BÙI HUY HIỀN

BÀI TẬP
ĐẠI SỐ ĐẠI CƯƠNG

(Tái bản lần thứ ba)

NHÀ XUẤT BẢN GIÁO DỤC

11 – 2007/CXB/203 – 2119/GD Mã số : 7K150T7 – DAI

LỜI NÓI ĐẦU

Cuốn *Đại số đại cương* của tác giả Hoàng Xuân Sính từ lâu nay đã là một tài liệu hữu ích cho nhiều người làm toán và cả những người học toán. Đặc biệt nó đã là "sách cẩm nang" của nhiều giáo viên dạy toán trong các trường Đại học Sư phạm, Cao đẳng Sư phạm và của sinh viên các trường này.

Trong cuốn sách đó tác giả đã đưa ra một khối lượng bài tập tương đối phong phú, đa dạng và đầy đủ. Tuy vậy, trong đó có nhiều bài tập nhiều độc giả chưa tự giải được. Để giúp cho độc giả có một tài liệu hoàn chỉnh về bộ sách Đại số Đại cương và thuận lợi trong khi sử dụng nó, chúng tôi biên tập cuốn *Bài tập đại số đại cương* này.

Ngoài việc giải tường minh tất cả các bài tập trong cuốn *Đại số đại cương* của tác giả Hoàng Xuân Sính chúng tôi có lựa chọn đưa thêm một số bài tập nhằm giúp độc giả tham khảo và đi sâu hơn vào những nội dung cơ bản trong cuốn sách lí thuyết đã đề cập đến. Chúng tôi không có tham vọng đưa vào đây những bài tập quá khó hoặc có nội dung không gắn với mục đích đã nêu trên.

Cuốn sách này gồm hai phần. Phần I tóm tắt lí thuyết và các đề toán, phần II là lời giải và hướng dẫn. Mỗi phần gồm sáu chương, thứ tự các chương được trình bày theo đúng thứ tự các chương mục trong cuốn *Đại số đại cương*.

Trong phần đề toán, đầu mỗi chương có giành một phần để tóm tắt lí thuyết. Trong phần lời giải đối với những bài tập dễ hoặc cách giải đơn giản chúng tôi chỉ cho lời giải vắn tắt. Đối với những

bài có nhiều cách giải khác nhau chúng tôi chỉ trình bày một cách giải ngắn gọn nhất.

Khi viết cuốn sách này chúng tôi đã nhận được nhiều điều chỉ dẫn quý báu của Giáo sư Tiến sĩ Khoa học Hoàng Xuân Sính, tác giả cuốn Đại số Đại cương. Chúng tôi xin bày tỏ lòng biết ơn chân thành đối với Giáo sư.

Hà Nội, tháng 3 năm 1996
Tác giả

LỜI TỰA CHO LẦN TÁI BẢN CHỈNH LÍ

Cuốn *Bài tập Đại số Đại cương* được xuất bản lần đầu vào năm 1996. Từ khi phát hành, nó đã được nhiều độc giả tìm đọc và sử dụng. Vì lí do đó cho tới nay cuốn sách đã được tái bản nhiều lần với số lượng phát hành khá lớn.

Do sự phát triển không ngừng của Toán học hiện đại nên chương trình giảng dạy môn Toán ở nhiều trường Đại học luôn thay đổi. Đặc biệt, gần đây chương trình Đại số và Số học ở Khoa Toán của các trường Đại học đã có sự thay đổi và điều chỉnh đáng kể nhằm đáp ứng sự phát triển chung của Toán học và phù hợp với năng lực học tập của sinh viên trong giai đoạn mới.

Theo yêu cầu của Nhà xuất bản Giáo dục và theo yêu cầu của nhiều độc giả, một lần nữa, chúng tôi cho tái bản cuốn sách này và bổ sung thêm nhiều bài tập mang tính chất định tính.

Chúng tôi xin chân thành cám ơn những độc giả đã có nhiều ý kiến đóng góp cho cuốn sách trong những lần phát hành trước. Hi vọng cuốn sách này vẫn sẽ là tài liệu học tập và tham khảo hữu ích cho sinh viên và học viên Cao học ở các trường Đại học.

Hà Nội, tháng 1 năm 2005
Tác giả

BẢNG KÍ HIỆU

Kí hiệu	*Định nghĩa*
$\neg, -$	Kí hiệu của phép phủ định
$\neg p, \bar{p}$	Phủ định của p
$\wedge$	Kí hiệu của phép hội
$p \wedge q$	p và q
$\vee$	Kí hiệu của phép tuyển
$p \vee q$	p hoặc q
$\rightarrow$	Kí hiệu của phép kéo theo
$p \rightarrow q$	p kéo theo q
$\leftrightarrow$	Kí hiệu của phép tương đương
$p \leftrightarrow q$	p tương đương q
$\models p$	p là một luật lôgic
$\exists$	Lượng từ tồn tại
$\exists x\ P(x)$	Tồn tại x, P(x)
$\forall$	Lượng từ tổng quát
$\forall x\ P(x)$	Với mọi x, P(x)
$P(x, y, \ldots, z) \equiv Q(x, y, \ldots, z)$	P (x, y, …, z) bằng Q(x, y, …, z)
	P (x, y, …, z) tương đương lôgic với Q(x, y, …, z)
$\mathbb{N}$	Tập hợp các số tự nhiên
$\mathbb{Z}$	Tập hợp các số nguyên

$\mathbb{Q}$	Tập hợp các số hữu tỉ
$\mathbb{R}$	Tập hợp các số thực
$\mathbb{C}$	Tập hợp các số phức
$a \setminus b$	a là ước của b
$\begin{cases} A \subset B\ (A \subseteq B) \\ B \supseteq A\ (B \supseteq A) \end{cases}$	A là tập con của tập hợp B
$A - B$	Hiệu của hai tập hợp A và B
$A \cup B$	Hợp của hai tập hợp A và B
$A \cap B$	Giao của hai tập hợp A và B
$\varnothing$	Tập hợp rỗng
$C_A B$	Phần bù của tập hợp B trong A
$A \times B$	Tích Đề-các của hai tập hợp A và B
$(a_i)_{i \in I}$	Họ phần tử chỉ số hoá bởi tập I
$(A_i)_{i \in I}$	Họ tập hợp chỉ số hoá bởi tập I
(a, b)	Cặp phần tử
A^2	Bình phương Đề-các của tập A
$\prod_{i \in I} A_i$	Tích Đề-các của họ tập hợp A_i
A^I	Luỹ thừa Đề-các bậc I của tập hợp A
$\left.\begin{array}{l} f : X \to Y \\ \overset{f}{X \to Y} \end{array}\right\}$	Ánh xạ f từ X đến Y

1_X, id_X	Ánh xạ đồng nhất của tập X
Hom (X, Y)	Tập hợp các ánh xạ từ X đến Y
S(X)	Tập hợp các song ánh từ X đến Y
<A>	Nhóm sinh bởi tập hợp A
<x>	Nhóm xyclic sinh bởi phần tử x
S_n	Nhóm các phép thế bậc n
$\mathcal{P}(X)$	Tập hợp các bộ phận của tập hợp X
C(G)	Tâm của nhóm G
(a)	Iđêan chính sinh bởi phần tử a
$A \cong B$	Hai nhóm (vành, trường) A và B đẳng cấu với nhau
A[x]	Vành đa thức của ẩn x trên vành A
A(x)	Trường phân thức của ẩn x trên miền nguyên A
$A[x_1, x_2, \ldots, x_n]$	Vành đa thức của n ẩn $x_1, x_2, \ldots, x_n$ trên vành A
C(a) $\bar{a}$	Lớp các phần tử tương đương với phần tử a
Imf	Ảnh của đồng cấu f
Kerf	Hạt nhân của đồng cấu f
G/H	Nhóm thương của nhóm G trên nhóm con chuẩn tắc H
V/I	Vành thương của vành V trên iđêan I

Chương I
CƠ SỞ LÔGIC TOÁN
TẬP HỢP VÀ QUAN HỆ

A. TÓM TẮT LÍ THUYẾT

I. Cơ sở lôgic toán

Những câu phản ánh đúng hoặc sai thực tế khách quan được gọi là những *mệnh đề*. Ta quy ước mệnh đề có giá trị 1 nếu nó đúng và có giá trị 0 nếu nó sai. Mỗi mệnh đề có một và chỉ một trong hai tính chất đúng hoặc sai nên nó chỉ có thể nhận một trong hai giá trị 1 hoặc 0. Các giá trị 1 và 0 được gọi là *giá trị chân lí* của mệnh đề.

Từ các mệnh đề đã cho, bằng một quy tắc nhất định, ta có thể tìm được mệnh đề mới hoàn toàn xác định. Một quy tắc như vậy gọi là một *phép toán lôgic*.

Định nghĩa. *Phủ định* của mệnh đề p, kí hiệu là $\overline{p}$ hoặc $\neg p$ (đọc là không p), là một mệnh đề sai khi p đúng và đúng khi p sai.

Định nghĩa. *Hội* của hai mệnh đề p và q, kí hiệu là $p \wedge q$ (đọc là p và q), là một mệnh đề đúng khi cả p và q đều đúng và sai trong các trường hợp còn lại.

Định nghĩa. *Tuyển* của hai mệnh đề p và q, kí hiệu là $p \vee q$ (đọc là p hoặc q), là một mệnh đề sai khi cả p và q đều sai và đúng trong các trường hợp còn lại.

Định nghĩa. *Mệnh đề kéo theo* $p \rightarrow q$ (đọc là p kéo theo q) là một mệnh đề chỉ sai khi p đúng và q sai, còn đúng trong mọi trường hợp còn lại.

Mệnh đề p *tương đương với* q, kí hiệu là $p \leftrightarrow q$, là một mệnh đề đúng khi và chỉ khi cả hai mệnh đề p và q cùng đúng hoặc cùng sai.

Ta có bảng giá trị chân lí đối với các phép toán lôgic trên như sau :

p	q	$\bar{p}$	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$
0	0	1	0	0	1	1
0	1	1	0	1	1	0
1	0	0	0	1	0	0
1	1	0	1	1	1	1

Định nghĩa. Mỗi *công thức của đại số mệnh đề* là một dãy các kí hiệu thuộc bốn loại :

- Các hằng 1, 0 kí hiệu của mệnh đề đúng hoặc sai ;

- Các biến mệnh đề p, q, i, s, t...;

- Các kí hiệu của các phép toán lôgic $\bar{}$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$;

- Các dấu ngoặc () chỉ thứ tự các phép toán.

Một cách chính xác hơn ta định nghĩa các *hằng* và các *biến mệnh đề* là những *công thức*. Nếu p là công thức thì $\bar{p}$ cũng là công thức. Nếu p và q là những công thức thì $(p \wedge q)$, $(p \vee q)$, $(p \rightarrow q)$, $(p \leftrightarrow q)$ là những công thức.

Định nghĩa. Cho P (a, b, c, ... , g) và Q(a, b, c, ...,g) là hai công thức của các biến mệnh đề a, b, c,..., g. Công thức P(a, b, c,..., g) gọi là *bằng* hay *tương đương lôgic* với công thức Q(a, b, c, ..., g), kí hiệu là

$$P(a, b, c,..., g) \equiv Q(a, b, c, ... , g),$$

nếu chúng nhận giá trị bằng nhau với mọi hệ những giá trị có thể có của các biến mệnh đề.

Công thức P được gọi là *hằng đúng* nếu nó nhận giá trị 1với mọi hệ những giá trị có thể có của các biến mệnh đề. Một công thức hằng đúng còn được gọi là một luật lôgic kí hiệu $\models P$. Công thức P là *hằng sai* nếu nó nhận giá trị 0 với mọi hệ những giá trị có thể có của các biến mệnh đề.

Định nghĩa. Cho $A_1, A_2, \ldots, A_n$ và B là những công thức. Ta nói rằng có một *quy tắc suy luận* với các tiền đề là $A_1, A_2, \ldots, A_n$ và hệ quả lôgic là B nếu và chỉ nếu với mọi hệ giá trị của các biến mệnh đề có mặt trong $A_1, A_2, \ldots, A_n, B$ làm cho $A_1, A_2, \ldots, A_n$ có giá trị bằng 1 thì B cũng có giá trị bằng 1. Ta kí hiệu

$$\frac{A_1, A_2, \ldots, A_n}{B}.$$

Định nghĩa. *Vị từ* n *ngôi* xác định trên tập hợp $M \neq \varnothing$ $(n \geq 1)$ là một ánh xạ xác định trên tập hợp M^n lấy giá trị trong $I = \{0, 1\}$. Vị từ n ngôi còn được gọi là một *hàm mệnh đề* n *biến*.

Miền đúng của vị từ $F(x_1, x_2, \ldots, x_n)$, kí hiệu là $E_{F(x_1, x_2, \ldots, x_n)}$, là tập hợp tất cả các dãy $(a_1, a_2, \ldots, a_n) \in M^n$ sao cho $F(a_1, a_2, \ldots, a_n) = 1$.

Cho F(x) là vị từ 1-ngôi xác định trên tập M.

Định nghĩa. *Lượng từ phổ biến* của F(x), kí hiệu là $\forall x\, F(x)$, đọc là "với mọi x, F(x)", là một mệnh đề đúng khi $E_{F(x)} = M$ và sai khi $E_{F(x)} \neq M$.

Định nghĩa. *Lượng từ tồn tại* của F(x), kí hiệu là $\exists x\, F(x)$, đọc là "tồn tại x, F(x)", là một mệnh đề đúng khi $E_{F(x)} \neq \varnothing$ và sai khi $E_{F(x)} = \varnothing$.

Các định nghĩa trên đây được mở rộng một cách tự nhiên cho vị từ n - ngôi.

II. Tập hợp và quan hệ

1. Tập hợp

Những vật, những đối tượng toán học... được tụ tập do một tính chất chung nào đó thành lập những tập hợp. Các vật x trong tập hợp X được gọi là các *phần tử* của X, kí hiệu là $x \in X$.

Phủ định của $x \in X$ kí hiệu là $x \notin X$.

Hai tập hợp A và B là *bằng nhau* nếu và chỉ nếu mọi phần tử thuộc A thì thuộc B và ngược lại, kí hiệu $A = B$. Tập hợp A được gọi là một *tập con* hay một *bộ phận* của tập hợp B nếu với mọi x, $x \in A$ thì $x \in B$, kí hiệu là $A \subset B$ hoặc $B \supset A$. Như vậy $A = B$ khi và chỉ khi $A \subset B$ và $B \subset A$. Thông thường bộ phận A của tập hợp B được xác định bởi tính chất τ nào đó thì ta kí hiệu như sau

$$A = \{x \in B \mid x \text{ có tính chất } \tau\}.$$

2. Các phép toán trên tập hợp

Định nghĩa. *Hiệu* của hai tập hợp A và B là tập hợp

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

Nếu $B \subset A$ thì $A - B$ được gọi là phần bù của B trong A, kí hiệu là $C_A B$.

Tập hợp $A - A$ được gọi là tập rỗng, đó là tập không chứa một phần tử nào, kí hiệu là $\varnothing$.

Tập hợp các bộ phận của tập hợp X được kí hiệu là $\mathscr{P}(X)$.

Định nghĩa. *Hợp* của hai tập hợp A và B, kí hiệu là $A \cup B$, là tập hợp

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

Định nghĩa. *Giao* của hai tập hợp A và B, kí hiệu là $A \cap B$, là tập hợp

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

Định nghĩa. *Tích Đề-các* của hai tập hợp A và B, kí hiệu là $A \times B$, là tập hợp

$$A \times B = \{(a, b) \mid a \in A \text{ và } b \in B\}.$$

Trong tập hợp $A \times B$, ta có $(a, b) = (u, v) \Leftrightarrow a = u, b = v$.

Nếu $A = B$ thì $A \times A$ được kí hiệu là A^2.

3. Ánh xạ

Định nghĩa. Một *ánh xạ* f từ tập hợp X đến tập hợp Y là một quy tắc chọ tương ứng mỗi phần tử $x \in X$ một phần tử xác định thuộc Y, kí hiệu f(x).

Tập hợp X gọi là *nguồn* và tập hợp Y được gọi là *đích* của ánh xạ f.

Giả sử f là một ánh xạ từ X đến Y.

Bộ phận $\Gamma = \{(x, f(x)) \in X \times Y \mid x \in X\}$ được gọi là *đồ thị* của ánh xạ f. Nếu $A \subset X$ thì bộ phận $f(A) = \{y \in Y \mid \exists a \in A, f(a) = y\}$ được gọi là *ảnh* của tập A qua f và nếu $B \subset Y$ thì bộ phận $f^{-1}(B) = \{x \in X \mid f(x) \in B\}$ được gọi là *tạo ảnh* của B qua f.

Ánh xạ f từ X đến Y được gọi là một *đơn ánh* nếu với mọi x_1 và x_2 thuộc X quan hệ $x_1 \neq x_2$ kéo theo $f(x_1) \neq f(x_2)$; f được gọi là một *toàn ánh* nếu $f(X) = Y$. Một ánh xạ vừa là đơn ánh, vừa là toàn ánh được gọi là một *song ánh*.

Định nghĩa. Cho hai ánh xạ $f : X \to Y$ và $g : Y \to Z$

ánh xạ $gf : X \to Z$

$$x \mapsto gf(x) = f(f(x))$$

được gọi là *tích* (hợp thành) của ánh xạ f và ánh xạ g.

Định lí. Tích của hai đơn ánh là một đơn ánh, tích của hai toàn ánh là một toàn ánh và do đó tích của hai song ánh là một song ánh.

Định lí. Phép lấy tích các ánh xạ có tính chất kết hợp.

Định nghĩa. Cho ánh xạ $f : X \to Y$. Nếu có $g : Y \to X$ sao cho

$$gf = 1_X \text{ và } fg = 1_Y$$

thì g được gọi là *nghịch đảo* hay *ánh xạ ngược* của f, kí hiệu là $g = f^{-1}$.

Định lí. Ánh xạ f có ánh xạ ngược khi và chỉ khi f là một song ánh.

4. Tập hợp chỉ số

Giả sử I là một tập khác rỗng, $f : I \to X$. Khi đó các phần tử $x_i = f(i)$, $i \in I$ lập thành một *họ những phần tử* của X chỉ số hoá bởi tập I, còn tập I được gọi là *tập chỉ số*, kí hiệu $(x_i)_{i \in I}$.

5. Hợp, giao, tích Đề-các của một họ tập hợp

Định nghĩa. Giả sử $(X_i)_{i \in I}$ là một họ tập hợp được chỉ số hoá bởi tập I, $I \neq \varnothing$.

Hợp của họ $(X_i)_{i \in I}$, kí hiệu là $\bigcup_{i \in I} X_i$, là tập hợp gồm các x sao cho x thuộc ít nhất một tập hợp của họ $(X_i)_{i \in I}$.

Giao các họ $(X_i)_{i \in I}$, kí hiệu là $\bigcap_{i \in I} X$, là tập hợp các x sao cho x thuộc tất cả các tập hợp của họ $(X_i)_{i \in I}$.

Định nghĩa. Tích Đề-các của họ $(X_i)_{i \in I}$, kí hiệu là $\prod_{i \in I} X_i$, là tập hợp các họ $(x_i)_{i \in I}$ những phần tử của $X = \bigcup_{i \in I} X_i$ sao cho $x_i \in X_i$ với

mọi $i \in I$. Đặc biệt, nếu tất cả $X_i = X$ với mọi $i \in I$ thì $\prod_{i \in I} X_i$ được kí hiệu là X^I.

6. Quan hệ

Định nghĩa. Một *quan hệ hai ngôi* trên tập hợp X là một bộ phận R của tích Đề-các X^2. Nếu hai phần tử a và b thuộc X mà $(a, b) \in R$ thì ta bảo a có quan hệ R với b và kí hiệu a R b.

Định nghĩa. Quan hệ hai ngôi $R \subset X^2$ được gọi là một *quan hệ tương đương* nếu các điều kiện sau đây thoả mãn :

a) Phản xạ : với mọi a thuộc X, a R a.

b) Đối xứng : với mọi a, b thuộc X nếu a R b thì b R a;

c) Bắc cầu : với mọi a, b, c thuộc X nếu a R b và b R c thì a R c.

Giả sử R là một quan hệ tương đương trên tập X và $a \in X$.

Tập hợp

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

gọi là *lớp tương đương* của a đối với quan hệ R. Ta còn kí hiệu lớp đó là $\bar{a}$.

Ta luôn có

- $\forall a \in X, a \in C(a)$.
- $\forall a \in X, \forall b \in X, a \, R \, b \Leftrightarrow C(a) = C(b)$.
- $\forall a \in X, \forall b \in X$ nếu $C(a) \cap C(b) \neq \varnothing$ thì $C(a) = C(b)$.

Một *sự chia lớp* trên tập hợp X là một tập những bộ phận khác rỗng của X đôi một rời nhau và mỗi phần tử của X thuộc một trong các bộ phận đó. Giả sử R là một quan hệ tương đương trong tập hợp X, thế thì tập các lớp tương đương của X đối với R thành lập một sự chia lớp trên X, kí hiệu

$$X/_R = \{C(a) \mid a \in X\}.$$

Tập này được gọi là *tập thương* của của X theo quan hệ R.

Định nghĩa. Quan hệ hai ngôi $R \subset X^2$ được gọi là một *quan hệ thứ tự* nếu nó thoả mãn các tính chất sau :

a) Phản xạ : với mọi a thuộc X, a R a;

b) Phản đối xứng : với mọi a, b thuộc X, nếu a R b và b R a thì a = b;

c) Bắc cầu : với mọi a, b, c thuộc X, nếu a R b và b R c thì a R c.

Nếu trong X có một quan hệ thứ tự thì X được gọi là một tập sắp thứ tự. Một quan hệ thứ tự thường được kí hiệu là $\leq$, đọc là "bé hơn hay bằng" hoặc $\geq$, đọc là "lớn hơn hay bằng".

Định nghĩa. Cho $\leq$ là một quan hệ thứ tự trong tập X. Phần tử $a \in X$ được gọi là phần tử tối tiểu (tối đại) nếu $\forall x \in X$, $x \leq a$ ($a \leq x$) suy ra x = a. Phần tử $a \in X$ được gọi là phần tử bé nhất (lớn nhất) nếu $\forall x \in X$, $a \leq x$ ($x \leq a$).

Tập sắp thứ tự X được gọi là tập sắp thứ tự tốt nếu mọi tập con khác rỗng của X đều có phần tử bé nhất.

B. BÀI TẬP

1.1. Hãy chứng tỏ rằng mỗi dòng kí hiệu ghi ở dưới đây là một công thức và lập bảng giá trị chân lí của nó, trong đó p, q, r là những công thức :

a) $p \to (q \to r)$;

b) $\overline{(p \vee q)} \wedge r$;

c) $((\overline{p} \wedge q) \wedge \overline{r} \to \overline{q}) \to (p \vee r)$.

1.2. Hãy chứng minh :

a) $(u \to v) \to w \equiv \overline{w} \to \overline{u \to v}$;

b) $p \to (q \to r) \equiv (p \wedge q) \to r$;

c) $(p \to r) \vee (q \to r) \equiv q \to (p \to r)$;

d) $(p \wedge q) \wedge \overline{(p \wedge q)} \vee (\overline{p} \wedge q) \vee \overline{(\overline{p} \wedge q)} \equiv 1$.

1.3. Hãy chứng minh :

a) $(p \vee q) \equiv \overline{(\overline{p} \wedge \overline{q})}$; b) $p \to q \equiv \overline{(p \wedge \overline{q})}$;

c) $p \leftrightarrow q \equiv p \leftrightarrow q \equiv \overline{p \wedge \overline{q}} \wedge \overline{q \wedge \overline{p}}$

1.4. Dùng phép biến đổi đồng nhất để chứng minh các đẳng thức :

a) $(p \to q) \to q \equiv p \vee q$; b) $(p \vee q) \wedge (p \vee \overline{q}) \wedge \equiv p$;

c) $(p \wedge q) \vee (\overline{p} \wedge q) \vee (\overline{p} \wedge \overline{q}) \equiv p \to q$;

d) $p \vee (\overline{p} \wedge q) \equiv p \vee q$;

e) $\overline{p \wedge \overline{q}} \to (\overline{q} \to p) \equiv \overline{p \to q} \vee p \vee q$.

1.5. Chứng minh các đẳng thức sau bằng phép biến đổi đồng nhất và lập bảng giá trị chân lí :

a) $p \to (q \to r) \equiv (p \wedge q) \to r$

b) $p \to (q \to r) \equiv q \to (p \to r)$

c) $(\overline{p} \wedge q \wedge r) \vee (\overline{p} \wedge q \wedge r) \vee (p \wedge r) \equiv (p \to q) \wedge r$.

1.6. Dùng phép biến đổi đồng nhất đưa các công thức sau đây về dạng đơn giản hơn :

a) $(\overline{(\overline{p} \vee q)} \to (p \vee q)) \wedge q$;

b) $\overline{(\overline{p} \vee \overline{q})} \vee ((p \to q) \wedge p)$;

c) $(p \to q) \wedge (q \to r) \to (p \to r)$;

d) $\overline{(p \to q) \wedge (p \to \overline{q})}$;

e) $\overline{(p \wedge q \wedge (p \to \overline{q}))}$.

1.7. Đưa công thức sau về dạng chỉ chứa phép $\vee$, $^-$

a) $(p \to r) \to (p \wedge r)$; b) $(\overline{p} \wedge q) \to (\overline{q} \wedge p)$.

1.8. Đưa công thức sau về dạng chỉ chứa phép $\wedge$, $^-$

a) $(p \vee q) \to (\overline{p} \to r)$ b) $(p \to q) \vee (\overline{p} \to \overline{q})$.

1.9. Đưa công thức sau về dạng chỉ chứa phép $\to$, $^-$

a) $p \vee (q \wedge ((p \wedge q) \vee r))$; b) $\overline{(p \wedge q)} \vee (p \wedge \overline{(p \wedge q)})$.

