : X và $\{0\}$. Thực vậy, giả sử A là một iđêan của X và $A \neq \{0\}$. Vậy có một phần tử $x \neq 0$ thuộc A. Vì A là một iđêan nên $x^{-1}x = 1 \in A$. Do đó $A = X$ (§1, 4, định lí 7). Vậy hạt nhân của mọi đồng cấu

$$f : X \to Y$$

từ một trường X đến một trường Y chỉ có thể hoặc là $\{0\}$ hoặc là X. Trong trường hợp $\mathrm{Ker}f = \{0\}$ thì f là một đơn cấu (§1, 5, định lí 12), $\mathrm{Ker}f = X$ thì f là đồng cấu không.

3. Trường các thương

Giả sử X là một miền nguyên. Theo định nghĩa, các phần tử khác 0 của X đều là chính quy, nhưng điều đó chưa đảm bảo chúng có nghịch đảo trong X, chẳng hạn trong vành các số nguyên $\mathbf{Z}$ chỉ trừ 1 và -1 có nghịch đảo trong $\mathbf{Z}$ còn các số khác thì không. Bây giờ ta đặt vấn đề nhúng X vào một trường $\overline{X}$ sao cho mọi phần tử khác 0 của X có nghịch đảo trong $\overline{X}$. X là một miền nguyên nên X là một vị nhóm nhân giao hoán. Theo (ch II, §2, 5 định lí 17) ta có thể nhúng X vào một vị nhóm nhân giao hoán $\overline{X}$ sao cho mọi phần tử chính quy của X có nghịch đảo trong X. Nếu ta có thể trang bị cho $\overline{X}$ thêm

phép toán cộng để X là một trường thì vấn đề được giải quyết xong. Cụ thể ta có

Định lí 2. *Giả sử X là một miền nguyên, X^* là bộ phận các phần tử khác 0 của X. Có một trường $\overline{X}$ và một đơn cấu (vành) f từ X đến $\overline{X}$ có các tính chất sau :*

1°) *Các phần tử của $\overline{X}$ có dạng $f(a)f(b)^{-1}$ với $a \in X$, $b \in X^*$.*

2°) *Cặp $(\overline{X}, f)$ là duy nhất sai kém một đẳng cấu, nghĩa là nếu có cặp (Y, g) thỏa mãn điều kiện 1° thì có một đẳng cấu $\varphi : \overline{X} \to Y$ sao cho tam giác*

$$\begin{array}{ccc} X & \xrightarrow{f} & \overline{X} \\ & {\scriptstyle g}\searrow \quad \swarrow{\scriptstyle \varphi} & \\ & Y & \end{array}$$

là giao hoán.

Chứng minh. Vì X là một miền nguyên nên X là một vị nhóm nhân giao hoán. Ta xây dựng vị nhóm nhân giao hoán $\overline{X}$ và ánh xạ f như trong định lí 17 của (ch II, §2, 5). Bây giờ ta hãy xét hai phần tử $x = \overline{(a, b)}$ và $y = \overline{(c, d)}$ tùy ý của $\overline{X}$. Phần tử $\overline{(ad + bc, bd)}$ chỉ phụ thuộc vào x và y ; thật vậy giả sử $x = \overline{(a', b')}$, vậy $ab' = a'b$, ta suy ra $(ad + bc)b'd = (a'd + b'c)bd$, tức là $\overline{(ad + bc, bd)} = \overline{(a'd + b'c, b'd)}$. Tương tự đối với y. Ta thấy ngay rằng $\overline{X}$ cùng với phép cộng $(x, y) \mapsto x + y = \overline{(ad + bc, bd)}$ là một nhóm giao hoán ; phần tử không là $\overline{(0, 1)}$; phần tử đối của $x = \overline{(a, b)}$ là $-x = \overline{(-a, b)}$. Mặt khác $\overline{X}$ cùng với phép nhân $(x, y) \mapsto xy = \overline{(a, b)}\,\overline{(c, d)} = \overline{(ac, bd)}$, như ta đã biết, là một vị nhóm giao hoán. Thêm nữa ta có thể thử để thấy phép nhân phân phối đối với phép cộng. Vậy $\overline{X}$ là một vành giao hoán có đơn vị. Mọi phần tử $x = \overline{(a, b)}$ khác phần tử $\overline{(0, 1)}$, do đó $a \neq 0$, có nghịch đảo là $x^{-1} = \overline{(b, a)}$. Vậy $\overline{X}$ là một trường. Ánh xạ $f : X \to \overline{X}$ cho tương ứng với mỗi phần tử $a \in X$ phần tử $\overline{(a, 1)} \in \overline{X}$ có tính chất

$$f(a + b) = f(a) + f(b)$$

ngoài các tính chất đã biết trong định lí 17 của (ch II, §2, 5). Do đó f là một đơn cấu (vành) từ X đến $\overline{X}$. Cặp (X, f) xây dựng như vậy có tính chất 1°. Cuối cùng giả sử (Y, g) là cặp cũng thỏa mãn tính chất 1° của bài toán. Ánh xạ

$$\varphi : \overline{X} \to Y$$

$$x = f(a)f(b)^{-1} \mapsto g(a)g(b)^{-1}$$

là một song ánh bảo tồn phép nhân : $\varphi(xy) = \varphi(x)\varphi(y)$, như ta đã biết. Mặt khác ta cũng dễ dàng thử rằng

$$\varphi(x + y) = \varphi(x) + \varphi(y) \text{ với mọi } x, y \in \overline{X}.$$

Từ đó φ là một đẳng cấu và hiển nhiên ta có $g = \varphi f$.

Vì f là một đơn cấu (vành) nên ta đồng nhất các phần tử $a \in X$ với các phần tử $f(a) \in f(X)$. Lúc đó mỗi phần tử $x \in \overline{X}$ có thể viết dưới dạng ab^{-1} với $a \in X$ và $b \in X^*$. Ta còn kí hiệu phần tử ab^{-1} bằng a/b (ch II, §2, 1). Vậy $a = a/1 = ab/b$ với mọi $a \in X$ và $b \in X^*$. Hai phần tử a/b và c/d là bằng nhau khi và chỉ khi $ad = bc$. Các quy tắc cộng và nhân là

$$a/b + c/d = (ad + bc)/bd$$

$$(a/b)(c/d) = ac/bd.$$

Đối của a/b là $-a/b = a/-b$. Nghịch đảo của a/b với $a \neq 0$ là b/a. Ta thấy lại các quy tắc của số hữu tỉ.■

Định nghĩa 3. Giả sử X là một miền nguyên, $\overline{X}$ là một trường. $\overline{X}$ gọi là một *trường các thương* của miền nguyên X nếu có một đơn cấu (vành) $f : X \to \overline{X}$ sao cho cặp $(\overline{X}, f)$ thỏa mãn tính chất 1°) của định lí 2.

Từ định nghĩa 3 và định lí 2 ta suy ra trường các thương của mọi miền nguyên tồn tại và xác định duy nhất (ly lai một đẳng cấu).

Ví dụ. Trường các thương của vành các số nguyên $\mathbf{Z}$ là trường các số hữu tỉ $\mathbf{Q}$.

BÀI TẬP

1. Chứng minh mọi miền nguyên hữu hạn là một trường.

2. Chứng minh vành các số nguyên mod n là một trường khi và chỉ khi n là nguyên tố.

3. Chứng minh rằng trường các số hữu tỉ không có trường con nào khác ngoài bản thân nó.

4. Chứng minh rằng bộ phận

$A = \{a + b\sqrt{2} \mid a, b \in Q\}$ là một trường con của trường số thực **R**.

5. Chứng minh rằng bộ phận

$$A = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in Q\}$$

là một trường con của trường số thực **R**.

6. Giả sử X là một trường, e là phần tử đơn vị của X. Xét bộ phận

$$A = \{ne \mid n \in \mathbf{Z}\}$$

a) Chứng minh A là một vành con của vành X, A có phải là một miền nguyên không ?

b) Chứng minh A đẳng cấu với vành các số nguyên **Z** khi e có cấp vô hạn, và đẳng cấu với vành các số nguyên mod p khi e có cấp p.

c) Trong trường hợp e có cấp p, hãy chứng minh A là một trường.

7. Giả sử X là một trường, Y là một tập hợp đã cho cùng với hai phép toán cộng và nhân trong Y, $f : X \to Y$ là một song ánh từ X đến Y thỏa mãn

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

với mọi $a, b \in X$.

Chứng minh Y là một trường và $X = Y$

8. Hãy tìm :

a) Các tự đồng cấu của trường các số hữu tỉ.

b) Các tự đồng cấu của trường các số phức giữ nguyên các số thực.

c) Các tự đồng cấu của trường các số thực.

9. Chứng minh rằng tập hợp các ma trận có dạng

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}.$$

với a, b là những số thực là một trường đối với phép cộng và phép nhân ma trận, trường này đẳng cấu với trường các số phức.

10. Chứng minh rằng tập hợp các ma trận có dạng

$$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}$$

với $a, b \in \mathbf{Q}$ là một trường (các phép toán vẫn là các phép cộng và nhân các ma trận) đẳng cấu với trường A ở bài tập 4.

11. Tìm trường các thương của miền nguyên A trong bài tập 6.

12. Chứng minh rằng mọi trường đều có trường con bé nhất (quan hệ thứ tự là quan hệ bao hàm) đẳng cấu hoặc với trường số hữu tỉ, hoặc với trường các số nguyên mod p với p là một số nguyên tố (bài tập 11).

13. Giả sử X là một trường, A là một vành con của vành X.

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 X, và lúc đó A là một miền nguyên.

b) Giả sử A là miền nguyên. Chứng minh rằng bộ phận

$$P = \{ ab^{-1} \mid a, b \in A, b \neq 0 \}$$

là một trường con của X và P là trường các thương của A.

c) Chứng minh rằng P là trường con bé nhất trong các trường con của X chứa A.

14. Giả sử p là một số nguyên tố. Chứng minh rằng tập hợp các số hữu tỉ có dạng m/n, trong đó n nguyên tố với p, là một miền nguyên. Tìm trường các thương của miền nguyên này.

CHƯƠNG IV

VÀNH ĐA THỨC

§1. VÀNH ĐA THỨC MỘT ẨN

1. Vành đa thức một ẩn

Khái niệm đa thức là khái niệm mà ta đã làm quen ít nhiều ở phổ thông. Ta gọi là đa thức, một tổng có dạng

$$a_o + a_1x + \ldots + a_mx^m$$

trong đó các a_i, $i = 0, \ldots, n$, là những số thực và x là một chữ. Phép cộng và phép nhân đa thức là

$$(a_o + a_1x + \ldots + a_mx^m) + (b_o + b_1x + \ldots + b_nx^n) =$$

$$a_o + b_o + \ldots + (a_m + b_m)x^m + b_{m+1}x^{m+1} + \ldots + b_nx^n.$$

$$(a_o + a_1x + \ldots + a_mx^m)(b_o + b_1x + \ldots + b_nx^n) =$$

$$a_ob_o + (a_ob_1 + a_1b_o)x + \ldots + (a_ob_k + a_1b_{k-1} + \ldots +$$

$$+ a_kb_o)x^k + \ldots + a_mb_nx^{m+n} \text{ trong đó ta giả sử } n \geq m.$$

Ở đây chúng ta hãy định nghĩa đa thức một cách tổng quát hơn và chính xác hơn. Giả sử A là một vành giao hoán, có đơn vị kí hiệu là 1. Gọi P là tập hợp các dãy

$$(a_o, a_1, \ldots, a_n, \ldots)$$

trong đó các $a_i \in A$ với mọi $i \in \mathbf{N}$ và bằng 0 tất cả trừ một số hữu hạn. Như vậy P là một bộ phận của lũy thừa đề các $A^{\mathbf{N}}$

(ch I, §1, 15). Ta định nghĩa phép cộng và phép nhân trong P như sau

(1) $(a_o, a_1, \ldots, a_n, \ldots) + (b_o, b_1, \ldots, b_n, \ldots) =$

$(a_o + b_o, a_1 + b_1, \ldots, a_n + b_n, \ldots)$

(2) $(a_o, a_1, \ldots, a_n, \ldots)(b_o, b_1, \ldots, b_n, \ldots) =$

$(c_o, c_1, \ldots, c_n, \ldots)$

với

$$c_k = a_o b_k + a_1 b_{k-1} + \ldots + a_k b_o = \sum_{i+j=k} a_i b_j, \; k = 0, 1, 2, \ldots$$

Vì các a_i và b_i bằng 0 tất cả trừ một số hữu hạn nên các $a_i + b_i$ và c_i cũng bằng 0 tất cả trừ một số hữu hạn, cho nên (1) và (2) cho ta hai phép toán trong P. Ta hãy chứng minh P là một vành giao hoán có đơn vị. Trước hết hiển nhiên phép cộng là giao hoán và kết hợp. Phần tử không là dãy

$$(0, 0, \ldots, 0, \ldots),$$

phần tử đối của dãy $(a_o, a_1, \ldots, a_n, \ldots)$ là dãy $(-a_o, -a_1, \ldots, -a_n, \ldots)$. Vậy P là một nhóm cộng giao hoán. Vì A là giao hoán, nên

$$\sum_{i+j=k} a_i b_j = \sum_{i+j=k} b_j a_i \quad ,$$

do đó phép nhân là giao hoán. Do phép nhân trong A có tính chất kết hợp và phân phối đối với phép cộng, nên với mọi $m = 0, 1, 2, \ldots$ ta có thể viết

$$\sum_{h+k=m} a_h \left(\sum_{i+j=k} b_i c_j \right) = \sum_{h+i+j=m} a_h (b_i c_j) =$$

$$\sum_{h+i+j=m} (a_h b_i) c_j = \sum_{j+l=m} \left(\sum_{h+i=l} a_h b_i \right) c_j$$

từ đó ta có phép nhân trong P là kết hợp. Dãy

$$(1, 0, \ldots, 0, \ldots)$$

là phần tử đơn vị của P. Vậy P là một vị nhóm nhân giao hoán. Cuối cùng luật phân phối trong A cho phép ta viết

$$\sum_{i+j=k} a_i(b_j + c_j) = \sum_{i+j=k} a_i b_j + \sum_{i+j=k} a_i c_j$$

với mọi $k = 0, 1, 2, \ldots$, ta suy ra từ đó luật phân phối trong P.

Bây giờ ta hãy xét dãy

$$x = (0, 1, 0, \ldots, 0, \ldots)$$

Ta có theo quy tắc nhân (2)

$$x^2 = (0, 0, 1, 0, \ldots, 0, \ldots)$$
$$x^3 = (0, 0, 0, 1, \ldots, 0, \ldots)$$
$$\vdots$$
$$x^n = (\underbrace{0, 0, \ldots, 0}_{n}, 1, 0, \ldots)$$

Ta quy ước viết

$$x^0 = (1, 0, \ldots, 0, \ldots)$$

Mặt khác ta xét ánh xạ

$$A \to P$$
$$a \mapsto (a, 0, \ldots, 0, \ldots)$$

Ánh xạ này hiển nhiên là một đơn cấu (vành). Do đó từ giờ ta đồng nhất phần tử $a \in A$ với dãy $(a, 0, \ldots, 0, \ldots) \in P$, và vì vậy A là một vành con của vành P. Vì mỗi phần tử của P là một dãy

$$(a_0, a_1, \ldots, a_n, \ldots)$$

trong đó các a_i bằng 0 tất cả trừ một số hữu hạn, cho nên mỗi phần tử của P có dạng

$$(a_0, a_1, \ldots, a_n, 0, \ldots)$$

trong đó $a_0, \ldots, a_n \in A$ không nhất thiết khác 0. Việc đồng nhất a với $(a, 0, \ldots, 0, \ldots)$ và việc đưa vào dãy x cho phép ta viết

$$(a_0, \ldots, a_n, 0, \ldots) = (a_0, 0, \ldots) + (0, a_1, 0, \ldots) +$$
$$\ldots + (0, \ldots, a_n, 0, \ldots) = (a_0, 0, \ldots) + (a_1, 0, \ldots)\ (0, 1, 0, \ldots) +$$
$$+ \ldots + (a_n, 0, \ldots)\ (\underbrace{0, \ldots, 0}_{n}, 1, 0, \ldots) = a_0 + a_1x + \ldots + a_nx^n =$$
$$= a_0x^0 + a_1x + \ldots + a_nx^n.$$

Người ta thường kí hiệu các phần tử của P viết dưới dạng

$$a_o + a_1x + \ldots + a_nx^n$$

bằng $f(x)$, $g(x)$...

Định nghĩa 1. Vành P gọi là *vành đa thức của ẩn x lấy hệ tử trong A*, hay vắn tắt *vành đa thức của ẩn x trên A*, và kí hiệu là $A[x]$. Các phần tử của vành đó gọi là đa thức của ẩn x lấy hệ tử trong A. Trong một đa thức

$$f(x) = a_ox^o + a_1x + \ldots + a_nx^n.$$

các a_i, $i = 0, 1, \ldots, n$ gọi là các *hệ tử* của đa thức. Các a_ix^i gọi là các *hạng tử* của đa thức, đặc biệt $a_ox^o = a_o$ gọi là *hạng tử tự do*.

2. Bậc của một đa thức

Xét một dãy $(a_o, a_1, \ldots, a_n, \ldots)$

thuộc vành P. Vì các a_i bằng 0 tất cả trừ một số hữu hạn nên nếu

$$(a_o, a_1, \ldots, a_n, \ldots) \neq (0, 0, \ldots, 0, \ldots)$$

thì bao giờ cũng có một chỉ số n sao cho $a_n \neq 0$ và $a_i = 0$, $i > n$. Theo như trên, ta viết

$$(a_o, a_1, \ldots, a_n, 0, \ldots) = a_ox^o + a_1x + \ldots + a_nx^n.$$

Định nghĩa 2. *Bậc* của đa thức khác 0

$$f(x) = a_ox^o + \ldots + a_{n-1}x^{n-1} + a_nx^n$$

với $a_n \neq 0$, $n \geq 0$, là n. Hệ tử a_n gọi là *hệ tử cao nhất* của $f(x)$.

Như vậy ta chỉ định nghĩa bậc của một đa thức khác 0. Đối với đa thức 0 ta bảo nó không có bậc.

Định lí 1. *Giả sử f(x) và g(x) là hai đa thức khác 0.*

(i) *Nếu bậc f(x) khác bậc g(x), thì ta có*

$$f(x) + g(x) \neq 0 \text{ và bậc } (f(x) + g(x)) = \max(\text{bậc } f(x), \text{bậc } g(x)).$$

Nếu bậc f(x) = bậc g(x), và nếu thêm nữa

$$f(x) + g(x) \neq 0, \text{ thì ta có}$$

$$\text{bậc } (f(x) + g(x)) \leqslant \max(\text{bậc } f(x), \text{bậc } g(x)).$$

(ii) *Nếu* $f(x)\,g(x) \neq 0$, *thì ta có*

$$\text{bậc } (f(x)\,g(x)) \leqslant \text{bậc } f(x) + \text{bậc } g(x).$$

Việc chứng minh không có gì khó khăn, xin nhường cho bạn đọc.

Định lí 2. *Nếu A là một miền nguyên f(x) và g(x) là hai đa thức khác 0 của vành A[x], thì* $f(x)\,g(x) \neq 0$ *và* $\text{bậc } (f(x)\,g(x)) = \text{bậc } f(x) + \text{bậc } g(x)$.

Chứng minh. Giả sử $f(x), g(x) \in A[x]$ là hai đa thức khác 0

$$f(x) = a_o + \ldots + a_m x^m \quad (a_m \neq 0)$$

$$g(x) = b_o + \ldots + b_n x^n \quad (b_n \neq 0)$$

Theo quy tắc nhân đa thức ta có

$$f(x)g(x) = a_o b_o + \ldots + (a_o b_k + \ldots + a_k b_o)\,x^k + \ldots + a_m b_n x^{n+m}.$$

a_m và b_n khác 0, nên $a_m b_n \neq 0$ (*A* không có ước của không), do đó $f(x)\,g(x) \neq 0$ và $\text{bậc } (f(x)\,g(x)) = m + n = \text{bậc } f(x) + \text{bậc } g(x)$. ■

Hệ quả. *Nếu A là miền nguyên, thì A [x] cũng là miền nguyên.*

3. Phép chia với dư

Trong mục 2 ta đã thấy nếu *A* là một miền nguyên thì *A*[*x*] cũng là một miền nguyên. Ta tự đặt câu hỏi : nếu *A* là một trường thì *A* [*x*] có phải là một trường không ? Câu hỏi được

trả lời ngay tức khắc, $A[x]$ không phải là một trường vì đa thức x chẳng hạn không có nghịch đảo. Tuy vậy trong trường hợp này $A[x]$ là một miền nguyên đặc biệt, nó là một vành ơclit (ch V, §2) nghĩa là một vành trong đó có phép chia với dư.

Định lí 3. *Giả sử A là một trường, $f(x)$ và $g(x) \neq 0$ là hai đa thức của vành $A[x]$; thế thì bao giờ cũng có hai đa thức duy nhất $q(x)$ và $r(x)$ thuộc $A[x]$ sao cho*

$$f(x) = g(x)\, q(x) + r(x), \text{ với bậc } r(x) < \text{bậc } g(x)$$

$$\text{nếu } r(x) \neq 0.$$

Chứng minh. Trước hết ta hãy chứng minh tính duy nhất. Giả sử

$$f(x) = g(x)\, q'(x) + r'(x), \text{ với bậc } r'(x) < \text{bậc } g(x)$$

$$\text{nếu } r'(x) \neq 0$$

Ta suy ra

$$0 = g(x)\,(q(x) - q'(x)) + r(x) - r'(x).$$

Nếu $r(x) = r'(x)$, ta có $g(x)\,(q(x) - q'(x)) = 0$, vì $g(x) \neq 0$ và $A[x]$ là một miền nguyên, nên suy ra $q(x) - q'(x) = 0$ tức là $q(x) = q'(x)$. Giả sử $r(x) \neq r'(x)$, vậy

bậc $(r(x) - r'(x))$ = bậc $(g(x)(q(x) - q'(x))$ = bậc $g(x)$ + bậc $(q(x) - q'(x))$ (định lí 2).

Mặt khác theo giả thiết và định lí 1

bậc $(r(x) - r'(x)) \leqslant$ max (bậc $r(x)$, bậc $r'(x)$) < bậc $g(x) \leqslant$ bậc $g(x)$ + bậc $(q(x) - q'(x))$,

điều này mâu thuẫn với đẳng thức trên. Chú ý : nếu một trong hai đa thức $r(x)$ và $r'(x)$ bằng 0 thì ta không thể nói đến bậc của nó, nhưng điều đó không ảnh hưởng tới việc chứng minh, vì lúc đó bậc $(r(x) - r'(x))$ bằng bậc $r(x)$ nếu $r'(x) = 0$ và bằng bậc $r'(x)$ nếu $r(x) = 0$.