1.10. Đưa công thức sau về dạng chỉ chứa phép $\vee$, $^-$

a) $p \vee q \to (\overline{p} \wedge q)$; b) $\overline{p \wedge q} \to (p \to q)$;

c) $((p \vee q) \wedge r) \to (p \vee q)$;

d) $(p \vee q) \wedge (\overline{p} \vee q) \wedge (p \vee q)$.

1.11. Đưa công thức sau về dạng chỉ chứa phép $\wedge$, $^-$

a) $p \vee (p \wedge q) \vee (\overline{p} \wedge \overline{q})$; b) $(p \to q) \vee (p \vee \overline{q})$;

c) $(p \wedge q) \vee (p \wedge r) \vee r$;

d) $(p \wedge \overline{q}) \vee (q \vee \overline{p}) \wedge p \vee (p \wedge (p \vee q))$.

1.12. Lập công thức đối ngẫu và công thức phủ định của các công thức sau :

a) $(p \vee \overline{q}) \wedge r$;

b) $\overline{p \vee \overline{q}} \wedge (p \vee (\overline{q} \wedge r)$;

c) $(p \wedge \overline{p \wedge q \wedge r}) \wedge (\overline{p \wedge r})$.

1.13. Dựa vào bảng giá trị chân lí hãy tìm xem trong những công thức sau đây, công thức nào hằng đúng, công thức nào hằng sai?

a) $(p \wedge q) \to (p \vee q)$;

b) $(p \to q) \to (\overline{q} \to \overline{p})$;

c) $p \to (p \wedge q)$;

d) $(p \wedge q) \wedge (\overline{p \vee q})$;

e) $(\overline{p} \wedge \overline{q}) \to (\overline{q} \wedge p)$;

f) $(p \vee q) \to (p \to r)$;

g) $(p \to r) \to (p \to r) \to (p \vee q) \to r$;

h) $(\overline{p} \wedge q \wedge r) \vee (p \wedge \overline{q} \wedge r) \vee (p \wedge q \wedge \overline{r}) \vee (\overline{p} \wedge \overline{q} \wedge \overline{r})$.

1.14. Chứng minh các công thức sau đây là những công thức hằng đúng, viết các luật tương ứng :

a) $p \to \overline{p}$;

b) $p \to (q \to p)$;

c) $(p \wedge q) \to p$;

d) $p \to (p \vee q)$;

e) $(p \wedge (p \to q)) \to q$;

f) $(\overline{q} \wedge (\overline{p} \to q)) \to \overline{p}$;

g) $((p \to q) \wedge (q \to r)) \to (p \to r)$;

h) $(p \wedge \overline{q}) \to (\overline{p \to q})$.

1.15. Chứng minh các công thức sau đây là hằng sai :

a) $(p \to q) \wedge p \wedge q$;

b) $p \wedge (\overline{q \to p})$.

1.16. Hãy chứng tỏ rằng các công thức sau đây không hằng đúng và không hằng sai :

a) $(p \vee q) \to r$; b) $(p \wedge q) \to (p \to q)$;

c) $((p \to r) \wedge (q \to r)) \to (p \to q)$.

1.17. Chứng minh các suy luận sau :

$$\frac{p}{q \to p};$$

$$\frac{p, p \to q, q \to r}{r};$$

$$\frac{p \to q}{(p \to r) \to (p \to r)};$$

$$\frac{q \to r}{(p \to q) \to (p \to r)};$$

$$\frac{p \to (q \to r)}{(p \to q) \to (p \to r)};$$

$$\frac{p, q}{p \wedge q};\ \frac{p, q}{p};\ \frac{p, q}{q};\ \frac{p}{p \vee q};\ \frac{q}{p \vee q};$$

$$\frac{p \to q, p \to r}{p \to (q \wedge r)};$$

$$\frac{p \to r, q \to r}{(p \vee q) \to r};$$

$$\frac{p \to q, r \to t}{(p \wedge r) \to (q \wedge t)};$$

$$\frac{p \to q, r \to t}{(p \vee r) \to (q \vee t)};$$

$$\frac{p \vee q, \bar{p}}{q}; \quad \frac{p \vee q, \bar{q}}{p};$$

$$\frac{\bar{p}}{p \to q}; \quad \frac{\bar{p} \to p}{p};$$

$$\frac{\overline{p \to q} \to (r \wedge \bar{r})}{p \to q}; \quad \frac{(p \wedge \bar{q}) \to (r \wedge \bar{r})}{p \to q};$$

$$\frac{(p \wedge \bar{q}) \to \bar{p}}{p \to q}; \quad \frac{\bar{q} \to p}{p \to q}.$$

1.18. Giả sử S và T là hai công thức. Chứng minh rằng có các quy tắc suy luận $\frac{S}{T}$ và $\frac{T}{S}$ khi và chỉ khi $S \equiv T$.

1.19. Chứng minh rằng nếu mệnh đề $p_1 \vee p_2 \vee \ldots \vee p_n$ đúng và nếu các mệnh đề $q_1, q_2, \ldots, q_n$ bài xích lẫn nhau từng đôi một (không có hai mệnh đề cùng đúng) và tất cả các mệnh đề :

$$p_1 \to q_1$$

$$p_2 \to q_n$$

$$\ldots$$

$$p_n \to p_n$$

đúng thì tất cả các mệnh đề :

$$q_1 \to p_1$$

$$q_2 \to p_2$$

$$\ldots$$

$$q_n \to p_n$$

cũng đúng.

1.20. Một trong năm bạn của tổ I đánh vỡ kính cửa sổ. Khi được hỏi, các em lần lượt trả lời :

- Chỉ có thể hoặc là Bảo, hoặc là Tuấn – An nói.

- Tôi không đánh vỡ, cả Khôi cũng thế – Bảo cãi lại .

- Cả hai đều không đúng – Tuấn lên tiếng.

- Không phải thế Tuấn ạ, một bạn nói đúng, một bạn nói sai – Đức tiếp lời.

- Đức nói không đúng – Khôi can thiệp.

Thầy giáo chủ nhiệm lớp (mà hiển nhiên ta có thể tin tưởng được), tin chắc rằng ba trong năm em đã nói đúng.

Hỏi ai đánh vỡ kính?

1.21. Thẩm phán hỏi cung ba người bị nghi là phạm tội. Trong buổi lấy cung, A nói rằng lời khai của B không đúng, B nói rằng lời khai của C không đúng. Cuối cùng C nói rằng A nói sai và B nói sai. Dựa trên các lời khai đó thẩm phán có thể biết ai trong ba người bị tình nghi nói đúng hay không?

1.22. Bốn bạn A, B, C, D quyết định đi tham quan. Mỗi người sẽ đi một trong bốn thành phố khác nhau : Hà Nội, Hải Phòng, Nha Trang, Thành phố Hồ Chí Minh. Hỏi ai đi thành phố nào, biết rằng :

1) Nếu A không đi Hà Nội thì C không đi Hải Phòng.

2) Nếu B không đi Hà Nội, không đi Thành phố Hồ Chí Minh thì A đi Hà Nội;

3) Nếu C không đi Thành phố Hồ Chí Minh thì B đi Nha Trang.

4) Nếu D không đi Hà Nội thì B đi Hà Nội.

5) Nếu D đi Hải Phòng thì B không đi Hà Nội.

1.23. Sáu sinh viên A, B, C, D, E, M thi kì thi vô địch về môn Toán. Hai trong sáu người làm được bài. Khi Trưởng đoàn hỏi các em, ai làm được bài thì nhận được các câu trả lời như sau :

1) A và C làm được bài.

2) Chỉ B và E làm được bài.

3) Chỉ M và B làm được bài.

4) A và M làm được bài.

5) A và D làm được bài.

Bốn câu trong năm câu trả lời trên đúng một nửa, còn một câu sai hoàn toàn. Vậy ai đã làm được bài?

1.24. Một thí sinh đến trước một máy chấm thi. Có năm câu hỏi cần trả lời "có" hay "không". Trả lời đúng thì máy cho một điểm.

Một thí sinh nhận thấy mình không biết nên trả lời đúng cho một câu nào. Nhưng anh ta biết rằng :

1) Các câu đầu và cuối phải trả lời ngược nhau.

2) Câu thứ hai và thứ tư phải trả lời như nhau.

3) Ít nhất một trong hai câu đầu phải trả lời bằng khẳng định;

4) Nếu câu thứ tư trả lời "có" thì câu thứ năm phải trả lời "không".

Sau khi tính toán, thí sinh biết rằng có thể được 4 điểm và nếu may mắn thì được 5 điểm. Hỏi thí sinh đó đã tính toán như thế nào? Anh ta đã trả lời ra sao?

1.25. Xác định xem trong số các câu sau đây câu nào là mệnh đề, câu nào là hàm mệnh đề? Trong trường hợp câu là hàm mệnh đề hãy tìm miền đúng của nó.

a) $2^0 = 1$; b) $x^0 = 1$; c) $x^2 \geq 0$;

d) $ax^2 + bx + c > 0$ với a. b. c là những số thực khác 0 ;

e) Đường thẳng x song song với đường thẳng y.

1.26. Tìm miền đúng của các hàm mệnh đề sau :

a) φ(x) : "x là ước chung của 12 và 18".

b) φ(x, y) : "x và y là các số nguyên thoả mãn 2x + 6y = 5".

c) f(x, y) : "x và y là các số thực thỏa mãn $x^2 + y^2 = 1$".

1.27. Hãy phát biểu thành lời mỗi câu tương ứng với các hàm mệnh đề sau :

a) $(p(x,y) \wedge q(y,z)) \rightarrow (p(x,z))$. Trong đó p(x, y) là "x chia hết cho y", q(y, z) là "y bằng z".

b) $(\overline{p(x)} \wedge \overline{q(x)}) \rightarrow r(x)$. Trong đó :

p(x) là "x là số nguyên tố"; q(x) là "x là số lẻ"; r(x) là "x chia hết cho 2".

1.28. Giả sử φ(x) là một hàm mệnh đề của biến x xác định trên tập X. Ta kí hiệu $E_{\varphi(x)}$ là miền đúng của φ(x). Hãy chứng minh các đẳng thức sau đây :

a) $E_{\varphi(x) \vee \psi(x)} = E_{\varphi(x)} \cup E_{\psi(x)}$;

b) $E_{\varphi(x) \vee \psi(x)} = E_{\varphi(x)} \cap E_{\psi(x)}$;

c) $E_{\overline{\varphi(x)}} = C_X(E_{\varphi(x)})$, trong đó X là miền xác định của hàm mệnh đề φ(x).

d) $E_{(\varphi(x) \rightarrow \psi(x))} = C_X(E_{\varphi(x)}) \cup E_{\psi(x)}$, trong đó X là miền xác định của hàm mệnh đề φ(x).

b) $E_{\varphi(x)\vee\psi(x)} = E_{\varphi(x)} \cap E_{\psi(x)}$;

c) $E_{\overline{\varphi(x)}} = C_X(E_{\varphi(x)})$, trong đó X là miền xác định của hàm mệnh đề $\varphi(x)$.

d) $E_{(\varphi(x)\to\psi(x))} = C_X(E_{\varphi(x)}) \cup E_{\psi(x)}$, trong đó X là miền xác định của hàm mệnh đề $\varphi(x)$.

1.29. Cho ba hàm mệnh đề $\varphi(x)$, $\psi(x)$ và $\theta(x)$ xác định trên miền X. Đặt $A = E_{\varphi(x)}$, $B = E_{\psi(x)}$, $C = E_{\theta(x)}$ (xem hình vẽ dưới đây).

Hãy xác định miền đúng của các hàm mệnh đề sau bằng các miền gạch chéo.

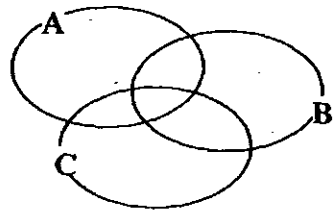
a) $\varphi(x) \vee \psi(x) \vee \theta(x)$;

b) $\varphi(x) \wedge \psi(x) \wedge \theta(x)$;

c) $[\varphi(x) \wedge \psi(x)] \vee \theta(x)$;

d) $[\varphi(x) \vee \psi(x)] \wedge \theta(x)$;

e) $(\varphi(x) \to \psi(x)) \wedge \theta(x)$;



Hình 1

f) $(\overline{\varphi(x) \to \psi(x)}) \vee \theta(x)$.

1.30. Hãy chứng minh các đẳng thức tập hợp sau đây :

a) $C_X\left(E_{\varphi(x)\to\overline{\psi(x)}}\right) = E_{\varphi(x)\to\overline{\psi(x)}}$

b) $C_X\left(E_{\varphi(x)\wedge\overline{\psi(x)}}\right) = C_X\left(E_{\varphi(x)}\right) \cup C_X\left(E_{\psi(x)}\right)$.

Trong đó $\varphi(x)$ và $\psi(x)$ là những hàm mệnh đề xác định trên miền X.

c) $(\exists x \in \mathbb{R})\,(\forall y \in \mathbb{R})\,(x + y = 6)$;

d) $(\forall x \in \mathbb{R})\,(\exists y \in \mathbb{R})\,(x + y = 6)$.

1.32. Hãy dùng kí hiệu để viết các mệnh đề sau rồi chỉ ra tính đúng sai của nó.

a) Tồn tại số thực x sao cho với mọi số thực y có $yx = y$.

b) Với mọi số thức x, y tồn tại số thực z sao cho $x + z = y$.

c) Không tồn tại số hữu tỉ x sao cho $x^2 = 3$.

1.33. Cho x, y, x là những số thực. Trước các vị từ sau, hãy đặt các lượng từ thích hợp để có được mệnh đề đúng :

a) $(x + y)\,z = xz + yz$; b) $x + 1 > y$;

c) $2x + 3x = 5$; d) $(x = y) \vee (x > y) \vee (x < y)$.

1.34. Tìm phủ định của các mệnh đề sau đây :

a) $(\forall x \in \mathbb{R},\ \forall y \in \mathbb{R},\ \forall z \in \mathbb{R})\,(x + y = z)$;

b) $(\forall \varepsilon \in \mathbb{R}^+,\ \exists \delta \in \mathbb{R}^+,\ \forall x \in \mathbb{R} : |x - a| < \delta)\ |f(x) - f(a)| < \varepsilon$.

Trong đó $\mathbb{R}^+$ là tập hợp các số thực dương.

1.35. Cho $X = \{a_1, a_2, \ldots, a_n\}$ là tập hợp hữu hạn gồm n phần tử. Chứng minh rằng nếu $\varphi(x)$ là một hàm mệnh đề xác định trên X thì có

a) $(\forall x \in X)\ \varphi(x) \equiv \varphi(a_1) \wedge \varphi(a_2) \wedge \ldots \wedge \varphi(a_n)$;

b) $(\exists x \in X)\ \varphi(x) \equiv \varphi(a_1) \vee \ldots \vee \varphi(a_n)$.

Hãy dùng các đẳng thức trên để chứng minh :

c) $\overline{(\forall x \in X)\ \varphi(x)} \equiv (\exists x \in X)\ \overline{\varphi(x)}$;

d) $\overline{(\exists x \in X)\ \varphi(x)} \equiv (\forall x \in X)\ \overline{\varphi(x)}$.

1.36. 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 rằng có ít nhất một tập hợp A_i không chứa một tập nào trong các tập còn lại.

1.37. Chứng minh rằng $A - (A - B) = B$ khi và chỉ khi $B \subset A$.

1.38. Giả sử X là một tập hợp có n phần tử và r là một số tự nhiên khác 0 và bé hơn hay bằng n. Tính :

a) Số các bộ phận của X có r phần tử;

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

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

a) $A = \{ x \in \mathbb{R} \mid 1 \leq x \leq 3 \}$;

b) $B = \mathbb{R}$;

c) $A = B = \mathbb{Z}$.

1.40. Biểu diễn hình học tập hợp X các (x, y) của mặt phẳng Đề-các có dạng (x, x) với $0 \leq x \leq 1$ hoặc có dạng $(x, x + 1)$ với $x \geq 0$.

1.41. 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) $A \cap \varnothing = \varnothing$;

d) $A \cup \varnothing = A$.

1.42. Tập hợp X ở bài 1.40 có phải là đồ thị của một ánh xạ từ $\mathbb{R}$ đến $\mathbb{R}$ hay không?

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

1.44. Tập hợp $G = \left\{ \left(x, \frac{1}{x-1} \right) \middle| \, x \in \mathbb{R}, x \neq 1 \right\}$ có thể coi là đồ thị của một ánh xạ như thế nào? Biểu diễn hình học tập hợp đó.

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

1.46. Giả sử n là một số tự nhiên cho trước,

$f : \mathbb{N} \to \mathbb{N}$ là một ánh xạ được xác định bởi

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

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

1.47. Giả sử $f : X \to Y$ và $g : Y \to X$ là hai ánh xạ và $h = gf$ là ánh xạ tích của chúng. 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 ảnh, nếu thêm g là đơn ánh thì f là toàn ánh.

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

1.49. 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 $fg = 1_Y$.

1.50. Cho ba ánh xạ $f : X \to Y$; $g, g' : V \to X$. Chứng minh :

a) Nếu f là đơn ánh và $fg = fg'$ thì $g = g'$.

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

1.51. Cho ba ánh xạ : $f : X \to Y$; $h, h' : Y \to Z$ chứng minh :

a) Nếu f là một toàn ánh thì $h.f = h'f$ suy ra $h' = h$.

b) Nếu với mọi h, h', với mọi Z mà $hf = h'f$ kéo theo $h' = h$ thì f là toàn ánh.

1.52. Chứng minh rằng 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.

1.53. Chứng minh rằng điều kiện cần và đủ để cho một bộ phận G của tích Đề-các $X \times Y$ là đồ thị của một ánh xạ từ X đến Y là ánh xạ $G \to X$

$$(x,y) \mapsto x$$

là một song ánh.

1.54. Giả sử $(A_i)_{i\in I}$ là một họ những bộ phận của tập hợp X. B là một tập hợp tuỳ ý. Chứng minh :

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

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

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

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

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

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

1.55. Giả sử $f : X \to Y$ là một ánh xạ. $(A_i)_{i\in I}$ là một họ những bộ phận của X, $(B_j)_{j\in J}$ là một họ những bộ phận của Y. Chứng minh :

a) $f(\bigcup_{i\in I} A_i) = \bigcup_{i\in I} f(A_i)$;

b) $f(\bigcap_{i\in I} A_i) \subset \bigcap_{i\in I} f(A_i)$;

c) $f^{-1}(\bigcup_{i\in j} B_j) = \bigcup_{j\in j} f^{-1}(B_j)$;

d) $f^{-1}(\bigcap_{j\in j} B_j) = \bigcap_{j\in j} f^{-1}(B_j)$.

1.56. Ta kí hiệu Hom(X, Y) là tập hợp tất cả các ánh xạ từ X đến Y. Chứng minh :

a) Có một song ánh từ Hom(X, Y) đến Y^X.

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

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

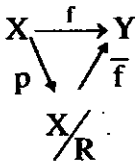
1.57. Giả sử $f : X \to Y$ là một ánh xạ. R là bộ phận của X^2 gồm các cặp (x, x') sao cho f(x) = f(x').

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

b) Xét tập hợp $X/_R$ và ánh xạ

$$p : X \to X/_R$$
$$x \mapsto C(x)$$

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



nghĩa là $f = \bar{f}p$.

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

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

(a, b) S (c, d) khi và chỉ khi ad = bc.

Chứng minh :

a) S là một quan hệ tương đương;

b) Có một song ánh từ tập thương $\mathbb{Z}\times\mathbb{N}^*/_S$ đến tập các số hữu tỉ $\mathbb{Q}$.

1.59. Giả sử S là một quan hệ hai ngôi xác định trong $\mathbb{Z}$ bởi các cặp (x, y) với $x, y \in \mathbb{Z}$ và x + y lẻ. Chứng minh :

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

b) S không phải là quan hệ thứ tự, cũng không phải là quan hệ tương đương.

1.60. Cũng câu hỏi trong bài tập 1.59. Thay giả thiết x + y lẻ bởi giả thiết x + y chẵn.

1.61. Giả sử X là một tập hợp, T là một quan hệ hai ngôi có tính chất phản xạ, đối xứng trong X. Ta xác định 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 $x_1 T x_2, x_2 T x_3 \ldots, x_{n-1} T x_n$. 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 $S \subset H$.

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

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

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

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

b) S có là quan hệ tương đương trong $X - \{0\}$ hay không? Nếu có, hãy xác định các lớp tương đương.

1.64. Cho $S \subset X^2$ là một quan hệ hai ngôi trong tập hợp X. Ta gọi là quan hệ ngược của S, kí hiệu là S^{-1}, tập con của X^2 xác định bởi $(x, y) \in S^{-1}$ khi và chỉ khi $(y, x) \in S$. Chứng minh :

a) Nếu S là một quan hệ thứ tự thì S^{-1} cũng là một quan hệ thứ tự.

b) Nếu S là một quan hệ tương đương thì S^{-1} cũng là một quan hệ tương đương.

1.65. Giả sử S là một quan hệ tương đương trong tập hợp X. Chứng minh rằng nếu $S \neq \{(x, x) \mid x \in X\}$, thì S không phải là một quan hệ thứ tự trong X.

1.66. Cho tập hợp $X = \mathbb{N}^n$ $(n \geq 1)$. Trong X ta xác định quan hệ S như sau :

$(a_1, a_2, \ldots, a_n)$ S $(b_1, b_2, \ldots, b_n)$ khi và chỉ khi

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

hoặc có một chỉ số i $(i = 1, 2, \ldots, n)$ sao cho

$$a_1 = b_1, a_2 = b_2, \ldots, a_{i-1} = b_{i-1}, a_i < b_i.$$

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

1.67. Giả sử $f : X \to \mathbb{N}$ là một đơn ánh từ tập hợp X đến tập các số tự nhiên $\mathbb{N}$. Quan hệ hai ngôi S trong X xác định bởi x S x'

khi và chỉ khi $f(x) \leq f(x')$. Chứng minh S là một quan hệ thứ tự toàn phần.

1.68. Cho hai tập hợp X và Y. Gọi $\Phi(X, Y)$ là tập hợp các ánh xạ từ các tập con của X đến Y. Xét quan hệ S trong $\Phi(X, Y)$ xác định như sau :

f S g khi và chỉ khi g là mở rộng của 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.

1.69. Chứng minh rằng 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.

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

1.71. Chứng minh các tập hợp trong bài tập 1.66 và 1.67 là sắp thứ tự tốt (tập hợp sắp thứ tự X được gọi là sắp thứ tự tốt nếu mọi bộ phận khác rỗng của X đều có phần tử bé nhất).

Chương II
NỬA NHÓM VÀ NHÓM

A. TÓM TẮT LÍ THUYẾT

1. Nửa nhóm

Định nghĩa. Một *phép toán hai ngôi* trong tập hợp X là một ánh xạ $T : X^2 \to X$. Ảnh của $(x, y) \in X^2$ qua ánh xạ T được gọi là *hợp thành* của x và y đối với phép toán T, kí hiệu là xTy.

Thông thường phép toán T được kí hiệu là . (phép nhân) hoặc + (phép cộng) hợp thành x.y còn được viết là xy.

Phần tử $e \in X$ được gọi là *phần tử trung lập* (đối với phép toán T) nếu và chỉ nếu với mọi $x \in X$ có eTx = xTe = x.

Phép toán hai ngôi T trong tập hợp X được gọi là *kết hợp* nếu và chỉ nếu với mọi x, y, $z \in X$ ta có xT(yTz) = (xTy)Tz.

Phép toán hai ngôi T trong tập hợp X được gọi là *giao hoán* nếu và chỉ nếu với mọi x, $y \in X$ ta có xTy = yTx.

Định nghĩa. 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 được gọi là một *vị nhóm.*

Một nửa nhóm mà phép toán của nó là giao hoán được gọi là *nửa nhóm giao hoán.*

2. Nhóm

Định nghĩa. Ta gọi là *nhóm* một vị nhóm X trong đó mọi phần tử của X đều có phần tử đối xứng, nghĩa là với mọi $x \in X$ có một $x' \in X$ sao cho x'x = xx' = e (e là phần tử trung lập của vị nhóm X). Nếu phép toán trong X là giao hoán thì X được gọi là một nhóm giao hoán hay nhóm Aben.

Nếu tập hợp X có hữu hạn phần tử thì nhóm X được gọi là một nhóm có cấp hữu hạn. Số phần tử của X được gọi là cấp của X và kí hiệu là |X|.

Nếu tập X có vô số phần tử thì X được gọi là nhóm có cấp vô hạn.

Trong một nhóm X ta có các tính chất sau đây:

a) Phần tử trung lập của X là duy nhất.

b) Với mỗi phần tử $x \in X$, phần tử đối xứng x' của x là duy nhất (nếu phép toán trong X là phép nhân (.) thì kí hiệu $x' = x^{-1}$, nếu phép toán trong X là phép cộng (+) thì kí hiệu $x' = -x$).

c) Với mọi x, y, z thuộc X, đẳng thức

$$xy = xz \quad (yx = zx) \text{ kéo theo } y = z.$$

d) Với mọi a, b thuộc X, phương trình

$$ax = b \quad (ya = b) \text{ có nghiệm duy nhất thuộc X.}$$

e) Với mọi a, b thuộc X

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

Nếu đặt $a^0 = e$ thì với mọi số nguyên m, n ta có:

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

$$a^n.a^m = a^{n+m}$$

$$(a^n)^m = a^{nm}.$$

Định lí. Giả sử X là một nửa nhóm khác rỗng, thế thì các tính chất sau là tương đương:

(i) X là một nhóm;

(ii) Tồn tại phần tử $e \in X$ sao cho với mọi $a \in X$, $ea = a$ và với mọi $a \in X$, tồn tại $a' \in X$ sao cho $a'a = e$;

(iii) Với mọi a và b thuộc X, các phương trình $ax = b$ và $ya = b$ có nghiệm trong X.

3. Nhóm con

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

Định lí. Giả sử A là một bộ phận khác rỗng của một nhóm X thế thì 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.

Giả sử U là một bộ phận của nhóm X, khi đó giao của họ các nhóm con của X chứa U là một nhóm con của X chứa U, nó được gọi là *nhóm con của* X *sinh ra bởi* U, kí hiệu là <U>. Nếu $U=\{x\}$ thì nhóm con của X sinh bởi U được gọi là *nhóm con xyclic* của X sinh bởi phần tử x, x được gọi là *phần tử sinh* của < x >. Nhóm X được gọi là xyclic nếu nó được sinh ra bởi một phần tử x$\in$X.

Nếu < x > là nhóm có cấp n thì n được gọi là cấp của phần tử x.

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

Hệ quả. Cấp của một nhóm hữu hạn X là bội của cấp của mọi phần tử của X.

4. Nhóm con chuẩn tắc

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

Định lí. Một nhóm con A của một nhóm X là chuẩn tắc nếu và chỉ nếu với mọi x $\in$ X ta có xA = Ax với $xA=\{xa\,|\,a\in A\}$ và $Ax=\{ax\,|\,a\in A\}$.

5. Nhóm thương

Định nghĩa. Nếu A là một nhóm con chuẩn tắc của một nhóm X thì $X/A = \{xA \mid x \in A\}$ cùng với phép toán $xA.yA = xyA$ là một nhóm, gọi là *nhóm thương* của X trên A.

6. Đồng cấu

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

$$f(ab) = f(a)f(b), \text{ với mọi a và b thuộc X.}$$

Nếu X = Y thì đồng cấu f được gọi là một *tự đồng cấu* của X.

Một đồng cấu là một đơn ánh được gọi là một *đơn cấu*, một đồng cấu là một toàn ánh được gọi là một *toàn cấu*, một đồng cấu song ánh được gọi là một *đẳng cấu*. Nếu có một đẳng cấu từ một nhóm X đến một nhóm Y thì ta nói rằng *hai nhóm X và Y đẳng cấu với nhau*, kí hiệu là $X \cong Y$.

Giả sử $f : X \to Y$ là một đồng cấu, tập hợp $Imf = f(X)$ được gọi là *ảnh* của đồng cấu f và $Kerf = f^{-1}(e_Y)$ được gọi là *hạt nhân* của đồng cấu f (e_Y là phần tử trung lập của nhóm Y).

Giả sử $f : Y \to X$ là một đồng cấu. Khi đó ta có các tính chất sau:

a) $f(e_X) = e_Y$; e_X, e_Y theo thứ tự là phần tử trung lập của X và của Y.

b) $f(a^{-1}) = [f(a)]^{-1}$;

c) Nếu A là một nhóm con của nhóm X thì f(A) là một nhóm con của Y. Đặc biệt Imf là một nhóm con của nhóm Y.

d) Nếu B là một nhóm con chuẩn tắc của Y thì $f^{-1}(B)$ là một nhóm con chuẩn tắc của X. Đặc biệt Kerf là một nhóm con chuẩn tắc của X.

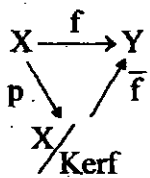
e) f là một đơn cấu khi và chỉ khi $\text{Ker}f = \{e_X\}$.

g) f là một toàn cấu khi và chỉ khi $\text{Im}f = Y$.

h) Nếu f là một đẳng cấu thì f^{-1} cũng là một đẳng cấu.

Định lí. Nếu $f : X \to Y$ và $g : Y \to Z$ là những đồng cấu thì $gf : X \to Z$ cũng là một đồng cấu.

Định lí (định lí đồng cấu). Giả sử $f : X \to Y$ là một đồng cấu. Thế thì có một đơn cấu duy nhất $\bar{f} : X/\text{Ker}f \to Y$ sao cho tam giác



giao hoán, tức là $f = \bar{f}p$; $\text{Im}\bar{f} = \text{Im}f$, trong đó

$$p : X \to X/\text{Ker}f$$
$$x \mapsto \bar{x}$$

là toàn cấu chính tắc.

Như vậy nếu f là toàn cấu thì $Y \cong X/\text{Ker}f$.

B. BÀI TẬP

2.1. Giả sử X là một tập hợp tuỳ ý. Xét ánh xạ

$$X^2 \to X$$
$$(x, y) \mapsto x$$

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

2.2. 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 có suy ra ab = ba hay không?

2.3. Gọi X là tập thương của $\mathbb{Z}$ trên quan hệ đồng dư theo modun n.

a) Với mỗi cặp $(\bar{a}, \bar{b})$ ta cho tương ứng lớp tương đương $\overline{ab}$. Chứng minh khi đó có một ánh xạ từ X^2 đến X.

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

c) Nếu cho tương ứng mỗi cặp $(\bar{a}, \bar{b})$ là lớp $\overline{ab}$. Chứng minh lúc đó X cũng là một vị nhóm giao hoán.

2.4. Giả sử là một tập thương của $\mathbb{Z} \times \mathbb{N}^*$ trên quan hệ tương đương S xác định bởi (a, b) S (c, d) khi và chỉ khi ad = bc.

Ta kí hiệu các phần tử C(a, b) của X bằng $\frac{a}{b}$ với $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$.

a) Với mỗi cặp $(\frac{a}{b}, \frac{c}{d})$ cho tương ứng lớp tương đương $\frac{ad+bc}{bd}$. Chứng minh rằng như vậy ta có một ánh xạ từ X^2 đến X.

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

c) Nếu 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.

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

a) Chứng minh $\mathbb{N}^n$ cùng với phép toán

$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$ là một vị nhóm giao hoán.

b) Trong $\mathbb{N}^n$ đã xác định quan hệ thứ tự (chương I. bài 1.66), chứng minh nếu $\alpha, \beta \in \mathbb{N}^n$ sao cho $\alpha < \beta$ thì

$$\alpha + \gamma < \beta + \gamma \text{ với mọi } \gamma \in \mathbb{N}^n.$$

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

2.7. Chứng minh các tập hợp sau đây với phép toán thông thường 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 cho trước 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 khác 0 với phép nhân;

9) Tập hợp các số phức với modun bằng 1 với phép nhân;

10) Tập hợp các số hữu tỉ có dạng 2^n, $n \in \mathbb{Z}$ 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 có dạng $a + b\sqrt{3}$ với a và b thuộc $\mathbb{Z}$ cùng với phép cộng ;

14) Tập hợp các số thực có dạng $a + b\sqrt{3}$ với phép nhân (ở đó $a, b \in \mathbb{Q}$ và $a^2 + b^2 \neq 0$) ;

15) Tập hợp các số phức có dạng a + bi với phép cộng (ở đó $a, b \in \mathbb{Z}$) ;

16) Tập hợp các vectơ n chiều của không gian $\mathbb{R}^n$ với phép cộng vectơ ;

17) Tập hợp các ma trận thực vuông cấp n với phép cộng ma trận ;

18) Tập hợp các ma trận thực vuông cấp n không suy biến với phép nhân ma trận;

19) Tập hợp các ma trận thực vuông cấp n với định thức bằng 1 với phép nhân ma trận;

20) Tập hợp các đa thức (với hệ số thực) với phép cộng các đa thức;

21) Tập hợp gồm đa thức 0 và các đa thức có bậc không quá n (n là một số tự nhiên cho trước) với phép cộng các đa thức.

Trong các nhóm trên đây nhóm nào là nhóm con của nhóm nào?

2.8. Cho X là một nửa nhóm khác rỗng. Với mỗi $a \in X$ 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 $aX = Xa = X$.

2.9. Cho X là một tập tuỳ 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.

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

2.11. Cho một họ khác rỗng những nhóm $(X_i)_{i\in I}$ mà các phép toán kí hiệu bằng dấu nhân. Chứng minh rằng tập hợp tích Đề-các $\prod_{i\in I} X_i$ với phép toán xác định như sau

$$(x_i)_{i\in I} . (y_i)_{i\in I} = (x_i y_i)_{i\in I}$$

là một nhóm (gọi là tích của các nhóm X_i).

2.12. Giả sử $(X_i)_{i\in I}$ là một họ khác rỗng những nhóm.

$X = \prod_{i\in I} X_i$ là tích trực tiếp của họ $(X_i)_{i\in I}$. Các ánh xạ p_i cho bởi $p_i : X \to X_i$

$$x \mapsto x_i, \ i \in I.$$

a) Chứng minh rằng các ánh xạ p_i đều là toàn cấu với mọi $i \in I$.

b) Cho Y là một nhóm và các ánh xạ $(f_i : Y \to X_i)_{i\in I}$ là một họ những đồng cấu. Chứng minh rằng tồn tại duy nhất đồng cấu $\bar{f} : Y \to X$ sao cho với mọi $i \in I$ ta có $f_i = p_i \bar{f}$.

2.13. Chứng minh rằng $\mathbb{Z}_m \times \mathbb{Z}_n$ là một nhóm xyclic khi và chỉ khi m và n nguyên tố cùng nhau.

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

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

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

2.17. Cho Y là một bộ phận của 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 2.9). Tìm số phần tử của S(X, Y) trong trường hợp X có n phần tử, Y có một phần tử.

2.18. Trong nhóm các phép thế S_4 chứng minh rằng các phép thế sau : e, a = (12) (34), b = (13) (24) và c = (14) (23) lập thành một nhóm con của S_4. Nhóm con đó có giao hoán hay không?

2.19. 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 nhóm X thì $A^{-1} = A$

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

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

2.22. Trong một nhóm X chứng minh rằng nhóm con sinh ra bởi tập $\varnothing$ là nhóm con $\{e\}$, e là đơn vị của X.

2.23. Giả sử S là một bộ phận khác rỗng của một nhóm X. Chứng minh rằng các phần tử của nhóm con sinh bởi S là các phần tử có dạng $x_1x_2 \ldots x_n$ với $x_1, x_2, \ldots, x_n$ thuộc $S \cup S^{-1}$. Tìm nhóm con của nhóm nhân các số hữu tỉ dương sinh bởi bộ phận các số nguyên tố.

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

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

2.26. Cho a, b là hai phần tử tuỳ ý của một nhóm, chứng minh ab và ba có cùng cấp.

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

2.28. 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.

2.29. Cho A là một nhóm con của nhóm X. Giả sử tập thương X/A có hai phần tử. Chứng minh A là chuẩn tắc.

2.30. Trong nhóm có các phép thế S_n. Chứng minh A_n – tập hợp các phép thế chẵn, là nhóm con chuẩn tắc của S_n.

2.31. 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.

2.32. Giả sử X là một nhóm, ta gọi bộ phận $C(X) = \{a \in X \mid ax = xa$ với mọi $x \in X\}$ là tâm của X . Chứng minh rằng C(X) là một nhóm con giao hoán và mọi nhóm con của C(X) là một nhóm con chuẩn tắc của X.

2.33. Tìm tất cả các nhóm con và nhóm con chuẩn tắc của nhóm các phép thế S_3.

2.34. 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 bởi tập hợp các hoán tử của tất cả các phần tử x, y của X là một nhóm con chuẩn tắc của X và nhóm thương X/A là Aben. Nhóm con A được gọi là *nhóm con hoán tử* của X và kí hiệu [x; x].

2.35. Chứng minh rằng muốn cho nhóm thương X/H của một nhóm X là Aben cần và đủ là nhóm con chuẩn tắc H chứa nhóm con các hoán tử của X.

2.36. Tìm nhóm các hoán tử của nhóm các phép thế S_3.

2.37. Chứng minh rằng mọi nhóm cấp bé hơn hay bằng 5 đều là Aben.

2.38. Hãy tìm các nhóm thương của:

a) Nhóm cộng các số nguyên là bội của 3 trên nhóm cộng các số nguyên là bội của 15.

b) Nhóm cộng các số nguyên là bội của 4 trên nhóm cộng các số nguyên là bội của 24.

2.39. Cho D là tập hợp các đường thẳng Δ trong mặt phẳng có phương trình là $y = ax + b$ (a và b là những số thực, $a \neq 0$).

Ánh xạ

$$D \times D \to D$$

$$(\Delta_1, \Delta_2) \mapsto \Delta_3$$

trong đó Δ_1, Δ_2, Δ_3 lần lượt là các đường thẳng có phương trình $y_1 = a_1x + b_1$, $y_2 = a_2x + b_2$, $y_3 = a_1a_2x + b_1 + b_2$ xác định một phép toán hai ngôi trong D.

a) Chứng minh D là một nhóm với phép toán trên.

b) Chứng minh ánh xạ $\varphi : D \to \mathbb{R}^*$

$$\Delta \mapsto a$$

trong đó $\mathbb{R}^*$ là nhóm nhân các số thực khác 0 và Δ là đường thẳng có phương trình $y = ax + b$ là một đồng cấu.

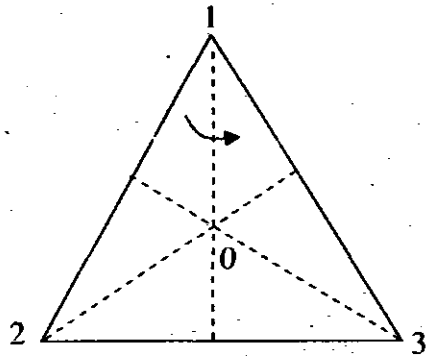
c) Xác định $\text{Ker}\varphi$?

2.40. Một phép đối xứng của một hình hình học là một phép thế của tập hợp X các điểm của hình đó và bảo toàn khoảng cách. Chứng minh rằng tập hợp các phép đối xứng của một hình hình học là một nhóm với phép nhân ánh xạ.

2.41. Kí hiệu Δ_3 là nhóm đối xứng của một tam giác đều. Chứng minh rằng

$$\Delta_3 = \{1_\Delta, R, R^2, D_1, D_2, D_3\}$$

trong đó R là phép quay tâm O, góc quay 120^o, D_i là các phép đối xứng qua đường cao đi qua các đỉnh i ($i = 1, 2, 3$). Hãy lập bảng toán cho Δ_3 và suy ra rằng $\Delta_3 \cong S_3$.



Hình 2

2.42. Cho G_1, G_2 là những nhóm với đơn vị theo thứ tự là e_1, e_2 và $G = G_1 \times G_2$ là tích của G_1 và G_2.

$A = G_1 \times \{e_2\}$ và $B = \{e_1\} \times G_2$. Xét các ánh xạ

$$P_1 : G \to G_1 \qquad P_2 : G \to G_2$$

$$(x_1, x_2) \mapsto x_1 \qquad (x_1, x_2) \mapsto x_2$$

$$q_1 : G_1 \to G \qquad q_2 : G_2 \to G$$

$$x_1 \mapsto (x_1, e_2) \qquad x_2 \mapsto (e_1, x_2).$$

a) Chứng minh p_1, p_2 là những toàn cấu. Xác định $Kerp_1$ và $Kerp_2$.

b) Chứng minh q_1, q_2 là những đơn cấu. Xác định Imq_1 và Imq_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 $AB = BA = G$.

2.43. Chứng minh rằng mọi nhóm xyclic hữu hạn cấp n đều đẳng cấu với nhau (đẳng cấu với nhóm cộng các số nguyên modun n).

2.44. Chứng minh rằng mọi nhóm xyclic cấp vô hạn đều đẳng cấu với nhau (đẳng cấu với nhóm cộng các số nguyên $\mathbb{Z}$).

2.45. Chứng minh rằng

Mỗi nhóm xyclic cấp vô hạn chỉ có hai phần tử sinh. Mỗi nhóm xyclic cấp vô hạn chỉ có hai tự đẳng cấu.

2.46. Giả sử X là một nhóm và Y là một tập hợp được trang bị một phép toán hai ngôi. Giả sử có một song ánh $f : X \to Y$ thoả 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. Hơn nữa, nếu X là Aben thì Y cũng là Aben và nếu X là xyclic thì Y cũng là xyclic.

2.47. Cho X và Y là hai nhóm xyclic có các phần tử sinh theo thứ tự là x và y, có cấp là s và t.

a) Chứng minh quy tắc φ cho ứng với mỗi phần tử $x^n \in X$ phần tử $(y^k)^n \in Y$, với k là một số tự nhiên khác 0 cho trước, là một đồng cấu khi và chỉ khi sk là bội của t.

b) Chứng minh rằng nếu $sk = mt$ và φ là đẳng cấu thì $(s, m) = 1$.

2.48. 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 $\mathrm{Ker}\varphi$.

2.49. 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 một nhóm Aben.

2.50. 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.

2.51. 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.

2.52. Trong tập hợp $X = \mathbb{Z}^3$, $\mathbb{Z}$ 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 hai ngôi đó là một nhóm.

b) Chứng minh rằng nhóm con A sinh 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 $a, b \in \mathbb{Z}$.

2.53. Chứng minh rằng nhóm cộng các số thực đẳng cấu với nhóm nhân các số thực dương.

2.54. Chứng minh rằng nhóm cộng các số phức có dạng a + bi với $a, b \in \mathbb{Z}$ đẳng cấu với nhóm tích $\mathbb{Z} \times \mathbb{Z}$ (ở đó $\mathbb{Z}$ là nhóm cộng các số nguyên).

2.55. Giả sử X là một nhóm xyclic cấp n sinh bởi phần tử a. Xét phần tử $b = a^k \in X$. Chứng minh:

a) Cấp b bằng $\frac{n}{d}$ với d là ước chung lớn nhất của n và k.

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

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

2.57. Chứng minh rằng:

a) Mọi nhóm cấp bốn hoặc đẳng cấu với $\mathbb{Z}_4$ hoặc đẳng cấu với $\mathbb{Z}_2 \times \mathbb{Z}_2$.

b) Mọi nhóm cấp sáu hoặc đẳng cấu với $\mathbb{Z}_6$ hoặc đẳng cấu với nhóm các phép thế S_3.

2.58. Chứng minh rằng mọi nhóm thương của một nhóm xyclic là một nhóm xyclic, ảnh đồng cấu của một nhóm xyclic là một nhóm xyclic.

2.59. Trong nhóm cộng các số nguyên $\mathbb{Z}$, chứng minh với hai số nguyên m, n ta có:

a) $m\mathbb{Z} \cap n\mathbb{Z} = b\mathbb{Z}$ với b là bội chung nhỏ nhất của m và n;

b) $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ với d là ước chung lớn nhất của m và n;

c) $m\mathbb{Z}/mn\mathbb{Z}$ đẳng cấu với $\mathbb{Z}/n\mathbb{Z}$.

2.60. Giả sử A và B là hai nhóm con chuẩn tắc của nhóm X sao cho $A \cap B = \{e\}$ và X = AB. Chứng minh rằng X đẳng cấu với nhóm tích $A \times B$.

2.61. Giả sử A và B là hai nhóm con chuẩn tắc của nhóm X. Chứng minh:

a) AB là một nhóm con chuẩn tắc của X.

b) $A \cap B$ là một nhóm con chuẩn tắc của X và cũng là một nhóm con chuẩn tắc của A.

c) Tồn tại một đơn cấu $\varphi : {}^{X}/_{A \cap B} \to \left({}^{X}/_{A}\right) \times \left({}^{X}/_{B}\right)$

d) ${}^{A}/_{A \cap B}$ đẳng cấu với ${}^{AB}/_{B}$.

2.62. Cho H là một nhóm con của nhóm G. Ánh xạ $f : G \to G'$ là một đẳng cấu. Chứng minh rằng f(H) là một nhóm con chuẩn tắc của G'. Nếu f chỉ là một đồng cấu thì f(H) có là nhóm con chuẩn tắc của G' không?

2.63. Chứng minh rằng nếu A là một nhóm con chuẩn tắc của X thì tồn tại một song ánh từ tập hợp các nhóm con chuẩn tắc của X chứa A đến tập hợp các nhóm con chuẩn tắc của ${}^{X}/_{A}$.

2.64. Nhóm con chuẩn tắc H được gọi là một nhóm con *chuẩn tắc tối đại* của nhóm G nếu $H \neq G$ và với mọi nhóm con chuẩn tắc K của G, $K \supsetneq H$ thì $K = G$. Chứng minh rằng H là nhóm con chuẩn tắc tối đại của G khi và chỉ khi nhóm thương ${}^{G}/_{H}$ là một nhóm đơn.

2.65. Cho H và K là hai nhóm con chuẩn tắc tối đại khác nhau của nhóm G. Chứng minh:

a) $HK = G$;

b) $H \cap K$ là nhóm con chuẩn tắc tối đại của H và của K, đồng thời ta có

$${}^{G}/_{H} \cong {}^{K}/_{H \cap K} \text{ và}$$

$$G/H \cong H/H \cap K.$$

2.66. Chứng minh rằng có một đồng cấu duy nhất từ nhóm cộng các số hữu tỉ $\mathbb{Q}$ đến nhóm cộng các số nguyên $\mathbb{Z}$. Từ đó suy ra nhóm cộng các số hữu tỉ không phải là một nhóm xyclic.

2.67. Cho X là một nhóm. Kí hiệu Aut(X) là tập các *tự đẳng cấu* của nhóm X. Chứng minh rằng :

a) Aut(X) là một nhóm với phép nhân ánh xạ.

b) $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$ (với $\mathbb{Z}$ là nhóm cộng các số nguyên).

2.68. Cho A là một nhóm cộng Aben. Kí hiệu End(A) là *tập các đồng cấu của nhóm* A. Chứng minh:

a) End(A) là một nhóm Aben với phép cộng sau:

$$\forall f, g \in \mathrm{End}(A),\ (f+g)(a) = f(a)+g(a),\ \forall a \in A.$$

b) $\mathrm{End}(\mathbb{Z}) \cong \mathbb{Z}$ (với $\mathbb{Z}$ là nhóm các số nguyên).

c) $\mathrm{End}(\mathbb{Q}) \cong \mathbb{Q}$ (với $\mathbb{Q}$ là nhóm các số hữu tỉ).

2.69. Cho X là một nhóm. Với mỗi phần tử $a \in X$ ta xét ánh xạ

$$f_a : X \to X$$
$$x \mapsto axa^{-1}$$

a) Chứng minh rằng f_a là một tự đẳng cấu của X, gọi là tự đẳng cấu trong xác định bởi phần tử a.

b) Chứng minh rằng tập hợp các tự đẳng cấu trong của X lập thành một nhóm con của nhóm các tự đẳng cấu của X (bài tập 2.50).

c) Chứng minh rằng nhóm con H của X là chuẩn tắc nếu và chỉ nếu $f_a(H) = H$ với mọi tự đẳng cấu trong f_a của X.

d) Chứng minh nhóm các tự đẳng cấu trong của X đẳng cấu với nhóm thương $X/C(X)$ với C(X) là tâm của nhóm X (bài tập 2.32).

2.70. Cho $f : X \to Y$ là một đồng cấu từ nhóm hữu hạn X đến nhóm Y. Chứng minh:

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

b) Cấp của f(X) chia hết cấp của X.

2.71. 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.

2.72. 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 cyclic cấp 18 đến một nhóm cyclic cấp 6.

2.73. Giả sử $\mathbb{C}^*$ là nhóm nhân các số phức khác 0, H là tập hợp các số phức của $\mathbb{C}^*$ nằm trên trục thực và trục ảo. Chứng minh rằng H là nhóm con của $\mathbb{C}^*$ và nhóm thương $\mathbb{C}^*/H$ đẳng cấu với nhóm nhân U các số phức có modun bằng 1.

2.74. Chứng minh rằng nhóm thương $\mathbb{R}/\mathbb{Z}$ đẳng cấu với nhóm nhân U các số phức có modun bằng 1.

2.75. Gọi X là nhóm nhân các ma trận vuông cấp n không suy biến trên trường số thực. 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.

2.76. Áp dụng định lí Lagorăngiơ để chứng minh định lí Fecma: "Giả sử p là một số nguyên tố, a là một số nguyên bất kì ta luôn có $a^p \equiv a \pmod{p}$".

2.77. Giả sử $f : X \to Y$ là một đồng cấu từ một nhóm nhân X đến một nhóm nhân Y; $K = \text{Ker} f$ là hạt nhân của đồng cấu f và :

$$i : K \to X$$
$$x \mapsto i(x) = x$$

là phép nhúng chính tắc. Chứng minh:

a) fi là ánh xạ đơn vị từ K vào Y.

b) Với mọi nhóm G, và với mọi đồng cấu $g : G \to X$ sao cho fg là ánh xạ đơn vị tồn tại duy nhất đồng cấu $\overline{g} : G \to K$ sao cho $g = i\overline{g}$.

2.78. Giả sử $G = G_1 \times G_2$ là nhóm tích của G_1 và G_2, hai phép chiếu chính tắc $p_1 : G \to G_1$ và $p_2 : G \to G_2$ (bài 2.42). Chứng minh rằng với mọi nhóm X và với mọi cặp đồng cấu $g_1 : X \to G_1$, $g_2 : X \to G_2$ tồn tại duy nhất đồng cấu $g : X \to G$ sao cho $g_1 = p_1.\overline{g}$ và $g_2 = p_2.\overline{g}$.

2.79. Giả sử $G = G_1 \times G_2$ là nhóm tích của hai nhóm Aben G_1 và G_2; hai phép nhúng chính tắc $q_1 : G_1 \to G$ và $q_2 : G_2 \to G$ (bài 2.42). Chứng minh rằng với mọi nhóm Aben Y và với mọi cặp đồng cấu $h_1 : G_1 \to Y$, $h_2 : G_2 \to Y$ tồn tại duy nhất đồng cấu $\overline{h} : G \to Y$ sao cho $h_1 = \overline{h}q_1$ và $h_2 = \overline{h}q_2$.

2.80. Giả sử G, H và K là ba nhóm $f : G \to H$, $g : G \to K$ là hai đồng cấu với f là một toàn cấu. Chứng minh rằng các điều kiện sau đây là tương đương:

a) Tồn tại một đồng cấu $h : H \to K$ sao cho ta có $g = hf$;

b) $\text{Ker}f \subset \text{Ker}g$.