Còn sự tồn tại của $q(x)$ và $r(x)$ thì suy ra từ thuật toán dưới đây. Tìm $q(x)$ và $r(x)$ gọi là thực hiện phép chia $f(x)$ cho $g(x)$. Đa thức $q(x)$ gọi là *thương*, đa thức $r(x)$ là *dư* của $f(x)$ cho $g(x)$. Việc tìm thương và dư là tức khắc nếu bậc $f(x)$ < bậc $g(x)$. Ta

chỉ cần đặt $q(x) = 0$, $r(x) = f(x)$. Trong trường hợp trái lại ta dùng nhận xét sau đây :

Nếu ta biết một đa thức $h(x)$ sao cho

$$f_1(x) = f(x) - g(x)\,h(x)$$

có bậc thực sự bé hơn bậc của $f(x)$ thì bài toán trở thành đơn giản hơn : tìm thương và dư của $f_1(x)$ cho $g(x)$. Thật vậy, nếu $f_1(x) = g(x)\,q_1(x) + r_1(x)$, ta suy ra

$$f(x) = g(x)\,(h(x) + q_1(x)) + r_1(x)$$

từ đó

$$q(x) = h(x) + q_1(x),\ r(x) = r_1(x)$$

Trong thực tiễn, với

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_0$$

$g(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_0$, $b_n \neq 0$ và $n \leq m$ ta nhận xét rằng, lấy $h(x) = \dfrac{a_m}{b_n}\,x^{m-n}$, thì đa thức $f_1(x) = f(x) - g(x)\,h(x)$ có bậc thực sự bé hơn bậc của $f(x)$, hoặc $f_1(x)$ bằng 0. Trong trường hợp $f_1(x) = 0$, dư $r(x) = 0$ và thương $q(x) = h(x)$. Nếu $f_1(x) \neq 0$ ta tiếp tục với $f_1(x)$, ta được $f_2(x)$... Dãy đa thức $f_1(x)$, $f_2(x)$... có bậc giảm dần. Khi ta đi đến một đa thức có bậc thực sự bé hơn bậc của $g(x)$ thì đa thức đó chính là dư $r(x)$. Nếu một đa thức của dãy bằng 0 thì dư $r(x) = 0$. Để nhìn thấy rõ hơn ta hãy viết ra các bước mà ta đã thực hiện để được dãy $f_1(x)$, $f_2(x)$,...

$$f_1(x) = f(x) - g(x)\,h(x)$$

$$f_2(x) = f_1(x) - g(x)\,h_1(x)$$

$$\ldots\ldots\ldots\ldots$$

$$f_k(x) = f_{k-1}(x) - g(x)\,h_{k-1}(x)$$

với $f_k(x) = 0$ hoặc bậc $f_k(x) <$ bậc $g(x)$. Cộng vế với vế các đẳng thức đó lại, ta được

$$f(x) = g(x)(h(x) + h_1(x) + \ldots + h_{k-1}(x)) + f_k(x),$$

từ đó

$$q(x) = h(x) + h_1(x) + \ldots + h_{k-1}(x),\ r(x) = f_k(x).\ \blacksquare$$

Ví dụ. Trong thực tiễn để thực hiện phép chia $f(x)$ cho $g(x)$ người ta sắp đặt như sau để lập dãy $f_1(x)$, $f_2(x)$...

1) A là trường số hữu tỉ.

$$\begin{array}{l|l} -x^3 - 7x^2 + 2x - 4 & -2x^2 + 2x - 1 \\ \hline -x^3 + x^2 - \frac{1}{2}x & \frac{1}{2}x + 4 \\ \hline -8x^2 + \frac{5}{2}x - 4 & \\ -8x^2 + 8x - 4 & \\ \hline -\frac{11}{2}x & \end{array}$$

Từ đó

$$-x^3 - 7x^2 + 2x - 4 = (-2x^2 + 2x - 1)\left(\frac{1}{2}x + 4\right) - \frac{11}{2}x.$$

2) A là trường các số nguyên mod 11.

$$\begin{array}{l|l} -\bar{1}x^3 - \bar{7}x^2 + \bar{2}x - \bar{4} & -\bar{2}x^2 + \bar{2}x - \bar{1} \\ \hline -\bar{1}x^3 + \bar{1}x^2 - \bar{6}x & \bar{6}x + \bar{4} \\ \hline -\bar{8}x^2 + \bar{8}x - \bar{4} & \\ -\bar{8}x^2 + \bar{8}x - \bar{4} & \\ \hline \bar{0} & \end{array}$$

Vậy

$$-\bar{1}x^3 - \bar{7}x^2 + \bar{2}x - \bar{4} = (-\bar{2}x^2 + \bar{2}x - \bar{1})(\bar{6}x + \bar{4})$$

Từ định nghĩa 2 (ch III, §1, 2) và định lí 3 ta có tức khắc hệ quả.

Hệ quả. *$f(x)$ chia hết cho $g(x)$ khi và chỉ khi dư trong phép chia $f(x)$ cho $g(x)$ bằng 0.*

4. Nghiệm của một đa thức

Định nghĩa 3. Giả sử c là một phần tử tùy ý của vành A, $f(x) = a_0 + a_1x + ... + a_nx^n$ là một đa thức tùy ý của vành $A[x]$; phần tử

$$f(c) = a_0 + a_1c + ... + a_nc^n \in A$$

được bằng cách thay x bởi c gọi là *giá trị của $f(x)$ tại c*. Nếu $f(c) = 0$ thì c gọi là *nghiệm của $f(x)$*. Tìm nghiệm của $f(x)$ trong A gọi là *giải phương trình đại số bậc n*

$$a_nx^n + ... + a_0 = 0 \ (a_n \neq 0)$$

trong A.

Định lí 4. *Giả sử A là một trường, $c \in A$, $f(x) \in A[x]$. Dư của phép chia $f(x)$ cho $x - c$ là $f(c)$.*

Chứng minh. Nếu ta chia $f(x)$ cho $x - c$, dư hoặc bằng 0 hoặc là một đa thức bậc 0 vì bậc $(x - c)$ bằng 1. Vậy dư là một phần tử $r \in A$. Ta có

$$f(x) = (x - c)\, q(x) + r$$

Thay x bằng c, ta được

$$f(c) = 0 \cdot q(c) + r,$$

vậy $$r = f(c). \blacksquare$$

Hệ quả. *c là nghiệm của $f(x)$ khi và chỉ khi $f(x)$ chia hết cho $x - c$.*

Thực hiện phép chia

$$f(x) = a_0x^n + a_1x^{n-1} + ... + a_n$$

cho $x - c$, ta được các hệ tử của đa thức thương

$$q(x) = b_0x^{n-1} + b_1x^{n-2} + ... + b_{n-1}$$

cho bởi các công thức

$$b_o = a_o,\ b_i = a_i + cb_{i-1},\ i = 1, \ldots, n-1$$

và dư

$$r = a_n + cb_{n-1}.$$

Vì $r = f(c)$, ta suy ra một phương pháp (phương pháp Hoocne) để tính $f(c)$ bằng sơ đồ sau đây :

	a_o	a_1	...	a_{n-1}	a_n
c	b_o	b_1		b_{n-1}	r

trong đó mỗi phần tử của dòng thứ nhì được bằng cách cộng vào phần tử tương ứng của dòng thứ nhất tích của c với phần tử đứng trước dòng thứ nhì.

Định nghĩa 4. Giả sử A là một trường, $c \in A$, $f(x) \in A[x]$ và m là một số tự nhiên ≥ 1, c là *nghiệm bội cấp* m nếu và chỉ nếu $f(x)$ chia hết cho $(x - c)^m$ và $f(x)$ không chia hết cho $(x - c)^{m+1}$. Trong trường hợp $m = 1$ người ta còn gọi c là *nghiệm đơn*, $m = 2$ thì c là *nghiệm kép*.

Người ta coi một đa thức có một nghiệm bội cấp m như một đa thức có m nghiệm trùng với nhau.

5. Phần tử đại số và phần tử siêu việt

Giả sử A là một trường con của một trường K, $c \in K$ và

$$f(x) = a_o + a_1x + \ldots + a_nx^n$$

là một đa thức của vành $A[x]$. Lúc đó, vì $a_o, a_1, \ldots, a_n \in A$ nên $a_o, a_1, \ldots, a_n \in K$, do đó ta có thể coi $f(x)$ là một đa thức lấy hệ tử trong K và $f(c)$ là một phần tử thuộc K. Nếu $f(c) = 0$ thì c gọi là *nghiệm của một đa thức lấy hệ tử trong A*.

Định nghĩa 5. Giả sử A là một trường con của một trường K. Một phần tử $c \in K$ gọi là *đại số trên A* nếu c là nghiệm của một đa thức khác 0 lấy hệ tử trong A ; c gọi là *siêu việt trên A* trong trường hợp trái lại.

Như vậy bảo c là đại số trên A có nghĩa là tồn tại những phần tử $a_i \in A$ $(0 \leq i \leq n)$ không bằng không tất cả, sao cho $a_0 + a_1c + \ldots + a_nc^n = 0$.

Ví dụ. 1) Các phần tử của trường A đều đại số trên A.

2) Trong trường số thực $\mathbf{R}$, $\sqrt{2}$ là đại số trên trường số hữu tỉ $\mathbf{Q}$, x là siêu việt trên $\mathbf{Q}$. Trong trường số phức $\mathbf{C}$, mọi số phức là đại số trên trường số thực $\mathbf{R}$. Thực vậy, mọi số phức $z = a + bi$ là nghiệm của đa thức $x^2 - 2ax + a^2 + b^2$.

Giả sử A là một trường con của một trường K, $c \in K$ và $f(x) \in A[x]$. $f(c)$ gọi là một *đa thức của phần tử* c lấy hệ tử trong A. Bộ phận của K gồm các phần tử có dạng $f(c)$ kí hiệu là $A[c]$. Dễ dàng thấy $A[c]$ là một vành con của vành K, gọi là *vành đa thức của phần tử* c lấy hệ tử trong A. Ta có thể chứng minh $A[c]$ là vành con bé nhất của K chứa A và c.

Định lí 5. *Giả sử A là một trường con của một trường K và c là một phần tử của K. Nếu c là siêu việt trên A thì $A[c]$ đẳng cấu với vành đa thức $A[x]$ của ẩn x. Nếu c là đại số trên A thì $A[c]$ đẳng cấu với một vành thương của vành $A[x]$.*

Chứng minh. Xét ánh xạ

$$\varphi : A[x] \to K$$
$$f(x) \longmapsto f(c)$$

Hiển nhiên φ là một đồng cấu (vành) và $\mathrm{Im}\varphi = A[c]$.

Theo hệ quả của định lí 13 trong (ch III, §1, 5) ta có

$$A[c] = A[x] / \mathrm{Ker}\,\varphi$$

Trong trường hợp c là siêu việt trên A, $f(c) = 0$ khi và chỉ khi $f(x) = 0$. Vậy $\mathrm{Ker}\,\varphi = \{0\}$. Do đó

$$A[c] \cong A[x] / \{0\} = A[x]. \blacksquare$$

BÀI TẬP

1. Trong vành đa thức $A[x]$, (A là trường $\mathbf{Z}/3\mathbf{Z}$ các số nguyên mod 3), hãy tìm tất cả các đa thức có bậc là :

a) 2 ; b) 3 ; c) n.

2. Trong vành đa thức $\mathbf{Z}/5\mathbf{Z}[x]$ hãy thực hiện các phép nhân

$$(\bar{2}x^2 + \bar{4}x + \bar{1})(\bar{3}x^2 + \bar{1}x + \bar{2}).$$

$$(-\bar{2}x^2 + \bar{4}x + \bar{3})^2.$$

3. Trong vành đa thức $\mathbf{Z}/6\mathbf{Z}[x]$ hãy thực hiện phép nhân

$$(\bar{2}x^3 + \bar{4}x^2 + \bar{1}x)(\bar{3}x^2 + \bar{3}x + \bar{2})$$

Vành này có ước của 0 hay không ?

4. Trong vành $\mathbf{Z}/5\mathbf{Z}[x]$ hãy thực hiện phép chia

$$f(x) = -\bar{1}x^3 + \bar{2}x^2 + \bar{2}x + \bar{1}$$

cho

$$g(x) = -\bar{2}x^2 + \bar{2}x - \bar{1}.$$

5. Trong vành $\mathbf{Z}/7\mathbf{Z}[x]$ hãy xác định p để dư của phép chia $\bar{1}x^3 + \bar{p}x + \bar{5}$ cho $\bar{1}x^2 + \bar{5}x + \bar{6}$ bằng 0.

6. Trong vành $\mathbf{Q}[x]$ chứng minh rằng đa thức

$$(x+1)^{2n} - x^{2n} - 2x - 1$$

chia hết cho

a) $2x + 1$; b) $x + 1$; c) x.

7. Chứng minh rằng đa thức $x^2 + 14 \in \mathbf{Z}/15\mathbf{Z}[x]$ có 4 nghiệm trong $\mathbf{Z}/15\mathbf{Z}$.

8. Giả sử A là một trường và $f(x)$ là một đa thức bậc n của vành $A[x]$. Chứng minh $f(x)$ có không quá n nghiệm phân biệt trong A.

9. Định lí 3 có còn đúng nữa không nếu A là một vành và $g(x)$ là một đa thức có hệ tử cao nhất bằng đơn vị ?

10. Chứng minh rằng định lí 4 và hệ quả của nó còn đúng với A là một vành.

11. Chứng minh kết quả trong bài tập 8) còn đúng với A là một miền nguyên.

12. Xét đồng cấu φ trong định lí 5. Chứng minh Ker φ là một iđêan nguyên tố (ch III, §1, bài tập 14)).

§2. VÀNH ĐA THỨC NHIỀU ẨN

1. Vành đa thức nhiều ẩn

Trong §1 ta đã xây dựng vành đa thức một ẩn $A[x]$ lấy hệ tử trong một vành A. Đó là vành mà các phần tử là các dãy $(a_o, a_1, ..., a_n,...)$ trong đó các $a_i \in A$ bằng 0 tất cả trừ một số hữu hạn. Dãy (0, 1, 0,...) được kí hiệu là x. Tất nhiên nếu ta kí hiệu dãy đó là y thì ta lại kí hiệu vành đã xây dựng là $A[y]$ và gọi là vành đa thức của ẩn y. Bây giờ ta hãy định nghĩa vành đa thức của n ẩn lấy hệ tử trong một vành A bằng quy nạp như sau.

Định nghĩa 1. Giả sử A là một vành giao hoán có đơn vị. Ta đặt

$$\begin{aligned} A_1 &= A[x_1] \\ A_2 &= A_1[x_2] \\ A_3 &= A_2[x_3] \\ &\vdots \\ A_n &= A_{n-1}[x_n] \end{aligned}$$

vành $A_n = A_{n-1}[x_n]$ kí hiệu là $A[x_1, x_2, ..., x_n]$ và gọi là *vành đa thức của n ẩn* $x_1, x_2, ..., x_n$ *lấy hệ tử trong vành A*. Một phần tử của A_n gọi là một *đa thức của n ẩn* $x_1, x_2,..., x_n$ *lấy hệ tử trong vành A*, người ta kí hiệu nó bằng $f(x_1, x_2,..., x_n)$ hay $g(x_1, x_2,..., x_n)$...

Từ định nghĩa 1 ta có dãy vành

$$A_o = A \subset A_1 \subset A_2 \subset ... \subset A_n$$

trong đó A_{i-1} là vành con của A_i, $i = 1, 2,..., n$.

Bây giờ ta hãy xét vành $A_1[x_2] = A[x_1, x_2]$. Đó là vành đa thức của ẩn x_2 lấy hệ tử trong $A_1 = A[x_1]$. Vậy mỗi phần tử của $A[x_1, x_2]$ có thể viết dưới dạng

(1) $f(x_1x_2) = a_o(x_1) + a_1(x_1)x_2 + ... + a_n(x_1)x_2^n$ với các $a_i(x_1) \in A[x_1]$.

(2) $a_i(x_1) = b_{i0} + b_{i1}x_1 + ... + b_{im_i}x_1^{m_i}$, $i = 0, 1,..., n$

Vì $A[x_1, x_2]$ là một vành nên ta có phép nhân phân phối đối với phép cộng, do đó $f(x_1, x_2)$ còn có thể viết

(3) $f(x_1, x_2) = c_1x_1^{a_{11}}x_2^{a_{12}} + c_2x_1^{a_{21}}x_2^{a_{22}} + \ldots + c_mx_1^{a_{m1}}x_2^{a_{m2}}$

với các $c_i \in A$, các a_{i1}, a_{i2} là những số tự nhiên và $(a_{i1}, a_{i2}) \neq (a_{j1}, a_{j2})$ khi $i \neq j$. Các c_i gọi là các *hệ tử* và các $c_ix_1^{a_{i1}}x_2^{a_{i2}}$ gọi là các *hạng tử* của đa thức $f(x_1, x_2)$. Chẳng hạn xét đa thức $f(x_1, x_2) \in \mathbf{Z}[x_1, x_2]$ với $\mathbf{Z}$ là vành các số nguyên

$$f(x_1, x_2) = x_1^3 - 1 + (x_1 + 2)x_2 + (x_1^2 + 2x_1 - 1)x_2^2 =$$
$$= x_1^3 - 1 + x_1x_2 + 2x_2 + x_1^2x_2^3 + 2x_1x_2^3 - x_2^3$$

Đa thức $f(x_1, x_2) = 0$ khi và chỉ khi các hệ tử c_i của nó bằng 0 tất cả. Thật vậy nếu các $c_i = 0$ thì rõ ràng $f(x_1, x_2) = 0$. Đảo lại giả sử $f(x_1, x_2) = 0$. Viết $f(x_1, x_2)$ dưới dạng (1), ta được các đa thức (2) bằng 0 tất cả, tức là

$$b_{i0} = \ldots = b_{im_i} = 0 \quad i = 0, \ldots, n$$

Nhưng các $c_1, \ldots, c_m$ trong (3) chính là các $b_{i0}, \ldots, b_{im_i}$, $i = 0, \ldots, n$ do đó

$$c_1 = c_2 = \ldots = c_m = 0.$$

Bằng quy nạp ta chứng minh mỗi đa thức $f(x_1, x_2, \ldots, x_n)$ của vành $A[x_1, x_2, \ldots, x_n]$ có thể viết dưới dạng

(4) $f(x_1, x_2, \ldots, x_n) = c_1x_1^{a_{11}} \ldots x_n^{a_{1n}} + \ldots + c_mx_1^{a_{m1}} \ldots x_n^{a_{mn}}$ với các $c_i \in A$, các $a_{i1}, \ldots, a_{in}$, $i = 1, \ldots, m$, là những số tự nhiên và $(a_{i1}, \ldots, a_{in}) \neq (a_{j1}, \ldots, a_{jn})$ khi $i \neq j$. Các c_i gọi là các *hệ tử*, các $c_ix_1^{a_{i1}} \ldots x_n^{a_{in}}$ gọi là các *hạng tử* của đa thức $f(x_1, x_2, \ldots, x_n)$. Đa thức $f(x_1, x_2, \ldots, x_n) = 0$ khi và chỉ khi các hệ tử của nó bằng 0 tất cả.

Cho hai đa thức $f(x_1, \ldots, x_n)$ và $g(x_1, \ldots, x_n)$ bao giờ ta cũng có thể viết chúng dưới dạng sau đây

$$f(x_1, \ldots, x_n) = c_1x_1^{a_{11}} \ldots x_n^{a_{1n}} + \ldots + c_mx_1^{a_{m1}} \ldots x_n^{a_{mn}} \quad (5)$$

$$g(x_1, \ldots, x_n) = d_1x_1^{a_{11}} \ldots x_n^{a_{1n}} + \ldots + d_mx_1^{a_{m1}} \ldots x_n^{a_{mn}}$$

trong đó $(a_{i1}, \ldots, a_{in}) \neq (a_{j1}, \ldots, a_{jn})$ khi $i \neq j$.

Chẳng hạn, với $f(x_1, x_2) = x_1^2 + x_1x_2$ và $g(x_1, x_2) = 2x_1x_2^2 - x_1x_2 + x_2$, ta viết

$$f(x_1, x_2) = x_1^2 + 0x_1x_2^2 + x_1x_2 + 0x_2$$
$$g(x_1, x_2) = 0x_1^2 + 2x_1x_2^2 - x_1x_2 + x_2$$

Do các tính chất của các phép toán trong vành $A[x_1, \ldots, x_n]$ ta có tổng, hiệu, tích của $f(x_1, \ldots, x_n)$ và $g(x_1, \ldots, x_n)$ là

$$f(x_1, \ldots, x_n) \pm g(x_1, \ldots, x_n) = \sum_{i=1}^{m} (c_i \pm d_i) x_1^{a_{i1}} \ldots x_n^{a_{in}}$$

$$f(x_1, \ldots, x_n)\, g(x_1, \ldots, x_n) = \sum_{i,j} c_i d_j x_1^{a_{i1}+a_{j1}} \ldots x_n^{a_{in}+a_{jn}},$$
$$i = 1, \ldots, m \; ; \; j = 1, \ldots, m$$

Từ một đa thức bằng 0 khi và chỉ khi các hệ tử của nó bằng 0, ta suy ra hai đa thức $f(x_1, \ldots, x_n)$ và $g(x_1, \ldots, x_n)$ bằng nhau khi và chỉ khi chúng có các hạng tử y như nhau. Thật vậy xét hai đa thức $f(x_1, \ldots, x_n)$, $g(x_1, \ldots, x_n)$ tùy ý (5). Hiệu của chúng là

$$f(x_1, \ldots, x_n) - g(x_1, \ldots, x_n) = \sum_{i=1}^{m} (c_i - d_i) x_1^{a_{i1}} \ldots x_n^{a_{in}}$$

Do đó $f(x_1, \ldots, x_n) - g(x_1, \ldots, x_n) = 0$ khi và chỉ khi $c_i - d_i = 0$, $i = 1, \ldots, m$, tức là $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$ khi và chỉ khi $c_i = d_i$, $i = 1, \ldots, m$.

2. Bậc

Định nghĩa 2. Giả sử $f(x_1, \ldots, x_n) \in A[x_1, \ldots, x_n]$ là một đa thức khác 0

$$f(x_1, \ldots, x_n) = c_1 x_1^{a_{11}} \ldots x_n^{a_{1n}} + \ldots + c_m x_1^{a_{m1}} \ldots x_n^{a_{mn}}$$

với các $c_i \neq 0$, $i = 1, \ldots, m$ và $(a_{i1}, \ldots, a_{in}) \neq (a_{j1}, \ldots, a_{jn})$ khi $i \neq j$. Ta gọi là *bậc của đa thức* $f(x_1, \ldots, x_n)$ *đối với ẩn* x_i số mũ cao nhất mà x_i có được trong các hạng tử của đa thức

Nếu trong đa thức $f(x_1,..., x_n)$ ẩn x_1 không có mặt thì bậc của $f(x_1,..., x_n)$ đối với nó là 0.

Ta gọi là *bậc của hạng tử* $c_i x_1^{a_{i1}} ... x_n^{a_{in}}$ tổng các số mũ $a_{i1} + ... + a_{in}$ *của các ẩn*.

Bậc của đa thức (đối với toàn thể các ẩn) là số lớn nhất trong các bậc của các hạng tử của nó.

Đa thức 0 là đa thức không có bậc.

Nếu các hạng tử của $f(x_1, ..., x_n)$ có cùng bậc k thì $f(x_1,..., x_n)$ gọi là một *đa thức dẳng cấp* bậc k hay một *dạng* bậc k. Đặc biệt một dạng bậc nhất gọi là *dạng tuyến tính*, một dạng bậc hai gọi là *dạng toàn phương*, một dạng bậc ba gọi là *dạng lập phương*.

Ví dụ. Đa thức

$$f(x_1, x_2, x_3) = 2x_1x_2^3x_3^5 - x_1^2x_2 + 3x_3^9 + x_1^2 - 5x_1x_2^3x_3^2 - 4x_2^5x_3 + 6$$

có bậc là 9, nhưng đối với x_1 nó có bậc là 2.

Để sắp xếp các hạng tử của một đa thức $f(x_1, ..., x_n)$ khác 0 ta có thể sắp xếp nó theo các lũy thừa tăng hay giảm đối với một ẩn nào đó. Chẳng hạn, trong ví dụ trên ta có thể sắp xếp $f(x_1, x_2, x_3)$ theo các lũy thừa lùi của x_1.

$$f(x_1, x_2, x_3) = x_1^2(1 - x_2) + x_1(2x_2^3x_3^5 - 5x_2^3x_3^2) + 3x_3^9 - 4x_2^5x_3 + 6$$

hay theo các lũy thừa lùi của x_2

$$f(x_1, x_2, x_3) = -4x_2^5x_3 + x_2^3(2x_1x_3^5 - 5x_1x_3^2) - x_1^2x_2 + x_1^2 + 3x_3^9 + 6$$

hay theo các lũy thừa lùi của x_3

$$f(x_1, x_2, x_3) = 3x_3^9 + 2x_1x_2^3x_3^5 - 5x_1x_2^3x_3^2 - 4x_2^5x_3 - x_1^2x_2 + x_1^2 + 6.$$

Ngoài các cách sắp xếp đó, người ta còn có một cách sắp xếp gọi là *cách sắp xếp theo lối từ điển* (giống cách sắp xếp các chữ trong từ điển). Cách sắp xếp này dựa trên quan hệ thứ tự toàn phần đã xác định trong tích để các N^n ($n \geqslant 1$) với N là tập hợp các số tự nhiên (ch I, §2, bài tập 10). Ta có, theo quan hệ thứ tự đó,

$$(a_1, a_2,..., a_n) > (b_1, b_2,..., b_n)$$

nếu và chỉ nếu có một chỉ số $i = 1, 2, \ldots, n$ sao cho

$$a_1 = b_1, \ldots, a_{i-1} = b_{i-1}, a_i > b_i$$

Quay lại đa thức $f(x_1, x_2, x_3)$ trong ví dụ trên, các số mũ trong mỗi hạng tử cho ta một phần tử thuộc N^3, cụ thể ta có 7 phần tử thuộc N^3 : (1, 3, 5), (2, 1, 0), (0, 0, 9), (2, 0, 0), (1, 3, 2), (0, 5, 1), (0, 0, 0) mà theo quan hệ thứ tự đang xét chúng sắp thứ tự như sau

$$(2, 1, 0) > (2, 0, 0) > (1, 3, 5) > (1, 3, 2) > (0, 5, 1) > (0, 0, 9) > (0, 0, 0)$$

với (2, 1, 0) là phần tử lớn nhất. Viết các hạng tử tương ứng của $f(x_1, x_2, x_3)$ theo thứ tự trên

$$f(x_1, x_2, x_3) = -x_1^2x_2 + x_1^2 + 2x_1x_2^3x_3^5 - 5x_1x_2^3x_3^2 - 4x_2^5x_3 + 3x_3^9 + 6$$

gọi là sắp xếp $f(x_1, x_2, x_3)$ theo lối từ điển. Hạng tử $-x_1^2x_2$ tương ứng với phần tử lớn nhất (2, 1, 0) gọi là *hạng tử cao nhất* của $f(x_1, x_2, x_3)$.