Nếu các điều kiện đó thoả mãn thì:

c) h là duy nhất;

d) h là đơn ánh nếu và chỉ nếu $\text{Ker}f = \text{Ker}g$;

e) h là toàn ánh nếu và chỉ nếu g là toàn ánh.

2.81. Cho tập hợp X. Ta gọi F là nhóm tự do trên tập X và một ánh xạ $f : X \to F$ sao cho với mọi nhóm G và mọi ánh xạ $g : X \to G$. Tồn tại duy nhất đồng cấu $\overline{g} : F \to G$ để $g = \overline{g}f$. Chứng minh rằng:

a) f là đơn cấu và f(X) sinh ra nhóm F;

b) (F, f) xác định duy nhất sai khác một đẳng cấu.

2.82. Chứng minh rằng mỗi tập X đều tồn tại một nhóm tự do trên X.

2.83. Hãy tìm nhóm tự do trên tập X với:

a) $X = \varnothing$;

b) $X = \{a\}$;

c) $X = \{a, b\}$.

2.84. Chứng minh rằng mọi nhóm tự do trên tập hợp gồm một phần tử đều đẳng cấu với nhóm cộng các số nguyên $\mathbb{Z}$.

2.85. Chứng minh rằng mọi nhóm đều là ảnh đồng cấu của một nhóm tự do và do đó nó đẳng cấu với một nhóm thương của nhóm tự do.

2.86. Chứng minh rằng nếu (F, f) là nhóm Aben tự do trên tập X thì:

a) f là một đơn cấu và f(X) sinh ra F;

b) (F, f) xác định duy nhất sai khác một đẳng cấu.

2.87. Chứng minh rằng với mỗi tập X đã cho, tồn tại một nhóm Aben tự do trên X.

2.88. Hãy chứng minh:

a) Mọi nhóm Aben tự do trên tập X gồm n phần tử đều đẳng cấu với nhóm $\mathbb{Z}^n$, ở đó $\mathbb{Z}$ là nhóm các số nguyên.

b) Mọi nhóm Aben tự do đều đẳng cấu với một nhóm con của tích trực tiếp của một họ các nhóm đẳng cấu với nhóm cộng các số nguyên $\mathbb{Z}$.

2.89. Chứng minh rằng:

a) Mọi nhóm Aben đều đẳng cấu với một nhóm thương của một nhóm tự do.

b) Mọi nhóm con của nhóm Aben tự do đều là nhóm Aben tự do.

2.90. Cho (F, f) là một nhóm tự do trên tập X. Gọi [F, F] là nhóm con hoán tử của nhóm F. Hãy chứng minh:

a) Nhóm thương $A = F/[F, F]$ là một nhóm Aben.

b) Nhóm thương A cùng với ánh xạ $q : X \to F/[F, F]$ xác định bởi $q = pf$ là một nhóm Aben tự do trên tập X. Trong đó $p : F \to F/[F, F]$ là phép chiếu chính tắc.

Chương III
VÀNH VÀ TRƯỜNG

A. TÓM TẮT LÍ THUYẾT

1. Vành, miền nguyên

Định nghĩa. Ta gọi là *vành* một tập hợp X cùng với phép cộng và phép nhân đã cho trong X thoả mãn các điều kiện sau đây:

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 tuỳ ý x, y, z thuộc X ta có

$$x(y + z) = xy + xz \text{ và}$$

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

Phần tử trung lập của phép cộng gọi là *phần tử không*, kí hiệu là 0. Nếu phép nhân có phần tử trung lập thì phần tử đó gọi là đơn vị của X và thường kí hiệu là e hoặc 1. Nếu phép nhân là giao hoán thì X được gọi là *vành giao hoán*.

Định nghĩa. Phần tử a thuộc vành X được gọi là ước bên trái (bên phải) của 0 nếu $a \neq 0$ và có một phần tử $b \neq 0$ trong X sao cho $ab = 0$ ($ba = 0$).

Phần tử a được gọi là ước của 0 nếu nó vừa là ước bên phải, vừa là ước bên trái của 0.

Định nghĩa. Một vành giao hoán, có đơn vị $e \neq 0$, không có ước của 0 được gọi là *miền nguyên*.

Định lí. Một vành giao hoán, có đơn vị $e \neq 0$ là một miền nguyên khi và chỉ khi có luật giản ước của phép nhân đối với các phần tử khác 0.

2. Vành con iđêan và vành thương

Định nghĩa. Giả sử X là một vành, A là một bộ phận của X ổn định đối với phép cộng và phép nhân trong X. Ta gọi A là một *vành con* của X nếu và chỉ nếu A cùng với hai phép toán cảm sinh trên A là một vành.

Định lí. Giả sử A là một bộ phận khác rỗng của một vành X. thế thì A là vành con của X khi và chỉ khi với mọi $a, b \in A$ có $a - b \in A$ và $ab \in A$.

Giao của một họ khác rỗng bất kì của những vành con của vành X là một vành con của X.

Định nghĩa. Giả sử X là một vành. Ta gọi vành con A của vành X là *iđêan trái* (*phải*) nếu với mọi $a \in A$, $x \in X$, $xa \in A$ ($ax \in A$). Một vành con A gọi là *iđêan* của X nếu và chỉ nếu A vừa là iđêan trái, vừa là iđêan phải.

Nhận xét. Một bộ phận khác rỗng A của vành X là iđêan của X khi và chỉ khi với mọi $a, b \in A$, $a - b \in A$ và với mọi $a \in A$, $x \in X$, $ax \in A$ và $xa \in A$.

Định lí. Giao của một họ bất kì những iđêan của một vành X là một iđêan của X.

Định nghĩa. Giả sử U là một bộ phận của một vành X khi đó giao của họ các iđêan của X chứa U là một iđêan bé nhất của X chứa U, nó được gọi là *iđêan của* X *sinh bởi tập* U; kí hiệu là (U). Nếu $U = \{a\}$ thì iđêan sinh bởi U được gọi là *iđêan chính* sinh bởi a; kí hiệu là (a). Nếu X là một vành giao hoán có đơn vị thì

$$(a) = \{ax \mid x \in X\}.$$

Nếu iđêan A của X chứa đơn vị của vành X thì $A = X$.

Giả sử A là một iđêan của một vành X, khi đó A là một nhóm con chuẩn tắc của nhóm cộng X. Ta có một nhóm thương

$$X/A = \{x + A \mid x \in X\}$$

với phép cộng $(x + A) + (y + A) = (x + y) + A$.

Nhóm X/A cùng với phép nhân $(x + A)(y + A) = xy + A$ là một vành. Vành này được gọi là *vành thương* của vành X trên iđêan A.

3. Đồng cấu

Định nghĩa. Một *đồng cấu* (vành) là một ánh xạ từ một vành X đến một vành Y sao cho với mọi a, b thuộc X ta có

$$f(a + b) = f(a) + f(b),$$
$$f(ab) = f(a)f(b).$$

Nếu X = Y thì đồng cấu f được gọi là *tự đồng cấu* của X. Nếu f là một đơn ánh thì đồng cấu f được gọi là một *đơn cấu*. Nếu f là toàn ánh thì f được gọi là một *toàn cấu* và nếu f là một song ánh thì f được gọi là một *đẳng cấu*. Nếu có một ánh xạ $f : X \to Y$ đẳng cấu thì ta nói hai vành X và Y *đẳng cấu với nhau* và kí hiệu là $X \cong Y$.

Tính chất. Giả sử $f : X \to Y$ là một đồng cấu. Tập hợp f(X) được gọi là ảnh (của đồng cấu f), kí hiệu là Imf.

Tập hợp $f^{-1}(0_Y)$ được gọi là *hạt nhân* của đồng cấu f, kí hiệu là Kerf.

Giả sử $f : X \to Y$ là một đồng cấu từ một vành X đến một vành Y. Khi đó:

- $F(0_X) = 0_Y$.
- $F(-a) = -f(a)$ với mọi $a \in X$
- $f(a - b) = f(a) - f(b)$ với mọi $a, b \in X$.
- $f(a^n) = [f(a)]^n$ với mọi $a \in X$, với mọi $n \in \mathbb{N}^*$.

Định lí. Nếu A là một vành con của X thì f(A) là một vành con của Y. Đặc biệt Imf là một vành con của Y.

Định lí. Nếu B là một iđêan của Y thì $f^{-1}(B)$ là một iđêan của X. Đặc biệt Kerf là một iđêan của Y. Giả sử $f : X \to Y$ và $g : Y \to Z$ là hai đồng cấu thì $gf : X \to Z$ là một đồng cấu.

Định lí (định lí đồng cấu). Giả sử $f : X \to Y$ là một đồng cấu và

$$p : X \to X/\text{Kerf}$$
$$x \mapsto x + \text{Kerf}$$

là toàn cấu chính tắc thì tồn tại duy nhất một đơn cấu

$$\bar{f} : X/\text{Kerf} \to Y$$

sao cho $\bar{f}\, p = f$. Như vậy nếu f là một toàn cấu thì $Y \cong X/\text{Kerf}$.

4. Trường

Định nghĩa. Ta gọi một miền nguyên X là *trường* nếu mọi phần tử khác 0 của X đều có nghịch đảo trong vị nhóm nhân X.

Như vậy một vành giao hoán có đơn vị $1 \neq 0$ là một trường nếu và chỉ nếu $X - \{0\}$ là một nhóm với phép nhân trong X.

Định nghĩa. Một bộ phận A của một trường X được gọi là *trường con* của X nếu A ổn định đối với hai phép toán trong X và A cùng với hai phép toán cảm sinh là một trường.

Định lí. Bộ phận A có nhiều hơn một phần tử của một trường X là một trường con của trường X khi và chỉ khi:

a) Với mọi a, b thuộc A có $a - b \in A$;

b) Với mọi a, b thuộc A, $b \neq 0$ có $ab^{-1} \in A$.

Một trường X chỉ có hai iđêan tầm thường là $\{0\}$ và bản thân X.

5. Đặc số

Định nghĩa. Cho X là một vành giao hoán, có đơn vị e.

Nếu trong nhóm cộng X, phần tử e có cấp vô hạn thì X được gọi là *vành có đặc số* 0.

Nếu trong nhóm cộng X, phần tử e có cấp $m \neq 0$ thì X được gọi là *vành có đặc số* m.

Chú ý. Nếu X là vành có đặc số $m \neq 0$ và X là một miền nguyên thì m là một số nguyên tố.

6. Trường các thương

Định lí. Cho X là một miền nguyên. Khi đó tồn tại một trường $\overline{X}$ cùng với đơn cấu $\varphi : X \to \overline{X}$ sao cho với mọi $\alpha \in \overline{X}$, α viết được dưới dạng $\alpha = \varphi(a)\,[\varphi(b)]^{-1}$, trong đó a, b thuộc X và $b \neq 0$. Trường $\overline{X}$ được gọi là trường các thương của miền nguyên X.

B. BÀI TẬP

3.1. Chứng minh các tập hợp sau đây với phép cộng và phép nhân các số lập thành một vành giao hoán, có đơn vị

a) Tập hợp các số có dạng $a + b\sqrt{2}$ với $a, b \in \mathbb{Z}$;

b) Tập hợp các số phức có dạng $a + bi$ với $a, b \in \mathbb{Z}$.

3.2. 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.

3.3. 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.

3.4. Cho R là một vành và X là một tập tuỳ ý. R^X là tập các ánh xạ từ X đến R. Chứng minh rằng R^X là một vành với hai phép toán sau:

$$\forall f,g \in R^X,\ \forall x \in X,\ (f+g)(x) = f(x) + g(x).$$

$$\forall f,g \in R^X,\ \forall x \in X,\ fg(x) = f(x)g(x).$$

3.5. Cho H là tập các hàm số thực. Chứng minh rằng H là một vành giao hoán, có đơn vị với hai phép toán sau:

$$\forall f,g \in H\ \ (f+g)(x) = f(x) + g(x),\ \forall x \in \mathbb{R};$$

$$\forall f,g \in H\ \ fg(x) = f(x)g(x),\ \forall x \in \mathbb{R}.$$

3.6. Cho A là một nhóm cộng Aben. End(A) là tập các tự đồng cấu của nhóm A. Chứng minh rằng End(A) là một vành với hai phép toán sau:

$$\forall f, g \in \text{End}(A),\ (f+g)(a) = f(a) + g(a),\ \forall a \in A.$$

$$\forall f, g \in \text{End}(A),\ fg(a) = f(g(a)),\ \forall a \in A.$$

(Vành End(A) được gọi là vành các tự đồng cấu của nhóm AbenA).

3.7. Chứng tỏ rằng vành số nguyên, trường số hữu tỉ, trường số thực và trường số phức đều là những vành có đặc số 0.

3.8. Chứng minh rằng mọi vành, trường hữu hạn đều có đặc số khác 0.

3.9. Chứng minh rằng nếu một miền nguyên X mà có đặc số $m \neq 0$ thì m phải là một số nguyên tố.

3.10. Chứng minh rằng mọi trường có đặc số 0 đều chứa một trường con đẳng cấu với trường số hữu tỉ $\mathbb{Q}$. Mọi trường có đặc số $p \neq 0$ đều chứa một trường con đẳng cấu với $\mathbb{Z}_p$.

3.11. Giả sử đã cho trong một tập hợp X hai phép toán cộng và nhân sao cho:

a) X cùng với phép cộng là một nhóm;

b) X cùng với phép nhân là một vị nhóm;

c) Phép nhân phân phối đối với phép cộng.

Chứng minh X là một vành.

3.12. Tìm các ước của không trong vành $\mathbb{Z}/6\mathbb{Z}$.

3.13. Chứng minh $\mathbb{Z}/n\mathbb{Z}$ (với $n \neq 0$) là một miền nguyên khi và chỉ khi n là một số nguyên tố.

3.14. Chứng minh tập hợp $X = \mathbb{Z} \times \mathbb{Z}$ 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.

3.15. 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.

3.16. Các vành nói đến ở các bài tập 3.1, 3.2, 3.3 là những vành con của những vành nào?

3.17. Cho X là một vành tuỳ 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.

3.18. Cho X là một vành tuỳ ý, n là một số nguyên cho trước. Chứng minh bộ phận

$$A = \{x \in X \mid nx = 0\}$$

là một iđêan của X.

3.19. Cho X là một vành tuỳ 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.

3.20. Cho X là một vành giao hoán có đơn vị là 1. I và J là hai iđêan của X. $IJ = \left\{ \sum_{i=1}^{n} a_i b_i \,\middle|\, a_i \in I, b_i \in J, i = 1,\ldots,n, n \geq 1 \right\}$

Hãy chứng minh:

a) IJ là một iđêan của X.

b) Nếu $I + J = X$ thì $IJ = I \cap J$.

3.21. Cho m và n là hai số nguyên dương. Chứng minh rằng $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$ khi và chỉ khi m và n nguyên tố cùng nhau.

3.22. Cho I và J là hai iđêan của vành giao hoán, có đơn vị X.

$$p : X \to \left(X/I\right) \times \left(X/J\right)$$

$$a \mapsto (a + I, a + J).$$

Hãy chứng minh:

a) p là một đồng cấu;

b) p là một toàn cấu khi và chỉ khi $I + J = X$;

c) Hãy mở rộng các kết quả trên khi $I_1, I_2, \ldots, I_n$ (với $n \geq 2$) là những iđêan của vành A.

3.23. Giả sử X là một miền nguyên và n là cấp của phần tử đơn vị e trong nhóm cộng X. 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 số nguyên cho trước là một iđêan của X;

d) $X/mX \cong X$ nếu m là bội của n;

$X/mX \cong \{0\}$ nếu m không phải là bội của n.

3.24. Giả sử X là một vành giao hoán, có đơn vị. Một iđêan $A \neq X$ của X được 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 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 idêan nguyên tố;

b) X/A là trường khi và chỉ khi A là tối đại.

3.25. Cho f là một đồng cấu từ vành X đến vành Y (X và Y là những vành giao hoán có đơn vị).

a) Chứng minh rằng nếu f là một toàn cấu và I là một idêan của X thì f(I) là một idêan của I. Nếu f không là toàn cấu thì tính chất này còn đúng không? Tại sao?

b) Chứng minh rằng nếu p là một idêan nguyên tố của Y thì $f^{-1}(P)$ là một idêan nguyên tố của X. Kết quả này còn đúng không nếu thay giả thiết "nguyên tố" bằng giả thiết "tối đại"? Tại sao?

3.26. Cho X là một vành giao hoán có đơn vị. I là một idêan thực sự của vành X. Chứng minh rằng tồn tại một idêan tối đại của X chứa I.

3.27. Cho X là một vành giao hoán có đơn vị 1. Chứng minh rằng với mỗi phần tử $a \in X$, a không khả nghịch, đều có một idêan tối đại chứa a.

3.28. Cho X là vành giao hoán, có đơn vị. Chứng minh hai khẳng định sau đây tương đương với nhau :

i) X chỉ có một idêan tối đại duy nhất;

ii) Tập các phần tử không khả nghịch của X lập thành một idêan của X.

3.29. Cho X là một vành giao hoán có đơn vị. Chứng minh rằng

a) $N(X) = \{x \in X \mid \exists n \in \mathbb{N}^*, nx = 0\}$ là một idêan của X.

b) Tập N(X) là giao của tất cả các idêan nguyên tố của X.

3.30. Giả sử A là một vành, B là một tập hợp với hai phép toán cộng và nhân, $f : A \to B$ là một song ánh thoả mãn.

$$\forall a, b \in A,\ f(a + b) = f(a) + f(b)$$

$$\forall a, b \in A,\ f(ab) = f(a)f(b).$$

Chứng minh :

a) B là một vành.

b) Nếu A là một vành giao hoán thì B cũng là vành giao hoán.

c) Nếu A là một vành có đơn vị thì B cũng là một vành có đơn vị.

d) Nếu A là miền nguyên thì B cũng là miền nguyên.

3.31. Hãy tìm tất cả các tự đồng cấu của vành các số nguyên.

3.32. Tìm tập các tự đồng cấu của vành

$$\mathbb{Z}\left[\sqrt{2}\right] = \left\{ a + b\sqrt{2} \middle| a, b \in \mathbb{Z} \right\}.$$

3.33. Tìm tập các tự đồng cấu của vành $\mathbb{Z}[i] = \{ a + bi | a, b \in \mathbb{Z} \}$.

3.34. Giả sử $f : X \to X$ là một tự đồng cấu của vành X. Chứng minh rằng tập hợp $A = \{x \in X | f(x) = x\}$ là một vành con của X.

3.35. Giả sử X là một vành tuỳ ý, $\mathbb{Z}$ là vành các số nguyên. Xét tập hợp tích $X \times \mathbb{Z}$. Trong $X \times \mathbb{Z}$ ta định nghĩa các phép toán như sau:

$$(x_1, n_1) + (x_2, n_2) = (x_1 + x_2, n_1 + n_2),$$

$$(x_1, n_1)(x_2, n_2) = (x_1x_2 + n_1x_2 + n_2x_1, n_1n_2).$$

a) Chứng minh rằng $X \times \mathbb{Z}$ là một vành có đơn vị.

b) Ánh xạ $f : X \to X \times \mathbb{Z}$

$$x \mapsto (x, 0)$$

là một đơn cấu.

3.36. Cho A và B là hai vành tuỳ ý. Xét tập hợp tích Đêcác $X = A \times B$. trong tập 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 $\overline{A} = \{(a, 0) | a \in A\}$ và $\overline{B} = \{(0, b) | b \in B\}$

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

$$\overline{A} \cap \overline{B} = \{(0,0)\} \text{ và } X = \overline{A} + \overline{B}.$$

d) Giả sử A và B là những vành có đơn vị, hãy tìm các đơn vị của X, $\overline{A}$ và $\overline{B}$.

3.37. Giả sử X là một vành và $a \in X$. Chứng minh rằng:.

a) Ánh xạ $h_a : X \to X$

$$a \mapsto ax$$

là một đồng cấu (nhóm) từ nhóm cộng Aben X đến nhóm cộng Aben X.

b)Ánh xạ $h : X \to End(X)$

$$a \mapsto h(a) = h_a$$

là một đồng cấu từ vành X đến vành End(X) các tự đồng cấu của nhóm cộng Aben X.

c) Tìm Kerh. Chứng minh rằng h là đơn cấu khi X có đơn vị.

3.38. 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. 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?

3.39. Chứng minh mọi miền nguyên hữu hạn đều là một trường.

3.40. Chứng minh vành các số nguyên mod n là một trường khi và chỉ khi n là số nguyên tố.

3.41. Chứng minh rằng trường các số hữu tỉ không có trường con nào khác ngoài bản thân nó.

3.42. Chứng minh rằng bộ phận $A = \left\{ a + b\sqrt{2} \,\middle|\, a, b \in \mathbb{Q} \right\}$ là một trường con của trường số thực $\mathbb{R}$.

3.43. Chứng minh rằng bộ phận

$$A = \left\{ a + b\sqrt[3]{2} + c\sqrt[3]{4} \,\middle|\, a, b, c \in \mathbb{Q} \right\}$$

là một trường con của trường số thực $\mathbb{R}$.

3.44. Giả sử X là một trường, e là phần tử đơn vị của X. Xét bộ phận $A = \left\{ ne \,\middle|\, n \in \mathbb{Z} \right\}$.

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 $\mathbb{Z}$ khi X có đặc số 0, và đẳng cấu với vành các số nguyên mod p, khi X có đặc số p.

c) Trong trường hợp X đặc số $p \neq 0$, hãy chứng minh A là một trường.

3.45. 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 thoả 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 $X \cong Y$.

3.46. Hãy tìm

a) Các tự đồng cấu của trường các số hữu tỉ;

b) Các tự đồng cấu của trường các số thực;

c) Các tự đồng cấu của trường các số phức giữ nguyên các số thực.

3.47. Tìm tập các tự đẳng cấu của trường

$$\mathbb{Q}(\sqrt{2}) = \left\{ a + b\sqrt{2} \middle| a, b \in \mathbb{Q} \right\}.$$

3.48. Tìm tập các tự đẳng cấu của trường

$$\mathbb{Q}(i) = \left\{ a + bi \middle| a, b \in \mathbb{Q} \right\}.$$

3.49. Tìm tập các tự đẳng cấu của trường

$$\mathbb{Q}(\sqrt[3]{2}) = \left\{ a + b\sqrt[3]{2} + c\sqrt[3]{4} \middle| a, b, c \in \mathbb{Q} \right\}.$$

3.50. Chứng minh rằng tập hợp các mà 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.

3.51. Chứng minh rằng tập hợp các ma trận có dạng

$$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}$$

với $a, b \in \mathbb{Q}$ là một trường (với phép cộng và nhân các ma trận) đẳng cấu với trường A ở bài tập 3.42.

3.52. Tìm trường các thương của miền nguyên A trong bài tập 3.44.

3.53. 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 (p là một số nguyên tố).

3.54. 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 $P = \left\{ ab^{-1} \middle| a,b \in A, b \neq 0 \right\}$ 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.

3.55. Giả sử p là một số nguyên tố. Chứng minh rằng tập hợp các số hữu tỉ có dạng $\frac{m}{n}$, trong đó n nguyên tố với p, là một miền nguyên. Tìm trường các thương của miền nguyên này.

3.56. Cho A là một idêan, B là một vành con của một vành X có đơn vị. Chứng minh:

a) A + B là một vành con của vành X;

b) $A \cap B$ là một idêan của B;

c) A là một idêan của A + B;

d) $B/_{A \cap B} \cong {}^{A+B}/_{A}$.

3.57. Giả sử A và B là hai idêan của một vành X có đơn vị và $A \subset B$. Chứng minh rằng bộ phận

$$B/A = \{ x + A \mid x \in B \} \subset X/A$$

là một idêan của vành X/A và ta có đẳng cấu

$$\left(X/A\right) \Big/ \left(B/A\right) \cong X/B.$$

3.58. Giả sử X là một vành giao hoán có đơn vị; A, B là hai idêan của X sao cho X = A + B. Chứng minh rằng

$$X/AB \cong \left(X/A\right) \times \left(X/B\right).$$

3.59. Cho m là n là hai số tự nhiên nguyên tố cùng nhau. Chứng minh

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

3.60. Cho X là một vành, có đơn vị 1, U là tập hợp các ước của 1 trong X. Chứng minh rằng U là một nhóm với phép nhân trong X.

3.61. Tìm nhóm các ước của đơn vị trong vành $\mathbb{Z}/m\mathbb{Z}$. Từ đó chứng minh $a^{p-1} \equiv 1 \pmod{p}$ với p là một số nguyên tố và a không chia hết cho p.

3.62. Giả sử f là một đồng cấu từ một vành X đến một vành Y; K = Kerf và $i : K \to X$

$$x \mapsto x$$

là phép nhúng chính tắc. Chứng minh:

a) f.i là đồng cấu không từ K đến Y.

b) Với mọi vành Z, với mọi đồng cấu $g : Z \to X$ sao cho $fg = 0$, tồn tại duy nhất đồng cấu $\overline{g} : Z \to K$ sao cho $g = i\overline{g}$.

3.63. Giả sử $V = A \times B$ là tích của hai vành A và B (bài tập 3.36).

$p_1 : V \to A$ và $p_2 : V \to A$

$(a,b) \mapsto a$ $(a,b) \mapsto b$

là hai ánh xạ. Chứng minh:

a) p_1 và p_2 là những toàn cấu, gọi là các phép chiếu chính tắc;

b) Với mọi vành X, với mọi $f_1 : X \to A$ và $f_2 : X \to B$ tồn tại duy nhất đồng cấu $f : X \to V$ sao cho

$$f_1 = p_1 f \text{ và } f_2 = p_2 f.$$

3.64. Giả sử V, X, Y là ba vành; $f : V \to X$, $g : V \to Y$ là hai đồng cấu vành với f là toàn cấu. Chứng minh các điều kiện sau đây tương đương:

a) Tồn tại một đồng cấu $h : X \to Y$ sao cho $g = hf$;

b) $\text{Ker}f \subseteq \text{Ker}g$.

Khi các điều kiện đó được thoả mãn thì:

c) h là duy nhất;

d) h là đơn ánh nếu và chỉ nếu $\text{Ker}f = \text{Ker}g$;

e) h là toàn ánh nếu và chỉ nếu g là toàn ánh.

3.65. Cho $d = 7$ hoặc $d = 11$. Chứng minh:

a) Bộ phận $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \subset \mathbb{Q}\}$ là một trường con của trường số thực $\mathbb{R}$;

b) Các trường $\mathbb{Q}(\sqrt{11})$ và $\mathbb{Q}(\sqrt{7})$ không đẳng cấu với nhau.

3.66. Cho X là một miền nguyên. Chứng minh rằng X là một trường khi và chỉ khi X chỉ có hai iđêan tầm thường là $\{0\}$ và X.

3.67. Vành giao hoán có đơn vị X được gọi là vành sắp thứ tự nếu trong X có một quan hệ thứ tự toàn phần "$\leq$" thoả mãn các tính chất sau đây:

1) Với mọi a, b, c$\in$X, quan hệ $a \leq b$ kéo theo

$$a + c \leq b + c;$$

2) Các quan hệ $0 \leq a$ và $0 \leq b$ kéo theo $0 \leq ab$.

Cho X là một vành giao hoán. Chứng minh các tính chất sau là tương đương:

a) X là một vành sắp thứ tự;

b) Tồn tại một bộ phận $P \subset X$ khác rỗng, sao cho:

(i) $a \in P$ và $b \in P \Rightarrow a + b \in P$;

(ii) $a \in P$ và $b \in P \Rightarrow ab \in P$;

(iii) $P \cap (-P) = \{0\}$; $P \cup (-P) = X$ với $-P = \{-x \mid x \in P\}$.

(Tập hợp $P^* = P - \{0\}$ được gọi là tập con dương của X).

3.68. Chứng minh các tính chất sau đây trong một vành sắp thứ tự X:

(i) $a + x < a + y \Rightarrow x < y$

(ii) $a - x < a - y \Rightarrow x > y$

(iii) $c > 0 \Rightarrow (a \leq b \Rightarrow ac \leq bc)$

(iv) $a < 0 \Rightarrow (ax < ay \Rightarrow y < x)$

(v) $a > 0 \Rightarrow (ax < ay \Rightarrow x < y)$

(vi) $a \neq 0 \Rightarrow a^2 > 0$.

3.69. a) Chứng minh rằng mọi vành sắp thứ tự đều có đặc số 0.

b) Cho X là một vành sắp thứ tự với tập con dương của X là P. Một vành con A của X. Chứng minh rằng A là một vành sắp thứ tự với tập con dương là $A \cap P^*$.

3.70. Trong một vành sắp thứ tự, định nghĩa giá trị tuyệt đối của phần tử a là một phần tử $|a|$ cho bởi

$$|a| = \begin{cases} a & \text{nếu } a > 0 \\ 0 & \text{nếu } a = 0 \\ -a & \text{nếu } a < 0. \end{cases}$$

Chứng minh các quy tắc sau:

$|ab| = |a|.|b|$

$|a + b| \leq |a| + |b|$

$-|a| \leq a \leq |a|$

$|a| - |b| \leq |a-b|$

3.71. Giả sử A là một miền nguyên sắp thứ tự. $\overline{A}$ là trường các thương của A. Chứng minh rằng tồn tại duy nhất một quan hệ thứ tự trong $\overline{A}$ sao cho phép nhúng chính tắc

$$f : A \to \overline{A}$$
$$a \mapsto f(a)$$

bảo toàn thứ tự, nghĩa là nếu a là phần tử dương trong A thì f(a) là phần tử dương trong $\overline{A}$.

3.72. Cho X là một trường sắp thứ tự; $x, y \in X$ là hai phần tử mà $x < y$. Chứng minh tồn tại phần tử $z \in X$ sao cho $x < z < y$.

3.73. Trường sắp thứ tự X được gọi là sắp thứ tự Acsimet nếu với mọi $x, y \in X$, $0 < x$ tồn tại một số tự nhiên n sao cho $y < nx$. Chứng minh:

a) Trường số hữu tỉ $\mathbb{Q}$ và trường số thực $\mathbb{R}$ là những trường sắp thứ tự Acsimet;

b) Nếu X là một trường sắp thứ tự Acsimet thì với mọi x và y thuộc X, $x < y$, tồn tại $z \in \mathbb{Q}$ sao cho $x < z < y$.

3.74. Chứng minh rằng không có một quan hệ thứ tự nào trên tập các số phức $\mathbb{C}$ để $\mathbb{C}$ là một trường sắp thứ tự.

Chương IV
VÀNH ĐA THỨC

Trong toàn bộ chương này, các vành đã cho là vành giao hoán có đơn vị 1.

A. TÓM TẮT LÍ THUYẾT

1. Vành đa thức một ẩn

Giả sử A là một vành giao hoán với đơn vị 1, P là tập hợp các dãy $(a_0, a_1, ..., a_n, ...)$, trong đó $a_i \in A$ với mọi $i \in \mathbb{N}$ và bằng 0 tất cả trừ một số hữu hạn. Trong P, phép cộng và phép nhân được định nghĩa như sau:

1) $(a_0, a_1, ..., a_n, ...) + (b_0, b_1, ..., b_n ...) =$

$= (a_0 + b_0, a_1 + b_1, ..., a_n + b_n, ...)$

2) $(a_0, a_1, ..., a_n, ...) . (b_0, b_1, ..., b_n ...) = (c_0, c_1, ... c_n, ...)$ với $c_i = \sum_{k+l=i} a_k b_l$, $i = 0, 1, 2, ..., n, ...$

Với hai phép toán này, P là một vành giao hoán, có đơn vị.

Ánh xạ $A \to P$

$$a \mapsto (a, 0, ..., 0, ...)$$

là một đơn cấu vành, do vậy nếu ta đồng nhất phần tử $a \in A$ với dãy $(a, 0, ..., 0, ...) \in P$ thì A là một vành con của P.

Đặt $x = (0, 1, 0, ..., 0, ...)$, khi đó mỗi phần tử của P là dãy $(a_0, a_1, ..., a_n, 0, ...)$ với $a_i \in A$, $i = 0, 1, ..., n, ...$ có thể viết được dưới dạng

$$f(x) = a_0 + a_1 x + ... + a_n x^n.$$

f(x) được gọi là đa thức của ẩn x với hệ tử trên A. Phần tử không của vành P là $(0, 0, ..., 0, ...)$ gọi là đa thức không, kí hiệu là 0.

Nếu $a_n \neq 0$ $(n \geq 0)$ thì n được gọi là bậc của đa thức f(x), kí hiệu : bậc của f(x) (hay degf(x)). Đa thức 0 là đa thức không có bậc.

Vành P được gọi là *vành đa thức của ẩn* x *trên* A, kí hiệu là

$$P = A[x].$$

Cho f(x) và g(x) thuộc P[x]; h(x) = f(x) + g(x) và k(x) = f(x)g(x). Nếu $f(x) \neq 0$, $g(x) \neq 0$, $h(x) \neq 0$ và $k(x) \neq 0$ thì

bậc $h(x) \leq \max$ (bậc f(x), g(x));

bậc k(x) ≤ bậc f(x) + bậc g(x).

Nếu A là miền nguyên thì deg(f(x)g(x)) = degf(x) + degg(x). Khi đó ta có vành A[x] cũng là một miền nguyên.

2. Phép chia với dư

Giả sử A là một trường. f(x) và g(x) thuộc A[x], $g(x) \neq 0$. Khi đó tồn tại duy nhất các đa thức q(x) và r(x) thuộc A[x] sao cho

$$f(x) = g(x)q(x) + r(x).$$

Nếu $r(x) \neq 0$ thì bậc r(x) nhỏ hơn bậc g(x). Đa thức q(x) được gọi là thương và r(x) được gọi là dư của phép chia f(x) cho g(x). Như vậy f(x) chia hết cho g(x) trong A[x] khi và chỉ khi dư trong phép chia f(x) cho g(x) bằng 0.

3. Nghiệm của đa thức

Định nghĩa. Cho A là một vành con của vành B và

$f(x) = a_0 + a_1x + \ldots + a_nx \in A[x]$. Khi đó với $\alpha \in B$

$f(\alpha) = a_0 + a_1\alpha + \ldots + a_n\alpha \in B$ được gọi là giá trị của đa thức f(x) tại α.

Định lí. Cho A là một trường, $f(x) \in A[x]$ và $\alpha \in A$. Dư trong phép chia f(x) cho $x - \alpha$ là $f(\alpha)$.

Định nghĩa. Phần tử $\alpha \in B$ được gọi là nghiệm của đa thức

$$f(x) = a_0 + a_1x + \ldots + a_nx^n \in A[x],$$

với A là một vành con của B, nếu

$$f(\alpha) = a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$$

Định nghĩa. Phần tử $\alpha \in B$ được gọi là phần tử *đại số* trên A nếu nó là nghiệm của một đa thức khác 0 trong A[x]. Trong trường hợp trái lại, α được gọi là phần tử *siêu việt* trên A.

Định lí. Giả sử A là một trường. $\alpha \in A$ là nghiệm của đa thức $f(x) \in A[x]$ khi và chỉ khi f(x) chia hết cho $x - \alpha$ trong A[x].

Sơ đồ Hooc-ne

Cho $f(x) = a_0 + a_1x + \ldots + a_nx^n \in A[x]$, $\alpha \in A$, giả sử $f(x) = (x - \alpha)g(x)$. Khi đó $g(x) = b_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-1} \in A[x]$ với b_i được xác định trong sơ đồ sau :

	a_0	a_1	$\cdots$	a_k	$\cdots$	a_{n-1}	a_n
α	$b_0 = a_0$	$b_1 = a_1 + \alpha b_0$	$\cdots$	$b_k = a_k + \alpha b_{k-1}$	$\cdots$	b_1	$f(\alpha)$

4. Trường phân thức

Định nghĩa

Cho A là một miền nguyên (trường), A[x] là vành đa thức của ẩn x trên A. Trường các thương của vành A[x] được gọi là trường phân thức của ẩn x trên A và kí hiệu là A(x).

Như vậy $A(x) = \left\{ \dfrac{f(x)}{g(x)} \,\middle|\, f(x), g(x) \in A[x], g(x) \neq 0 \right\}$,

trong đó $\dfrac{f(x)}{g(x)} = \dfrac{f'(x)}{g'(x)} \Leftrightarrow f(x)g'(x) = f'(x)g(x)$.

5. Vành đa thức nhiều ẩn

Bằng quy nạp, ta xây dựng vành đa thức nhiều ẩn trên vành A như sau:

$$A_1 = A[x_1]$$

$$A_2 = A_1[x_2]$$

...

$$A_n = A_{n-1}[x_n]$$

Vành $A_n = A_{n-1}[x_{n-1}]$ kí hiệu là $A[x_1, x_2, ..., x_n]$ được gọi là *vành đa thức của* n *ẩn* $x_1, x_2, ..., x_n$ *trên* A. Các phần tử của $A[x_1, x_2, ..., x_n]$ kí hiệu là $f(x_1, x_2, ..., x_n)$, có dạng

$$f(x_1, x_2, ..., x_n) = C_1 x_1^{a_{11}} x_2^{a_{12}} ... x_n^{a_{1n}} + C_2 x_1^{a_{21}} x_2^{a_{22}} ... x_n^{a_{2n}} + \\ + ... C_m x_1^{a_{m1}} x_2^{a_{m2}} ... x_n^{a_{mn}}$$

trong đó $C_i \in A$, $i = 1, ..., m$ và $(a_{i1}, a_{i2}, ..., a_{in}) \in \mathbb{N}^n$, $i = 1, 2, ..., m$.

Chú ý. Nếu A là một miền nguyên thì $A[x_1, x_2, ..., x_n]$ cũng là một miền nguyên.

Cho miền nguyên A. Trường các thương của $A[x_1, x_2, ..., x_n]$ được gọi là trường phân thức của n ẩn $x_1, x_2, ..., x_n$ kí hiệu là $A(x_1, x_2, ..., x_n)$. Như vậy

$$A(x_1, ..., x_n) = \left\{ \frac{f(x_1,...,x_n)}{g(x_1,...,x_n)} \,\middle|\, \begin{array}{c} f(x_1,...,x_n), g(x_1,...,x_n) \in A[x_1,...,x_n], \\ g(x_1,...,x_n) \neq 0 \end{array} \right\}$$

Định nghĩa. Đa thức $f(x_1, x_2, ..., x_n)$ được gọi là một *đa thức đối xứng* nếu

$$f(x_1, x_2, ... x_n) = f(x_{i_1}, x_{i_2}, ..., x_{i_n})$$

trong đó $(i_1, i_2, ..., i_n)$ là một hoán vị bất kì của $\{1, 2, ..., n\}$. Các đa thức sau đây được gọi là các *đa thức đối xứng cơ bản*

$$\sigma_1 = x_1 + x_2 + ... x_n$$

$$\sigma_2 = x_1x_2 + x_1x_3 + \ldots + x_1x_n + x_2x_3 + \ldots + x_{n-1}x_n$$

...

$$\sigma_n = x_1x_2 \ldots x_n$$

Định lí. Mọi đa thức đối xứng đều viết được dưới dạng một đa thức của các đa thức đối xứng cơ bản.

B. BÀI TẬP

4.1. Trong vành đa thức $\mathbb{Z}_3[x]$ hãy tìm tất cả các đa thức có bậc là:

a) 2; b) 3; c) n.

4.2. Tìm các ước của đơn vị trong các vành sau:

a) $\mathbb{Z}[x]$; b) $\mathbb{Q}[x]$;

c) A[x], A là một trường;

d) A[x], A là một miền nguyên.

4.3. Cho A là vành giao hoán có đơn vị. Chứng minh rằng đa thức $f(x) = ax + u$ là khả nghịch, trong đó u là một ước của 1 và a là phần tử luỹ linh (tức là tồn tại số nguyên dương n sao cho $a^n = 0$). Hãy phát biểu kết quả trên khi f(x) có bậc $n > 1$.

4.4. Cho $\varphi : A \to B$ là một đồng cấu từ vành A đến vành B.

Chứng minh rằng ánh xạ $\overline{\varphi} : A[x] \to B[x]$

$$f(x) = \sum_{i=0}^{n} a_i x^i \to \sum_{i=0}^{n} \varphi(a_i) x^i$$

là một đồng cấu.

Nếu φ là một đẳng cấu thì $\overline{\varphi}$ cũng là một đẳng cấu.

4.5. Trong vành $\mathbb{Z}_8[x]$, chứng minh rằng các đa thức sau đây khả nghịch:

a) $1 + 4x$; b) $1 + 4x + 4x^2$;

c) $1 + 4x + \ldots + 4x^n$.

4.6. Chứng minh rằng nếu A là một miền nguyên vẹn sắp thứ tự thì vành đa thức A[x] cũng vậy. Tồn tại ít nhất hai cách sắp thứ tự trong A[x] như sau:

a) $f(x) = \sum_{i=0}^{n} a_i x^i > 0 \Leftrightarrow$ hệ tử cao nhất là dương trong A.

b) $f(x) = \sum_{i=0}^{n} a_i x^i$ bậc n, $f(x) > 0 \Leftrightarrow a_0 > 0$.

4.7. Đạo hàm hình thức của đa thức $f(x) = \sum_{i=0}^{n} a_i x^i$ là đa thức $f(x) = \sum_{i=1}^{n} i a_i x^{i-1}$. Chứng minh các quy tắc sau:

a) $(cf(x))' = cf'(x)$, $\forall c \in R$, $\forall f(x) \in R[x]$;

b) $(f(x) + g(x))' = f'(x) + g'(x)$, $\forall f(x), g(x) \in R[x]$;

c) $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$, $\forall f(x), g(x) \in R[x]$;

d) $(f(x)^m)' = mf'(x)f(x)^{m-1}$, $\forall m \geq 1, \forall f(x) \in R[x]$;

4.8. Trong vành đa thức $\mathbb{Z}_5[x]$ hãy thực hiện các phép nhân

$(\bar{2}x^2 + \bar{4}x + \bar{1}).(\bar{3}x^2 + \bar{1}x + \bar{2})$;

$(-\bar{2}x^2 + \bar{4}x + \bar{3})^2$.

4.9. Trong vành $\mathbb{Z}_6[x]$ hãy thực hiện phép nhân

$(\overline{2}x^3 + \overline{4}x^2 + \overline{1}x).(\overline{3}x^2 + \overline{3}x + \overline{2})$

Vành này có ước của 0 hay không?

4.10. Trong vành $\mathbb{Z}_5[x]$ hãy thực hiện phép chia

$$f(x) = -\overline{1}x^3 + \overline{2}x^2 + \overline{2}x + 1 \text{ cho } g(x) = -\overline{2}x^2 + \overline{2}x - \overline{1}$$

4.11. Hãy xác định số nguyên p để dư của phép chia đa thức $\overline{1}x^3 + \overline{p}x + \overline{5}$ cho $\overline{1}x^2 + \overline{5}x + \overline{6}$ trong $\mathbb{Z}_7[x]$ bằng $\overline{0}$.

4.12. Trong vành $\mathbb{Q}[x]$ chứng minh rằng đa thức

$$f(x) = (x+1)^{2n} - x^{2n} - 2x - 1$$

chia hết cho

a) $2x + 1$; b) $x + 1$; c) x.

4.13. a) Chứng minh rằng đa thức $f(x) = \overline{1}x^2 + \overline{14} \in \mathbb{Z}_{15}[x]$ có bốn nghiệm trong $\mathbb{Z}_{15}$.

b) Tìm tất cả các nghiệm đa thức $g(x) = \overline{1}x^2 + \overline{20} \in \mathbb{Z}_{21}[x]$ trong vành $\mathbb{Z}_{21}$.

4.14. Cho A là một vành giao hoán với đơn vị 1. Các đa thức f(x) và g(x) thuộc A[x] với g(x) là đa thức có hệ tử cao nhất bằng 1. Chứng minh rằng tồn tại duy nhất hai đa thức q(x) và r(x) thuộc A[x] sao cho f(x) = g(x)q(x) + r(x). Nếu $r(x) \neq 0$ thì bậc r(x) bé hơn bậc g(x).

4.15. Cho A là một miền nguyên, $f(x) \in A[x]$.

a) Giả sử $u \in A$ là nghiệm của f(x). Chứng minh rằng f(x) chia hết cho $(x - u)$ trong A[x].

b) Giả sử $u_1, u_2, \ldots, u_m$ đều thuộc A là m nghiệm phân biệt của f(x). Chứng minh rằng $f(x) = (x - u_1)(x - u_2) \ldots (x - u_m)$ g(x) trong đó $g(x) \in A[x]$.

4.16. Cho A là một trường, $f(x) \in A[x]$ có bậc n ($n \geq 0$). Chứng minh rằng f(x) có không quá n nghiệm phân biệt trong A.

Tính chất này còn đúng không nếu:

a) A là một miền nguyên?

b) A là một vành có đơn vị tuỳ ý?

4.17. Cho A là một trường con của trường B. Phần tử $\alpha \in B$ là đại số trên A, $p(x) \in A[x]$ là đa thức có bậc thấp nhất trong A[x] và có nghiệm α. Chứng minh:

a) Inđêan sinh bởi đa thức p(x), $I = (p(x))$, là một idêan tối đại trong A[x];

b) Vành thương $A[x]/I$ đẳng cấu với $A[\alpha]$; từ đó suy ra $A[\alpha]$ là một trường ($A[\alpha] = \{f(\alpha) \mid f(x) \in A[x]\}$).

4.18. Cho f(x) là một đa thức thuộc vành A[x], a là một phần tử của vành A. Chứng minh rằng f(x) bất khả quy trong A[x] khi và chỉ khi f(x + a) bất khả quy trong A[x].

4.19. Cho $\varphi : A \to V$ là một đồng cấu từ A đến vành V sao cho $\varphi(1) = 1$. Chứng minh rằng với mỗi $u \in V$ tồn tại duy nhất một đồng cấu $\bar{\varphi} : A[x] \to V$ sao cho

$\bar{\varphi}|_A = \varphi$. Nói cách khác ta có biểu đồ sau giao hoán

Với q là phép nhúng chính tắc A vào A[x].

4.20. Cho A là một vành giao hoán, có đơn vị. I là một iđêan của A

$$I[x] = \left\{ \sum_{i=0}^{n} a_i x^i \in A[x] \;\middle|\; a_i \in I;\ i = 0, ..., n;\ n \geq 0 \right\}.$$

Chứng minh rằng:

a) I[x] là một iđêan của vành A[x];

b) $A[x]/I[x]$ đẳng cấu với $\left(A/I\right)[x]$;

c) I là iđêan nguyên tố của A khi và chỉ khi I[x] là iđêan nguyên tố của A[x];

d) Nếu I là iđêan tối đại của X thì I[x] có là iđêan tối đại của A[x] hay không?

4.21. Cho A là một miền nguyên. Chứng minh rằng tập hợp các đa thức thuộc A[x] có hạng tử tự do bằng 0 là một iđêan nguyên tố của A[x]. Nếu A là một trường thì tập các đa thức có hạng tử tự do bằng 0 có là iđêan tối đại của A[x] hay không?

4.22. Trong vành $\mathbb{Z}[x_1, x_2, x_3]$ hãy biểu diễn đa thức

$$x_1^4 + x_2^4 + x_3^4$$

qua các đa thức đối xứng cơ bản.

4.23. Trong vành $\mathbb{Z}_2[x_1, x_2, x_3]$ hãy 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.

4.24. Trong vành $\mathbb{R}[x, y]$ hãy biểu diễn các đa thức sau qua các đa thức đối xứng cơ bản:

a) $x^5 + y^5$;

b) $x^5 + 2x^3y^2 + 3x^2y^2 - x^4y - xy^4 + 2x^2y^3 + y^5$.

4.25. Tìm các số nguyên x, y, x sao cho

$$\begin{cases} xyz = 6 \\ x^3 + y^3 + z^3 = 36 \\ x + y + z = 6 \end{cases}.$$

4.26. Giải hệ phương trình

$$\begin{cases} x^2 + y^2 = 4 \\ x^3 + y^3 = 8 \end{cases}.$$

4.27. Giải hệ phương trình

$$\begin{cases} x^3 + y^3 + z^3 = a^3 \\ x^2 + y^2 + z^2 = b^2 \\ x + y + z = a \end{cases}.$$

4.28. Tìm nghiệm nguyên của phương trình

$$x + y = x^2 = xy + y^2.$$

4.29. Tìm nghiệm nguyên dương của phương trình

$$x^3 + y^3 + 1 = 3xy.$$

4.30. Tìm tổng lập phương các nghiệm của đa thức

$$f(x) = x^4 + x^3 + 2x^2 + x + 1.$$

4.31. Phân tích các đa thức sau thành các nhân tử:

a) $f(x, y) = 6x^4 - 11x^3y - 18x^2y^2 - 11xy^3 + 6y^4$;

b) $g(x, y, z) = 2(x^2y^2 + x^2z^2 + y^2z^2) - (x^4 + y^4 + z^4)$.

4.32. Chứng minh hằng đẳng thức

$$(x + y + z)(xy + xz + yz) - xyz = (x + y)(x + z)(y + z).$$

4.33. Chứng minh rằng nếu $x + y + z = 0$ thì

$$x^4 + y^4 + z^4 = 2(xy + xz + yz)^2$$

4.34. Chứng minh rằng nếu a, b; c là những số thực thoả mãn $a + b \geq c \geq 0$ thì ta có các bất đẳng thức

a) $a^2 + b^2 \geq \frac{c^2}{2}$; b) $a^4 + b^4 \geq \frac{c^4}{8}$;

c) $a^8 + b^8 \geq \frac{c^8}{128}$.

4.35. Cho x, y, z là ba số thực bất kì. Chứng minh

$$(x + y + z)^2 \geq 3(xy + xz + yz).$$

Đẳng thức xảy ra khi $x = y = z$.

4.36. Chứng minh rằng nếu a, b, c là những số thực bất kì thì ta có

$$(ab + ac + bc)^2 \geq 3abc(a + b + c).$$

4.37. Cho a, b, c là những số thực dương. Chứng minh

$$(x - y - z)(xy + yz + zx) \geq 9xyx.$$

4.38. Trong vành R[x, y], phân tích

$f(x, y) = x^3 + 3x^3y + 2x^2y + 3x^2y^2 + 2xy^2 + 3xy^3 + y^3$

thành tích những nhân tử bất khả quy.

4.39. Trong vành R[x, y, z] phân tích

$$f(x, y, z) = -x^4 - y^4 - z^4 + 2x^2y^2 + 2x^2z^2 + 2y^2z^2.$$

thành một tích những nhân tử bất khả quy.

4.40. Cho a, b, c là ba số thực sao cho $a + b + c = abc$.

Chứng minh rằng

$$a(b^2 - 1)(c^2 - 1) + b(a^2 - 1)(c^2 - 1) + c(a^2 - 1)(b^2 - 1) = 4abc.$$

4.41. Cho x, y, z là ba số thực sao cho $x + y + z = 0$.

Chứng minh rằng $x^4 + y^4 + z^4 = 2(xy + xz + yz)^2$.

Chương V
VÀNH CHÍNH VÀ VÀNH ƠCLIT

A. TÓM TẮT LÍ THUYẾT

1. Lý thuyết chia hết trong miền nguyên

Định nghĩa. Giả sử A là một miền nguyên với đơn vị 1. Hai phần tử a và b thuộc A. Phần tử b được gọi là *ước của* a nếu tồn tại phần tử $c \in A$ sao cho $a = bc$, kí hiệu $b \setminus a$.