Định lí 1. *Giả sử $f(x_1, \ldots, x_n)$ là một đa thức với hạng tử cao nhất là $cx_1^{a_1} \ldots x_n^{a_n}$, $g(x_1, \ldots, x_n)$ là một đa thức với hạng tử cao nhất là $dx_1^{b_1} \ldots x_n^{b_n}$ và giả sử $(a_1, \ldots, a_n) > (b_1, \ldots, b_n)$. Thế thì hạng tử cao nhất của đa thức tổng $f(x_1, \ldots, x_n) + g(x_1 \ldots, x_n)$ là $cx_1^{a_1} \ldots x_n^{a_n}$.*

Chứng minh. Ta hãy viết $f(x_1, \ldots, x_n)$ và $g(x_1, \ldots, x_n)$ dưới dạng

$$f(x_1, \ldots, x_n) = c_1x_1^{a_{11}} \ldots x_n^{a_{1n}} + \ldots + c_mx_1^{a_{m1}} \ldots x_n^{a_{mn}}$$

$$g(x_1, \ldots, x_n) = d_1x_1^{a_{11}} \ldots x_n^{a_{1n}} + \ldots + d_mx_1^{a_{m1}} \ldots x_n^{a_{mn}}$$

với $c_1x_1^{a_{11}} \ldots x_n^{a_{1n}} = cx_1^{a_1} \ldots x_n^{a_n}$, $d_1 = 0$

$(a_{i-1,1}, \ldots, a_{i-1,n}) > (a_{i1}, \ldots, a_{in})$ $i = 2, \ldots, m$.

Ta có $f(x_1, \ldots, x_n) + g(x_1, \ldots, x_n) =$

$$(c_1 + d_1)x_1^{a_{11}} \ldots x_n^{a_{1n}} + \ldots + (c_m + d_m)x_1^{a_{m1}} \ldots x_n^{a_{mn}}$$

Do đó hạng tử cao nhất của đa thức tổng là

$$(c_1 + d_1)x_1^{a_{11}} \ldots x_n^{a_{1n}} = cx_1^{a_1} \ldots x_n^{a_n}. \blacksquare$$

Hệ quả. *Giả sử* $f_1(x_1, \ldots, x_n), \ldots, f_k(x_1, \ldots, x_n)$ *là những đa thức có hạng tử cao nhất theo thứ tự là* $c_1x_1^{a_{11}} \ldots x_n^{a_{1n}}, \ldots, c_kx_1^{a_{k1}} \ldots x_n^{a_{kn}}$ *và giả sử*

$$(a_{11}, \ldots, a_{1n}) > (a_{21}, \ldots, a_{2n}) \ldots > (a_{k1}, \ldots, a_{kn})$$

Thế thì $c_1x_1^{a_{11}} \ldots x_n^{a_{1n}}$ *là hạng tử cao nhất của đa thức tổng* $f_1(x_1, \ldots, x_n) + \ldots + f_k(x_1, \ldots, x_n)$.

Tập hợp sắp thứ tự $\mathbf{N}^n$ còn là một vị nhóm giao hoán đối với phép cộng (ch II, §1, bài tập 5)

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$

Phép cộng này và quan hệ thứ tự trong $\mathbf{N}^n$ có tính chất

Bổ đề 1. *Nếu*

$$(a_1, \ldots, a_n) > (b_1, \ldots, b_n)$$

thì $(a_1 + c_1, \ldots, a_n + c_n) > (b_1 + c_1, \ldots, b_n + c_n)$

với mọi $(c_1, \ldots, c_n) \in \mathbf{N}^n$.

Chứng minh. Vì

$$(a_1, \ldots, a_n) > (b_1, \ldots, b_n)$$

nên có một chỉ số $i = 1, 2, \ldots, n$ sao cho

$$a_1 = b_1, \ldots, a_{i-1} = b_{i-1}, a_i > b_i$$

do đó

$$a_1 + c_1 = b_1 + c_1, \ldots, a_{i-1} + c_{i-1} = b_{i-1} + c_{i-1},$$
$$a_i + c_i > b_i + c_i. \blacksquare$$

Hệ quả. *Nếu*

$$(a_1, \ldots, a_n) > (b_1, \ldots, b_n)$$

và

$$(c_1, \ldots, c_n) > (d_1, \ldots, d_n)$$

thì $(a_1 + c_1, \ldots, a_n + c_n) > (b_1 + d_1, \ldots, b_n + d_n)$.

Chứng minh. **Theo bổ đề 1**

$$(a_1 + c_1, \ldots, a_n + c_n) > (b_1 + c_1, \ldots, b_n + c_n) > (b_1 + d_1, \ldots, b_n + d_n).$$ ■

Từ bổ đề 1 và hệ quả của nó, ta suy ra

Định lí 2. ***Giả sử*** $f(x_1, \ldots, x_n)$ ***và*** $g(x_1, \ldots, x_n)$ ***là hai đa thức khác 0 của vành*** $A[x_1, \ldots, x_n]$ ***có các hạng tử cao nhất theo thứ tự là*** $c_1 x_1^{a_{11}} \ldots x_n^{a_{1n}}$ ***và*** $d_1 x_1^{b_{11}} \ldots x_n^{b_{1n}}$. ***Nếu*** $c_1 d_1 \neq 0$ ***thì hạng tử cao nhất của đa thức tích*** $f(x_1, \ldots, x_n)\, g(x_1, \ldots, x_n)$ ***là*** $c_1 d_1 x_1^{a_{11}+b_{11}} \ldots x_n^{a_{1n}+b_{1n}}$.

Chứng minh. **Giả sử**

$$f(x_1, \ldots, x_n) = c_1 x_1^{a_{11}} \ldots x_n^{a_{1n}} + \ldots + c_l x_1^{a_{l1}} \ldots x_n^{a_{ln}}$$

$$g(x_1, \ldots, x_n) = d_1 x_1^{b_{11}} \ldots x_n^{b_{1n}} + \ldots + d_m x_1^{a_{m1}} \ldots x_n^{a_{mn}}$$

đã được sắp xếp theo lối từ điển. Điều đó có nghĩa là

$(a_{11}, \ldots, a_{1n}) > (a_{i1}, \ldots, a_{in})$ **với mọi** $i = 2, \ldots, l$

và $(b_{11}, \ldots, b_{1n}) > (b_{j1}, \ldots, b_{jn})$ **với mọi** $j = 2, \ldots, m$.

Ta hãy chứng minh

$$c_1 d_1 x_1^{a_{11}+b_{11}} \ldots x_n^{a_{1n}+b_{1n}}$$

là hạng tử cao nhất của đa thức tích

$$f(x_1, \ldots, x_n)\, g(x_1, \ldots, x_n).$$

Nhân $f(x_1, \ldots, x_n)$ **với** $g(x_1, \ldots, x_n)$ **ta được**

$$f(x_1, \ldots, x_n)\, g(x_1, \ldots, x_n) = \sum_{i,j} c_i d_j x_1^{a_{i1}+b_{j1}} \ldots x_n^{a_{in}+b_{jn}}$$

$$i = 1, \ldots, l$$

$$j = 1, \ldots, m$$

Mỗi hạng tử $c_i d_j x_1^{a_{i1}+b_{j1}} \ldots x_n^{a_{in}+b_{jn}}$ **cho ta phần tử**

$$(a_{i1} + b_{j1}, \ldots, a_{in} + b_{jn}) \in \mathbf{N}^n$$

Theo bổ đề 1 và hệ quả của nó, ta có các bất đẳng thức

$$(a_{11} + b_{11}, \ldots, a_{1n} + b_{1n}) > (a_{11} + b_{j1}, \ldots, a_{1n} + b_{jn})$$

$$j = 2, \ldots, m$$

$$(a_{11} + b_{11}, \ldots, a_{1n} + b_{1n}) > (a_{i1} + b_{11}, \ldots, a_{in} + b_{1n}),$$

$$i = 2, \ldots, l$$

$$(a_{11} + b_{11}, \ldots, a_{1n} + b_{1n}) > (a_{i1} + b_{j1}, \ldots, a_{in} + b_{jn}),$$

$$i = 2, \ldots, l \; ; \; j = 2, \ldots, m$$

Vậy hạng tử

$$c_1 d_1 x_1^{a_{11}+b_{11}} \ldots x_n^{a_{1n}+b_{1n}}$$

chính là hạng tử cao nhất của đa thức tích. ■

Hệ quả. *Nếu A là một miền nguyên thì $A[x_1, \ldots, x_n]$ cũng vậy.*

3. Đa thức đối xứng

Giả sử A là một vành giao hoán có đơn vị. Trước hết ta hãy xét vành đa thức 2 ẩn $A[x_1, x_2]$. Trong vành này ta chú ý tới hai đa thức đặc biệt sau đây

$$f(x_1, x_2) = x_1 + x_2, \; g(x_1, x_2) = x_1 x_2 .$$

Các đa thức này có tính chất : nếu ta thay x_1 bằng x_2 và x_2 bằng x_1 thì đa thức không thay đổi

$$f(x_1, x_2) = x_1 + x_2 = x_2 + x_1 = f(x_2, x_1)$$
$$g(x_1, x_2) = x_1 x_2 = x_2 x_1 = g(x_2, x_1)$$

Trong vành $A[x_1, x_2]$ không phải chỉ có hai đa thức đó có tính chất như vậy, chẳng hạn đa thức

$$\varphi(x_1, x_2) = x_1^3 + x_2^3 - x_1 x_2$$

cũng cho ta

$$\varphi(x_1, x_2) = \varphi(x_2, x_1)$$

Một cách tổng quát

Định nghĩa 3. Giả sử A là một vành giao hoán có đơn vị, $f(x_1, ..., x_n)$ là một đa thức của vành $A[x_1, ..., x_n]$. Ta bảo $f(x_1, ..., x_n)$ là một *đa thức đối xứng của n ẩn* nếu

$$f(x_1, x_2, ..., x_n) = f(x_{\tau(1)}, x_{\tau(2)}, ..., x_{\tau(n)})$$

với mọi phép thế

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

$f(x_{\tau(1)}, ..., x_{\tau(n)})$ suy ra từ $f(x_1, ..., x_n)$ bằng cách thay trong $f(x_1, ..., x_n)$ x_1 bởi $x_{\tau(1)}, ..., x_n$ bởi $x_{\tau(n)}$.

Ví dụ. Trong vành $Z[x_1, x_2, x_3]$ đa thức

$$f(x_1, x_2, x_3) = x_1^2x_2 + x_2^2x_3 + x_3^2x_1 + x_1x_2^2 + x_2x_3^2 + x_3x_1^2 + 2x_1x_2x_3$$

là đối xứng. Thật vậy ta thấy ngay rằng

$$f(x_1, x_2, x_3) = f(x_2, x_3, x_1) = f(x_3, x_1, x_2) = f(x_2, x_1, x_3) = f(x_3, x_2, x_1) = f(x_1, x_3, x_2).$$

Muốn có $f(x_3, x_2, x_1)$ chẳng hạn, ta thay x_1 bằng x_3, x_2 bằng x_2, x_3 bằng x_1 trong $f(x_1, x_2, x_3)$, ta được

$$f(x_3, x_2, x_1) = x_3^2x_2 + x_2^2x_1 + x_1^2x_3 + x_3x_2^2 + x_2x_1^2 + x_1x_3^2 + 2x_3x_2x_1,$$

do đó $$f(x_1, x_2, x_3) = f(x_3, x_2, x_1).$$

Định lí 3. *Bộ phận gồm các đa thức đối xứng của vành $A[x_1, ..., x_n]$ là một vành con của vành $A[x_1, ..., x_n]$.*

Chứng minh. Giả sử $f(x_1, ..., x_n)$ và $g(x_1, ..., x_n)$ là những đa thức đối xứng, nghĩa là

$$f(x_1, ..., x_n) = f(x_{\tau(1)}, ..., x_{\tau(n)})$$

và

$$g(x_1, ..., x_n) = g(x_{\tau(1)}, ..., x_{\tau(n)})$$

với mọi phép thế τ. Thế thì

$$f(x_1, ..., x_n) - g(x_1, ..., x_n) =$$

$$f(x_{\tau(1)}, ..., x_{\tau(n)}) - g(x_{\tau(1)}, ..., x_{\tau(n)}) ;$$

$$f(x_1, ..., x_n)\, g(x_1, ..., x_n) =$$

$$f(x_{\tau(1)}, ..., x_{\tau(n)})\, g(x_{\tau(1)}, ..., x_{\tau(n)})$$

với mọi phép thế τ. ■

Các phần tử của A là những đa thức đối xứng đặc biệt. Thật vậy mọi phần tử $a \in A$ có thể viết

$$a = a x_1^0 x_2^0 \dots x_n^0 .$$

Mọi đa thức đối xứng $f(x_1, ..., x_n) \notin A$ nhất thiết phải chứa tất cả n ẩn và phải có cùng một bậc đối với mỗi ẩn đó : thật vậy nếu $f(x_1, ..., x_n)$ có một hạng tử trong đó chứa một ẩn x_i với số mũ là k, thì nó cũng có hạng tử suy ra từ hạng tử ấy bằng cách thay thế x_i bởi x_j , tức là hạng tử chứa x_j với cùng số mũ k.

Các đa thức sau đây

$$\sigma_1 = x_1 + x_2 + \dots + x_n$$

$$\sigma_2 = x_1 x_2 + x_1 x_3 + \dots + x_{n-1} x_n$$

$$\sigma_3 = x_1 x_2 x_3 + x_1 x_2 x_4 + \dots + x_{n-2} x_{n-1} x_n$$

$$\dots$$

$$\sigma_{n-1} = x_1 x_2 \dots x_{n-1} + x_1 x_2 \dots x_{n-2} x_n + \dots x_2 x_3 \dots x_n$$

$$\sigma_n = x_1 x_2 \dots x_n$$

cũng là những đa thức đối xứng, gọi là các *đa thức đối xứng cơ bản*. Chúng đóng một vai trò quan trọng trong lí thuyết các đa thức đối xứng do định lí dưới đây. Trước khi đề cập tới định

lí đó, ta hãy đưa vào kí hiệu sau đây. Giả sử $g(x_1, ..., x_n)$ là một đa thức của $A[x_1, ..., x_n]$, phần tử của $A[x_1, ..., x_n]$ có được bằng cách thay trong $g(x_1, ..., x_n)$: x_1 bởi σ_1, x_2 bởi σ_2, ..., x_n bởi σ_n gọi là một đa thức của các đa thức đối xứng cơ bản, kí hiệu là $g(\sigma_1, ..., \sigma_n)$. Chẳng hạn với $n = 2$ và $g(x_1, x_2) = x_1^2 - x_2$ thì $g(\sigma_1, \sigma_2) = \sigma_1^2 - \sigma_2$. Vì $\sigma_1, ..., \sigma_n$ là những đa thức đối xứng nên $g(\sigma_1, ..., \sigma_n)$ cũng là một đa thức đối xứng theo định lí 3. Chẳng hạn

$$g(\sigma_1, \sigma_2) = \sigma_1^2 - \sigma_2 = (x_1 + x_2)^2 - x_1x_2 = x_1^2 + x_1x_2 + x_2^2$$

là một đa thức đối xứng của x_1 và x_2. Như vậy, mọi đa thức của các đa thức đối xứng cơ bản $\sigma_1, ..., \sigma_n$ là một đa thức đối xứng của n ẩn $x_1, ..., x_n$. Điều đảo lại cũng đúng, nó là nội dung của định lí 4 sau đây, dựa trên các bổ đề :

Bổ đề 2. *Giả sử $f(x_1, ..., x_n)$ là một đa thức đối xứng khác 0 và $ax_1^{a_1}x_2^{a_2}...x_n^{a_n}$ là hạng tử cao nhất của nó. Thế thì $a_1 \geq a_2 \geq ... \geq a_n$.*

Chứng minh. Ta phải chứng minh $a_{i-1} \geq a_i$ với mọi $i = 2, ..., n$. Vì $f(x_1, ..., x_n)$ là đối xứng, nên $f(x_1, ..., x_n)$ phải chứa hạng tử $ax_1^{a_1}...x_{i-1}^{a_i}x_{i-1}^{a_{i-1}}...x_n^{a_n}$ suy ra từ hạng tử $ax_1^{a_1}...x_{i-1}^{a_{i-1}}x_i^{a_i}...x_n^{a_n}$ bằng cách thay x_{i-1} bởi x_i và x_i bởi x_{i-1}. Nếu $a_i > a_{i-1}$ thì

$$(a_1, ..., a_{i-2}, a_i, a_{i-1}, ..., a_n) > (a_1, ..., a_{i-2}, a_{i-1}, a_i, ..., a_n)$$

do đó

$$ax_1^{a_1}...x_{i-1}^{a_i}x_i^{a_{i-1}}...x_n^{a_n}$$

không phải là hạng tử cao nhất, mâu thuẫn với giả thiết. ■

Bổ đề 3. *Giả sử $a_1, ..., a_n$ là những số tự nhiên sao cho*

$$a_1 \geq a_2 \geq ... \geq a_n$$

Thế thì đa thức

$$f(x_1, ..., x_n) = \sigma_1^{a_1 - a_2} \sigma_2^{a_2 - a_3} ... \sigma_{n-1}^{a_{n-1} - a_n} \sigma_n^{a_n}$$

trong đó $\sigma_1, ..., \sigma_n$ *là các đa thức đối xứng cơ bản, có hạng tử cao nhất là*

$$x_1^{a_1} x_2^{a_2} ... x_n^{a_n}$$

Chứng minh. Các hạng tử cao nhất của $\sigma_1, \sigma_2, ..., \sigma_{n-1}, \sigma_n$ theo thứ tự là

$$x_1, x_1 x_2, ..., x_1 x_2 ... x_{n-1}, x_1 x_2 ... x_n .$$

Áp dụng định lí 2 ta có hạng tử cao nhất của $f(x_1, ..., x_n)$ là

$$x_1^{a_1 - a_2} (x_1 x_2)^{a_2 - a_3} ... (x_1 x_2 ... x_{n-1})^{a_{n-1} - a_n} (x_1 x_2 ... x_n)^{a_n} =$$

$$= x_1^{a_1} x_2^{a_2} ... x_n^{a_n}. \blacksquare$$

Bổ đề 4. *Giả sử* a_1 *là một số tự nhiên. Bộ phận* M *của* $\mathbf{N}^n$, *với* $\mathbf{N}$ *là tập hợp các số tự nhiên, gồm các phần tử*

$$(t_1, t_2, ..., t_n)$$

sao cho $$a_1 \geqslant t_1 \geqslant t_2 \geqslant ... \geqslant t_n$$

là hữu hạn.

Chứng minh. Gọi L là tập hợp hữu hạn gồm các số tự nhiên 0, 1, ..., a_1 . Hiển nhiên L^n hữu hạn và $M \subset L^n$, do đó M hữu hạn. $\blacksquare$

Bổ đề 5. *Giả sử* $g(\sigma_1, ..., \sigma_n)$ *là một đa thức của các đa thức đối xứng cơ bản*

$$g(\sigma_1, ..., \sigma_n) = c_1 \sigma_1^{a_{11}} ... \sigma_n^{a_{1n}} + ... + c_m \sigma_1^{a_{m1}} ... \sigma_n^{a_{mn}}$$

trong đó $c_i \neq 0$; $i = 1, ..., m$, *và* $(a_{i1}, ..., a_{in}) \neq (a_{j1}, ..., a_{jn})$ $i \neq j$. *Thế thì* $g(\sigma_1, ..., \sigma_n) \neq 0$.

Chứng minh. Thay σ_1 bằng $x_1 + x_2 + ... + x_n$, ..., σ_n bằng $x_1x_2 ... x_n$ trong $g(\sigma_1, ..., \sigma_n)$ ta được một đa thức của các ẩn $x_1, x_2, ..., x_n$:

$$g(x_1 + x_2 + ... + x_n, ..., x_1x_2 ... x_n) = f(x_1, ..., x_n) =$$

$$= \sum_{i=1}^{m} f_i(x_1, ..., x_n)$$

với

$$f_i(x_1, ..., x_n) = c_i(x_1 + x_2 + ... + x_n)^{a_{i1}} ... (x_1x_2 ... x_n)^{a_{in}}$$

$$i = 1, 2, ..., m.$$

Hạng tử cao nhất của đa thức $f_i(x_1, ..., x_n)$ theo định lí 2 là

$$c_i x_1^{a_{i1}} (x_1x_2)^{a_{i2}} ... (x_1x_2 ... x_n)^{a_{in}} = c_i x_1^{k_{i1}} x_2^{k_{i2}} ... x_n^{k_{in}}$$

với $a_{i1} + a_{i2} + ... + a_{in} = k_{i1}$

$a_{i2} + ... + a_{in} = k_{i2}$

. . . . . .

$a_{in} = k_{in}$

Hạng tử cao nhất của mỗi đa thức $f_i(x_1, ..., x_n)$ cho ta phần tử $(k_{i1}, k_{i2}, ..., k_{in}) \in \mathbb{N}^n$. Ta có

$$(k_{i1}, k_{i2}, ..., k_{in}) \neq (k_{j1}, k_{j2}, ..., k_{jn}) \text{ khi } i \neq j$$

vì nếu

$$(k_{i1}, k_{i2}, ..., k_{in}) = (k_{j1}, k_{j2}, ..., k_{jn}) \text{ với } i \neq j$$

thì $a_{i1} = k_{i1} - k_{i2} = k_{j1} - k_{j2} = a_{j1}$

$a_{i2} = k_{i2} - k_{i3} = k_{j2} - k_{j3} = a_{j2}$

. . . . . .