Tập hợp U các ước của đơn vị 1 lập thành một nhóm với phép nhân, gọi là *nhóm nhân các phần tử khả nghịch của* A. Hai phần tử a và b được gọi là liên kết với nhau nếu $a \setminus b$ và $b \setminus a$.

Phần tử b được gọi là *ước thực sự* của a nếu b không khả nghịch; $b \setminus a$ và a không là ước của b.

Phần tử b được gọi là *bất khả quy* nếu b không khả nghịch và b không có ước thực sự.

Phần tử b được gọi là *nguyên tố* nếu b không khả nghịch và quan hệ $b \setminus ac$ kéo theo $b \setminus a$ hoặc $b \setminus c$ với mọi a và c thuộc A.

Định lí. Trong miền nguyên A mọi phần tử nguyên tố đều bất khả quy.

Định nghĩa. Phần tử c được gọi là *ước chung* của a và b nếu $c \setminus a$ và $c \setminus b$. Phần tử d được gọi là *ước chung lớn nhất* của a và b nếu d là ước chung của a và b và mọi ước chung của a và b đều là ước của d.

2. Vành chính

Định nghĩa. Miền nguyên A được gọi là *vành chính* nếu mọi iđêan của A đều là iđêan chính.

Tính chất. Trong vành chính A :

- Ước chung lớn nhất của hai phần tử bất kì luôn luôn tồn tại.
- Mọi phần tử bất khả quy đều là nguyên tố.
- Mọi dãy tăng nghiêm ngặt các iđêan

$$I_1 \subset I_2 \subset \ldots \subset I_n \subset \ldots$$

đều dừng.

Định lí. Trong vành chính A, mọi phần tử khác 0 và khác ước của 1 đều phân tích được một cách duy nhất thành một tích những nhân tử bất khả quy sai khác thứ tự và các ước của đơn vị.

3. Vành Ơclit

Định nghĩa. Vành Ơclit là một miền nguyên A cùng với ánh xạ

$$\delta : A^* = A - \{0\} \to \mathbb{N}$$
$$a \mapsto \delta(a)$$

sao cho:

a) Nếu $b \setminus a$ và $a \neq 0$ thì $\delta(b) \leq \delta(a)$;

b) Với hai phần tử a, b tuỳ ý của A, $b \neq 0$, tồn tại q và r thuộc A sao cho $a = bq + r$. Nếu $r \neq 0$ thì $\delta(r) < \delta(b)$.

Định lí. Mọi vành Ơclit đều là vành chính.

Dựa vào tính chất sau đây để tìm ước chung lớn nhất của hai phần tử.

Nếu $a = bq + r$ thì ước chung lớn nhất của a và b bằng ước chung lớn nhất của b và r.

Trong vành Ơclit ta tìm ước chung lớn nhất của a và b bằng thuật toán Ơclit.

B. BÀI TẬP

5.1. Trong vành đa thức $\mathbb{R}[x]$, với $\mathbb{R}$ là trường số thực, chứng minh các đa thức $ax^2 + bx + c$ với $b^2 - 4ac < 0$ là những đa thức bất khả quy. Điều đó có còn đúng nữa không nếu thay trường số thực $\mathbb{R}$ bởi trường số phức $\mathbb{C}$?

5.2. Cho a và b là hai phần tử của miền nguyên X. Chứng minh rằng:

a) a là ước của b khi và chỉ khi $aX \supset bX$.

b) a là liên kết với b khi và chỉ khi $aX = bX$.

b) a là liên kết với b khi và chỉ khi $aX = bX$.

5.3. Cho X là một miền nguyên. Chứng minh rằng các tính chất sau đây tương đương với nhau:

i) Mọi dãy tăng những iđêan chính của X đều dừng.

ii) Mọi dãy giảm những ước thực sự đều dừng.

iii) Mọi họ khác rỗng những iđêan chính của X đều có phần tử tối đại.

5.4. Xét vành 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 nữa 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.

5.5. Trong vành $\mathbb{Z}[x]$ xét xem các đa thức sau đây có phải là bất khả quy hay không:

$$f(x) = 2x + 8;$$

$$g(x) = x^2 + 1;$$

$$h(x) = x^2 + 2x - 2.$$

5.6. Giả sử a và b là hai phần tử nguyên tố cùng nhau của vành chính A. Chứng minh iđêan sinh ra bởi a và b là vành A.

5.7. 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 một iđêan tối đại.

5.8. Trong một vành chính, chứng minh các iđêan nguyên tố khác (0) là các iđêan tối đại.

5.9. Chứng minh một trường là một vành chính.

5.10. Vành thương của một vành chính có phải là một vành chính không?

5.11. Vành con của một vành chính có phải là một vành chính không?

5.12. Vành $\mathbb{Z}[x]$ có phải là một vành chính không?

5.13. Giả sử $A = \left\{a + b\sqrt{3}i \mid a, b \in \mathbb{Z}\right\}$.

a) Chứng minh rằng A cùng với phép cộng và phép nhân các số phức là một miền nguyên.

b) Chứng minh rằng 2, $1 + \sqrt{3}i$, $1 - \sqrt{3}i$ là những phần tử bất khả quy của A nhưng không phải là những phần tử nguyên tố. Từ đó suy ra A không phải là một vành chính.

5.14. Chứng minh rằng vành

$$A = \left\{a + b\sqrt{2}i \mid a, b \in \mathbb{Z}\right\}$$

là một vành chính.

5.15. Chứng minh rằng vành $\mathbb{Z}[x]$ không là vành chính nhưng vành thương $\mathbb{Z}[x]/(x^2+2)$ là một vành chính.

5.16. Chứng minh rằng $\mathbb{Z}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\right\}$ là một vành Ơclit.

5.17. Chứng minh rằng $\mathbb{Z}[x]/(x^2+2)$ là một vành Ơclit.

5.18. Giả sử a và b là hai phần tử của một vành chính có dạng phân tích như sau:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n}.$$

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, 2, ..., n.

Chứng minh phần tử $d = p_1^{\gamma_1} p_2^{\gamma_2} ... p_n^{\gamma_n}$ với $\gamma_i = \min(\alpha_i, \beta_i)$, i = 1, ..., n là một ước chung lớn nhất của a và b.

5.19. Chứng minh rằng vành A[x] là một vành chính khi và chỉ khi miền nguyên A là một trường.

5.20. Miền nguyên A được gọi là vành Gao–xơ nếu mọi phần tử khác 0, không khả nghịch đều phân tích được một cách duy nhất (nếu không kể đến thứ tự các nhân tử và các ước của đơn vị) thành một tích những nhân tử bất khả quy. Hãy chứng minh ;

a) Mọi vành chính đều là vành Gao–xơ;

b) Trong một vành Gao-xơ luôn tồn tại ước chung lớn nhất của hai phần tử bất kì;

c) Trong một vành Gao-xơ mọi dãy giảm những ước thực sự

$$a_1, a_2, ..., a_n, ...$$

trong đó a_1 khác 0 và khác ước của đơn vị, a_{i+1} là ước thực sự của a_i, i = 1, ..., n – 1 đều dừng.

d) Nếu miền nguyên A thoả mãn tính chất b) và c) thì A là một vành Gao–xơ.

5.21. Chứng minh rằng vành

$A = \left\{ a + b\sqrt{2}i \mid a, b \in \mathbb{Z} \right\}$ là một vành Ơclit.

5.22. Chứng minh rằng một trường là một vành Ơclit.

5.23. Giả sử A là một vành Ơclit. Chứng minh rằng A là một trường khi và chỉ khi $\delta(x)$ là hằng với mọi $x \in A^*$.

5.24. Giả sử vành A với ánh xạ $\delta : A^* \to \mathbb{N}$ là một vành Ơclit.

Chứng minh tồn tại ánh xạ Ơclit

$$\delta' : A^* \to \mathbb{N}$$

sao cho $\delta'(A^*) = \{a, \ldots, n\}$ với $n \geq 0$ hay $\delta'(A^*) = \mathbb{N}$.

5.25. 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.

5.26. Giả sử A là một miền nguyên. Chứng minh điều kiện cần để A là vành 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.

5.27. Chứng minh vành

$$A = \left\{ a + b\frac{1+i\sqrt{19}}{2} \;\middle|\; a, b \in \mathbb{Z} \right\}$$

không phải là một vành Ơclit. (Người ta có thể chứng minh A là vành chính).

5.28. Giả sử $f(x) = x^5 + x^3 + x^2 + x + 1$

$$g(x) = x^3 + 2x^2 + x + 1.$$

Tìm ước chung lớn nhất của f(x) và g(x) trong $\mathbb{Q}[x]$.

5.29. Tìm ước chung lớn nhất của f(x) và g(x) trong $\mathbb{Z}_3[x]$ với

$$f(x) = \bar{1}x^5 + \bar{1}x^3 + \bar{1}x^2 + \bar{1}x + 1$$

$$g(x) = \bar{1}x^3 + \bar{2}x^2 + \bar{1}x + \bar{1}.$$

5.30. Giả sử $\mathbb{R}(\sqrt{-3}) = \{a + b\sqrt{3}\,i \mid a, b \in \mathbb{R}\}$;

$$\mathbb{Q}(\sqrt{-3}) = \{a + b\sqrt{3}\,i \mid a, b \in \mathbb{Q}\};$$

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

Chứng minh rằng

a) $\mathbb{R}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{2})$ là những trường với phép cộng và nhân thông thường các số;

b) $\mathbb{R}(\sqrt{-3}) \cong \mathbb{R}[x]/(x^2 + 3)$

với (x^2+3) là iđêan sinh bởi $x^2 + 3$ trong $\mathbb{R}[x]$;

c) $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2 - 2)$ với $(x^2 - 2)$ là iđêan sinh bởi $x^2 - 2$ trong $\mathbb{Q}[x]$;

5.31. Giả sử E là một trường mở rộng của trường K. Một phần tử u thuộc E, f(x) là đa thức bất khả quy trong K[x] nhận u là nghiệm; giả sử $g(x) \in K[x]$ cũng nhận u là nghiệm. Chứng minh rằng trong K[x]:

a) f(x) là đa thức có bậc thấp nhất nhận u là nghiệm;

b) g(x) chia hết cho f(x);

c) Vành thương $K[x]/f(x)$ đẳng cấu với K[u] với (f(x)) là iđêan sinh bởi f(x) trong K[x]. Chứng minh K[u] là một trường.

5.32. Giả sử E là một trường mở rộng của trường K. Phần tử $u \in E$ và $f(x) \in K[x]$ là đa thức bất khả quy bậc n nhận u làm nghiệm. Chứng minh K[u] là một không gian vectơ trên K với phép cộng trong E và phép nhân các phần tử của K với

các phần tử của K[u] (phép nhân vô hướng) là phép nhân trong E.

Tìm cơ sở và số chiều của không gian K[u].

5.33. Tìm các tự đẳng cấu của trường:

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

5.34. Giả sử $X = \mathbb{Q}^2 = \{(a, b) \mid a, b \in \mathbb{Q}\}$

Trong X xác định hai 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 X với hai phép toán trên là một trường đẳng cấu với $\mathbb{Q}(\sqrt{2})$.

b) Tìm các tự đẳng cấu của X. Từ đó suy ra rằng tập hợp các tự đẳng cấu của X là một nhóm xyclic với phép nhân ánh xạ.

5.35. Cho f(x) là một đa thức với hệ số nguyên có hệ số cao nhất bằng 1. Chứng minh rằng nếu f(x) bất khả quy trong $\mathbb{Z}_p[x]$ (p là một số nguyên tố) thì nó bất khả quy trong $\mathbb{Q}[x]$.

5.36. Cho A là một trường, a và b là hai phần tử cho trước thuộc A. Chứng minh rằng ánh xạ $\varphi : A[x] \to A[x]$

$$f(x) \mapsto f(ax + b)$$

là một tự đẳng cấu của A[x]. Nếu a khả nghịch thì φ là một tự đẳng cấu của A[x].

5.37. Cho $f(x) = x^5 - x^4 - 3x^3 + 2x + 4$. Phân tích f(x) thành một tích những đa thức bất khả quy trên các trường số $\mathbb{Q}$; $\mathbb{Q}(\sqrt{2})$, $\mathbb{R}$ và $\mathbb{C}$.

5.38. Cho A là một vành Gao-xơ, $\overline{A}$ là trường các thương của A. $f(x) = a_0 + a_1x + \ldots + a_nx_n \in A[x]$ được gọi là một đa thức nguyên bản nếu ước số chung lớn nhất của các hệ tử $a_0, a_1, \ldots a_n$ bằng 1. Chứng minh rằng :

a) Tích của hai đa thức nguyên bản là một đa thức nguyên bản.

b) Nếu đa thức $f(x) \in A[x]$; f(x) khả quy trong $\overline{A}[x]$ thì nó cũng khả quy trong A[x].

5.39. Chứng minh rằng nếu A là một vành Gao-xơ thì vành A[x] cũng là vành Gao-xơ. Tính chất này còn đúng không nếu thay giả thiết "vành Gao-xơ" bằng giả thiết "vành chính" hoặc "vành Oclit".

5.40. Trong vành Q[x], hãy tìm đa thức f(x) bất khả quy, có hệ số cao nhất bằng 1, nhận u làm nghiệm với:

a) $u = \sqrt{2} + \sqrt{3}$;

b) $u = \sqrt{2} - \sqrt{3}$;

c) $u = \sqrt{2} + \sqrt{3}i$.

5.41. Với u đã cho trong bài 5.40a), hãy tìm số chiều của Q[u] trên Q.

Chương VI
ĐA THỨC TRÊN CÁC TRƯỜNG SỐ

A. TÓM TẮT LÍ THUYẾT

1. Đa thức với hệ số thực và phức

Trong chương này, ta xét vành A[x] với A là một trong các trường số : Trường số phức $\mathbb{C}$; Trường số thực $\mathbb{R}$; Trường số hữu tỉ $\mathbb{Q}$.

Đối với đa thức với hệ số thực hoặc phức ta có các kết quả sau:

Định lí. Mọi đa thức bậc lẻ với hệ số thực có ít nhất một nghiệm thực.

Định lí. Mọi đa thức bậc n với hệ số phức ($n \geq 1$) đều có ít nhất một nghiệm phức.

Định lí. Đa thức bất khả quy trên trường số phức là và chỉ là các đa thức bậc nhất.

Định lí. Mọi đa thức bậc n ($n \geq 1$) trong trường số phức đều phân tích được thành tích n nhân tử bậc nhất.

Định lí. Các đa thức bất khả quy của $\mathbb{R}[x]$ là và chỉ là các đa thức bậc nhất hoặc đa thức bậc hai với biệt số âm.

Định lí (định lí cơ bản). Mọi đa thức bậc n ($n \geq 1$) với hệ số phức có đúng n nghiệm phức.

2. Phương trình bậc ba và bốn

Một phương trình bậc ba có dạng

$$x^3 + ax^2 + bx + c = 0 \text{ với } a, b, c \in A \qquad (1)$$

bao giờ cũng có thể đưa được về phương trình bậc ba dạng

$$y^3 + py + q = 0 \qquad (2)$$

bằng cách đặt $y = x + \frac{a}{3}$.

• Để giải phương trình (2) ta đặt

$$y = u + v$$

$$-\frac{p}{3} = uv .$$

Khi đó u và v được xác định bởi các công thức sau:

$$u \in \left\{ \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \right\}$$

$$v \in \left\{ \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \right\}.$$

Giả sử u_1 là một giá trị của $\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$ khi đó phần tử v_1 tương ứng với nó là một trong ba giá trị của $\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$ sao cho $u_1 v_1 = -\frac{p}{3}$.

Gọi ε là một căn nguyên thuỷ bậc ba của 1 thì ta có công thức nghiệm của phương trình (2) là :

$$y_1 = u_1 + v_1 ;$$

$$y_2 = u_1\varepsilon + v_1\varepsilon^2 ;$$

$$y_3 = u_1\varepsilon^2 + v_1\varepsilon .$$

Để giải phương trình bậc bốn

$$x^4 + ax^3 + bx^2 + cx + d = 0 \qquad (1')$$

ta đưa về giải các phương trình

$$x^2 + \frac{ax}{2} + \frac{y_0}{2} = \alpha x + \beta;$$

$$x^2 + \frac{ax}{2} + \frac{y_0}{2} = -\alpha x - \beta.$$

Trong đó y_0 là một nghiệm của phương trình

$$y^3 - by^2 + (ac - 4d)y - [d(a^2 - 4b) + c^2] = 0. \qquad (2')$$

Phương trình (2') được gọi là phương trình giải bậc ba của phương trình (1').

3. Đa thức với hệ số hữu tỉ

Việc tìm nghiệm hữu tỉ của một đa thức với hệ số hữu tỉ bao giờ cũng đưa được về việc tìm nghiệm hữu tỉ của một đa thức với hệ số nguyên.

Nếu α là một nghiệm hữu tỉ của đa thức

$$f(x) = x^n + a_1x^{n-1} + \ldots + a^n \in \mathbb{Z}[x]$$

thì α là một số nguyên và là ước của a_n. Hơn nữa α phải thoả mãn hai điều kiện sau:

a) $\dfrac{f(1)}{\alpha - 1}$ nguyên,

b) $\dfrac{f(-1)}{\alpha + 1}$ nguyên.

Để xét tính bất khả quy của đa thức với hệ số hữu tỉ trong vành $\mathbb{Q}[x]$ ta có thể dựa vào điều kiện đủ sau:

Tiêu chuẩn Aidenstaino :

Định lí. Giả sử

$$f(x) = a_0 + a_1x + \ldots + a_nx^n \ (n > 1)$$

là một đa thức với hệ số nguyên. Nếu có một số nguyên tố p sao cho p không chia hết hệ số cao nhất a_n, p chia hết tất cả các hệ số còn lại và p^2 không chia hết số hạng tự do a_0 thì đa thức f(x) bất khả quy trong $\mathbb{Q}[x]$.

B. BÀI TẬP

6.1. Trong vành $\mathbb{C}[x]$ hãy phân tích các đa thức sau thành một tích những đa thức bất khả quy:

a) $x^2 + i$;

b) $x^4 - 1 - i$;

c) $x^2 - 4i + 3$;

d) $x^7 - 1 - i\sqrt{3}$.

6.2. Biểu diễn hình học các nghiệm của đa thức

$f(x) = x^p - 1$, $p \geq 1$;

$g(x) = (x - a)^m - b$ (với $a \neq 0$, $m \geq 1$).

Từ đó suy ra rằng f(x) và g(x) có không quá hai nghiệm chung.

6.3. Tìm các nghiệm phức của đa thức

$$f(x) = (1 - x^2)^3 + 8x^3.$$

Phân tích đa thức f(x) thành một tích những đa thức bất khả quy với hệ số thực.

6.4. Dùng thuật toán Ơclit tìm ước chung lớn nhất của hai đa thức trong $\mathbb{Q}[x]$.

a) $f(x) = x^4 + x^3 - 3x^2 + 4x - 1$ và

$g(x) = x^8 + x^2 - x - 1$;

b) $f(x) = x^6 + 3x^4 - 4x^3 - 3x^2 + 8x - 5$ và

$g(x) = x^5 + x^2 - x + 1$;

c) $f(x) = x^5 + x^4 - x^3 - 3x^2 - 3x - 1$ và

$g(x) = x^4 - 2x^3 - x^2 - 2x + 1$;

d) $f(x) = x^4 - 4x^3 + 1$ và

$g(x) = x^3 - 3x^2 + 1$;

e) $f(x) = (x - 1)^3(x + 2)^2(x - 3)(x - 4)$ và

$g(x) = (x - 1)^2(x + 2)(x + 5)$.

6.5. Trong $\mathbb{C}[x]$ hãy thực hiện phép chia.

a) $x^4 - 2x^3 + 4x^2 - 6x + 8$ cho $(x - 1)$;

b) $4x^3 + x^2$ cho $(x + i + 1)$;

c) $x^4 + ix^3 - ix^2 + x + 1$ cho $(x^2 - ix + 1)$;

d) $x^5 + \sqrt{2}\,x^4 - 2x^3 - 3(\sqrt{2} + 1)x^2 - (\sqrt{2} + 3)x - 1$ cho $(x^2 + \sqrt{2}\,x + 1)$;

e) $x^4 + 2x^3 + 4x^2 + 2$ cho $[x^2 + 1(1 - i)x + 1 + i]$

6.6. Dùng thuật toán Ơclit tìm các đa thức p(x) và q(x) sao cho $f(x)p(x) + g(x)q(x) = d(x)$, trong đó d(x) là ước chung lớn nhất của f(x) và g(x), với

a) $f(x) = x^4 + 2x^3 - x^2 - 4x - 2$ và

$g(x) = x^4 + x^3 - x^2 - 2x - 2$;

b) $f(x) = 4x^4 - 3x^3 - 16x^2 + 5x + 9$ và

$g(x) = 2x^3 - x^2 - 5x + 4$.

6.7. Trong vành $\mathbb{C}[x]$ chứng minh rằng đa thức $f(x)$ chia hết cho đa thức $g(x)$ khi và chỉ khi mọi nghiệm của $g(x)$ cũng là nghiệm của $f(x)$ và mọi nghiệm bội cấp k của $g(x)$ cũng là nghiệm bội cấp không bé hơn k của $f(x)$.

6.8. Trong vành $\mathbb{Q}[x]$ chứng minh rằng đa thức

$$f(x) = x^{3k} + x^{3l+1} + x^{3n+2} \ (k, l, n \in \mathbb{N})$$

chia hết cho đa thức $g(x) = x^2 + x + 1$.

6.9. Trong vành $\mathbb{Q}[x]$ 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.

6.10. 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) $x^3 - 3x^2 - 6x + 4 = 0$.

6.11. Chứng minh (ứng dụng đa thức đối xứng)

$$(x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2 = -4p^3 - 27q^2$$

Với x_1, x_2, x_3 là các nghiệm của phương trình

$$x^3 + px + q = 0.$$

6.12. Giải các phương trình

a) $x^4 - 3x^3 + x^2 + 4x - 6 = 0$;

b) $x^4 - 4x^3 + 3x + 2x - 1 = 0$;

c) $x^4 - 2x^3 + 8x^2 + 2x + 7 = 0$;

d) $x^4 + 6x^3 + 6x^2 - 8 = 0$.

6.13. Giả sử $\alpha = 1 + i$.

a) Biểu diễn α dưới dạng lượng giác. Tìm modun và argumen 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 $n \leq 8$.

d) Chứng minh rằng mọi số phức z tuỳ ý đều có thể biểu diễn một cách duy nhất dưới dạng

$$z = x + y\alpha,$$

với x và y là những số thực.

e) Chứng minh rằng ánh xạ $f : \mathbb{C} \to M$

$$z = x + y\alpha \mapsto \begin{bmatrix} x & y \\ -2y & x+2y \end{bmatrix}$$

từ vành số phức đến vành các ma trận vuông cấp hai trên trường số thực là một đẳng cấu. Từ đó suy ra rằng tập hợp các ma trận vuông cấp hai dạng

$$\begin{bmatrix} x & y \\ -2y & x+2y \end{bmatrix}$$

là một trường.

6.14. Tìm đa thức với hệ số thực có bậc bé nhất sao cho:

a) Chia cho $(x - 1)^2$ còn dư $2x$ và chia cho $(x - 2)^3$ còn dư $3x$.

b) Chia cho $x^4 - 2x^3 - 2x^2 + 10x - 7$ còn dư $x^2 + x + 1$ và chia cho $x^4 - 2x^3 - 3x^2 + 13x - 10$ còn dư $2x^2 - 3$.

6.15. 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) $x^5 + 2x^4 + 6x^3 + 3x^2 - 12x - 48$.

6.16. Giả sử phân số tối giản $\frac{p}{q}$ là một nghiệm của đa thức

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x].$$

Chứng minh rằng:

a) $p \setminus a_0$ và $q \setminus a_n$;

b) $p - nq$ là ước của $f(m)$, với m nguyên; đặc biệt $p - q$ là ước của $f(1)$ và $p + q$ là ước của $f(-1)$.

6.17. Áp dụng bài 6.16 để tìm nghiệm hữu tỉ của đa thức

$$f(x) = 10x^5 - 81x^4 + 90x^3 - 102x^2 + 80x - 21.$$

6.18. Chứng minh rằng đa thức $f(x)$ với hệ số nguyên không có nghiệm nguyên nếu $f(0)$ và $f(1)$ đều là những số lẻ.

6.19. Giả sử $p(x)$ là đa thức với hệ số nguyên và $p(x)$ bất khả quy trong $\mathbb{Z}[x]$. Chứng minh rằng trong $\mathbb{Z}[x]$ nếu $p(x) \setminus f(x)g(x)$ thì hoặc $p(x) \setminus f(x)$ hoặc $p(x) \setminus g(x)$.

6.20. Trong vành $\mathbb{Z}(x)$ chứng minh rằng mọi đa thức khác 0 và khác ± 1 đều có thể viết được dưới dạng một tích những đa thức bất khả quy.

6.21. Dùng tiêu chuẩn Aidenstainơ để chứng minh các đa thức sau là bất khả quy trong $\mathbb{Q}[x]$:

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 là một số nguyên tố;

d) $x^3 - 3x + 1$.

6.22. Tìm điều kiện cần và đủ để đa thức

$$f(x) = x^4 + px^2 + q$$

là bất khả quy trong $\mathbb{Q}[x]$.

6.23. Giả sử $f(x) = (x - a_1)(x - a_2) \ldots (x - a_n) - 1$ với a_i là những số nguyên phân biệt, $i = 1, \ldots, n$. Chứng minh rằng $f(x)$ bất khả quy trong $\mathbb{Q}[x]$.

6.24. Cho $a_1, a_2, \ldots, a_n$ là những số nguyên đôi một khác nhau. Chứng minh đa thức

$$f(x) = (x - a_1)^2(x - a_2)^2 \ldots (x - a_n)^2 - 1$$

bất khả quy trong $\mathbb{Q}[x]$.