$a_{in} = k_{in} = k_{jn} = a_{jn}$

với $i \neq j$, mâu thuẫn với giả thiết. Vì $\mathbf{N}^n$ sắp thứ tự toàn phần nên bộ phận hữu hạn gồm các phần tử $(k_{i1}, k_{i2}, ..., k_{in})$ $i = 1, 2, ..., m$ có phần tử lớn nhất, chẳng hạn $(k_{11}, k_{12}, ..., k_{1n})$ là phần tử lớn nhất. Theo hệ quả của định lí 1, $c_1 x_1^{k_{11}} ... x_n^{k_{1n}}$ là hạng tử cao nhất của $f(x_1, ..., x_n)$. Vậy

$$g(\sigma_1, ..., \sigma_n) = f(x_1, ..., x_n) \text{ là khác 0. } \blacksquare$$

Hệ quả. *Giả sử*

$$h(x_1, ..., x_n) = c_1 x_1^{a_{11}} ... x_n^{a_{1n}} + ... + c_m x_1^{a_{m1}} ... x_n^{a_{mn}}$$

và

$$h'(x_1, ..., x_n) = c'_1 x_1^{a_{11}} ... x_n^{a_{1n}} + ... + c'_m x_1^{a_{m1}} ... x_n^{a_{mn}}$$

là hai đa thức trong đó $(a_{i1}, ..., a_{in}) \neq (a_{j1}, ..., a_{jn})$ *khi* $i \neq j$, *sao cho*

$$h(\sigma_1, ..., \sigma_n) = h'(\sigma_1, ..., \sigma_n) ;$$

thế thì $\quad c_i = c'_i, \; i = 1, 2, ..., m.$

Chứng minh. Giả sử có $c_1 \neq c'_1$. Đặt

$$g(\sigma_1, ..., \sigma_n) = h(\sigma_1, ..., \sigma_n) - h'(\sigma_1, ..., \sigma_n) =$$

$$= (c_1 - c'_1) \sigma_1^{a_{11}} ... \sigma_n^{a_{1n}} + ... + (c_m - c'_m) \sigma_1^{a_{m1}} ... \sigma_n^{a_{mn}} .$$

Vì $c_1 \neq c'_1$, nên $c_1 - c'_1 \neq 0$. Theo bổ đề 5 :

$$g(\sigma_1, ..., \sigma_n) \neq 0$$

Nhưng theo giả thiết $g(\sigma_1, ..., \sigma_n) = 0$, mâu thuẫn. $\blacksquare$

Định lí 4. *Giả sử* $f(x_1, x_2, ..., x_n) \in A[x_1, x_2, ..., x_n]$ *là một đa thức đối xứng khác 0. Thế thì có một và chỉ một đa thức*

$$h(x_1, x_2, ..., x_n) \in A[x_1, x_2, ..., x_n]$$

sao cho $\quad f(x_1, x_2, ..., x_n) = h(\sigma_1, \sigma_2, ..., \sigma_n)$

trong đó $\sigma_1, \sigma_2, ..., \sigma_n$ *là các đa thức đối xứng cơ bản.*

Chứng minh. Ta hãy sắp xếp $f(x_1, ..., x_n)$ theo lối từ điển, giả sử

$$\alpha x_1^{a_1} x_2^{a_2} ... x_n^{a_n}$$

là hạng tử cao nhất của $f(x_1, ..., x_n)$. Theo bổ đề 2, ta có

$$a_1 \geqslant a_2 \geqslant ... \geqslant a_n$$

Bổ đề 3 cho ta biết đa thức

$$\alpha \sigma_1^{a_1 - a_2} \sigma_2^{a_2 - a_3} ... \sigma_{n-1}^{a_{n-1} - a_n} \sigma_n^{a_n}$$

cũng có hạng tử cao nhất là

$$\alpha x_1^{a_1} x_2^{a_2} ... x_n^{a_n} .$$

Xét hiệu

$$f_1(x_1, ..., x_n) = f(x_1, ..., x_n) - \alpha \sigma_1^{a_1 - a_2} \sigma_2^{a_2 - a_3} ... \sigma_n^{a_n}$$

Nếu $f_1(x_1, ..., x_n) \neq 0$, ta hãy sắp xếp nó theo lối từ điển và giả sử

$$\beta x_1^{b_1} x_2^{b_2} ... x_n^{b_n}$$

là hạng tử cao nhất của nó.

Theo định lí 3 : $f_1(x_1, ..., x_n)$ cũng là một đa thức đối xứng, và do đó theo bổ đề 2

$$b_1 \geqslant b_2 \geqslant ... \geqslant b_n .$$

Mặt khác, từ biểu thức của hiệu hai đa thức (mục 1), ta có

$$(a_1, a_2, ..., a_n) > (b_1, b_2, ..., b_n)$$

do đó

$$a_1 \geqslant b_1 .$$

Xét hiệu

$$f_2(x_1, ..., x_n) = f_1(x_1, ..., x_n) - \beta \sigma_1^{b_1 - b_2} \sigma_2^{b_2 - b_3} ... \sigma_n^{b_n}$$

Nếu $f_2(x_1, ..., x_n) \neq 0$, ta hãy sắp xếp nó theo lối từ điển và giả sử

$$\gamma x_1^{c_1} \dots x_n^{c_n}$$

là hạng tử cao nhất của nó ; cũng lí luận như đối với $f_1(x_1, ..., x_n)$ ta được

$$c_1 \geqslant c_2 \geqslant \dots \geqslant c_n$$

với $$(b_1, b_2, ..., b_n) > (c_1, c_2, ..., c_n) .$$

Quá trình đó không thể dài ra vô tận, vì các phần tử $(a_1, ..., a_n)$, $(b_1, ..., b_n)$, $(c_1, ..., c_n)$ ... mà ta được là những phần tử của tập hợp M hữu hạn trong bổ đề 4. Vậy quá trình hẳn phải chấm dứt, tức là sau một số hữu hạn bước ta sẽ phải được

$$0 = f_k(x_1, ..., x_n) - \lambda \sigma_1^{l_1 - l_2} \sigma_2^{l_2 - l_3} \dots \sigma_n^{l_n} .$$

Ta suy ra từ đó rằng

$$f(x_1, x_2, ..., x_n) = \alpha \sigma_1^{a_1 - a_2} \sigma_2^{a_2 - a_3} \dots \sigma_n^{a_n} + \beta \sigma_1^{b_1 - b_2} \sigma_2^{b_2 - b_3} \dots$$

$$\dots \sigma_n^{b_n} + \dots + \lambda \sigma_1^{l_1 - l_2} \sigma_2^{l_2 - l_3} \dots \sigma_n^{l_n} .$$

Vậy đa thức $h(x_1, x_2, ..., x_n)$ cần tìm là đa thức

$$h(x_1, x_2, ..., x_n) = \alpha x_1^{a_1 - a_2} x_2^{a_2 - a_3} \dots x_n^{a_n} + \beta x_1^{b_1 - b_2} x_2^{b_2 - b_3} \dots$$

$$\dots x_n^{b_n} + \dots + \lambda x_1^{l_1 - l_2} x_2^{l_2 - l_3} \dots x_n^{l_n} .$$

Giả sử có một đa thức

$$h'(x_1, ..., x_n)$$

sao cho $$h'(\sigma_1, ..., \sigma_n) = f(x_1, ..., x_n).$$

Thế thì

$$h(\sigma_1, ..., \sigma_n) = h'(\sigma_1, ..., \sigma_n).$$

Áp dụng hệ quả của bổ đề 5 ta có

$$h(x_1, ..., x_n) = h'(x_1, ..., x_n). \blacksquare$$

Phép chứng minh của định lí 4 không những cho ta biết sự tồn tại và duy nhất của đa thức $h(x_1, ..., x_n)$, nó còn cho ta một phương pháp thuận tiện để thành lập $h(x_1, ..., x_n)$. Việc tìm đa thức $h(x_1, ..., x_n)$ sao cho $f(x_1, ..., x_n) = h(\sigma_1, ..., \sigma_n)$ gọi là biểu thị đa thức đối xứng $f(x_1, ..., x_n)$ qua các đa thức đối xứng cơ bản $\sigma_1, ..., \sigma_n$.

Ví dụ. Trong vành đa thức $Z[x_1, x_2, x_3]$ với hệ số nguyên hãy biểu thị đa thức đối xứng

$$x_1^3 + x_2^3 + x_3^3 + 2x_1x_2 + 2x_1x_3 + 2x_2x_3$$

qua các đa thức đối xứng cơ bản $\sigma_1, \sigma_2, \sigma_3$.

Trước hết ta nhận xét rằng

$$2x_1x_2 + 2x_1x_3 + 2x_2x_3 = 2\sigma_2$$

Vậy chỉ cần xét đa thức đối xứng

$$f(x_1, x_2, x_3) = x_1^3 + x_2^3 + x_3^3 .$$

Hạng tử cao nhất của nó là $x_1^3 = x_1^3x_2^0x_3^0$. Theo định lí 4 ta lập đa thức

$$f_1(x_1, x_2, x_3) = f(x_1, x_2, x_3) - \sigma_1^{3-0}\sigma_2^{0-0}\sigma_3^0$$

$$= x_1^3 + x_2^3 + x_3^3 - (x_1 + x_2 + x_3)^3$$

$$= -(3x_1^2x_2 + 3x_1^2x_3 + 3x_1x_2^2 + 3x_1x_3^2 + 3x_2^2x_3 + 3x_2x_3^2 + 6x_1x_2x_3).$$

Vẫn theo định lí 4, ta lại sắp xếp nó theo lối từ điển và tìm hạng tử cao nhất của $f_1(x_1, x_2, x_3)$. Nhưng trong trường hợp cụ thể này ta nhận xét rằng

$$x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2 =$$

$$= (x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3) - 3x_1x_2x_3$$

Do đó $f_1(x_1, x_2, x_3) = -3\sigma_1\sigma_2 + 3\sigma_3$.

Cuối cùng

$$f(x_1, x_2, x_3) = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$$

và

$$x_1^3 + x_2^3 + x_3^3 + 2x_1x_2 + 2x_1x_3 + 2x_1x_3 + 2x_2x_3 =$$

$$= \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 + 2\sigma_2 .$$

Trong thực tiễn người ta còn đưa ra một số nhận xét để việc biểu diễn được nhanh chóng hơn. Ta hãy xét trước hết một đa thức đối xứng đẳng cấp $f(x_1, ..., x_n) \in A[x_1, ..., x_n]$ có hạng tử cao nhất là

$$a x_1^{a_1} x_2^{a_2} ... x_n^{a_n} .$$

Vậy bậc của $f(x_1, ..., x_n)$ là $a_1 + a_2 + ... + a_n$. Vì các đa thức đối xứng cơ bản $\sigma_1, \sigma_2, ..., \sigma_n$ là đẳng cấp có bậc theo thứ tự là 1, 2, ..., n, nên đa thức tích

$$a \sigma_1^{a_1 - a_2} \sigma_2^{a_2 - a_3} ... \sigma_n^{a_n}$$

cũng đẳng cấp và có bậc là

$$a_1 - a_2 + 2(a_2 - a_3) + ... + na_n = a_1 + a_2 + ... + a_n .$$

Do đó

$$f_1(x_1, x_2, ..., x_n) = f(x_1, x_2, ..., x_n) - a \sigma_1^{a_1 - a_2} \sigma_2^{a_2 - a_3} ... \sigma_n^{a_n}$$

cũng đẳng cấp và có bậc là $a_1 + a_2 + ... + a_n$ nếu nó khác 0. Sắp xếp $f_1(x_1, ..., x_n)$ theo lối từ điển và giả sử $\beta x_1^{b_1} ... x_n^{b_n}$ là hạng tử cao nhất của nó thế thì

$$b_1 + b_2 + ... + b_n = a_1 + a_2 + ... + a_n$$

và $$(a_1, a_2, ..., a_n) > (b_1, b_2, ..., b_n) .$$

Theo định lí 4 ta có một dãy hữu hạn phần tử của $\mathbf{N}^n$

$$(6) \quad (a_1, ..., a_n) > (b_1, ..., b_n) > (c_1, ..., c_n) > ...$$

thỏa mãn tính chất

$$a_1 \geqslant \ldots \geqslant a_n$$

$$(7) \quad b_1 \geqslant \ldots \geqslant b_n$$

. . .

và trong trường hợp ở đây

$$(8)\ a_1 + \ldots + a_n = b_1 + \ldots + b_n = \ldots$$

Do có thêm tính chất (8) nên số phần tử của dãy (6) giảm đi nhiều. Tập hợp các phần tử của dãy (6) là một bộ phận của tập hợp hữu hạn

$$M = \{(t_{11}, \ldots, t_{1n}), \ldots, (t_{m1}, \ldots, t_{mn})\}$$

trong đó

$$t_{i1} \geqslant t_{i2} \geqslant \ldots \geqslant t_{in}$$

và

$$t_{i1} + t_{i2} + \ldots + t_{in} = a_1 + a_2 + \ldots + a_n$$

với $i = 1, 2, \ldots, m$. Theo định lí 4, $f(x_1, \ldots, x_n)$ viết dưới dạng

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{m} \tau_i \sigma_1^{t_{i1} - t_{i2}} \sigma_2^{t_{i2} - t_{i3}} \ldots \sigma_n^{t_{in}}$$

với $\tau_i \in A$ và $\tau_i = 0$ nếu $(t_{i1}, \ldots, t_{in})$ không có mặt trong dãy (6).

Ta hãy quay lại đa thức

$$f(x_1, x_2, x_3) = x_1^3 + x_2^3 + x_3^3 .$$

Tập hợp M ở đây là

$$M = \{(3, 0, 0), (2, 1, 0), (1, 1, 1)\}.$$

Do đó

$$f(x_1, x_2, x_3) = \tau_1 \sigma_1^{3-0} \sigma_2^{0-0} \sigma_3^{0} + \tau_2 \sigma_1^{2-1} \sigma_2^{1-0} \sigma_3^{0} +$$

$$+ \tau_3 \sigma_1^{1-1} \sigma_2^{1-1} \sigma_3^{1} = \sigma_1^3 + \tau_2 \sigma_1 \sigma_2 + \tau_3 \sigma_3 ;$$

τ_1 là hệ tử của hạng tử cao nhất của $f(x_1, x_2, x_3)$, do đó $\tau_1 = 1$. Muốn có τ_2, τ_3, người ta thay x_1, x_2, x_3 theo thứ tự bằng 1, 1, 0 ta được

$$2 = 8 + 2\tau_2$$

do đó $\tau_2 = -3$. Sau đó thay x_1, x_2, x_3 theo thứ tự bằng 1, 1, −1 ta có

$$1 = 1 + 3 - \tau_3$$

hay

$$\tau_3 = 3$$

Vậy $f(x_1, x_2, x_3) = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$

Phương pháp vừa dùng gọi là phương pháp với hệ tử bất định.

Chú ý : Không phải bao giờ phương pháp này cũng có hiệu lực nếu A là một vành hay hơn nữa là một miền nguyên, nhưng hữu hạn.

Trong trường hợp đa thức $f(x_1, \ldots, x_n)$ không phải là đẳng cấp thì ta nhận xét rằng các hạng tử cùng một cấp của nó lập thành một đa thức đối xứng đẳng cấp, do đó ta có $f(x_1, \ldots, x_n)$ là tổng của những đa thức đối xứng đẳng cấp, chẳng hạn trong ví dụ trên

$$x_1^3 + x_2^3 + x_3^3 + 2x_1x_2 + 2x_1x_3 + 2x_2x_3$$

là tổng của đa thức đối xứng đẳng cấp bậc 3

$$x_1^3 + x_2^3 + x_3^3$$

và đa thức đối xứng đẳng cấp bậc 2

$$2x_1x_2 + 2x_1x_3 + 2x_2x_3$$

Ứng dụng. Tìm các số nguyên α, β, γ sao cho

$$\alpha\beta\gamma = 6,$$
$$\alpha^3 + \beta^3 + \gamma^3 = 36,$$
$$\alpha + \beta + \gamma = 6.$$

Theo ví dụ trên ta có

$$\alpha^3 + \beta^3 + \gamma^3 = (\alpha + \beta + \gamma)^3 - 3(\alpha + \beta + \gamma)(\alpha\beta + \alpha\gamma + \beta\gamma) + 3\alpha\beta\gamma$$

Ta suy ra $\alpha\beta + \alpha\gamma + \beta\gamma = 11$.

Mặt khác xét đa thức $f(x) \in \mathbf{Z}[x]$

$$f(x) = (x - \alpha)(x - \beta)(x - \gamma).$$

Giả sử $a \in \mathbf{Z}$, ta có

$$f(a) = (a - \alpha)(a - \beta)(a - \gamma).$$

Vì $f(a) = 0$ khi và chỉ khi một trong các thừa số $a - \alpha$, $a - \beta$, $a - \gamma$ bằng 0, cho nên các nghiệm của $f(x)$ là α, β, γ. Khai triển $f(x)$ ta được

$$f(x) = x^3 - (\alpha + \beta + \gamma)x^2 + (\alpha\beta + \alpha\gamma + \beta\gamma)x - \alpha\beta\gamma$$

$$= x^3 - 6x^2 + 11x - 6$$

vì $\alpha + \beta + \gamma = 6$, $\alpha\beta + \alpha\gamma + \beta\gamma = 11$, $\alpha\beta\gamma = 6$.

Đa thức $f(x)$ có tổng các hệ số bằng 0, do đó $f(x)$ có một nghiệm là 1. Theo hệ quả của định lí 4 trong (§1, 4), $f(x)$ chia hết cho $x - 1$. Chia $f(x)$ cho $x - 1$ ta được

$$f(x) = (x - 1)(x^2 - 5x + 6).$$

Đa thức $x^2 - 5x + 6$ cho ta hai nghiệm là 2 và 3. Vậy các số nguyên α, β, γ cần tìm là 1, 2, 3.

BÀI TẬP

1. Trong vành $\mathbf{Z}[x_1, x_2, x_3]$ biểu diễn đa thức $x_1^4 + x_2^4 + x_3^4$ qua các đa thức đối xứng cơ bản.

2. Trong vành $\mathbf{Z}2\mathbf{Z}[x_1, x_2, x_3]$ biểu diễn đa thức $\bar{1}x_1^4 + \bar{1}x_2^4 + \bar{1}x_3^4$ qua các đa thức đối xứng cơ bản.

3. Giải hệ phương trình

$$\begin{cases} x + y + z = -3 \\ x^3 + y^3 + z^3 = -27 \\ x^4 + y^4 + z^4 = 113 \end{cases}$$

CHƯƠNG V

VÀNH CHÍNH VÀ VÀNH ƠCLIT

§1. VÀNH CHÍNH

1. Tính chất số học trong vành

Trong chương này chúng ta nghiên cứu các tính chất số học của vành, nghĩa là các tính chất đối với quan hệ chia hết (ch III, §1, 2).

Giả sử A là một miền nguyên mà phần tử đơn vị kí hiệu là 1. Các ước của đơn vị còn gọi là các *phần tử khả nghịch*, chúng lập thành một nhóm nhân U mà 1 là phần tử đơn vị. Chẳng hạn trong vành Z các số nguyên các phần tử khả nghịch là 1 và −1 ; trong vành đa thức K [x] với K là một trường, các đa thức bậc 0 nghĩa là các phần tử khác 0 của K là các phần tử khả nghịch.

Sau đây là một số tính chất về chia hết trong một miền nguyên mà việc chứng minh không có gì khó khăn.

Bổ đề 1. (i) $a \mid a$.

(ii) $c \mid b$ và $b \mid a$ *kéo theo* $c \mid a$.

(iii) u *khả nghịch,* $u \mid a$ *với mọi* a.

(iv) *Nếu* $b \mid u$ *với* u *khả nghịch, thì* b *khả nghịch.*

(v) *Quan hệ S xác định như sau :* $xS\,x'$ *khi* $x' = ux$ *với* u *khả nghịch, là một quan hệ tương đương ;* x *và* x' *gọi là liên kết.*

Ví dụ. 1) Hai phần tử của nhóm nhân U là liên kết.

2) Trong vành các số nguyên **Z** hai số nguyên a và $-a$ là liên kết.

3) Trong vành đa thức $K[x]$ với K là một trường, hai đa thức $f(x)$ và $af(x)$, $a \in K$ và $a \neq 0$, là liên kết.

Bổ đề 2. *x và x' là liên kết khi và chỉ khi $x \mid x'$ và $x' \mid x$.*

Giả sử $a \in A$, tập hợp các bội xa, $x \in A$, của A là một iđêan của A ký hiệu Aa hay aA, iđêan này là iđêan sinh ra bởi a, người ta gọi nó là một iđêan chính (ch III, §1, 4).

Bổ đề 3. *$a \mid b$ khi và chỉ khi $Aa \supset Ab$.*

Hệ quả. *x và x' là liên kết khi và chỉ khi $Ax = Ax'$. Đặc biệt u là khả nghịch khi và chỉ khi $Au = A$.*

Định nghĩa 1. Các phần tử liên kết với x và các phần tử khả nghịch là *các ước không thực sự* của x, còn các ước khác của x là các *ước thực sự* của x.

Ví dụ. ± 2 và ± 3 là các ước thực sự của 6, còn ± 1 và ± 6 là các ước không thực sự.

Định nghĩa 2. Giả sử x là một phần tử khác 0 và không khả nghịch của A ; x gọi là một *phần tử bất khả quy* của A nếu x không có ước thực sự.

Ví dụ. 1) Các số nguyên tố và các số đối của chúng là các phần tử bất khả quy của vành **Z**.

2) Đa thức $x^2 + 1$ là đa thức bất khả quy của vành $\mathbf{R}[x]$, **R** là trường số thực. Nhưng trong vành $\mathbf{C}[x]$ với **C** là trường số phức thì $x^2 + 1$ không phải là bất khả quy vì nó có ước thực sự chẳng hạn $x + i$ và $x - i$.

Định nghĩa 3. Nếu $c \mid a$ và $c \mid b$ thì c gọi là *ước chung* của a và b. Phần tử c gọi là *ước chung lớn nhất của a và b* nếu c là ước chung của a và b và nếu mọi ước chung của a và b là ước của c.

Từ bổ đề 2 ta có hai ước chung lớn nhất của a và b là liên kết, do đó có thể coi là bằng nhau nếu không kể nhân tử khả

nghịch. Ta cũng định nghĩa tương tự ước chung lớn nhất của nhiều phần tử.

2. Vành chính

Định nghĩa 4. Một miền nguyên A gọi là *vành chính* nếu mọi iđêan của nó là iđêan chính.

Ví dụ 1. Vành Z các số nguyên là vành chính. Thật vậy, giả sử I là một iđêan của Z. Nếu $I = \{0\}$ thì I là iđêan sinh bởi 0. Nếu $I \neq \{0\}$, giả sử a là số nguyên dương bé nhất của I và b là một phần tử tùy ý của I. Ta có thể giả sử $b \geqslant 0$, vì nếu $b < 0$ thì $-b > 0$ và $-b$ cũng thuộc I, do đó ta lấy $-b$. Lấy b chia cho a, ta được

$$b = aq + r$$

với r là dư, nên $0 \leqslant r < a$. Mặt khác $r = b - aq \in I$. Nếu $r \neq 0$ thì a không phải là số nguyên dương bé nhất của I, mâu thuẫn. Do đó $r = 0$ và $b = aq$, tức là $I = a\mathbb{Z}$ là iđêan sinh ra bởi a.

Miền nguyên A ở đây được giả sử là một vành chính. Các phần tử mà ta xét là thuộc A.

Bổ đề 4. *Ước chung lớn nhất của hai phần tử a và b bất kỳ tồn tại.*

Chứng minh. Gọi I là iđêan sinh ra bởi a và b. Các phần tử I có dạng $ax + by$ với $x, y \in A$ (ch III, §1, 4, định lí 6). Mặt khác vì A là vành chính nên I sinh ra bởi một phần tử d nào đó, phần tử d cũng thuộc I nên d có dạng

(1) $d = ax + by,\ x, y \in A$

Ta hãy chứng minh d là ước chung của a và b. Vì $a, b \in I = dA$, nên

$$a = da',\ b = db',\ a', b' \in A.$$

Do đó d là ước chung của a và b. Thêm nữa nếu c là một ước chung của a và b, tức là có $a'', b'' \in A$ sao cho $a = ca''$, $b = cb''$, thế thì (1) trở thành

$$d = c(a''x + b''y)$$

Vậy d là ước chung lớn nhất của a và b. ■

Hệ quả. *Nếu e là một ước chung lớn nhất của a và b, thì có $r, s \in A$ sao cho*

$$e = ar + bs$$

Chứng minh. Xét ước chung lớn nhất d của bổ đề 4. d và e là liên kết (mục 1), tức là có một phần tử khả nghịch u sao cho

$$e = du$$

Nhân hai vế của (1) với u

$$e = du = axu + byu = ar + bs, \ r = xu, \ s = yu. \blacksquare$$

Định nghĩa 5. *a và b là nguyên tố cùng nhau nếu chúng nhận 1 làm ước chung lớn nhất.*

Từ hệ quả của bổ đề 4 ta suy ra

Bổ đề 5. *Nếu a, b nguyên tố cùng nhau thì có $r, s \in A$ sao cho*

$$1 = ar + bs.$$

Hệ quả. *Nếu $c \mid ab$ và c, a nguyên tố cùng nhau, thì $c \mid b$.*

Chứng minh. Vì c, a nguyên tố cùng nhau nên theo bổ đề 5 có $r, s \in A$ sao cho

$$1 = ar + cs.$$

Nhân hai vế của đẳng thức với b

$$b = abr + bcs.$$

Vì $c \mid ab$ nên có $q \in A$ sao cho $ab = cq$. Do đó,

$$b = c(qr + bs)$$

tức là $c \mid b$. ■

Bổ đề 6. *Giả sử x là một phần tử bất khả quy và a là một phần tử bất kì. Thế thì hoặc $x \mid a$ hoặc x và a là nguyên tố cùng nhau.*

Chứng minh. Vì x là bất khả quy nên các ước của x là các phần tử liên kết với x và các phần tử khả nghịch. do đó một

ước chung lớn nhất của x và a chỉ có thể là một phần tử liên kết với x hoặc một phần tử khả nghịch. Trong trường hợp thứ nhất ta có $x \mid a$, trong trường hợp thứ hai x và a là nguyên tố cùng nhau. ■

Bổ đề 7. *Giả sử x là một phần tử khác 0 và không khả nghịch. Các mệnh đề sau đây là tương đương :*

a) *x là bất khả quy*

b) *$x \mid ab$ thì $x \mid a$ hoặc $x \mid b$.*

Chứng minh. a) kéo theo b). Theo bổ đề 6 ta có hoặc $x \mid a$ hoặc x và a nguyên tố cùng nhau. Nếu x và a nguyên tố cùng nhau theo hệ quả của bổ đề 5 ta có $x \mid b$.

b) kéo theo a). Giả sử a là một ước của x, thế thì có $b \in A$ sao cho

$$x = ab.$$

Vì $x \mid x$, nên $x \mid ab = x$. Theo b) $x \mid a$ hoặc $x \mid b$. Nếu $x \mid a$ thì kết hợp với $a \mid x$ ta có x và a liên kết. Nếu $x \mid b$ thì kết hợp với $b \mid x$ ta có $x = ub$, u là khả nghịch. Do đó

$$x = ab = ub.$$

Nhưng $x \neq 0$, nên $b \neq 0$, do đó ta suy ra $a = u$ vì A là miền nguyên. Cho nên một ước a của x chỉ có thể hoặc là liên kết với x hoặc là khả nghịch, vậy x là bất khả quy. ■

Bổ đề 8. *Trong một họ không rỗng bất kỳ F những iđêan của A sắp thứ tự theo quan hệ bao hàm, có một iđêan M của họ F là tối đại trong F* (ch I, §2, 3, định nghĩa 7).

Chứng minh. Giả sử I_0 là một iđêan của F. Hoặc I_0 là tối đại trong F và như vậy là xong, hoặc có một iđêan I_1 của F sao cho $I_1 \neq I_0$ và $I_1 \supset I_0$. Nếu I_1 là tối đại trong F thì thế là xong, nếu không ta lại có một iđêan I_2 của F sao cho $I_2 \neq I_1$ và $I_2 \supset I_1$. Tiếp tục quá trình này, hoặc là ta được một iđêan M của F tối đại trong F, hoặc là ta được một dãy vô hạn những iđêan phân biệt trong F :

$$I_0 \subset I_1 \ldots \subset I_n \subset I_{n+1} \subset \ldots$$

Ta giả sử trường hợp sau xảy ra. Gọi I là hợp

$$I = \bigcup_{n \in N} I_n.$$

Dễ dàng thấy I là một iđêan của A. Vì A là một vành chính nên iđêan I được sinh ra bởi một phần tử $x \in I$. Theo định nghĩa của hợp, có một số tự nhiên n sao cho $x \in I_n$. Điều này kéo theo $I \subset I_n$ và do đó $I_n = I_{n+1}$, mâu thuẫn với giả thiết các iđêan của dãy là phân biệt. ■

Định lí 1. *Giả sử x là một phần tử khác 0 và không khả nghịch. Thế thì x có thể viết dưới dạng*

(2) $x = p_1 p_2 \cdots p_n$

với các p_1, $i = 1, \ldots, n$, là những phần tử bất khả quy.

Chứng minh. Gọi F là tập hợp các phần tử không khả nghịch $x \neq 0$ sao cho x không viết được dưới dạng (2). Ta hãy chứng minh $F = \emptyset$. Giả sử $F \neq \emptyset$. Ta kí hiệu bằng $\mathcal{F}$ họ các iđêan Ax với $x \in F$. Theo bổ đề 8, F có một phần tử m sao cho Am là tối đại trong $\mathcal{F}$. Trước hết m không bất khả quy, vì nếu m bất khả quy thì m có dạng (2). m không bất khả quy thì m có ước thực sự, chẳng hạn a là một ước thực sự của m, điều đó có nghĩa là có $b \in A$ sao cho

$$m = ab$$

Như vậy b cũng là một ước của m, b không thể là khả nghịch vì sẽ kéo theo a liên kết với m, b không thể liên kết với m vì sẽ kéo theo a khả nghịch, do đó b phải là ước thực sự của m. Vì a và b là những ước thực sự của m, nên theo bổ đề 3 và hệ quả của nó ta có

$$Am \subset Aa, \quad Am \neq Aa$$

và

$$Am \subset Ab, \quad Am \neq Ab$$

Do Am là tối đại trong $\mathcal{F}$ nên Aa và Ab không thuộc $\mathcal{F}$, do đó a và b không thuộc F ; a và b đều khác 0, khác khả nghịch và không thuộc F, nên a và b phải viết được dưới dạng (2)

$$a = p_1 \cdots p_i,$$
$$b = p_{i+1} \cdots p_n,$$

điều này kéo theo

$$m = ab = p_1 \cdots p_i p_{i+1} \cdots p_n,$$

mâu thuẫn với $m \in F$. ■

Định lí 2. *Giả sử*

$$x = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$$

với $p_1, \ldots, p_m, q_1, \ldots, q_n$ *là những phần tử bất khả quy. Thế thì* $m = n$, *và với một sự đánh số thích hợp ta có* $q_i = u_i p_i$, $i = 1, \ldots, m$.

Chứng minh. Theo bổ đề 7 nhân tử bất khả quy p_1 của x phải là ước của một q_i nào đó. Vì A là giao hoán nên ta có thể giả thiết rằng p_1 là ước của q_1. Nhưng q_1 là bất khả quy, nó không có ước thực sự, do đó p_1 là ước không thực sự của q_1. Thêm nữa p_1 không khả nghịch, cho nên phải có p_1 và q_1 liên kết, tức là $q_1 = u_1 p_1$ với u_1 khả nghịch. Như vậy ta được $p_1 p_2 \cdots p_m = u_1 p_1 q_2 \cdots q_n$.

Vì $p_1 \neq 0$ ta suy ra

$$p_2 \cdots p_m = u_1 q_2 \cdots q_n.$$

Theo bổ đề 7, p_2 là ước của một q_i nào đó với $i \geq 2$. Ta có thể giả thiết rằng p_2 là ước của q_2. Do đó ta được $q_2 = u_2 p_2$ với u_2 khả nghịch. Như vậy ta được

$$p_2 p_3 \cdots p_m = u_1 u_2 p_2 q_3 \cdots q_n.$$

Vì $p_2 \neq 0$ ta suy ra

$$p_3 \cdots p_m = u_1 u_2 q_3 \cdots q_n.$$

Sau khi đã lập lại quá trình đó m lần, ta được $m \leq n$ và

$$1 = u_1 u_2 \cdots u_m q_{m+1} \cdots q_n.$$

Vì q_n không khả nghịch nên ta phải có $m = n$. ■

Như vậy định lí 1 cho ta biết mọi phần tử $x \neq 0$ không khả nghịch của một vành chính đều có thể phân tích thành tích những phần tử bất khả quy và định lí 2 cho ta biết sự phân tích là duy nhất nếu không kể đến các nhân tử khả nghịch.

Ví dụ. Trong vành các số nguyên **Z** ta có

$$18 = 2 \cdot 3 \cdot 3 = (-2)3\ (-3) = 2(-3)(-3)...$$

Gọi K là trường các thương (ch III, §2, 3) của vành chính A, thế thì mọi phần tử $a \in K$ đều có thể viết dưới dạng $a = a/b$ với $a, b \in A$ nguyên tố cùng nhau. Thật vậy giả sử $a = a'/b'$, với $a', b' \in A$. Gọi $d \in A$ là ước chung lớn nhất của a' và b' ; ta có $a' = ad$ và $b' = bd$, với $a, b \in A$. Hiển nhiên a, b nguyên tố cùng nhau và $a = a/b$.

Bây giờ ta hãy chứng minh một tính chất số học quan trọng khác của vành chính ngoài tính chất đã cho ở định lí 1.

Định lí 3. *Giả sử K là trường các thương của vành chính A, $\alpha \in K$ là một* nghiệm của đa thức

$$f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_o \ (a_i \in A).$$

Thế thì $\alpha \in A$.

Chứng minh. Theo như trên ta có thể viết $\alpha = a/b$, với $a, b \in A$ nguyên tố cùng nhau. Vì $f(\alpha) = 0$ nên ta suy ra, sau khi thay α bằng a/b và nhân với b^n :

$$a^n + b(a_{n-1}a^{n-1} + ... + a_1ab^{n-2} + a_ob^{n-1}) = 0.$$

Như vậy b chia hết a^n ; vì b nguyên tố với a nên áp dụng liên tiếp hệ quả của bổ đề 5 ta được b chia hết a. Do đó b là một phần tử khả nghịch của A, tức là $b^{-1} \in A$, điều này kéo theo $\alpha = ab^{-1} \in A$. ■

Từ tính chất của vành chính cho bởi định lí 3, ta định nghĩa :

Định nghĩa 6. Giả sử K là trường các thương của một miền nguyên A. Nếu mọi $\alpha \in K$ là nghiệm của một đa thức có dạng

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_o \ (a_i \in A)$$

đều thuộc A, thì A gọi là *vành đóng nguyên*.

Khái niệm vành đóng nguyên đóng vai trò quan trọng trong lí thuyết số.

Chúng ta mới chỉ đưa ra một ví dụ về vành chính, đó là vành các số nguyên **Z**, trong khi các tính chất của vành chính rất phong phú và được sử dụng nhiều trong toán ; khó khăn cho ví dụ về vành chính nằm ở chỗ chúng ta chỉ mới nắm được những khái niệm ban đầu của môn Đại số. Bây giờ ta hãy cố gắng đưa ra một ví dụ thứ hai về vành chính.

Ví dụ 2. Xét vành các số nguyên Gaoxơ :

$$A = \mathbf{Z}[i] = \{ a + bi \mid a, b \in \mathbf{Z}\}$$

Chúng ta hãy chứng minh A là vành chính. Muốn vậy, chúng ta hãy nhắc lại khái niệm mô đun của một số phức $z = \alpha + \beta i$, $\alpha, \beta \in \mathbf{R}$, kí hiệu $|z|$: $|z| = \sqrt{\alpha^2 + \beta^2}$, ($|z|=0 \Leftrightarrow \alpha = \beta = 0$) mà trong trường hợp $z \in A$, thì $|z|^2 \in \mathbf{N}$

nghĩa là $|z|^2$ là một số tự nhiên. Thêm nữa, ta thấy ngay

$$\mathbf{Q}[i] = \{\alpha + \beta i \mid \alpha, \beta \in \mathbf{Q}\}$$

là trường các thương của A. Trên trục số, ta cũng thấy ngay cho một số hữu tỉ α, bao giờ ta cũng tìm thấy một số nguyên a sao cho $|\alpha - a| \leqslant \frac{1}{2}$. Do đó ta có thể khẳng định được rằng :

$$(*)\ \forall x \in \mathbf{Q}\ [i],\ \exists\ z \in A,\ |x - z|^2 \leqslant \frac{1}{2} < 1.$$

Bây giờ ta hãy lấy một iđêan I không tầm thường của A. Tập hợp

$$X = \{|z|^2 \mid 0 \neq z \in I\}$$

là một bộ phận khác rỗng của **N** và không chứa 0. Vì **N** sắp thứ tự tốt, nên X có phần tử bé nhất, gọi u là số phức thuộc I sao cho $|u|^2$ là số tự nhiên bé nhất của X. Xét một phần tử tùy

ý $v \in I$. Hiển nhiên $\frac{v}{u} \in \mathbf{Q}$ [i]. Theo khẳng định (*), tồn tại $z \in A$ sao cho

$$\left|\frac{v}{u} - z\right|^2 < 1$$

hay $$|v - zu|^2 < |u|^2.$$

Nhưng $u, v \in I$, $z \in A$, vậy $v - zu \in I$. Mặt khác $|u|^2$ là phần tử bé nhất của X, nên $v - zu = 0$, hay $v = zu$, hay $I = Au$. Vậy A là vành chính.

BÀI TẬP

1. Trong vành đa thức $\mathbf{R}[x]$ với $\mathbf{R}$ là trường số thực, chứng minh các đa thức $ax^2 + bx + c$ với $b^2 - 4ac < 0$ là những đa thức bất khả quy. Điều đó có còn đúng nữa không nếu coi các đa thức đó thuộc vành $\mathbf{C}[x]$ với $\mathbf{C}$ là trường số phức ?

2. Xét vành đa thức $K[x]$ với K là một trường.

a) Chứng minh rằng mọi đa thức bậc nhất của $K[x]$ đều là bất khả quy. Nếu K là một miền nguyên thì điều đó còn đúng không ?

b) Chứng minh rằng các đa thức bậc hai và bậc ba của $K[x]$ là bất khả quy khi và chỉ khi chúng không có nghiệm trong K.

3. Trong vành $\mathbf{Z}[x]$ với $\mathbf{Z}$ là vành các số nguyên, xét xem các đa thức sau đây có phải là bất khả quy hay không

$$f(x) = 2x + 5,$$

$$g(x) = x^2 + 1,$$

$$h(x) = x^2 + 2x - 2 ?$$

4. Giả sử a, b là hai phần tử của một vành chính A, nguyên tố cùng nhau. Chứng minh iđêan sinh ra bởi a và b chính là A.

5. Giả sử p là một phần tử khác 0 của một vành chính A. Chứng minh p là bất khả quy khi và chỉ khi Ap là iđêan tối đại (ch. III, §1, bài tập 14).

6. Trong một vành chính chứng minh các iđêan nguyên tố (ch III, §1, bài tập 14) khác {0} là các iđêan tối đại.

7. Chứng minh một trường là một vành chính.

8. Vành thương của một vành chính có phải là một vành chính không ?

9. Vành con của một vành chính có phải là một vành chính không ?

10. Vành Z[x] có phải là một vành chính không ?

11. Giả sử A là tập hợp các số phức có dạng $a + b\sqrt{-3}$ với $a, b \in \mathbf{Z}$.

a) Chứng minh rằng A cùng với phép cộng và phép nhân các số phức là một miền nguyên.

b) Chứng minh rằng 2, $1 + \sqrt{-3}$, $1 - \sqrt{-3}$, là những phần tử bất khả quy của A. Từ đó suy ra A không phải là vành chính.

12. Chứng minh vành

$$A = \{a + bi\sqrt{2} \mid a, b \in \mathbf{Z}\}$$

là chính

13. Giả sử a và b là hai phần tử của một vành chính có dạng phân tích như sau :

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$$

trong đó các p_i là những phần tử bất khả quy, các α_i và β_i là những số tự nhiên, $i = 1, \dots, n$. Chứng minh phần tử

$$d = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \dots p_n^{\min(\alpha_n, \beta_n)}$$

là một ước chung lớn nhất của a và b, trong đó $\min(\alpha_i, \beta_i)$ là phần tử bé nhất của $\{\alpha_i, \beta_i\}$, i = 1,..., n.

§2. VÀNH ÓCLIT (EUCLIDE)

1. Vành Oclit

Định nghĩa 1. Giả sử A là một miền nguyên, A^* là tập hợp các phần tử khác 0 của A. Miền nguyên A cùng với một ánh xạ (gọi là *ánh xạ Oclit*)

$$\delta : A^* \to \mathbf{N}$$

từ A^* đến tập hợp các số tự nhiên N thỏa mãn các tính chất :

1° Nếu $b|a$ và $a \neq 0$ thì $\delta(b) \leqslant \delta(a)$;

2° Với hai phần tử a và b tùy ý của A, $b \neq 0$, có q và r thuộc A sao cho $a = bq + r$ và $\delta(r) < \delta(b)$ nếu $r \neq 0$;

gọi là một *vành Oclit*.

Phần tử r gọi là dư. Nếu $r = 0$ thì b chia hết a và theo 1° ta có $\delta(b) \leqslant \delta(a)$. Như vậy điều kiện cần để một phần tử b là ước của một phần tử $a \neq 0$ là $\delta(b) \leqslant \delta(a)$.

Người ta bảo một vành Oclit là một vành trong đó có phép chia với dư.

Ví dụ. 1) Vành các số nguyên Z cùng với ánh xạ

$$\delta : \mathbf{Z}^* \to \mathbf{N}$$
$$n \longmapsto |n|$$

là một vành Oclit.

2) Vành đa thức $K[x]$, với K là một trường, là một vành oclit. Ánh xạ δ ở đây là ánh xạ cho tương ứng với một đa thức $f(x) \neq 0$ bậc của nó.

3) Vành các số nguyên Gaoxơ là vành Oclit với $\delta(z) = |z|^2$. Tính chất 1° của Định nghĩa 1 nhìn thấy dễ dàng, còn tính chất 2° có thể dựa vào chứng minh trong ví dụ 2 của (§1. 2).

Định lí 1. *Nếu A là một vành Oclit thì A là một vành chính.*

Chứng minh. Ta hãy chứng minh mọi iđêan của A là chính. Giả sử I là một iđêan của A. Nếu $I = \{0\}$ thì I là iđêan sinh ra bởi 0. Giả sử $I \neq \{0\}$. Gọi a là phần tử khác 0 của I sao cho $\delta(a)$ là bé nhất trong tập hợp $\delta(I^*)$, I^* là tập hợp các phần

tử khác 0 của I. Giả sử x là một phần tử tùy ý của I. Theo tính chất 2^o ta có $q, r \in A$ sao cho

$$x = aq + r$$

Vì $a, x \in I$, nên $r = x - aq \in I$. Nếu $r \neq 0$ ta có $\delta(r) < \delta(a)$, mâu thuẫn với giả thiết $\delta(a)$ là bé nhất trong $\delta(I^*)$. Vậy $r = 0$ và $I = Aa$. ■

Ta đã biết trong một vành chính, ước chung lớn nhất của hai phần tử a và b bất kỳ tồn tại (§1, 2, bổ đề 4).

Nếu A là một vành Ơclit thì không những ước chung lớn nhất của hai phần tử tồn tại, mà ta còn có thể thực hiện những phép chia (với dư) liên tiếp để có ước chung lớn nhất. Điều đó dựa trên bổ đề sau đây :

Bổ đề 1. *Giả sử A là một vành chính, a, b, q, r là những phần tử của A thỏa mãn quan hệ*

$$a = bq + r$$

Thế thì ước chung lớn nhất của a và b là ước chung lớn nhất của b và r.

Chứng minh. Gọi I là iđêan sinh ra bởi a, b và J là iđêan sinh ra bởi b, r. Từ $a = bq + r$, ta suy ra $a \in J$, do đó $I \subset J$. Từ $r = a - bq$, ta suy ra $r \in I$, do đó $J \subset I$. Vậy $I = J$. Nhưng A là một vành chính, nên tồn tại $d \in I$ sao cho $Ad = I$. Theo bổ đề 4 của (§1, 2), d là ước chung lớn nhất của a và b. Nhưng $I = J$, nên d cũng là ước chung lớn nhất của b và r. ■

Bây giờ giả sử A là một vành Ơclit và ta đặt vấn đề tìm ước chung lớn nhất của hai phần tử $a, b \in A$. Nếu $a = 0$ thì rõ ràng ước chung lớn nhất của a và b là b, vì vậy ta hãy giả sử cả a lẫn b đều khác 0. Thực hiện phép chia a cho b ta được

$$a = bq_o + r_o \text{ với } \delta(r_o) < \delta(b) \text{ nếu } r_o \neq 0$$

Nếu $r_o \neq 0$ ta lại chia b cho r_o :

$$b = r_o q_1 + r_1 \text{ với } \delta(r_1) < \delta(r_o) \text{ nếu } r_1 \neq 0.$$

Nếu $r_1 \neq 0$ ta lại chia r_o cho r_1 :

$$r_o = r_1 q_2 + r_2 \text{ với } \delta(r_2) < \delta(r_1) \text{ nếu } r_2 \neq 0.$$

Quá trình chia như vậy phải chấm dứt sau một số hữu hạn bước vì dãy các số tự nhiên

$$\delta(b) > \delta(r_0) > \delta(r_1) > \delta(r_2) \ldots$$

không thể giảm vô hạn, tức là sau một số lần chia, ta phải đi tới một phép chia mà dư bằng 0

$$r_{k-1} = r_k q_{k-1} + 0.$$

Áp dụng bổ đề 1 ta có r_k = ước chung lớn nhất của r_k và 0 = ước chung lớn nhất của r_{k-1} và r_k = ước chung lớn nhất của r_{k-2} và r_{k-1} = ... = ước chung lớn nhất của r_2 và r_1 = ước chung lớn nhất của r_0 và r_1 = ước chung lớn nhất của b và r_0 = ước chung lớn nhất của a và b.

Ví dụ. Tìm ước chung lớn nhất của

$$f(x) = x^6 - 2x^5 + x^4 - x^2 + 2x - 1$$

và $$g(x) = x^5 - 3x^3 + x^2 + 2x - 1.$$

Trước khi thực hiện các phép chia liên tiếp ta hãy nhận xét rằng ước chung lớn nhất của a và b bằng ước chung lớn nhất của c' và b, với c' liên kết của a. Bây giờ ta chia $f(x)$ cho $g(x)$

$$\begin{array}{l|l}
x^6 - 2x^5 + x^4 - x^2 + 2x - 1 & x^5 - 3x^3 + x^2 + 2x - 1 \\
\hline
x^6 - 3x^4 + x^3 + 2x^2 - x & x - 2 \\
\hline
-2x^5 + 4x^4 - x^3 - 3x^2 + 3x - 1 & \\
-2x^5 + 6x^3 - 2x^2 - 4x + 2 & \\
\hline
4x^4 - 7x^3 - x^2 + 7x - 3 &
\end{array}$$

Ta nhận thấy rằng nếu chia $g(x)$ cho $r_0(x) = 4x^4 - 7x^3 - x^2 + 7x - 3$ ta sẽ bị hệ số phân, do đó áp dụng nhận xét trên ta chia $4g(x)$ cho $r_0(x)$.

$$\begin{array}{l|l}
4x^5 - 12x^3 + 4x^2 + 8x - 4 & 4x^4 - 7x^3 - x^2 + 7x - 3 \\
\hline
4x^5 - 7x^4 - x^3 + 7x^2 - 3x & x \\
\hline
7x^4 - 11x^3 - 3x^2 + 11x - 4 &
\end{array}$$

Theo bổ đề 1 ước chung lớn nhất của $4g(x)$ và $r_o(x)$ bằng ước chung lớn nhất của $7x^4 - 11x^3 - 3x^2 + 11x - 4$ và $r_o(x)$. Nhưng nếu chia $7x^4 - 11x^3 - 3x^2 + 11x - 4$ cho $r_o(x)$ ta sẽ bị hệ số phân, do đó áp dụng nhận xét trên ta chia $4(7x^4 - 11x^3 - 3x^2 + 11x - 4)$ cho $r_o(x)$.

$$\begin{array}{l|l} 28x^4 - 44x^3 - 12x^2 + 44x - 16 & 4x^4 - 7x^3 - x^2 + 7x - 3 \\ \hline 28x^4 - 49x^3 - 7x^2 + 49x - 21 & 7 \\ \hline 5x^3 - 5x^2 - 5x + 5 & \end{array}$$

Đáng lẽ chia $r_o(x)$ cho $r_1(x) = 5x^3 - 5x^2 - 5x + 5$, ta chia $r_o(x)$ cho $\frac{1}{5} r_1(x)$ để tránh hệ số phân

$$\begin{array}{l|l} 4x^4 - 7x^3 - x^2 + 7x - 3 & x^3 - x^2 - x + 1 \\ \hline 4x^4 - 4x^3 - 4x^2 + 4x & 4x - 3 \\ \hline -3x^3 + 3x^2 + 3x - 3 & \\ -3x^3 + 3x^2 + 3x - 3 & \\ \hline 0 & \end{array}$$

Vậy ước chung lớn nhất của $f(x)$ và $g(x)$ là $x^3 - x^2 - x + 1$.