6.25. Hãy chứng minh định lí Aidenstainơ khi thay vành số nguyên $\mathbb{Z}$ bởi vành Gao-xơ bất kì và $\mathbb{Q}$ bởi trường các thương của vành Gao-xơ đã cho.

PHẦN II. LỜI GIẢI VÀ HƯỚNG DẪN

CHƯƠNG I
CƠ SỞ LÔGIC TOÁN. TẬP HỢP VÀ QUAN HỆ

1.1. a) Dòng kí hiệu $p \to (q \to r)$ là một công thức vì p, q, r là những công thức.

$q \to r$ là công thức.

$p \to (q \to r)$ là công thức.

Bảng giá trị chân lí của các công thức này là:

p	q	r	$p \to r$	$p \to (q \to r)$
1	1	1	1	1
1	1	0	0	0
1	0	1	1	1
1	0	0	0	1
0	1	1	1	1
0	1	0	0	1
0	0	1	1	1
0	0	0	1	1

Đối với các câu b), c) làm tương tự.

1.2. a) Để chứng minh đẳng thức này ta có thể lập bảng giá trị chân lí từng vế của đẳng thức. Cũng có thể chứng minh bằng cách sau đây :

Ta có $p \to q \equiv \overline{q} \to \overline{p}$. Nếu thay p bởi $u \to v$ và q bởi w thì ta được ngay đẳng thức cần chứng minh.

Các câu b), c), e), làm tương tự.

1.3. Chứng minh bằng cách lập bảng giá trị chân lí từng vế của đẳng thức. Ý nghĩa của các đẳng thức này là chỉ cần hai phép toán lôgic $\neg$, $\wedge$ (phép phủ định và phép hội) đủ để xác định các phép toán lôgic còn lại.

1.4. a) Biến đổi vế trái ta có

$$\begin{aligned}(p \to q) \to q &\equiv \overline{p \to q} \vee q \\ &\equiv (p \wedge \overline{q}) \vee q \\ &\equiv (p \vee q) \wedge (\overline{q} \vee q) \\ &\equiv (p \vee q) \wedge 1 \\ &\equiv p \vee q .\end{aligned}$$

1.5. Biến đổi đồng nhất:

a) $$\begin{aligned}p \to (q \to r) &\equiv \overline{p} \vee (q \to r) \\ &\equiv \overline{p} \vee (\overline{q} \vee r) \\ &\equiv (\overline{p} \vee \overline{q}) \vee r \\ &\equiv \overline{p \wedge q} \vee r \\ &\equiv (p \wedge q) \to r\end{aligned}$$

Bạn đọc tự lập bảng giá trị chân lí.

1.6. a) Rút gọn

$$\begin{aligned}\left(\left(\overline{\overline{p} \vee q}\right) \to (p \vee q)\right) \wedge q &\equiv ((\overline{p} \vee q) \vee (p \vee q)) \wedge q \\ &\equiv (\overline{p} \vee p \vee q \vee q) \wedge q \\ &\equiv (1 \vee q) \wedge q \\ &\equiv 1 \wedge q \\ &\equiv q .\end{aligned}$$

1.7. Để giải các bài tập loại này ta chú ý rằng có các đẳng thức sau đây:

$$p \to q \equiv \overline{p} \vee q;$$

$$p \wedge q \equiv \overline{\overline{p} \vee \overline{q}}.$$

1.8. Để giải các bài tập loại này cần chú ý rằng có các đẳng thức sau đây:

$$p \to q \equiv \overline{p \wedge \overline{q}};$$

$$p \vee q \equiv \overline{\overline{p} \wedge \overline{q}}.$$

1.9. Ta có $p \vee q \equiv \overline{q} \to p \wedge q \equiv \overline{p \to \overline{q}}$ vì có các đẳng thức sau đây:

$$p \to q \equiv \overline{p} \vee q;$$

$$p \to q \equiv \overline{p \wedge \overline{q}}.$$

Dựa vào các đẳng thức trên để giải các bài tập loại này.

1.10. Làm tương tự như bài 1.7.

1.11. Làm tương tự như bài 1.8.

1.12. a) Đối ngẫu của $(p \vee \overline{q}) \wedge r$ là $(p \wedge \overline{q}) \vee r$

Phủ định của $(p \vee \overline{q}) \wedge r$ là $\overline{p \vee \overline{q} \wedge r} \equiv \overline{(p \vee \overline{q})} \vee \overline{r}$

$$\equiv (\overline{p} \wedge q) \vee \overline{r}.$$

1.13. a) Lập bảng giá trị chân lí ta có $(p \wedge q) \to (q \vee p)$ là công thức hằng đúng.

c) Lập bảng giá trị chân lí cho kết quả $p \to (q \wedge p)$ không là hằng đúng cũng không là hằng sai.

1.14. Có thể chứng minh bằng cách lập bảng giá trị chân lí, cũng có thể dùng biến đổi đồng nhất.

e) Đưa công thức $(p \wedge (p \to q)) \to q$ về dạng chỉ chứa $\vee$, $\wedge$ ta có

$$(p \wedge (p \to q)) \to q \equiv 1$$

Vậy có luật $\models (p \wedge (p \to q)) \to q$.

1.15. Có hai cách chứng minh. Lập bảng giá trị chân lí hoặc biến đổi đồng nhất. Ta nên biến đổi đồng nhất.

1.16. a) Nếu cho $p = 1, q = 1, r = 1$ thì $(p \vee q) \to r = 1$.

Nếu cho $p = 1, q = 1, r = 0$ thì $(p \vee q) \to r = 0$.

Vậy $(p \vee q) \to r$ không hằng đúng cũng không hằng sai.

1.17. Ta hãy chứng minh quy tắc suy luận:

$$\frac{p, p \to q, q \to r}{r}.$$

Cách 1. Lập bảng giá trị chân lí

p	q	r	$p \to q$	$q \to r$	$q \wedge (p \to q) \wedge (q \to r)$	$p \wedge (p \to q) \wedge (q \to r) \to r$
1	1	1	1	1	1	1
1	1	0	1	0	0	1
1	0	1	0	1	0	1
1	0	0	0	0	0	1
0	1	1	1	1	0	1
0	1	0	1	1	0	1
0	0	1	1	1	0	1
0	0	0	1	1	0	1

Căn cứ vào bảng ta thấy khi $p, p \to q, q \to r$ cùng nhận giá trị 1 thì r cũng nhận giá trị 1. Vậy theo định nghĩa ta có quy tắc suy luận

$$\frac{p, p \to q, q \to r}{r}.$$

Cách 2. Theo định lí giữa quy tắc suy luận và luật lôgic ta có quy tắc suy luận

$$\frac{p, p \to q, q \to r}{r}.$$

khi và chỉ khi có luật

$$\models ((p \wedge (p \to q) \wedge (q \to r)) \to r).$$

Để chứng minh luật này, ta dùng biến đổi đồng nhất hoặc lập bảng giá trị chân lí.

1.18. Chứng minh rằng nếu có $\frac{S}{T}$ và $\frac{T}{S}$ thì $S \equiv T$.

Thật vậy do có $\frac{S}{T}$ nên ta có $\models (T \to S)$. (1)

Tương tự, do có $\frac{T}{S}$ nên có $\models (S \to T)$. (2)

Từ (1) và (2) suy ra $\models (S \leftrightarrow T)$ nghĩa là $S \equiv T$.

Đảo lại, nếu $S \equiv T$ thì ta có $\models (S \to T)$ và $\models (T \to S)$ vậy có $\frac{S}{T}$ và $\frac{T}{S}$.

1.19. Giả sử không phải tất cả các mệnh đề

$$q_1 \to p_1$$

$$q_2 \to p_2$$

$$\dots$$

$$q_n \to p_n$$

đều đúng. Chẳng hạn mệnh đề $q_i \to p_i$ sai, với một i nào đó. Điều này xảy ra khi $q_i = 1$ và $p_i = 0$. Vì $p_1 \vee p_2 \vee \dots \vee p_n = 1$ nên phải có $p_j = 1$ với $j \neq i$. Nhưng $p_j \to q_j = 1$ nên $q_j = 1$. Điều này trái với giả thiết các q_i bài xích lẫn nhau. Vậy điều giả sử trên là sai. Nghĩa là tất cả các mệnh đề $q_i \to p_i$ đúng với mọi $i = 1, 2, \dots, n$.

1.20. Ta kí hiệu b là khẳng định "Bảo đánh vỡ kính", $\bar{b}$ là khẳng định "Bảo không đánh vỡ kính". Các chữ t, k, ... và phủ định của chúng có nghĩa tương tự.

Ta viết các câu nói của các em thành công thức :

An: $A = b \vee t$;

Bảo: $B = \bar{b} \wedge \bar{k}$;

Tuấn: $T = \bar{A} \wedge \bar{B} = \overline{(b \vee t)} \wedge \overline{(\bar{b} \wedge \bar{k})}$;

$= (\bar{b} \wedge \bar{t}) \wedge (b \vee k) = \bar{b} \wedge \bar{t} \wedge k$

Đức: $D = (A \wedge \bar{B}) \vee (\bar{A} \wedge B) = b \vee (\bar{t} \wedge \bar{k})$;

(Chú ý rằng $(t \wedge k)$ là sai vì theo giả thiết chỉ một người đánh vỡ kính).

Khôi: $K = \bar{D} = \overline{b \vee (\bar{t} \vee \bar{k})} = \bar{b} \wedge (t \wedge k)$;

Theo giả thiết ba em nói đúng. Từ các công thức A, B, T, P, K ta lập các hội bằng cách lấy trong mỗi hội ba công thức. Trong các hội đó chỉ có một hội là đúng, các hội kia sai. Có cả thảy $C_5^3 = 10$ hội có thể được. Đó là:

$$A \wedge B \wedge T, A \wedge B \wedge D, A \wedge B \wedge K, A \wedge T \wedge D, A \wedge T \wedge K.$$

$$A \wedge D \wedge K, B \wedge T \wedge D, B \wedge T \wedge K, B \wedge D \wedge K, T \wedge D \wedge K.$$

Vì các công thức A và T, B và T, D và T hội lại cho mâu thuẫn, nên từ mười tổ hợp chỉ xét hai:

$$A \wedge B \wedge D \text{ và } A \wedge B \wedge K.$$

Nhưng ta dễ thấy rằng hội của B và D mâu thuẫn. Vì vậy hội duy nhất đúng là $A \wedge B \wedge K$. Đó là:

$$A \wedge B \wedge K = (b \vee t) \wedge \bar{b} \wedge \bar{k} \wedge (t \vee k) \equiv t \wedge \bar{b} \wedge \bar{k}.$$

Từ đó ta kết luận rằng Tuấn đánh vỡ kính.

1.21. Ta kí hiệu a, b, c, theo thứ tự là các mệnh đề A, B, C, nói đúng sự thật,và kí hiệu các phủ định của chúng là $\bar{a}$, $\bar{b}$, $\bar{c}$.

A có thể nói đúng sự thật, có thể nói không đúng. Vì vậy lời khai của anh ta có thể viết dưới dạng công thức

$$A = (a \wedge \bar{b}) \vee (\bar{a} \wedge b) = 1.$$

Tương tự, lời khai của B có thể viết

$$B = (b \wedge \bar{c}) \vee (\bar{b} \wedge c) = 1.$$

C có thể nói đúng sự thật, trong trường hợp này A và B nói sai, khi đó ta viết $c \wedge \bar{a} \wedge \bar{b}$. Nhưng C cũng có thể nói sai, trong trường hợp này ít nhất một trong hai A hoặc B nói đúng. Khi đó ta viết $\bar{c} \wedge (a \vee b)$. Như vậy lời khai của C có thể viết:

$$C = (c \wedge \bar{a} \wedge \bar{b}) \vee (\bar{c} \wedge (a \vee b)) = 1.$$

Ta có

$$A \wedge B = ((a \wedge \bar{b}) \vee (\bar{a} \wedge b)) \wedge ((b \wedge \bar{c}) \vee (\bar{b} \wedge c)) \equiv \bar{a} \wedge b \wedge \bar{c}.$$

$$A \wedge B \wedge C = (\bar{a} \wedge \bar{b} \wedge \bar{c}) \wedge ((c \wedge \bar{a} \wedge \bar{b}) \vee (\bar{c} \wedge (a \vee b))) \equiv \bar{a} \wedge b \wedge \bar{c} = 1$$

Vậy A và C nói không thật, B nói thật.

1.22. B đi Hà Nội, C đi Thành phố Hồ Chí Minh, A đi Hải Phòng, D đi Nha Trang.

1.23. Ta dùng chữ a để chỉ rằng A làm được bài, các chữ b, c, d, e, m có nghĩa tương tự. Theo giả thiết ta có:

$a \wedge c = 0 ; b \wedge c = 0 ; m \wedge b = 0 ; a \wedge m = 0 ; a \wedge d = 0.$ (1)

Trong năm tuyển $(a \vee c), (b \vee e), (m \vee b), (a \vee m), (a \vee d)$ (2)

có bốn là đúng và một là sai. Vậy hội của chúng là sai.

Ta có :

$(a \vee c) \wedge (b \vee e) \equiv (a \wedge b) \vee (a \wedge e) \vee (c \wedge b) \vee (c \wedge e)$;

$(a \vee c) \wedge (b \vee e) \wedge (m \vee b) \equiv (c \wedge e \wedge m) \vee (a \wedge b) \vee (c \wedge b)$;

$(a \vee c) \wedge (b \vee e) \wedge (m \vee b) \wedge (a \vee m) \equiv (a \wedge b) \vee (c \wedge e \wedge m)$;

$$(a \vee c) \wedge (b \vee e) \wedge (m \vee b) \wedge (a \vee m) \wedge (a \vee d) \equiv$$
$$\equiv (a \wedge b) \vee (c \wedge e \wedge m \wedge d) = 0.$$

Vậy $a \wedge b = 0$.

Ta lấy hội bốn trong năm mệnh đề của (2). Có năm hội như thế và chỉ có một hội đúng.

Ta đã có

$$K = (a \vee c) \wedge (b \vee e) \wedge (m \vee b) \wedge (a \vee m) \equiv$$
$$\equiv (a \wedge b) \vee (c \wedge e \wedge m).$$

Công thức này sai vì $(a \wedge b) = 0$, và theo giả thiết chỉ có hai học sinh làm được bài.

Ta xét $P = (a \vee c) \wedge (b \vee e) \wedge (m \vee b) \wedge (a \vee d) \equiv$

$$\equiv (c \wedge e \wedge m \wedge d) \vee (c \wedge b \wedge d)$$

Công thức này cũng sai.

Ta xét $H = (a \vee c) \wedge (m \vee d) \wedge (a \vee m) \wedge (a \vee d) \equiv (c \wedge m \wedge d)$.

Công thức này cũng sai.

$T = (b \vee c) \wedge (m \vee b) \wedge (a \vee m) \wedge (a \vee d) \equiv (d \wedge m \wedge e)$

Công thức này cũng sai. Vậy công thức thứ năm phải là đúng, tức là

$$F = (a \vee c) \wedge (b \vee e) \wedge (a \vee m) \wedge (a \vee d) \equiv$$

$$\equiv (a \wedge c) \vee (c \wedge e \wedge m \wedge d) = 1.$$

Từ đó suy ra $a \wedge c = 1$. Vậy A và E làm được bài.

1.25. a) Câu $2^0 = 1$ là một mệnh đề, các câu còn lại đều là những hàm mệnh đề.

b) và c) Miền đúng của hai hàm mệnh đề "$x^0 = 1$" và "$x^2 \geq 0$" là tập hợp tất cả các số thực.

d) Miền đúng của hàm mệnh đề "$ax^2 + bx + c > 0$" là:

Nếu $a > 0$ thì miền đúng của nó là tập các số thực nằm ngoài khoảng hai nghiệm (nếu có).

Nếu $a < 0$ thì miền đúng của nó là tập các số thực nằm trong khoảng hai nghiệm (nếu có).

e) Miền đúng của hàm mệnh đề "đường thẳng x song song với đường thẳng y" là tập hợp các đường thẳng song song với đường thẳng y.

1.26. a) Miền đúng của $\varphi(x)$ là $\{\pm 1, \pm 2, \pm 3, \pm 6\}$.

b) Miền đúng của $\varphi(x)$ là tập hợp các nghiệm nguyên của phương trình vô định $2x + 6y = 5$. Phương trình này vô nghiệm. Vậy miền đúng của $\varphi(x)$ là $\varnothing$.

c) Miền đúng của $\varphi(x)$ là tập các điểm nằm trên đường tròn đơn vị trên hệ trục toạ độ Đề-các.

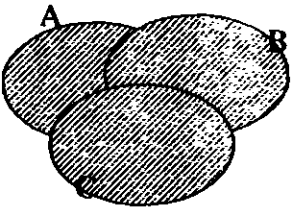
1.27. a) "Nếu x chia hết cho y và y bằng z thì x chia hết hết cho z"

b) "Nếu x không là số nguyên tố và x không là số lẻ thì x chia hết cho 2."

1.28. Chứng minh theo định nghĩa của miền đúng của hàm mệnh đề.

1.29. a) Miền đúng của hàm mệnh đề

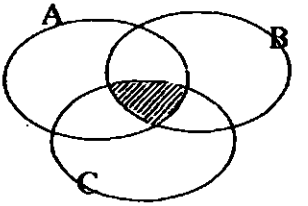
$\varphi(x) \vee \psi(x) \vee \theta(x)$ là hình 3



Hình 3

b) Miền đúng của hàm mệnh đề

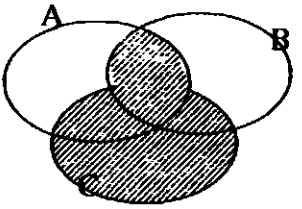
$\varphi(x) \wedge \psi(x) \wedge \theta(x)$ là hình 4



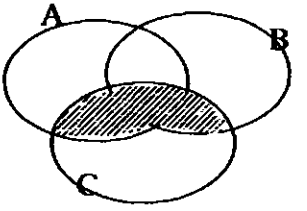
Hình 4

c) Miền đúng của hàm mệnh đề

$[\varphi(x) \wedge \psi(x)] \vee \theta(x)$ là hình 5



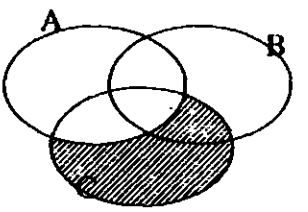
Hình 5



Hình 6

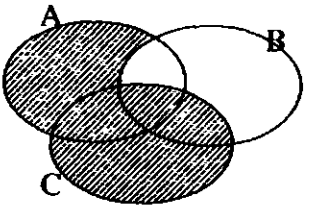
d) Miền đúng của hàm mệnh đề $[\varphi(x) \vee \psi(x)] \wedge \theta(x)$ là hình 6

e) Miền đúng của hàm mệnh đề $[\varphi(x) \to \psi(x)] \wedge \theta(x)$ là hình 7



Hình 7

f) Miền đúng của hàm mệnh đề $\overline{[\varphi(x) \to \psi(x)]} \vee \theta(x)$ là hình 8



Hình 8

1.31. a) "Với mọi số thực x, $|x| = -x$". Mệnh đề này sai.

b) Tồn tại số thực x sao cho $|x| = -x$". Mệnh đề này đúng vì tồn tại số $0 \in \mathbb{R}$, $|0| = 0 = -0$.

1.32. a) Mệnh đề này có thể viết như sau

$(\exists x \in \mathbb{R})\,[(\forall y \in \mathbb{R})(yx = y)]$.

Mệnh đề này đúng vì $1 \in \mathbb{R}$, với mọi số thực y có $1.y = y$.

1.33. a) $(\forall x \in \mathbb{R},\ \forall y \in \mathbb{R},\ \forall z \in \mathbb{R})\ ((x + y)z = xz + yz)$.

1.34. a) Phủ định của mệnh đề

$(\forall x \in \mathbb{R},\ \forall y \in \mathbb{R},\ \forall z \in \mathbb{R})\ (x + y = z)$ là

$(\exists x \in \mathbb{R}, \exists y \in \mathbb{R}, \exists z \in \mathbb{R})(x + y \neq z)$.

1.36. Giả sử $A_{i_1} \in \{A_1, A_2, ..., A_n\}$. Nếu A_{i_1} không chứa tập nào còn lại thì A_{i_1} là tập cần tìm. Nếu nó chứa A_{i_2}, ta lại lập luận như với A_{i_1}. Ta sẽ được một dãy giảm

$$A_{i_1} \supset A_{i_2} \supset A_{i_3} \supset ... \supset A_{i_k} \supset ... \qquad (1)$$

Dãy không vô tận vì chỉ có một số hữu hạn tập A_i.

Dãy (1) phải dừng, nghĩa là có ít nhất một tập A_{i_k} không chứa một tập nào trong các tập còn lại.

Ta có thể đưa ra cách giải khác (quy nạp theo n).

Hiển nhiên đúng cho n = 1. Giả sử đúng cho n – 1 và A_{n-1} là tập không chứa tập A_i nào, i = 1, ..., n – 2. Xét quan hệ giữa hai tập hợp A_{n-1} và A_n. Ta có hoặc

1) $A_n \subset A_{n-1}$, vậy A_n là tập cần tìm; hoặc

2) $A_{n-1} \subset A_n$, vậy A_{n-1} là tập cần tìm; hoặc

3) $A_n \not\subset A_{n-1}$ và $A_{n-1} \not\subset A_n$.

Vậy ta có A_{n-1} là tập cần tìm. Nếu trang bị cho tập hợp $\{A_1, ..., A_n\}$ quan hệ thứ tự là quan hệ bao hàm thì bài toán có thể phát biểu dưới dạng tìm phần tử tối tiểu. Ta cũng có thể phát biểu bài toán bằng tìm phần tử tối đại. Tổng quát hơn, ta có thể xét một tập hợp gồm n phần tử sắp thứ tự và tìm phần tử tối tiểu hay tối đại.

1.37. Giả sử $B \subset A$. Nếu $x \in B$ thì $x \in A$ và $x \notin A - B$ do vậy $x \in A - (A - B)$. Giả sử $x \in A - (A - B)$, như vậy $x \in A$ và

$x \notin A - B$ hay $x \in A$ và $\{x \notin A$ hoặc $x \in B\}$. Không thể xảy ra $x \notin A$ nên chỉ còn lại $x \in B$. Vậy có đẳng thức

$$A - (A - B) = B.$$

Bây giờ giả sử $A - (A - B) = B$. Hiển nhiên có bao hàm thức $A - (A - B) \subset A$ nên $B \subset A$.

1.38. a) Giả sử $X = \{x_1, x_2, \ldots, x_n\}$ là một tập hợp gồm n phần tử và $1 \le r \le n$. Ta xét dãy (sắp thứ tự) $(x_{i_1}, x_{i_2}, \ldots, x_{i_r})$ những phần tử của X đôi một khác nhau. Có bao nhiêu cách lựa chọn các phần tử x_{i_j} thì có bấy nhiêu dãy kể trên. Trước hết với x_{i_1} ta có n cách lựa chọn từ n phần tử của tập X. Với x_{i_2} $(\neq x_{i_1})$ có $n-1$ cách chọn từ $n-1$ phần tử của tập hợp $X_1 = X - \{x_{i_1}\}$ sau khi đã cố định x_{i_1} rồi. Với x_{i_3} có $n-2$ cách chọn từ $n-2$ phần tử của tập hợp $X_2 = X_1 - \{x_{i_2}\}$ sau khi cố định x_{i_1} và x_{i_2} ... Cuối cùng với x_{i_r} có $n - r + 1$ cách chọn từ $n - r + 1$ phần tử của tập hợp $X_{r-1} = X_{r-2} - \{x_{i_{r-1}}\}$.

Vậy có tất cả $n(n-1)\ldots(n-r+1)$ cách chọn dãy

$$(x_{i_1}, x_{i_2}, \ldots, x_{i_r}). \qquad (1)$$

Bây giờ giả sử $\{x_{i_1}, x_{i_2}, \ldots, x_{i_r}\}$ (2)

là một tập con của X gồm r phần tử. Khi đó với mỗi hoán vị của (2) ta được một dãy (1). Như vậy với mỗi một tập con (2) của X ta có r ! dãy (1).