2. Ứng dụng

Bây giờ ta hãy áp dụng các kết quả đã thu được về vành chính và vành Oclit để nghiên cứu vành đa thức $K[x]$ với K là một trường.

Trước hết các phần tử khả nghịch của $K[x]$ là các phần tử khác 0 của K. Các đa thức liên kết của đa thức $f(x)$ là các đa thức có dạng $af(x)$ với $0 \neq a \in K$. Các đa thức bậc nhất $ax + b$ là bất khả quy, chúng có một nghiệm duy nhất $-\frac{b}{a}$ trong K.

Đó là các đa thức bất khả quy duy nhất có nghiệm trong K. Các đa thức bất khả quy khác nghĩa là các đa thức bất khả quy có bậc lớn hơn 1 không có nghiệm trong K. Thật vậy giả sử $p(x)$ là một đa thức bất khả quy có bậc lớn hơn 1 và có một nghiệm $c \in K$. Theo (Chương IV, §1, 4, hệ quả của định lí 4) $p(x)$ chia hết cho $x - c$

$$p(x) = (x - c)\, q(x).$$

Vì bậc $(p(x)) > 1$ nên bậc $(q(x)) \geqslant 1$, do đó $x - c$ là ước thực sự của $p(x)$, mâu thuẫn với giả thiết $p(x)$ bất khả quy. Theo (§1, 2, định lí 1) mọi đa thức $f(x)$ có bậc $\geqslant 1$ có thể viết dưới dạng sau, sai khác một nhân tử khả nghịch.

$$f(x) = (a_1x + b_1)^{m_1} \dots (a_kx + b_k)^{m_k} p_1(x)^{n_1} \dots p_l(x)^{n_l}$$

trong đó các $a_ix + b_i$, $i = 1, \dots, k$, là những đa thức bậc nhất không liên kết, các $p_j(x)$, $j = 1, \dots, l$, là những đa thức bất khả quy có bậc > 1 không liên kết, các m_i và n_j là những số tự nhiên. Nếu các m_i đều bằng 0 thì ta bảo rằng $f(x)$ không chứa nhân tử tuyến tính. Việc chứa hay không chứa nhân tử tuyến tính khiến cho $f(x)$ có nghiệm hay không trong K. Thật vậy giả sử $c \in K$, ta có

$$f(c) = (a_1c + b_1)^{m_1} \dots (a_kc + b_k)^{m_k} p_1(c)^{n_1} \dots p_l(c)^{n_l}.$$

Vì các $p_j(c) \neq 0$, $j = 1, \dots, l$, nên $f(c) = 0$ khi và chỉ khi c là một trong các phần tử $-\dfrac{b_i}{a_i}$, $i = 1, \dots, k$. Thêm nữa áp dụng định lí 2 (§1, 2) về sự duy nhất của dạng phân tích ta có : nếu $f(x)$ chứa nhân tử tuyến tính $a_ix + b_i$ với lũy thừa m_i thì $f(x)$ chia hết cho $\left(x + \dfrac{b_i}{a_i}\right)^{m_i}$ và $f(x)$ không chia hết cho $\left(x + \dfrac{b_i}{a_i}\right)^{m_i + 1}$. Do đó $-\dfrac{b_i}{a_i}$ là nghiệm bội cấp m_i của $f(x)$. Đảo lại giả sử c là một nghiệm bội cấp m của $f(x)$, thế thì vì $f(x)$

chia hết cho $(x - c)^m$ và không chia hết cho $(x - c)^{m+1}$ nên trong dạng phân tích của $f(x)$ phải có nhân tử tuyến tính $x - c$ với lũy thừa là m. Kết luận : các nghiệm của $f(x)$ trong K cùng với số bội của chúng được cung cấp bởi các nhân tử tuyến tính và lũy thừa của chúng trong dạng phân tích $f(x)$ thành tích những đa thức bất khả quy và đảo lại. Vì

$$\text{bậc } (f(x)) \geq m_1 + m_2 + \ldots + m_k$$

nên ta có

Định lí 2. *Giả sử $f(x)$ là một đa thức bậc $n > 1$ của vành $K[x]$, với K là một trường. Thế thì $f(x)$ có không quá n nghiệm trong K, các nghiệm có thể phân biệt có thể trùng nhau.*

Nếu dạng phân tích của f(x) chỉ chứa những phân tử tuyến tính

$$f(x) = (a_1x + b_1)^{m_1} \ldots (a_kx + b_k)^{m_k}$$

thì lúc đó

$$n = \text{bậc } f(x) = m_1 + \ldots + m_k$$

và số nghiệm của $f(x)$ trong K bằng số bậc của $f(x)$. Giả sử ta ở trong trường hợp này, gọi $\alpha_1, \alpha_2, \ldots, \alpha_n$ là n nghiệm của $f(x)$ trong K, các nghiệm có thể phân biệt có thể trùng nhau, và giả sử

(1) $f(x) = c_0x^n + c_1x^{n-1} + \ldots + c_{n-1}x + c_n$.

$f(x)$ phải có dạng phân tích là

$$f(x) = c_0(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n).$$

sau khi nhân các đa thức $x - \alpha_i, i = 1, \ldots, n$, ta được

(2) $f(x) = c_0 [x^n - x^{n-1}(\alpha_1 + \alpha_2 + \ldots + \alpha_n) +$

$+ x^{n-2}(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \ldots + \alpha_{n-1}\alpha_n) + \ldots + (-1)^n\alpha_1\alpha_2 \ldots \alpha_n]$

So sánh (1) và (2) ta được *công thức Vieta* :

$$\alpha_1 + \alpha_2 + \ldots + \alpha_n = -\frac{c_1}{c_0}$$

$$a_1a_2 + a_1a_3 + \ldots + a_{n-1}a_n = \frac{c_2}{c_o}$$

$$a_1a_2a_3 + a_1a_2a_4 + \ldots + a_{n-2}a_{n-1}a_n = -\frac{c_3}{c_o}$$

. . .

$$a_1a_2 \ldots a_n = (-1)^n \frac{c_n}{c_o}.$$

Ta nhận thấy rằng các vế trái của các công thức trên chẳng qua là các đa thức đối xứng cơ bản của các phần tử $a_1, a_2, \ldots, a_n$ (ch IV. §2. 3).

Bây giờ ta xét một đa thức bất khả quy $p(x)$ có bậc lớn hơn 1 của vành $K[x]$. Theo như trên đã nói, $p(x)$ không có nghiệm trong K. Ta hãy đặt vấn đề xây dựng một trường E chứa K như một trường con sao cho $p(x)$ có nghiệm trong E.

Định lí 3. *Giả sử*

$$p(x) = a_o + a_1x + \ldots + a_nx^n \quad (n > 1)$$

là một đa thức bất khả quy của vành $K[x]$. Thế thì có một trường E xác định duy nhất (sự lại một đẳng cấu) sao cho

1) *K là một trường con của E.*

2) *$p(x)$ có một nghiệm ϑ trong E.*

3) *Mọi phần tử $z \in E$ viết duy nhất dưới dạng*

$$z = b_o + b_1\vartheta + \ldots + b_{n-1}\vartheta^{n-1}, \; b_i \in K, \; i = 0, \ldots, n-1.$$

Chứng minh. Gọi I là iđêan sinh ra bởi $p(x)$. I là tối đại (§1, bài tập 5). Như vậy vành thương $E = K[x]/I$ là một trường (chIII. §1. bài tập 14). Ta cũng có thể chứng minh E là một trường một cách trực tiếp như sau. E rõ ràng là một vành giao hoán có đơn vị là $1 + I$ khác phần tử $0 + I$; ta hãy chứng minh mọi phần tử $f(x) - I \neq 0 + I$ có nghịch đảo trong E. Vì $f(x) + I \neq 0 + I$, nên $f(x)$ không phải là bội của $p(x)$, do đó $f(x)$ và $p(x)$ nguyên tố cùng nhau (§1. 2. bổ đề 6). Theo (§1. 2, bổ đề 5), tồn tại $r(x), q(x) \in K[x]$ sao cho

$$f(x)\ r(x) + p(x)\ q(x) = 1.$$

Ta suy ra $(f(x) + I)(r(x) + I) = f(x)\ r(x) + I = 1 + I.$

Bây giờ ta xét toàn cấu chính tắc

$$h : K[x] \to K[x]/I$$

$$f(x) \mapsto f(x) + I.$$

Thu hẹp của h vào K là một đồng cấu

$$\bar{h} : K \to K[x]/I$$

mà ta hãy chứng minh nó là đơn cấu. Thật vậy, giả sử $a, b \in K$ sao cho

$$a + I = b + I.$$

Vậy $a - b \in I$, tức là $a - b$ là một bội của $p(x)$, điều này chỉ có thể xảy ra khi $a - b = 0$. $\bar{h}$ là một đơn cấu, cho nên ta hãy đồng nhất các phần tử $a \in K$ với $\bar{h}(a) \in K[x]/I = E$. Do đó K là một trường con của trường E. Ta kí hiệu $h(f(x)) = f(x) + I = \overline{f(x)}$. Với kí hiệu này ta có

$$\overline{p(x)} = \bar{a}_o + \bar{a}_1\bar{x} + \ldots + \bar{a}_n . \bar{x}^n = \bar{0}.$$

Nhưng ta đã đồng nhất các phần tử $a \in K$ với $\bar{h}(a) = h(a) = \bar{a}$ cho nên ta có thể viết

$$a_o + a_1\theta + \ldots + a_n\theta^n = 0$$

trong đó $\theta = \bar{x}$. Vậy $\theta \in E$ là một nghiệm của $p(x)$. Cuối cùng một phần tử tùy ý của E có dạng $\overline{f(x)}$ với $f(x)$ là một đa thức của $K[x]$. Lấy $f(x)$ chia cho $p(x)$, ta được

$$f(x) = p(x)\ q(x) + r(x)$$

với $r(x) = b_o + b_1x + \ldots + b_{n-1}x^{n-1}$ $b_o, b_1 \ldots, b_{n-1} \in K$, không nhất thiết khác 0. Lấy ảnh của $f(x)$ bởi h

$$\overline{f(x)} = \overline{p(x)q(x)} + \overline{r(x)} = 0 + \overline{r(x)} =$$

$$= \bar{b}_0 + \bar{b}_1\bar{x} + \ldots + \bar{b}_{n-1}\bar{x}^{n-1} = b_o + b_1\theta + \ldots + b_{n-1}\theta^{n-1}$$

Hai phần tử

$$\overline{f(x)} = b_o + b_1\theta + \ldots + b_{n-1}\theta^{n-1}$$

và $$\overline{g(x)} = c_o + c_1\theta + \ldots + c_{n-1}\theta^{n-1}$$

bằng nhau khi và chỉ khi $b_i = c_i$, $i = 0, \ldots, n-1$. Thật vậy giả sử $\overline{f(x)} = \overline{g(x)}$. Ta có

$$(b_o - c_o) + (b_1 - c_1)\theta + \ldots + (b_{n-1} - c_{n-1})\theta^{n-1} = 0$$

tức là đa thức

$$(b_o - c_o) + (b_1 - c_1)x + \ldots + (b_{n-1} - c_{n-1})x^{n-1}.$$

là bội của $p(x)$. Điều đó chỉ xảy ra khi và chỉ khi các hệ tử của đa thức bằng 0, nghĩa là $b_i = c_i$, $i = 0, \ldots, n-1$.

Như vậy ta đã chứng minh xong sự tồn tại của trường E. Giả sử bây giờ có một trường E' cũng có các tính chất 1^o, 2^o, 3^o. Gọi θ' là một nghiệm của $p(x)$ trong E'. Ta hãy xét đồng cấu φ xét trong (ch. IV. §1, 5, định lí 5)

$$\varphi : K[x] \to E'$$
$$f(x) \mapsto f(\theta')$$

Ta có $p(x) \in Ker\varphi$. Mặt khác $K[x]$ là một vành chính nên $Ker\varphi$ sinh ra bởi một đa thức $p'(x)$. Vì φ không phải là đồng cấu 0 nên $Ker\ \varphi \neq K[x]$, do đó $p'(x)$ không khả nghịch. Kết luận $p(x)$ và $p'(x)$ phải là liên kết, do đó $Ker\varphi = I$. Thêm nữa do tính chất 3^o, $E' \subset Im\varphi = K[\theta']$, vậy $E' = Im\varphi$, và ta có φ là toàn cấu. Áp dụng định lí 13 của (ch III, §1, 5) ta có một đơn cấu $\overline{\varphi} : K[x]\ I \to E'$ sao cho tam giác

$$\begin{array}{ccc} K[x] & \xrightarrow{\varphi} & E' \\ p & & \overline{\varphi} \\ K[x]\ I & = & E \end{array}$$

là giao hoán. Nhưng ở đây vì φ là một toàn ánh nên $\overline{\varphi}$ cũng là toàn ánh do đó $\overline{\varphi}$ là một đẳng cấu. Đẳng cấu $\overline{\varphi}$ được xác định bởi :

$$b_o + b_1\theta + \ldots + b_{n-1}\theta^{n-1} \mapsto b_o + b_1\theta' + \ldots + b_{n-1}\theta'^{n-1},$$

nó giữ nguyên các phần tử của K và biến θ thành θ'. Ta đã chứng minh xong tính duy nhất của trường E. ■

Áp dụng định lí 3 cho K là trường số thực $\mathbf{R}$, $p(x)$ là đa thức $x^2 + 1$, ta được E là trường số phức $\mathbf{C}$ trong đó các phần tử có dạng $a + bi$, với $a, b \in \mathbf{R}$ và i là một nghiệm của $x^2 + 1$. Vì $\mathbf{C} = \mathbf{R}[x]/I$, I là iđêan sinh ra bởi $x^2 + 1$, nên phép cộng và phép nhân thực hiện như phép cộng và phép nhân đa thức với chú ý là $i^2 = -1$.

Ta có

$$(a + bi) + (c + di) = a + c + (b + d)i ;$$

$$(a + bi)(c + di) = ac + (ad + bc)i + bdi^2$$
$$= ac - bd + (ad + bc)i.$$

Ta có thể xây dựng trường số phức $\mathbf{C}$ bằng cách lấy tích đề các $\mathbf{R}^2$ và xác định hai phép toán cộng và nhân trong R^2 như sau :

$$(a, b) + (c, d) = (a + c, b + d) ;$$

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

Dễ dàng chứng minh rằng $\mathbf{R}^2$ cùng với hai phép toán trên là một trường. Sau đó, bằng đơn cấu

$$\mathbf{R} \to \mathbf{R}^2$$
$$a \mapsto (a, 0)$$

ta đồng nhất a với $(a, 0)$ và đặt $i = (0, 1)$, ta được

$$i^2 = (-1, 0) = -1.$$

Vậy i là một nghiệm của đa thức $x^2 + 1 = 0$. Cuối cùng ta tìm thấy dạng quen thuộc của các số phức bằng cách viết

$$(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0)(0, 1) = a + bi.$$

Hệ quả. *Giả sử $f(x)$ là một đa thức có bậc $n > 1$ của vành đa thức $K[x]$. Thế thì bao giờ cũng có một trường chứa K như*

một trường con sao cho $f(x)$ có đúng n nghiệm trong đó, các nghiệm có thể phân biệt hay không.

Chứng minh. Gọi $p(x)$ là một nhân tử bất khả quy của $f(x)$ có bậc lớn hơn 1 (nếu các nhân tử bất khả quy của $f(x)$ đều bậc 1 thì $f(x)$ có các nghiệm trong K và vấn đề được giải quyết xong). Ta xây dựng trường E như trong định lí 3, đa thức $p(x)$ có nghiệm trong E, do đó $f(x)$ cũng vậy. Nếu $f(x)$ có n nghiệm trong E thì vấn đề được giải quyết xong, nếu không $f(x)$ phải có dạng

$$f(x) = (x - c_1)^{m_1} \dots (x - c_k)^{m_k} f_1(x)$$

với $c_i \in E$, $i = 1, \dots, k$, và $f_1(x) \in E[x]$ với $1 <$ bậc $f_1(x) <$ bậc $f(x)$. Ta lại mở rộng trường E thành trường E_1 để $f_1(x)$ có nghiệm trong E_1. Vì bậc của các đa thức là hữu hạn nên sau một số bước hữu hạn mở rộng ta phải được một trường E_l trong đó $f(x)$ có n nghiệm. ■

Chú ý. Giả sử $f(x) \in K[x]$ là một đa thức có bậc n lớn hơn 1 và E là một trường mở rộng của trường K (nghĩa là K là trường con của E) sao cho $f(x)$ có n nghiệm, phân biệt hay không, trong E. Các nghiệm $\alpha_1, \dots, \alpha_n$ thuộc E, nhưng theo công thức Vietơ, các đa thức đối xứng cơ bản của các phần tử $\alpha_1, \dots, \alpha_n$ bao giờ cũng thuộc K. Vì vậy nếu $g(\alpha_1, \dots, \alpha_n)$ là một đa thức đối xứng của các phần tử $\alpha_1, \dots, \alpha_n$, thì $g(\alpha_1, \dots, \alpha_n)$ là một phần tử thuộc K theo định lí 4 của (ch. IV, §2, 3).

Ví dụ. Xét đa thức $f(x) \in \mathbf{Q}[x]$, $\mathbf{Q}$ là trường số hữu tỉ.

$$f(x) = x^4 - x^2 - 2 = (x^2 + 1)(x^2 - 2).$$

Các đa thức $x^2 + 1$ và $x^2 - 2$ là những đa thức bất khả quy của $\mathbf{Q}[x]$. Ta hãy mở rộng $\mathbf{Q}$ theo phương pháp của định lí 3 để $x^2 + 1$ có nghiệm. Gọi $\mathbf{Q}(i)$ là trường mở rộng đó với i là một nghiệm của $x^2 + 1$. Vì $-i \in \mathbf{Q}(i)$, nên $\mathbf{Q}(i)$ chứa hai nghiệm

của $x^2 + 1$. Bây giờ ta lại mở rộng $\mathbf{Q}(i)$ để $x^2 - 2$ có nghiệm. Gọi $\sqrt{2}$ là một nghiệm của $x^2 - 2$ và kí hiệu bằng $\mathbf{Q}(i)(\sqrt{2})$ trường mở rộng đó, ta được hai nghiệm của $x^2 - 2$ trong $\mathbf{Q}(i)(\sqrt{2})$. Như vậy trong trường $\mathbf{Q}(i)(\sqrt{2})$, $f(x)$ có bốn nghiệm là $i, -i, \sqrt{2}, -\sqrt{2}$.

BÀI TẬP

1. Chứng minh rằng vành gồm các số phức có dạng $a + bi\sqrt{2}$ với $a, b \in \mathbf{Z}$ là một vành Ơclit.

2. Chứng minh một trường là một vành Ơclit,

3. Giả sử A là một vành Ơclit. Chứng minh A là một trường khi và chỉ khi $\delta(x)$ là hằng với mọi $x \in A^*$.

4. Giả sử A là một vành Ơclit với ánh xạ Ơclit

$$\delta : A^* \to \mathbf{N}.$$

Chứng minh tồn tại một ánh xạ Ơclit δ'

$$\delta' : A^* \to \mathbf{N}$$

sao cho $\delta'(A^*) = \{0, \ldots, n\}$, $n \geqslant 0$

hay $\delta'(A^*) = \mathbf{N}$.

5. Giả sử A là một vành Ơclit với ánh xạ Ơclit δ. Chứng minh $\delta(u)$ là phần tử bé nhất của $\delta(A^*)$ khi và chỉ khi u khả nghịch trong A.

6. Giả sử A là một miền nguyên. Chứng minh điều kiện cần để A Ơclit là tồn tại một phần tử không khả nghịch $x \in A$ sao cho mọi lớp của $A/(x)$ có một đại diện hoặc khả nghịch hoặc bằng 0 (đưa ánh xạ Ơclit δ của A về ánh xạ Ơclit δ' trong bài tập 4 và kết hợp với bài tập 5).

7. Chứng minh vành

$$\mathbf{Z}\left[\frac{1 + i\sqrt{19}}{2}\right] = \left\{a + b\left(\frac{1 + i\sqrt{19}}{2}\right) \mid a, b \in \mathbf{Z}\right\}$$

không phải là vành oclit bằng cách áp dụng bài tập 6. (Người ta có thể chứng minh $\mathbf{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ là vành chính, nhưng ở đây chúng ta không làm vì thiếu quá nhiều khái niệm của đại số).

8. Giả sử $f(x) = x^5 + x^3 + x^2 + x + 1$

$g(x) = x^3 + 2x^2 + x + 1$

a) Tìm ước chung lớn nhất của $f(x)$ và $g(x)$ trong $\mathbf{Q}[x]$

b) Tìm ước chung lớn nhất của $f(x)$ và $g(x)$ trong $\mathbf{Z}/3\mathbf{Z}[x]$ trong đó $\mathbf{Q}$ là trường số hữu tỉ $\mathbf{Z}/3\mathbf{Z}$ là trường các số nguyên mod 3.

9. Giả sử

$$\mathbf{R}(\sqrt{-3}) = \{a + b\sqrt{-3} \mid a, b \in \mathbf{R}\}$$
$$\mathbf{Q}(\sqrt{-3}) = \{a + b\sqrt{-3} \mid a, b \in \mathbf{Q}\}$$
$$\mathbf{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$$

trong đó $\mathbf{R}$ là trường các số thực, $\mathbf{Q}$ là trường các số hữu tỉ. Chứng minh rằng :

a) $\mathbf{R}(\sqrt{-3})$, $\mathbf{Q}(\sqrt{-3})$, $\mathbf{Q}(\sqrt{2})$ là những trường với phép cộng và phép nhân thông thường các số.

b) $\mathbf{R}(\sqrt{-3}) \simeq \mathbf{R}[x]/(x^2 + 3)$ với $(x^2 + 3)$ là iđêan sinh ra bởi $x^2 + 3$ trong $\mathbf{R}[x]$.

$\mathbf{Q}(\sqrt{2}) \simeq \mathbf{Q}[x]/(x^2 - 2)$ với $(x^2 - 2)$ là iđêan sinh ra bởi $x^2 - 2$ trong $\mathbf{Q}[x]$.

10. Giả sử E là một trường mở rộng của trường K, u là một phần tử thuộc E, $f(x)$ là một đa thức bất khả quy trong $K[x]$ nhận u làm nghiệm và giả sử rằng $g(x) \in K[x]$ cũng nhận u làm nghiệm. Chứng minh rằng trong $K[x]$:

a) $f(x)$ là đa thức có bậc thấp nhất nhận u làm nghiệm ;

b) $g(x)$ chia hết cho $f(x)$.

11. Giả sử $X = \mathbf{Q}^2$. Trong X ta xác định các phép toán cộng và nhân như sau :

$$(a, b) + (c, d) = (a + c, b + d)$$

$$(a, b) . (c , d) = (ac + 2bd, ad + bc)$$

a) Chứng minh rằng X cùng với hai phép toán đó là một trường.

b) Chứng minh rằng $X \simeq \mathbf{Q}(\sqrt{2})$

c) Tìm tất cả các tự đẳng cấu của X. Từ đó suy ra rằng tập hợp các tự đẳng cấu của X là một nhóm xyclic đối với phép nhân ánh xạ.

CHƯƠNG VI

ĐA THỨC TRÊN TRƯỜNG SỐ

§1. ĐA THỨC VỚI HỆ SỐ THỰC VÀ PHỨC

1. Trường số phức

Cho một đa thức với hệ số thực thì chưa chắc đa thức đó có nghiệm trong trường số thực, cụ thể đa thức $x^2 + 1$ không có nghiệm trong trường số thực. Dưới đây ta sẽ thấy mọi đa thức bậc n với hệ số phức có đúng n nghiệm phức. Để chứng minh ra hãy đưa vào các bổ đề sau đây :

Bổ đề 1. *Mọi đa thức với hệ số thực có bậc lẻ có ít nhất một nghiệm thực.*

Chứng minh. Giả sử

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0,\ a_n \neq 0,\ n \text{ lẻ}.$$

Qua giáo trình giải tích ta biết rằng với những giá trị dương và âm của x, khá lớn về giá trị tuyệt đối, hàm số $f(x)$ có các dấu trái nhau. Vậy có những giá trị thực của x, a và b chẳng hạn, sao cho

$$f(a) < 0,\ f(b) > 0.$$

Mặt khác hàm số $f(x)$ là liên tục, vì vậy có một giá trị c của x, nằm giữa a và b, sao cho $f(c) = 0$. ■

Ta chú ý rằng phép chứng minh của bổ đề 1 không đại số. nó đã lấy những kết quả của giải tích. Thêm nữa về ngôn ngữ ta đã gọi ánh xạ.

$$\begin{array}{ccc} \mathbf{R} & \to & \mathbf{R} \\ c & \mapsto & f(c) \end{array}$$

là hàm số $f(x)$.

Bổ đề 2. *Mọi đa thức bậc hai $ax^2 + bx + c$, với hệ số phức, bao giờ cũng có hai nghiệm phức.*

Chứng minh. Gọi ω_1 và ω_2 là hai căn bậc hai của $b^2 - 4ac$, ta có hai nghiệm của đa thức là $\dfrac{-b + \omega_1}{2a}$ và $\dfrac{-b + \omega_2}{2a}$. ■

Bổ đề 3. *Mọi đa thức bậc lớn hơn 0 với hệ số thực có ít nhất một nghiệm phức.*

Chứng minh. Mọi số tự nhiên $n > 0$ đều có thể viết dưới dạng $n = 2^m n'$, với m là một số tự nhiên và n' là một số tự nhiên lẻ. Ta hãy chứng minh bằng quy nạp theo m. Với $m = 0$ khẳng định là đúng theo bổ đề 1. Ta giả sử khẳng định là đúng cho $m - 1$ và chứng minh nó đúng cho m. Muốn vậy, ta hãy xét một đa thức $f(x)$ có bậc $n = 2^m n'$ $(m > 0)$ với hệ số thực. Coi $f(x)$ như một đa thức của vành $\mathbf{C}[x]$, với $\mathbf{C}$ là trường số phức, ta hãy xét một trường mở rộng E của $\mathbf{C}$ sao cho $f(x)$ có đúng n nghiệm $\alpha_1, \alpha_2, \ldots, \alpha_n$ trong E (ch V, §2, 2, hệ quả của định lí 3). Giả sử c là một số thực tùy ý, đặt

$$(1)\quad \beta_{ij} = \alpha_i\alpha_j + c(\alpha_i + \alpha_j),\ i \neq j.$$

Ta có C_n^2 phần tử β_{ij} thành lập bởi các tổ hợp chập 2 của n phần tử $\alpha_1, \ldots, \alpha_n$. Xét đa thức

$$(2)\quad g(x) = (x - \beta_{12})(x - \beta_{13}) \ldots (x - \beta_{n-1,n})$$

$$= x^l + a_1x^{l-1} + \ldots + a_l$$

Vì bậc của $g(x)$ bằng số các nhân tử $x - \beta_{ij}$ nên ta có

$$l = C_n^2 = \frac{n(n-1)}{2} = \frac{2^m n'(2^m n' - 1)}{2} = 2^{m-1}q,$$

với $q = n'(2^m n' - 1)$; vì n' và $2^m n' - 1$ là những số lẻ nên q là một số lẻ.

Ta lấy chứng minh các hệ tử $a_1, \ldots a_l$ của $g(x)$ đều là thực cả. Trước hết các hệ tử đó là các đa thức đối xứng cơ bản của các β_{ij}. Vậy theo (1) chúng là những đa thức của $\alpha_1, \ldots, \alpha_n$ với hệ số thực, vì c là một số thực. Hơn nữa chúng còn là những đa thức đối xứng của $\alpha_1, \ldots, \alpha_n$. Thật vậy nếu ta thay α_i bằng α_j và α_j bằng α_i thì β_{ij} vẫn giữ nguyên còn các β_{hi} và β_{hj} thì trao đổi cho nhau (h khác i và j), điều này chắc chắn không làm thay đổi các hệ tử $a_1, \ldots, a_l$. Do đó theo (ch V, §2, 2, chú ý) các hệ tử đó là những số thực. Vậy $g(x)$ là một đa thức với hệ số thực có bậc $2^{m-1}q$, với q là lẻ. Theo giả thiết quy nạp $g(x)$ có ít nhất một nghiệm phức dạng (1), tức là có ít nhất một cặp chỉ số (i, j) sao cho phần tử

$$\beta_{ij} = \alpha_i\alpha_j + c(\alpha_i + \alpha_j)$$

thuộc trường số phức C.

Nếu ta gán cho c một giá trị thực khác thì ta sẽ được một đa thức $g(x)$ khác, loại (2), thừa nhận một nghiệm phức dạng (1), nhưng nói chung với một cặp chỉ số (i, j) khác. Tuy vậy, nếu ta gán cho c lần lượt $C_n^2 + 1$ giá trị phân biệt thì nhất định phải được hai nghiệm phức dạng (1) với cùng một cặp chỉ số (i, j) vì ta chỉ có C_n^2 tổ hợp chập 2 của n phần tử. Vậy thế nào cũng có hai số thực c_1 và c_2 khác nhau sao cho các phần tử

$$\alpha_i\,\alpha_j + c_1\,(\alpha_i + \alpha_j)$$
$$\alpha_i\alpha_j + c_2(\alpha_i + \alpha_j)$$

ứng với cùng một cặp chỉ số i, j đều là phức. Đặt

$$a = \alpha_i\alpha_j + c_1(\alpha_i + \alpha_j),$$
$$b = \alpha_i\alpha_j + c_2(\alpha_i + \alpha_j).$$

Ta có $a, b \in C$. Ta suy ra

$$\alpha_i + \alpha_j = \frac{a - b}{c_1 - c_2}$$

$$\alpha_i\alpha_j = a - c_1\frac{a - b}{c_1 - c_2}.$$

Vậy $\alpha_i + \alpha_j$ và $\alpha_i\alpha_j$ đều là phức. Ta suy ra α_i và α_j là nghiệm của đa thức bậc hai

$$x^2 - (\alpha_i + \alpha_j)x + \alpha_i\alpha_j$$

với hệ số phức. Theo bổ đề 2, α_i và α_j là phức. Như vậy ta đã chứng minh đa thức $f(x)$ không những có một, mà có hai nghiệm phức.■

Định lí 1. *Mọi đa thức bậc lớn hơn 0 với hệ số phức có ít nhất một nghiệm phức.*

Chứng minh. Giả sử $f(x)$ là một đa thức bậc $n > 0$

$$f(x) = a_o + a_1x + \ldots + a_nx^n$$

với hệ số phức. Đặt

$$\overline{f(x)} = \bar{a}_0 + \bar{a}_1x + \ldots + \bar{a}_nx^n$$

với các $\bar{a}_i$ là các liên hợp của các a_i, $i = 0, \ldots, n$. Xét đa thức :

$$g(x) = f(x)\overline{f(x)}.$$

Ta có

$$g(x) = b_o + b_1x + \ldots + b_{2n}x^{2n}$$

với $$b_k = \sum_{i+j=k} a_i\bar{a}_j \qquad k = 0, 1, \ldots, 2n$$

vì $$\bar{b}_k = \sum_{i+j=k} \bar{a}_ia_j = b_k$$

nên các hệ số b_k là thực. Theo bổ đề 3, $g(x)$ có ít nhất một nghiệm phức $z = s + it$

$$g(z) = f(z)\,\overline{f(z)} = 0.$$

Do đó hoặc $f(z) = 0$ hoặc $\overline{f(z)} = 0$. Nếu $\overline{f(z)} = 0$

$$\overline{f(z)} = \bar{a}_o + \bar{a}_1\,z + \ldots + \bar{a}_nz^n = 0$$

thì $\overline{\bar{a}_o + \bar{a}_1z + \ldots + \bar{a}_nz^n} = a_o + a_1\bar{z} + \ldots + a_n\bar{z}^n = 0$

tức là $$f(\bar{z}) = 0$$

Như vậy hoặc z hoặc $\bar{z}$ là nghiệm của $f(x)$. ■

Hệ quả 1. *Các đa thức bất khả quy của vành* **C[x]**, **C** *là trường số phức, là các đa thức bậc nhất.*

Chứng minh. Theo (Ch. V, §2, 2), các đa thức bậc nhất là bất khả quy. Giả sử $f(x)$ là một đa thức của **C[x]** có bậc lớn hơn 1. Theo định lí 1, $f(x)$ có một nghiệm phức c. Vậy $f(x)$ có một ước thực sự $x - c$, do đó $f(x)$ không bất khả quy. ■

Hệ quả 2. *Mọi đa thức bậc $n > 0$ với hệ số phức có n nghiệm phức.*

Chứng minh. Giả sử $f(x)$ là một đa thức bậc $n > 0$ với hệ số phức. Theo hệ quả 1 dạng phân tích của $f(x)$ thành tích những đa thức bất khả quy phải là

$$f(x) = a(a_1x + b_1)^{m_1}(a_2x + b_2)^{m_2} \dots (a_kx + b_k)^{m_k}$$

trong đó a là một số phức khác 0 và

$$m_1 + m_2 + \dots + m_k = n.$$

Theo (Ch. V, §2, 2), n nghiệm phức của $f(x)$ là: m_1 nghiệm trùng với $-\frac{b_1}{a_1}$, ..., m_k nghiệm trùng với $-\frac{b_k}{a_k}$. ■

Chú ý. Nếu $f(x)$ là một đa thức với hệ số thực có một nghiệm phức $z = s + it$ $(t \neq 0)$, thì $f(x)$ cũng nhận liên hợp $\bar{z}$ của z làm nghiệm. Thật vậy, giả sử

$$f(x) = a_0 + a_1x + \dots + a_nx^n$$

và $$f(z) = a_0 + a_1z + \dots + a_nz^n = 0.$$

Ta suy ra

$$\overline{a_0 + a_1z + \dots + a_nz^n} = a_0 + a_1\bar{z} + \dots + a_n\bar{z}^n = 0,$$

tức là $$f(\bar{z}) = 0.$$

Do đó ta suy ra $f(x)$ chia hết cho đa thức bậc hai

$$g(x) = (x - z)(x - \bar{z}) = x^2 - (z + \bar{z})x + z\bar{z},$$

$z + \bar{z}$ và $z\bar{z}$ là những số thực.

Hệ quả 3. *Các đa thức bất khả quy của R[x], R là trường số thực, là các đa thức bậc nhất và các đa thức bậc hai* $ax^2 + bx + c$ *với biệt số* $b^2 - 4ac < 0$.

Chứng minh. Các đa thức bậc nhất và các đa thức bậc hai với biệt số âm rõ ràng là những đa thức bất khả quy của R[x]. Giả sử $p(x)$ là một đa thức bất khả quy của R[x] với bậc lớn hơn một. Theo (ch V, §2, 2), $p(x)$ không có nghiệm thực. Theo định lí 1, $p(x)$ có một nghiệm phức z và theo chú ý trên $p(x)$ chia hết cho đa thức bậc hai với hệ số thực

$$g(x) = x^2 - (z + \bar{z})x + z\bar{z}.$$

$g(x)$ không khả nghịch và là ước của phần tử bất khả quy $p(x)$, vậy $g(x)$ phải là liên kết của $p(x)$, tức là

$$p(x) = ug(x),\ 0 \neq u \in \mathbf{R}. \blacksquare$$

Từ hệ quả 3 ta suy ra mọi đa thức $f(x) \in \mathbf{R}[x]$ có bậc lớn hơn 0 đều có thể viết dưới dạng

$$(3)\ f(x) = u(a_1x + b_1)^{m_1} \ldots (a_kx + b_k)^{m_k}\ (\alpha_1x^2 + \beta_1x + \gamma_1)^{n_1} \ldots$$

$$\ldots (\alpha_lx^2 + \beta_lx + \gamma_l)^{n_l},$$

trong đó u là một số thực khác 0, các $a_ix + b_i$ là những đa thức bậc nhất, các $\alpha_jx^2 + \beta_jx + \gamma_j$ là những đa thức bậc hai với biệt số âm, các m_i và n_j là những số tự nhiên, $i = 1, \ldots, k$; $j = 1, \ldots, l$. Các nghiệm thực của $f(x)$ được cung cấp bởi các nhân tử tuyến tính $a_ix + b_i$ và các nghiệm phức bởi các nhân tử bậc hai $\alpha_jx^2 + \beta_jx + \gamma_j$. Mỗi nhân tử tuyến tính $a_ix + b_i$ cho ta một nghiệm thực $-\dfrac{b_i}{a_i}$, mỗi nhân tử bậc hai $\alpha_jx^2 + \beta_jx + \gamma_j$ cho ta hai nghiệm phức liên hợp

$$s_j + it_j \text{ và } s_j - it_j$$

với $$s_j = \frac{-\beta_j}{2\alpha_j} \text{ và } t_j = \frac{\sqrt{4\alpha_j\gamma_j - \beta_j^2}}{2\alpha_j}.$$

Vậy nếu $s_j + it_j$ là nghiệm bội cấp n_j của $f(x)$ thì $s_j - it_j$ cũng là nghiệm bội cấp n_j của $f(x)$.

Đa thức $f(x)$ không có nghiệm thực (nghiệm phức) nếu các lũy thừa m_i (các lũy thừa n_j) trong dạng phân tích (3) của $f(x)$ đều bằng 0.

2. Phương trình bậc ba và bốn

Theo như trên mọi đa thức với hệ số phức và có bậc lớn hơn 0 đều có các nghiệm trong trường số phức.

Đối với các đa thức bậc hai $ax^2 + bx + c$, ta có các nghiệm là

$$\frac{-b + \omega_1}{2a} \text{ và } \frac{-b + \omega_2}{2a}$$

trong đó ω_1 và ω_2 là hai căn bậc hai của $b^2 - 4ac$. Như vậy ta đã biểu thị các nghiệm của phương trình

$$ax^2 + bx + c = 0$$

qua các hệ số của phương trình bằng các phép tính cộng, trừ, nhân, chia, nâng lũy thừa, khai căn. Người ta nói người ta đã *giải phương trình bằng căn thức*. Ta sẽ thấy dưới đây ta có thể giải một phương trình bậc ba hay bậc bốn bằng căn thức.

Phương trình bậc ba. Ta hãy xét phương trình bậc ba với hệ số phức

$$x^3 + ax^2 + bx + c = 0.$$

Phương trình này trở thành

$$y^3 - py + q = 0 \quad (4)$$

nếu ta đặt

$$y = x - \frac{a}{3}.$$

Để giải phương trình (4) ta đặt

(5) $$y = u + v,$$

ta được sau khi thay vào (4)

(6) $$u^3 + v^3 + (u + v)(3uv + p) + q = 0.$$

Vấn đề của chúng ta bây giờ là tìm các số phức u và v thỏa mãn (6). Ta chú ý tới các số phức u và v có tính chất

(7) $$3uv + p = 0, \text{ hay } uv = -\frac{p}{3}.$$

Bao giờ cũng có những số phức u và v thỏa mãn (6) và (7). Thật vậy nếu u và v thỏa mãn (6) thì $u + v$ là một nghiệm của (4), vậy ta có (5) với y là một nghiệm phức của phương trình (4), do đó kết hợp với (7) ta có u và v là hai nghiệm của phương trình bậc hai

$$z^2 - yz - \frac{p}{3} = 0.$$

Như vậy rồi từ (6) và (7), ta được

$$u^3 + v^3 = -q, \; u^3 v^3 = -\frac{p^3}{27}.$$

Ta nhận thấy rằng u^3 và v^3 là các nghiệm của phương trình bậc hai

$$t^2 + qt - \frac{p^3}{27} = 0$$

(8) $$u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}},$$

$$v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

trong đó $\sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ là một căn bậc hai của $\frac{q^2}{4} + \frac{p^3}{27}$. Gọi u_1 là một căn bậc ba của

$$-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

và v_1 là một căn bậc ba của

$$-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$$

sao cho u_1v_1 thỏa mãn (7), thì ta cũng có u_2v_2 và u_3v_3 thỏa mãn (7) với

$$u_2=\varepsilon u_1,\ u_3=\varepsilon^2u_1 \text{ và } v_2=\varepsilon^2v_1,\ v_3=\varepsilon v_1$$

trong đó $\varepsilon=-\frac{1}{2}+i\frac{\sqrt{3}}{2}$, $\varepsilon^2=-\frac{1}{2}-i\frac{\sqrt{3}}{2}$

là hai căn bậc ba phức của đơn vị. Như vậy ta được ba cặp số phức (u_1, v_1), (u_2, v_2), (u_3, v_3) thỏa mãn (6) và (7). Ta đặt

$$(9)\quad \begin{cases} y_1=u_1+v_1; \\ y_2=\varepsilon u_1+\varepsilon^2v_1=-\frac{1}{2}(u_1+v_1)+\frac{i\sqrt{3}}{2}(u_1-v_1); \\ y_3=\varepsilon^2u_1+\varepsilon v_1=-\frac{1}{2}(u_1+v_1)-\frac{i\sqrt{3}}{2}(u_1-v_1). \end{cases}$$

Từ (9), sau khi tính toán và chú ý rằng u_1, v_1 thỏa mãn (6) và (7), ta được

$$y_1+y_2+y_3=0$$

$$y_1y_2+y_1y_3+y_2y_3=-3u_1v_1=p$$

$$y_1y_2y_3=u_1^3+v_1^3=-q.$$

Vậy

$$(y-y_1)(y-y_2)(y-y_3)=y^3-y^2(y_1+y_2+y_3)+$$

$$+y(y_1y_2+y_1y_3+y_2y_3)-y_1y_2y_3=y^3+py+q.$$

Đa thức y^3+py-q đã được phân tích thành tích những nhân tử tuyến tính, và ta được các nghiệm của nó là y_1, y_2, y_3 (9). Người ta thường viết tắt (9) dưới dạng

$$y = u + v = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} +$$

$$+ \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

gọi là công thức Các-đa-nô (Cardano). Như vậy ta đã giải được phương trình bậc ba (4) bằng căn thức.

Đặt $D = -4p^3 - 27q^2$, (8) và (9) cho ta

$$(y_1 - y_2)^2 (y_1 - y_3)^2 (y_2 - y_3)^2 = -108(u_1^3 - v_1^3)^2 = D.$$

Do đó (4) có nghiệm bội khi và chỉ khi $D = 0$.

Ví dụ. Giải phương trình bậc ba

$$x^3 - 3\left(\frac{1}{2} + \frac{i\sqrt{3}}{2}\right)x + 2i = 0.$$

Đặt $x = u + v$, ta được

$$u^3 + v^3 + 3(u + v)\left[uv - \left(\frac{1}{2} + \frac{i\sqrt{3}}{2}\right)\right] + 2i = 0.$$

Ta yêu cầu u và v thỏa mãn

$$uv = \frac{1}{2} + i\frac{\sqrt{3}}{2} \tag{10}$$

Do đó u^3 và v^3 là hai nghiệm của phương trình bậc hai

$$t^2 + 2it - 1 = (t + i)^2 = 0.$$

Phương trình này có một nghiệm kép.

$$u^3 = v^3 = -i.$$

$-i$ có một căn bậc ba là i. Đặt $u_1 = i$, ta suy ra từ (10)

$$v_1 = \frac{\frac{1}{2} + i\frac{\sqrt{3}}{2}}{u_1} = \frac{\sqrt{3}}{2} - \frac{i}{2}$$

Vậy theo (9) các nghiệm của phương trình là

$$x_1 = u_1 + v_1 = \frac{\sqrt{3}}{2} + \frac{i}{2},$$

$$x_2 = -\frac{1}{2}(u_1 + v_1) + \frac{i\sqrt{3}}{2}(u_1 - v_1) = -\sqrt{3} - i,$$

$$x_3 = -\frac{1}{2}(u_1 + v_1) - \frac{i\sqrt{3}}{2}(u_1 - v_1) = \frac{\sqrt{3}}{2} + \frac{i}{2},$$

trong đó $x_1 = x_3$, vậy $\frac{\sqrt{3}}{2} + \frac{i}{2}$ là nghiệm kép của phương trình.

Bây giờ ta hãy xét phương trình (4) trong trường hợp p và q là những số thực. Ta đặt

$$\Delta = \frac{p^3}{27} + \frac{q^2}{4},$$

vậy $$D = -4p^3 - 27q^2 = -108\Delta.$$

Ta hãy nghiên cứu các nghiệm của (4) theo Δ.

a) $\Delta > 0$. (8) cho ta biết u^3 và v^3 là thực. Gọi u_1 là căn bậc ba thực của u^3. Theo (7), v_1 là thực và theo (8), $u_1 \neq v_1$. Theo (8), phương trình (4) có một nghiệm thực y_1 và hai nghiệm phức liên hợp y_2 và y_3.

b) $\Delta = 0$. Theo (8), ta có $u^3 = v^3$ và là thực. Gọi u_1 là căn bậc ba thực của u^3, thì theo (7), v_1 cũng phải là căn bậc ba thực của v^3 và ta có $u_1 = v_1$. Vậy theo (9), ta có ba nghiệm thực y_1, y_2, y_3 với $y_2 = y_3$.

c) $\Delta < 0$. Theo bổ đề 1, phương trình (3) có một nghiệm thực, gọi nghiệm thực đó là y_1. Theo (8), u^3 và v^3 là hai số phức không phải là thực, do đó các căn bậc ba của chúng phải là phức (≠ thực). Mặt khác theo (7) và (9), ta có

$$u_1 + v_1 = y_1,\ u_1 v_1 = -\frac{p}{3}.$$

Vậy u_1 và v_1 là hai nghiệm của phương trình bậc hai

$$z^2 - y_1 z - \frac{p}{3} = 0$$

với hệ số thực, do đó u_1 và v_1 là phức liên hợp. Ta suy ra, trong (8), các nghiệm y_1, y_2, y_3 là thực. Trong trường hợp này vì $\Delta \neq 0$ nên $D \neq 0$, do đó y_1, y_2, y_3 là ba nghiệm phân biệt. Các số y_1, y_2, y_3 là thực, nhưng muốn tính chúng theo công thức Cac-đa-nô thì lại phải lấy căn bậc ba của những số phức. Người ta đã chứng minh được rằng, trong trường hợp $\Delta < 0$, không thể biểu thị các nghiệm của phương trình (3) bằng các căn thức với lượng thực dưới căn.

Phương trình bậc bốn. Phép giải một phương trình bậc bốn

$$x^4 + ax^3 + bx^2 + cx + d = 0$$

với hệ số phức tùy ý sẽ đưa về phép giải một phương trình phụ bậc ba gọi là phương trình giải bậc ba. Ta tiến hành như sau :

Chuyển ba hạng tử cuối sang vế phải rồi cộng $\frac{a^2x^2}{4}$ vào cả hai vế, ta được

$$\left(x^2 + \frac{ax}{2}\right)^2 = \left(\frac{a^2}{4} - b\right)x^2 - cx - d.$$

Sau đó ta cộng vào hai vế của phương trình này tổng

$$\left(x^2 + \frac{ax}{2}\right)y + \frac{y^2}{4}$$

trong đó y là một ẩn mới, ta được

$$(11)\qquad \left(x^2 + \frac{ax}{2} + \frac{y}{2}\right)^2 = \left(\frac{a^2}{4} - b + y\right)x^2 + \left(\frac{ay}{2} - c\right)x + \frac{y^2}{4} - d.$$

Ta hãy lựa chọn ẩn phụ y sao cho vế phải là một chính phương. Muốn thế thì chỉ việc làm triệt tiêu biệt số của tam thức bậc hai đối với x ở vế phải

$$\left(\frac{ay}{2} - c\right)^2 - 4\left(\frac{a^2}{4} - b + y\right)\left(\frac{y^2}{4} - d\right) = 0$$

hay

$$y^3 - by^2 + (ac - 4d)y - [d(a^2 - 4b) + c^2] = 0.$$

Đó là một phương trình bậc ba, gọi là *phương trình giải* của phương trình đã cho. Giả sử y_o là một nghiệm của phương trình đó. Điền y_o vào phương trình (10), ta được vế phải của phương trình là một chính phương

$$\left(x^2 + \frac{ax}{2} + \frac{y_o}{2}\right)^2 = (\alpha x + \beta)^2.$$

Từ đó

$$x^2 + \frac{ax}{2} + \frac{y_o}{2} = \alpha x + \beta,\ x^2 + \frac{ax}{2} + \frac{y_o}{2} = -\alpha x - \beta.$$

Hai phương trình bậc hai đó sẽ cho tất cả bốn nghiệm của phương trình bậc bốn. Vậy phép giải một phương trình bậc bốn đã được đưa về phép giải một phương trình bậc ba và hai phương trình bậc hai. Ta suy ra từ đó rằng phương trình bậc bốn giải được bằng căn thức.

Ví dụ. Giải phương trình bậc bốn

$$x^4 - 3x^3 + 3x^2 - 3x + 2 = 0.$$

Chuyển ba hạng tử cuối sang vế phải

$$x^4 - 3x^3 = -3x^2 + 3x - 2.$$

Sau đó cộng vào hai vế $\frac{9x^2}{4}$, ta được

$$\left(x^2 - \frac{3x}{2}\right)^2 = -\frac{3}{4}x^2 + 3x - 2$$

Cuối cùng cộng vào hai vế tổng $\left(x^2 - \frac{3x}{2}\right) y + \frac{y^2}{4}$;

(12) $\left(x^2 - \frac{3x}{2} + \frac{y}{2}\right)^2 =$

$$= x^2 \left(y - \frac{3}{4}\right) + 3x \left(1 - \frac{y}{2}\right) + \frac{y^2}{4} - 2$$

Ta yêu cầu y làm triệt tiêu biệt số

$$9 \left(1 - \frac{y}{2}\right)^2 - 4 \left(y - \frac{3}{4}\right) \left(\frac{y^2}{4} - 2\right) = 0,$$

hay sau khi khai triển

$$y^2 (y - 3) + y - 3 = (y - 3)(y^2 + 1) = 0.$$

Chọn $y = 3$, phương trình (12) trở thành

$$\left(x^2 - \frac{3x}{2} + \frac{3}{2}\right)^2 = \left(\frac{3x}{2} - \frac{1}{2}\right)^2 .$$

Từ đó $$x^2 - \frac{3x}{2} + \frac{3}{2} = \frac{3x}{2} - \frac{1}{2},$$

$$x^2 - \frac{3x}{2} + \frac{3}{2} = -\frac{3x}{2} + \frac{1}{2} .$$

hay $$x^2 - 3x + 2 = 0, x^2 + 1 = 0$$

Hai phương trình này cho ta bốn nghiệm 1, 2, i, $-i$.

Sự thực ra trong trường hợp cụ thể này ta nhìn thấy ngay nghiệm 1 của phương trình bậc bốn đã cho vì tổng số các hệ số bằng 0. Do đó ta có thể viết để làm nổi bật nghiệm 1.

$$x^4 - 3x^3 + 3x^2 - 3x + 2 = (x - 1)(x^3 - 2x^2 + x - 2).$$

Vậy vấn đề bây giờ là giải phương trình

$$x^3 - 2x^2 + x - 2 = 0$$

mà ta có thể viết

$$x^2 (x - 2) + x - 2 = (x - 2)(x^2 + 1) = 0$$

Từ đó, ta suy ra các nghiệm của phương trình.

Người ta chứng minh rằng không thể giải bằng căn thức các phương trình tổng quát bậc lớn hơn bốn (Aben, Galoa). Hơn thế nữa, Galoa đã tìm ra được tiêu chuẩn để biết một phương trình đã cho giải được bằng căn thức hay không.

BÀI TẬP

1. Trong vành $\mathbf{C}[x]$ ($\mathbf{C}$ là trường số phức) hãy phân tích các đa thức : $x^2 + i$, $x^4 - 1 - i$, $x^2 - 4i + 3$, $x^7 - 1 - i\sqrt{3}$ thành một tích những đa thức bất khả quy.

2. Biểu diễn hình học các nghiệm của đa thức

$$f(x) = x^n - 1 \quad ,$$

$$g(x) = (x - a)^m - b. \ (a \neq 0)$$

Từ đó suy ra rằng $f(x)$ và $g(x)$ có không quá hai nghiệm chung.

3. Tìm các nghiệm phức của đa thức

$$f(x) = (1 - x^2)^3 + 8x^3$$

Phân tích đa thức $f(x)$ thành tích những đa thức bất khả quy với hệ số thực.

4. Trong vành $\mathbf{C}[x]$ chứng minh rằng đa thức $f(x)$ chia hết cho đa thức $g(x)$ khi và chỉ khi mọi nghiệm của $g(x)$ đều là nghiệm của $f(x)$ và mọi nghiệm bội cấp k của $g(x)$ cũng là nghiệm bội cấp lớn hơn k của $f(x)$.

5. Trong vành $\mathbf{Q}[x]$ ($\mathbf{Q}$ là trường số hữu tỉ), chứng minh rằng đa thức $f(x) = x^{3k} + x^{3l+1} + x^{3n+2}$ chia hết cho đa thức $g(x) = x^2 + x + 1$ với k, l, n là những số tự nhiên tùy ý.

6. Trong vành $\mathbf{Q}[x]$, chứng minh rằng đa thức $f(x) = x^3 - 3n^2x + n^3$, với n là một số tự nhiên khác 0, là một đa thức bất khả quy.

7. Giả sử $\alpha = 1 + i$.

a) Biểu diễn α dưới dạng lượng giác. Tìm môđun và ac-gu-men của α^n và α^{-n}.

b) Viết α^n và α^{-n} dưới dạng $a + bi$.

c) Biểu diễn hình học các giá trị α^n và α^{-n} với $n \leqslant 8$.

d) Chứng minh rằng mọi số phức z tùy ý đều có thể biểu diễn được một cách duy nhất dưới dạng $z = x + y\alpha$ với x, y là những số thực.

e) Chứng minh rằng ánh xạ

$$f : \mathbf{C} \to M$$

$$z = x + y\,\alpha \mapsto \begin{bmatrix} x & y \\ -2y & x + 2y \end{bmatrix}$$

từ vành số phức đến vành các ma trận thực vuông cấp 2 là một đẳng cấu. Từ đó suy ra rằng tập hợp các ma trận thực vuông cấp 2 dạng $\begin{bmatrix} x & y \\ -2y & x + 2y \end{bmatrix}$ là một trường.

f) Tính

$$\begin{bmatrix} 0 & 1 \\ -2 & 2 \end{bmatrix}^n$$

8. Giải các phương trình bậc ba sau đây :

a) $4y^3 - 36y^2 + 84y - 20 = 0$.

b) $x^3 - x - 6 = 0$.

c) $x^3 + 18x + 15 = 0$.

d) $x^3 + 3x^2 - 6x + 4 = 0$.

9. Chứng minh (bằng đa thức đối xứng) :

$$(x_1 - x_2)^2 (x_2 - x_3)^2 (x_1 - x_3)^2 = -4p^3 - 27q^2$$

với x_1, x_2, x_3 là các nghiệm của phương trình

$$x^3 + px + q = 0.$$

10. Giải các phương trình

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) $x^4 + 6x^3 + 6x^2 - 8 = 0$.

§2. ĐA THỨC VỚI HỆ SỐ HỮU TỈ

1. Nghiệm hữu tỉ của một đa thức với hệ số hữu tỉ

Trước hết ta nhận xét rằng nếu

$$f(x) = a_n x^n + \ldots + a_0 \quad (a_n \neq 0)$$

là một đa thức với hệ số hữu tỉ thì $f(x)$ có thể viết dưới dạng

$$f(x) = b^{-1}(a_n x^n + \ldots + a_0) = b^{-1} g(x)$$

trong đó b là mẫu số chung của các phân số a_i và các a_i là những số nguyên. Vì $f(x)$ và $g(x)$ chỉ khác nhau một nhân tử bậc 0 nên các nghiệm của $f(x)$ là các nghiệm của $g(x)$. Vậy việc tìm nghiệm của một đa thức với hệ số hữu tỉ được đưa về việc tìm nghiệm của một đa thức với hệ số nguyên. Mặt khác ta cũng nhận xét rằng nếu c là nghiệm của đa thức $g(x)$

$$a_n c^n - a_{n-1} c^{n-1} + \ldots + a_1 c + a_0 = 0$$

ta có sau khi nhân hai vế với a_n^{n-1}

$$(a_n c)^n - a_{n-1}(a_n c)^{n-1} + \ldots + a_1 a_n^{n-2}(a_n c) + a_0 a_n^{n-1} = 0.$$

Ta có $c' = a_n c$ là nghiệm của đa thức

$$h(x) = x^n + a_{n-1} x^{n-1} + \ldots + a_1 a_n^{n-2} x + a_0 a_n^{n-1}$$

với hệ số nguyên và hệ số cao nhất bằng 1. Do đó muốn có các nghiệm của $g(x)$ ta chỉ việc tìm các nghiệm của $h(x)$.

Ta đặt vấn đề ở đây là tìm các nghiệm hữu tỉ của các đa thức $f(x)$ có dạng

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_o$$

với các a_i nguyên. Giả sử α là một nghiệm hữu tỉ của $f(x)$, thế thì theo định lí 3 của (Ch V, §1, 2), α phải là nguyên. Mặt khác, từ

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_o = 0$$

ta có thể viết

$$\alpha(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \ldots + a_1) = -a_o,$$

do đó $\alpha | a_o$. Như vậy các nghiệm nguyên của $f(x)$, nếu có, phải là những ước của a_o. Cho nên muốn tìm các nghiệm nguyên của $f(x)$ ta xét các ước của số hạng tự do a_o, và sau đó, thử xem các ước đó có phải là nghiệm của $f(x)$ hay không. Để hạn chế số lần thử người ta đưa vào nhận xét sau đây.

Giả sử α là một nghiệm nguyên của $f(x)$. Thế thì $f(x)$ chia hết cho $x - \alpha$

$$f(x) = (x - \alpha)q(x)$$

và theo sơ đồ Hoóc ne (Ch IV, §1, 4), $q(x)$ là một đa thức với hệ số nguyên. Do đó $q(1)$ và $q(-1)$ là những số nguyên và

$$\frac{f(1)}{1 - \alpha} = q(1), \quad \frac{f(-1)}{1 + \alpha} = -q(-1)$$

nếu α khác 1 và -1.

Vì vậy trước hết ta tính f(1) và f(−1) để xem 1 và −1 có phải là nghiệm của f(x), sau đó ta xét các ước $\alpha \neq \pm 1$ của a_o sao cho

$$\frac{f(1)}{1 - \alpha} \text{ và } \frac{f(-1)}{1 + \alpha}$$

là những số nguyên để thử xem chúng có phải là nghiệm của $f(x)$, và do đó số lần thử của ta bớt đi nói chung.

Ví dụ. Tìm nghiệm hữu tỉ của đa thức

$$f(x) = x^5 - 8x^4 + 20x^3 - 20x^2 + 19x - 12.$$

Trước hết ta có tổng các hệ số của $f(x)$ bằng 0 nên 1 là nghiệm của $f(x)$. Bằng sơ đồ Hoóc ne (Ch IV, §1, 4), ta tính các hệ số của đa thức thương $g(x)$ trong phép chia $f(x)$ cho $x - 1$

	1	−8	20	−20	19	−12
1	1	−7	13	−7	12	0

do đó các nghiệm còn lại của $f(x)$ là các nghiệm của $g(x)$

$$g(x) = x^4 - 7x^3 + 13x^2 - 7x + 12.$$

Ta nhận xét rằng $g(c) > 0$ với mọi $c < 0$, nên $g(x)$ không có nghiệm âm. Vì vậy ta chỉ xét các ước dương của số hạng tự do : 1, 2, 3, 4, 6, 12. Ta có $g(1) = 12$, $g(-1) = 40$. Vì các số

$$\frac{40}{3}, \frac{40}{7}, \frac{40}{13}$$

không phải là nguyên, nên 2, 6, 12 không phải là nghiệm của $g(x)$. Các số 3 và 4 đều làm cho

$$\frac{g(1)}{1-a} \text{ và } \frac{g(-1)}{1+a}$$

nguyên, nên chúng có thể là nghiệm của $g(x)$. Muốn thử xem chúng có phải là nghiệm của $g(x)$, ta chỉ việc tiếp tục vào bảng trên như sau :

	1	−8	20	−20	19	−12
1	1	−7	13	−7	12	0
3	1	−4	1	−4	0	
4	1	0	1	0		

Vậy ta có

$$f(x) = (x - 1)(x - 3)(x - 4)(x^2 + 1)$$

Các nghiệm nguyên của $f(x)$ là 1, 3, 4.

2. Đa thức bất khả quy của vành Q[x]

Đối với trường số thực **R** và trường số phức **C**, vấn đề xét xem một đa thức đã cho của vành **R**[x] hay **C**[x] có bất khả quy hay không rất đơn giản (§1, 1) ; nhưng trong vành **Q**[x] với **Q** là trường số hữu tỉ thì vấn đề phức tạp hơn nhiều. Đối với các đa thức bậc hai và ba của **Q**[x], việc xét xem có bất khả quy hay không được đưa về việc tìm nghiệm hữu tỉ của các đa thức đó (ch V, §1, bài tập 2) : các đa thức bậc hai và bậc ba của **Q**[x] là bất khả quy khi và chỉ khi chúng không có nghiệm hữu tỉ. Đối với các đa thức bậc lớn hơn ba thì vấn đề phức tạp hơn nhiều. Chẳng hạn đa thức $x^4 + 2x^2 + 1 = (x^2 + 1)^2$ rõ ràng không có nghiệm hữu tỉ nào, nhưng nó có một ước thực sự $x^2 + 1$, vậy không phải là bất khả quy.

Trong mục 1 ta đã nhận xét rằng mọi đa thức $f(x)$ với hệ số hữu tỉ đều có thể viết dưới dạng

$$f(x) = b^{-1} g(x)$$

trong đó b là một số nguyên khác 0, $g(x)$ là một đa thức với hệ số nguyên. Trong vành **Q**[x], $f(x)$ và $g(x)$ là liên kết vậy $f(x)$ là bất khả quy khi và chỉ khi $g(x)$ là bất khả quy. Do đó tiêu chuẩn Aidenstainơ mà ta đưa ra dưới đây để xét một đa thức của **Q**[x] có bất khả quy hay không là tiêu chuẩn cho các đa thức với hệ số nguyên.

Để chuẩn bị cho việc chứng minh tiêu chuẩn ấy, trước hết ta giới thiệu khái niệm đa thức nguyên bản và chứng minh hai bổ đề.

Định nghĩa 1. Giả sử f(x) là một đa thức với hệ số nguyên, f(x) gọi là *nguyên bản* nếu các hệ số của f(x) không có ước chung nào khác ngoài ± 1.

Cho một đa thức với hệ số nguyên $f(x) \in \mathbf{Z}[x]$, kí hiệu bằng a ước chung lớn nhất của các hệ số của $f(x)$, ta có

$$f(x) = af^*(x)$$

với $f^*(x) \in \mathbf{Z}[x]$ và các hệ số của $f^*(x)$ không có ước chung nào khác ngoài ± 1, tức là $f^*(x)$ nguyên bản.

Nếu $f(x) \in \mathbf{Q}[x]$ thì ta có thể viết $f(x)$ dưới dạng

$$f(x) = \frac{a}{b} f^*(x)$$

trong đó $f^*(x)$ nguyên bản và $a, b \in \mathbf{Z}$ nguyên tố cùng nhau.

Ví dụ. $f(x) = 6x^3 + \frac{12x^2}{5} - \frac{15}{2} = \frac{1}{10}(60x^3 + 24x^2 - 75)$

$$= \frac{3}{10}(20x^3 + 8x^2 - 25).$$

Các số 20, 8, −25 không có ước chung nào khác ngoài 1 và −1.

Bổ đề 1. *Tích của hai đa thức nguyên bản là một đa thức nguyên bản.*

Chứng minh. Giả sử

$$f(x) = a_0 + a_1x + \ldots + a_mx^m$$
$$g(x) = b_0 + b_1x + \ldots + b_nx^n$$

là hai đa thức nguyên bản. Ta chỉ cần chứng minh rằng cho một số nguyên tố p tùy ý, p không chia hết các hệ số của đa thức tích $f(x)g(x)$. Rõ ràng p không chia hết các hệ số của $f(x)$ và $g(x)$. Giả sử p chia hết $a_0, \ldots, a_{r-1}$, $b_0, \ldots, b_{s-1}$ và p không chia hết a_r và b_s. Ta xét hệ số c_{r+s} của đa thức tích $f(x)g(x)$.

$c_{r+s} = (\ldots + a_{r-1}b_{s+1}) + a_rb_s + (a_{r+1}b_{s-1} + \ldots)$ trong đó p chia hết các tổng trong các dấu ngoặc, nhưng không chia hết tích a_rb_s vì p là nguyên tố. Do đó p không chia hết c_{r+s}. ■

Bổ đề 2. *Nếu $f(x)$ là một đa thức với hệ số nguyên có bậc lớn hơn 0 và $f(x)$ không bất khả quy trong $\mathbf{Q}[x]$, thì $f(x)$ phân tích được thành một tích những đa thức bậc khác 0 với hệ số nguyên.*

Chứng minh. Giả sử $f(x)$ không bất khả quy trong $\mathbf{Q}[x]$, thế thì $f(x)$ có thể viết

$$f(x) = \varphi(x)\psi(x)$$

với $\varphi(x)$ và $\psi(x)$ là những ước thực sự của $f(x)$ trong $\mathbf{Q}[x]$. Theo như trên đã nhận xét, ta có thể viết

$$\varphi(x) = \frac{a}{b}\, g(x),\ \psi(x) = \frac{c}{d}\, h(x)$$

trong đó $g(x)$, $h(x)$ là những đa thức nguyên bản và a, b, c, d là những số nguyên. Do đó

$$f(x) = \frac{p}{q}\, g(x)\, h(x)$$

với $\frac{p}{q} = \frac{ac}{bd}$ và p, q nguyên tố cùng nhau. Ta kí hiệu các hệ số của đa thức tích $g(x)\ h(x)$ bằng e_i, thế thì theo bổ đề 1, $g(x)\ h(x)$ là nguyên bản, cho nên các e_i không có ước chung nào khác ngoài ± 1. Mặt khác vì $f(x) \in \mathbf{Z}[x]$ nên các số $\frac{pe_i}{q}$ phải là nguyên, do đó q chia hết mọi e_i vì q nguyên tố với p. Ta suy ra $q = \pm 1$, tức là

$$f(x) = \pm p\ g(x)\ h(x).$$

Vì $\varphi(x)$ và $\psi(x)$ là những ước thực sự của $f(x)$ trong $\mathbf{Q}[x]$, nên $g(x)$ và $h(x)$ là những đa thức bậc khác 0 của $\mathbf{Z}[x]$. ■

Tiêu chuẩn Aidenstainơ. *Giả sử*

$$f(x) = a_o + a_1x + \ldots + a_nx^n \quad (n > 1)$$

là một đa thức với hệ số nguyên, và giả sử có một số nguyên tố p sao cho p không chia hết hệ số cao nhất a_n, nhưng p chia hết các hệ số còn lại và p^2 không chia hết số hạng tự do a_o. Thế thì đa thức f(x) là bất khả quy trong $\mathbf{Q}[x]$.

Chứng minh. Giả sử $f(x)$ có những ước thực sự trong $\mathbf{Q}[x]$. Theo bổ đề 2, $f(x)$ có thể viết

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

trong đó

$$g(x) = b_o + b_1x + \ldots + b_rx^r \qquad b_i \in \mathbf{Z},\ 0 < r < n$$

$$h(x) = c_o + c_1x + \ldots + c_sx^s \qquad c_i \in \mathbf{Z},\ 0 < s < n$$

ta có

$$\begin{aligned} a_0 &= b_0c_0 \\ a_1 &= b_1c_0 + b_0c_1 \\ &\dots\dots \\ a_k &= b_kc_0 + b_{k-1}c_1 + \dots + b_0c_k \\ &\dots\dots \\ a_n &= b_rc_s \end{aligned}$$

Theo giả thiết p chia hết $a_0 = b_0c_0$; vậy vì p là nguyên tố, nên hoặc p chia hết b_0 hoặc p chia hết c_0. Giả sử p chia hết b_0, thế thì p không chia hết c_0, vì nếu thế thì p^2 sẽ chia hết $a_0 = b_0c_0$, trái với giả thiết. p không thể chia hết mọi hệ số của $g(x)$, vì nếu thế thì p sẽ chia hết $a_n = b_rc_s$, trái với giả thiết. Vậy giả sử b_k là hệ số đầu tiên của $g(x)$ không chia hết cho p. Ta hãy xét

$$a_k = b_kc_0 + b_{k-1}c_1 + \dots + b_0c_k,$$

trong đó a_k, b_{k-1}, ..., b_0 đều chia hết cho p. Vậy b_kc_0 phải chia hết cho p. Vì p là nguyên tố, ta suy ra hoặc b_k chia hết cho p, hoặc c_0 chia hết cho p, mâu thuẫn với giả thiết về b_k và c_0. ■

Ví dụ. 1) Đa thức $x^4 + 6x^3 - 18x^2 + 42x + 12$ là bất khả quy trong $\mathbf{Q}[x]$. Thật vậy ta có thể áp dụng tiêu chuẩn Aidenstaino với $p = 3$.

2) Đa thức

$$x^n - px^{n-1} - px^{n-2} - \dots - p$$

với p là một số nguyên tố tùy ý, là bất khả quy trong $\mathbf{Q}[x]$.

BÀI TẬP

1. Tìm nghiệm hữu tỉ của các đa thức

a) $x^3 - 6x^2 + 15x - 14$

b) $2x^3 - 3x^2 + 6x - 4$

c) $x^6 - 6x^5 - 11x^4 - x^3 - 18x^2 + 20x - 8$

d) $x^5 - 2x^4 + 6x^3 - 3x^2 - 42x - 48$

2. Giả sử $\frac{p}{q}$, với $p, q \in \mathbf{Z}$ nguyên tố cùng nhau, là nghiệm của đa thức

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_o$$

với hệ số nguyên. Chứng minh rằng :

a) $p \mid a_o$ và $q \mid a_n$

b) $p - mq$ là ước của $f(m)$

với m nguyên ; đặc biệt $p - q$ là ước của $f(1)$, $p + q$ là ước của $f(-1)$.

3. Áp dụng bài tập 2) để tính nghiệm hữu tỉ của đa thức

$$10x^5 - 81x^4 + 90x^3 - 102x^2 + 80x - 21$$

4. Chứng minh rằng đa thức $f(x)$ với hệ số nguyên không có nghiệm nguyên nếu $f(0)$ và $f(1)$ là những số lẻ.

5. Giả sử $p(x)$ là một đa thức với hệ số nguyên và $p(x)$ bất khả quy trong $\mathbf{Z}[x]$. Chứng minh rằng, trong $\mathbf{Z}[x]$, nếu $p(x) \mid f(x)g(x)$, thì hoặc $p(x) \mid f(x)$ hoặc $p(x) \mid g(x)$.

6. Trong vành $\mathbf{Z}[x]$ chứng minh rằng mọi đa thức, khác 0 và khác ± 1, đều có thể viết dưới dạng tích những đa thức bất khả quy.

7. Dùng tiêu chuẩn Aidenstainơ để chứng minh rằng các đa thức sau đây là bất khả quy trong $\mathbf{Q}[x]$.

a) $x^4 - 8x^3 + 12x^2 - 6x + 3$

b) $x^4 - x^3 + 2x + 1$

c) $x^{p-1} + x^{p-2} + \ldots + x + 1$ với p nguyên tố.

Hướng dẫn : đặt $x = y + 1$.

8. Tìm điều kiện cần và đủ để đa thức $x^4 + px^2 + q$ là bất khả quy trong $\mathbf{Q}[x]$.

9. Giả sử $f(x) = (x - a_1)(x - a_2) \ldots (x - a_n) - 1$, với các a_i là những số nguyên phân biệt. Chứng minh rằng $f(x)$ là bất khả quy trong $\mathbf{Q}[x]$.

MỤC LỤC

Công ty CP Sách Đại học Dạy nghề – Nhà xuất bản Giáo dục Việt Nam
giữ quyền công bố tác phẩm

ĐẠI SỐ ĐẠI CƯƠNG

Mã số: 7K108y3-DAI

Số đăng ký KHXB: 54-2013/CXB/80-81/GD

In 1.000 cuốn, QĐ in số: 63, khổ 14,5 x 20,5 cm

In tại: Công ty CP in Thái Nguyên

In xong và nộp lưu chiểu tháng 09 năm 2013