(r ! = 1. 2... r). Do đó số bộ phận của X gồm r phần tử là

$$\frac{n(n-1)(n-2)\ldots(n-r+1)}{r!} = \frac{n!}{(n-r)!r!}.$$

b) Đặt C_n^r là số tập con gồm r phần tử của X. Khi đó ta có $C_n^r = \frac{n!}{(n-r)!r!}$ với quy ước 0! = 1. Đặt $C_n^0 = \frac{n!}{n!0!} = 1$, khi đó số các phần tử của $\mathcal{P}(X)$ sẽ là

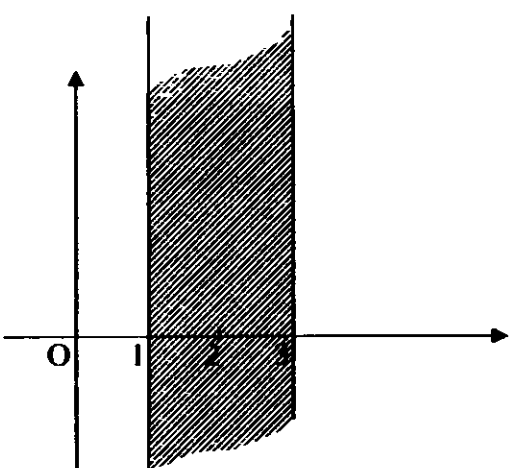
$$C_n^0 + C_n^1 + \ldots + C_n^n =$$

$$= \frac{n!}{0!n!} + \frac{n!}{1!(n-1)!} + \ldots + \frac{n!}{(n-r)!r!} + \ldots + \frac{n!}{n!0!} = 2^n$$

1.39. Biểu diễn hình học tập A × B với

$$A = \{x \in \mathbb{R} \mid 1 \le x \le 3\}$$

$$B = \mathbb{R}$$

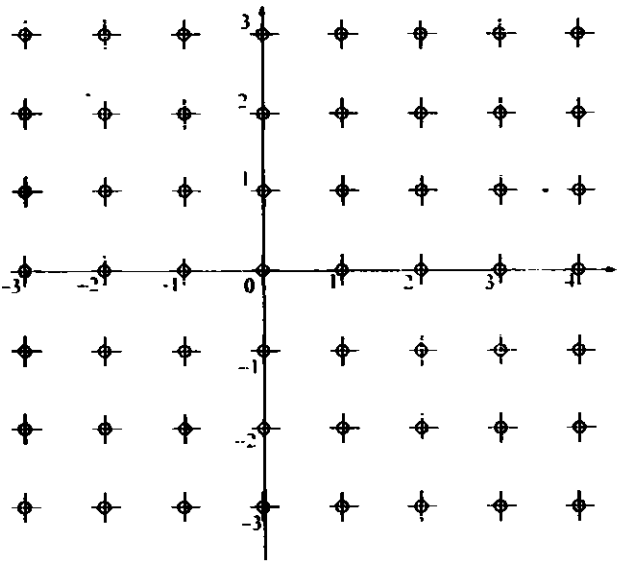


(A × B là phần có gạch chéo)

Hình 9

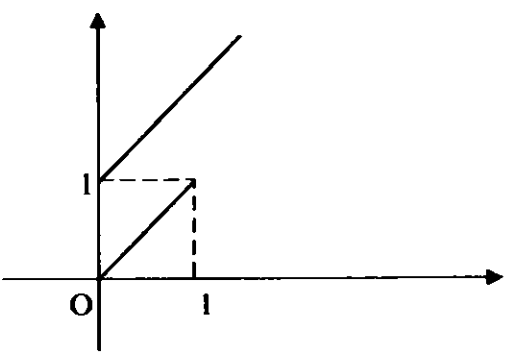
b) $\mathbb{Z} \times \mathbb{Z}$ là tập hợp các điểm có toạ độ nguyên

M = (a, b), a và b thuộc $\mathbb{Z}$.



Hình 10

1.40. Hình ảnh hình học của tập hợp X là đường gạch đậm trong hình 11.



Hình 11

1.41. Các chứng minh là hiển nhiên.

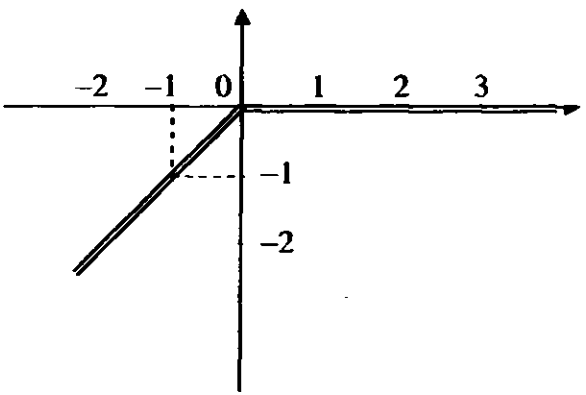
1.42. Tập hợp X không phải là đồ thị của một ánh xạ nào từ $\mathbb{R}$ đến $\mathbb{R}$ vì nếu nó là đồ thị của một ánh xạ $f : \mathbb{R} \to \mathbb{R}$ thì cặp $(-1, f(-1)) \in X$, nhưng cặp này không phụ thuộc X. Ta cũng có thể xét hai cặp (1, 1) và (1, 2) chúng đều thuộc X; Như vậy, tương ứng với 1 là hai phần tử 1và 2, trái với định nghĩa của ánh xạ.

1.43. Ta có ánh xạ $f : \mathbb{R} \to \mathbb{R}$ cho bởi quy tắc

$$f(x) = \begin{cases} x & \text{nếu } x < 0 \\ 0 & \text{nếu } x \geq 0 \end{cases}$$

nhận $G = \{(x,x) \mid x < 0\} \cup \{(x,0) \mid x \geq 0\}$ làm đồ thị của nó.

Hình ảnh hình học của G là đường gạch = trong hình 12.

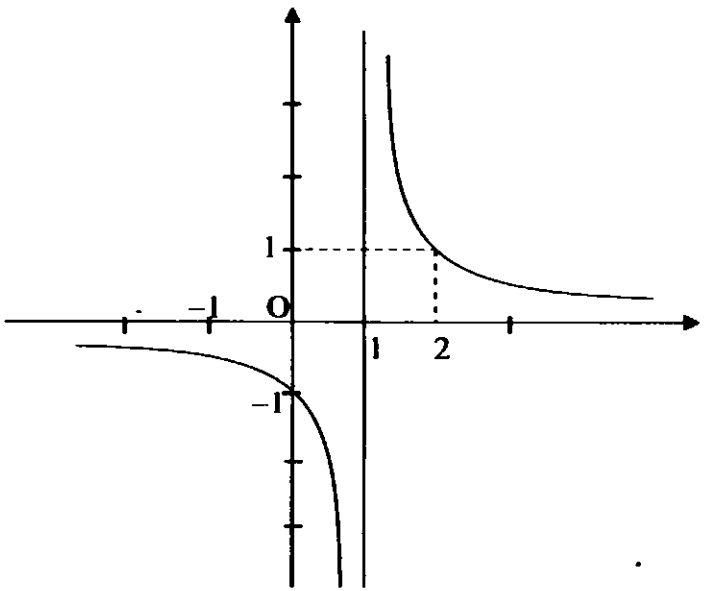


Hình 12

1.44. Tập $G = \{(x, \frac{1}{x-1}) \mid x \in \mathbb{R}, x \neq 1\}$ là đồ thị của ánh xạ

$$f : \mathbb{R} - \{1\} \to \mathbb{R}$$
$$x \mapsto \frac{1}{x-1}$$

Hình ảnh hình học của G là một hyperbol (h. 13)



Hình 13

1.45. a) Chứng minh $f(A \cup B) = f(A) \cup f(B)$.

Giả sử $y \in f(A \cup B)$. Khi đó tồn tại $x \in A \cup B$ sao cho $y = f(x)$, như vậy tồn tại $x \in A$ hoặc $x \in B$ sao cho $y = f(x)$ hay $y = f(x) \in f(A)$ hoặc $y = f(x) \in f(B)$ tức là $y \in f(A) \cup f(B)$.

Đảo lại, giả sử $y \in f(A) \cup f(B)$ khi đó $y \in f(A)$ hoặc $y \in f(B)$ do đó tồn tại $x \in A$ hoặc $x \in B$ để $y = f(x)$ hay tồn tại $x \in A \cup B$ để $y = f(x)$, vậy $y \in f(A \cup B)$.

Tóm lại ta có đẳng thức $f(A \cup B) = f(A) \cup f(B)$.

b) $f(A \cap B) \subset f(A) \cap f(B)$ (1)

Giả sử $y \in f(A \cap B)$ khi đó tồn tại $x \in A \cap B$ sao cho $y = f(x)$. Như vậy tồn tại $x \in A$ và $x \in B$ sao cho $y = f(x)$. Từ đó suy ra $y \in f(A)$ và $y \in f(B)$ tức là $y \in f(A) \cap f(B)$. Vậy có bao hàm thức (1). Không có bao hàm thức ngược lại với mọi f.

Chẳng hạn $f : \mathbb{Z} \to \mathbb{Z}$

$$n \mapsto f(n) = |n|$$

A là tập hợp các số nguyên dương ;

B là tập hợp các số nguyên âm :

$A \cap B = \varnothing$ nên $f(A \cap B) = \varnothing$.

$f(A) = \mathbb{N}^*$

$f(B) = \mathbb{N}^*$ vậy $f(A) \cap f(B) = \mathbb{N}^* \neq \varnothing$.

Ta có thể chứng minh được rằng bao hàm thức ngược lại của (1) xảy ra nếu f là một đơn ánh.

Các bao hàm thức và đẳng thức còn lại chứng minh tương tự.

1.46. Ta lần lượt xét các trường hợp:

Nếu $n = 0$ thì f là ánh xạ đồng nhất, do đó f là một song ánh.

Nếu $n = 1$ thì ta có $f(0) = 1$

$$f(1) = 2$$

$$\dots$$

$$f(k) = k + 1$$

Trường hợp này f là một đơn ánh nhưng không toàn ánh vì 0 không có tạo ảnh. Nếu $n > 1$ thì f là một đơn ánh nhưng cũng không là toàn ánh vì trong trường hợp này $n + 1$ không có tạo ảnh. Thật vậy, rõ ràng $n + 1 > n$ nên nó không thể là ảnh của những số $k < n$. ($f(k) = n - k$). Nhưng nếu có số $k \geq n$ mà $f(k) = n + 1$ thì ta phải có đẳng thức $n + k = n + 1$ mâu

thuẫn với $k \geq n > 1$. Đương nhiên trong các trường hợp này f không là song ánh. (Bạn đọc có thể chứng minh các số từ $n + 1$ đến $2n - 1$ không có tạo ánh).

1.47. a) Giả sử $h = gf$ là một đơn ánh, và giả sử $x_1, x_2 \in X$ sao cho $f(x_1) = f(x_2)$ khi đó ta có $g(f(x_1)) = g(f(x_2))$ hay $fg(x_1) = gf(x_2)$, suy ra $x_1 = x_2$, vậy f là một đơn ánh. Nếu f là một toàn ánh và giả sử y_1 và y_2 thuộc Y sao cho $g(y_1) = g(y_2) \in \mathbb{Z}$. Vì f là toàn ánh nên tồn tại x_1 và x_2 thuộc X sao cho $f(x_1) = y_1$ và $f(x_2) = y_2$. Từ đó suy ra

$$h(x_1) = gf(x_1) = g(f(x_1)) = g(y_1) = g(y_2) = g(f(x_2)) = gf(x_2) = h(x_2).$$

Vì h là đơn ánh nên $x_1 = x_2$.

Vậy $y_1 = f(x_1) = f(x_2) = y_2$. Ta có g là đơn ánh.

b) Giả sử $h = gf$ là một toàn ánh. $z \in \mathbb{Z}$ là một phần tử bất kì.

Vì h là toàn ánh nên tồn tại $x \in X$ sao cho $h(x) = z$. Khi đó ta có $y = f(x) \in Y$ thoả mãn $g(y) = g(f(x)) = gf(x) = h(x) = z$. Vậy g là một toàn ánh. Nếu giả thiết thêm g là một đơn ánh thì f cũng là một toàn ánh. Thật vậy, giả sử $y \in Y$ là một phần tử tuỳ ý, qua ánh xạ g ta có $g(y) = z \in X$, vì h là toàn ánh nên tồn tại $x \in X$ sao cho $h(x) = z$. Từ đó suy ra $g(y) = g(f(x))$. Vì g là đơn ánh nên $y = f(x)$. Vậy f là một toàn ánh.

1.48. Giả sử $f : X \to Y$ là một đơn ánh, vì $X \neq \varnothing$ nên $\exists x_0 \in X$. Đặt $Y_1 = Y - f(X)$. (Y_1 có thể rỗng). Vì f là đơn ánh nên $\forall y \in f(X)$ tồn tại duy nhất $x_y \in X$ sao cho $f(x_y) = y$. Ta có ánh xạ $g : Y \to X$ được xác định như sau:

$$g(y) = \begin{cases} x_1 & \text{nếu } y \in f(X) \\ x_0 & \text{nếu } y \in Y_1 \end{cases}$$

rõ ràng $\forall x \in X$, $gf(x) = g(f(x)) = x = 1_X(x)$, vậy $gf = 1_X$.

Đảo lại, giả sử $g : Y \to X$ sao cho $gf = 1_X$. Do 1_X là một đơn ánh nên theo bài tập 1.47 suy ra f là đơn ánh.

1.49. Giả sử $f : X \to Y$ là một toàn ánh khi đó với mỗi $y \in Y$, $f^{-1}(y) \neq \emptyset$. Với mỗi tập $f^{-1}(y)$ ta cố định hoá một phần tử x_y $(f(x_y) = y)$. Khi đó ta có một ánh xạ

$$g : Y \to X$$
$$y \mapsto x_y$$

thoả mãn

$$fg(y) = f(x_y) = y = 1_Y(y).$$

Vậy $fg = 1_Y$.

* Bạn đọc chú ý điều này: Thực ra, để có ánh xạ $g : Y \to X$ ta phải sử dụng tiên đề chọn.

Đảo lại, nếu có $g : Y \to X$ sao cho $fg = 1_Y$ thì theo bài tập 1.47, f là một toàn ánh, vì 1_Y là một toàn ánh.

1.50. a) Giả sử f là một đơn ánh và $fg = fg'$ khi đó với mọi $v \in V$, $gf(v) = fg'(v)$ hay $f(g(v)) = f(g'(v))$. Do f là đơn ánh nên $g(v) = g'(v)$. Vậy $g = g'$.

b) Nếu f không là đơn ánh (dĩ nhiên khi đó X có nhiều hơn một phần tử). Giả sử x_1 và x_2 thuộc X, $x_1 \neq x_2$ sao cho $f(x_1) = f(x_2)$. Xét tập hợp $V = \{1, 2\}$ và hai ánh xạ

$$g : V \to X \quad \text{và} \quad g' : V \to X$$
$$1 \mapsto x_1 \qquad\qquad 1 \mapsto x_1$$
$$2 \mapsto x_2 \qquad\qquad 2 \mapsto x_1$$

rõ ràng $g \neq g'$ và $\begin{cases} fg(1) = fg'(1) = f(x_1) \\ fg(2) = fg'(2) = f(x_1). \end{cases}$

Vậy $fg = fg'$. Theo giả thiết ta phải có $g = g'$. Mâu thuẫn này chứng tỏ f phải là một đơn ánh.

1.51. Giả sử f là một toàn ánh và $hf = h'f$.

Giả sử $y \in Y$ là một phần tử tuỳ ý, khi đó vì f là toàn ánh nên tồn tại $x \in X$ sao cho $f(x) = y$, do đó

$$h(y) = h[f(x)] = hf(x) = h'f(x) = h'[f(x)] = h'(y).$$

Vậy $h = h'$.

Đảo lại, giả sử f không là một toàn ánh, tức là tồn tại $y_0 \in Y$ mà $f^{-1}(y_0) = \emptyset$. Đặt $X = \{1, 2\}$ và xét hai ánh xạ

$$h : Y \to Z$$
$$y \mapsto 1$$
$$h' : Y \to Z$$
$$h'(y) = \begin{cases} 1 & \text{nếu } y \neq y_0 \\ 2 & \text{nếu } y = y_0 \end{cases}$$

rõ ràng $h' \neq h$ và $hf = h'f$. Theo giả thiết, $h = h'$. Mâu thuẫn. Vậy f phải là một toàn ánh.

1.52. Giả sử $f : X \to Y$ và $g : X \to Z$ là hai song ánh. Vì f là một song ánh nên tồn tại $f^{-1} : Y \to X$ khi đó f^{-1} cũng là một song ánh và ta có tích $gf^{-1} : Y \to Z$ là một song ánh.

1.53. Đặt $p : G \to X$.
$$(x, y) \mapsto x$$

Giả sử p là một song ánh, nghĩa là $p((x, y)) = p((x', y'))$ khi và chỉ khi $x = x'$ và $y = y'$; và p là một toàn ánh, điều này có

nghĩa với mọi $x \in X$ tồn tại (duy nhất) $(x, y) \in G$ sao cho $p((x, y)) = x$. Vậy theo định nghĩa thì G là đồ thị của ánh xạ $f : X \to Y$, $f(x) = y$ với $(x, y) \in G$.

Bây giờ giả sử G là đồ thị của một ánh xạ từ X đến Y. Như vậy trước hết p phải là một toàn ánh. Nếu (x, y) và $(x', y) \in G$ mà $p((x, y)) = p((x, y'))$, vì $p((x, y)) = x$ và $p((x', y')) = x'$ nên $x = x'$, do đó $y = y'$. Vậy p là một đơn ánh. Vậy p là một song ánh.

1.54. a) Hiển nhiên.

b) Hiển nhiên.

c) Giả sử $x \in B \cap (\bigcup_{i \in I} A_i)$ khi đó $x \in B$ và $x \in \bigcup_{i \in I} A_i$, như vậy $x \in B$ và $x \in A_{i_0}$ với một i_0 nào đó của I, $x \in B \cap A_{i_0}$ do đó $x \in \bigcup_{i \in I} (B \cap A_i)$. Đảo lại, giả sử $x \in \bigcup_{i \in I} (B \cap A_i)$ khi đó $\exists i_0 \in I$ để $x \in B \cap A_{i_0}$ hay $x \in B$ và $x \in A_{i_0}$ do đó $x \in B$ và $x \in \bigcup_{i \in I} A_i$.

Vậy $x \in B \cap (\bigcup_{i \in I} A_i)$

d), e), f) chứng minh tương tự như c).

1.55. Ta hãy chứng minh d).

Giả sử $x \in f^{-1}(\bigcap_{j \in J} B_j)$, như vậy $f(x) \in \bigcap_{j \in J} B_j$ suy ra $f(x) \in B_j$ với mọi $j \in J$ nên $x \in f^{-1}(B_j)$ với mọi $j \in J$ hay $x \in \bigcap_{j \in J} f^{-1}(B_j)$.

Ngược lại, nếu $x \in \bigcap_{j \in J} f^{-1}(B_j)$ thì $x \in f^{-1}(B_j)$ với mọi $j \in J$ hay $f(x) \in B_j$ với mọi $j \in J$, do đó $f(x) \in \bigcap_{j \in J} (B_j)$.

Vậy $x \in f^{-1}(\bigcap_{j\in J} B_j)$

1.56. a) Xét anh xạ ϕ : Hom $(X, Y) \to Y^X$

$$f \mapsto (f(x))_{x\in X}$$

Ta có ϕ là một song ánh. Thật vậy, giả sử f, g $\in$ Hom(X, Y) mà $\phi(f) = \phi(g)$, thì $(f(x))_{x\in X} = (g(x))_{x\in X}$, do vậy $f(x) = g(x)$ với mọi $x \in X$ hay f = g, tức là ϕ là một đơn ánh. Giả sử $(y_x)_{x\in X}$ là một phần tử bất kì của Y^X khi đó có ánh xạ

$$f : X \to Y$$
$$x \mapsto y_x$$

thoã mãn $\phi(f) = (y_x)_{x\in X}$. Vậy ϕ là một toàn ánh.

b) Đặt Y = {0, 1}, với mỗi $A \subset X$ ta xét ánh xạ sau

$$\chi_A : X \to Y,\ \chi_A(x) = \begin{cases} 1 & \text{nếu } x \in A \\ 0 & \text{nếu } x \in X - A \end{cases}$$

Khi đó có một song ánh từ $\mathscr{P}(X)$ đến Hom(X, Y) cho bởi:

$$\chi : \mathscr{P}(X) \to \text{Hom}(X, Y)$$
$$A \mapsto \chi_A$$

c) Vì Y có hai phần tử và X có n phần tử nên Y^X có số phần tử bằng 2^n, do đó theo a) Hom(X, Y) có 2^n phần tử; theo b) $\mathscr{P}(X)$ có 2^n phần tử.

1.57. a) Xét quan hệ $R \subset X^2$ cho bởi $(x, x') \in R$ khi và chỉ khi $f(x) = f(x')$, hay $x\ R\ x' \Leftrightarrow f(x) = f(x')$.

Vì $f(x) = f(x)$ nên xRx với mọi $x \in X$.

Giả sử xRx' nghĩa là $f(x) = f(x')$ hay $f(x') = f(x)$ như vậy có x'Rx.

Nếu xRx' và x'Rx" nghĩa là f(x) = f(x') và f(x') = f(x") thì f(x) = f(x"), do đó xRx". Vậy R là một quan hệ tương đương

b) $\bar{f}$ được cho bởi quy tắc sau $\bar{f}(C(x)) = f(x)$.

Quy tắc này không phụ thuộc vào đại diện x của lớp C(x). Thật vậy, giả sử C(x) = C(x') tức là xRx' hay f(x) = f(x') thì

$\bar{f}(C(x)) = f(x) = f(x') = \bar{f}(C(x'))$.

Với mọi $x \in X$ có $\bar{f}(p(x)) = \bar{f}(C(x)) = f(x)$, vậy $f = \bar{f}p$.

c) $\bar{f}$ là một đơn ánh vì nếu $\bar{f}(C(x)) = \bar{f}(C(x'))$ tức là f(x) = f(x') hay C(x) = C(x'). Bây giờ giả sử f là toàn ánh, như vậy với mọi $y \in Y$ tồn tại $x \in X$ sao cho f(x) = y. Đồng thời ta cũng có $C(x) \in X/R$ sao cho $\bar{f}(C(x)) = f(x) = y$. Vậy $\bar{f}$ là một toàn ánh, và do đó nó là một song ánh.

1.58. a) S là một quan hệ tương đương vì:

Với mọi $(a, b) \in X$ có ab = ba nên (a, b) S (a, b).

Giả sử (a, b) S (c, d) khi đó ad = bc hay cb = da. Đẳng thức cuối cùng chứng tỏ (c, d) S (a, b). Bây giờ giả sử (a, b) S (c, d) và (c, d) S (e, f). Khi đó có các đẳng thức ad = bc và cf = de. Từ đó suy ra adf = bcf và bcf = bde hay adf = bde giản ước cho d ta được af = eb. Vậy (a, b) S (e, f).

b) Ánh xạ $\varphi : \mathbb{Q} \to \mathbb{Z} \times \mathbb{N}^* / R$

$$\frac{p}{q} \mapsto \overline{(p,q)}$$

với $\overline{(p,q)}$ là lớp tương đương của (p, q) theo quan hệ S, là một song ánh từ $\mathbb{Q}$ đến $(\mathbb{Z} \times \mathbb{N}^*)/R$.

1.59. a) $S = \{(x, y) \in \mathbb{Z}^2 \mid x + y \text{ lẻ}\}$

không phải là đồ thị của một ánh xạ từ $\mathbb{Z}$ đến $\mathbb{Z}$ vì ta có

$$(x, x + 1) \in S \text{ và } (x, x + 3) \in S.$$

b) S không có tính chất phản xạ vì $x + x = 2x$ chẵn cho nên $(x, x) \notin S$. Do đó S không phải là một quan hệ thứ tự và cũng không phải là quan hệ tương đương.

1.60. Nếu $S = \{(x, y) \in \mathbb{Z}^2 \mid x + y \text{ chẵn}\}$ thì S cũng không phải là đồ thị của một ánh xạ từ $\mathbb{Z}$ đến $\mathbb{Z}$ vì $(x, x) \in S$ và $(x, 3x) \in S$, với x là một số nguyên bất kì.

S không phải là một quan hệ thứ tự vì ta có $(x, 3x) \in S$ và $(3x, x) \in S$ nhưng với $x \neq 0$ ta có $x \neq 3x$.

S là một quan hệ tương đương vì với mọi $x \in \mathbb{Z}$, $2x$ chẵn do đó $(x, x) \in S$. Nếu $(x, y) \in S$ tức là $x + y$ chẵn thì $y + x (= x + y)$ chẵn hay $(y, x) \in S$.

Cuối cùng nếu $(x, y) \in S$ và $(y, z) \in S$ thì $x + y$ chẵn và $y + z$ chẵn từ đó suy ra $x + z$ chẵn, vậy $(x, z) \in S$.

1.61. a) Để chứng minh S tương đương ta chỉ cần chứng minh S có tính chất đối xứng và bắc cầu. Theo cách xây dựng S, rõ ràng nếu x S y nghĩa là có $x_1 = x, x_2, \ldots, x_n = y$ sao cho $x_1 \, T \, x_2$, $x_2 \, T \, x_3, \ldots, x_{n-1} \, T \, x_n$ thì vì T là đối xứng nên ta cũng có $x_n \, T \, x_{n-1}, \ldots, x_3 \, T \, x_2, x_2 \, T \, x_1$. Vậy y S x, nghĩa là S có tính chất đối xứng. Bây giờ, giả sử x S y và y S z, khi đó tồn tại $x_1 = x, x_2, \ldots, x_n = y$ và $y_1 = y, y_2, \ldots, y_m = z$ sao cho $x_1 \, T \, x_2, \ldots x_{n-1} \, T \, x_n$ và $y_1 \, T \, y_2, \ldots y_{m-1} \, T \, y_m$. Kết hợp lại ta

có $x_1 = x, x_2, \ldots, x_n, y_1, y_2 \ldots y_m = z$ thoả mãn $x_1 T x_2, \ldots x_{n-1} T x_n, x_n T y_1, \ldots, y_{m-1} T y_m$. Vậy x S z hay S có tính chất bắc cầu. Hiển nhiên ta có $T \subset S$ theo cách xây dựng S.

b) Giả sử $H \subset X^2$ là một quan hệ tương đương sao cho $T \subset H$. Ta sẽ chứng minh $S \subset H$. Thật vậy giả sử $(x, y) \in S$ hay x S y nghĩa là tồn tại $x_1 = x, x_2 \ldots x_n = y$ sao cho $(x_1 T x_2, x_2 T x_3, \ldots, x_{n-1} T x_n)$. Vì $T \subset H$ nên cũng có $x_1 H x_2, x_2 H x_3, \ldots, x_{n-1} H x_n$. Do tính chất bắc cầu của H suy ra $x_1 H x_n$, hay x H y. vậy $(x, y) \in H$, hay $S \subset H$.

1.62. S là một quan hệ tương đương trong X.

1.63. a) S không phải là một quan hệ tương đương trong X vì nếu ta lấy P = O thì với hai điểm P_1 và P_2 bất kì của X ta luôn có O, P_1, O thẳng hàng và O, O, P_2 thẳng hàng tức là có $P_1 S O$ và $O S P_2$, trong khi đó chưa chắc O, P_1, P_2 thẳng hàng hay chưa chắc có $P_1 S P_2$ (có thể chọn P_1, P_2 sao cho $P_1O \perp P_2O$).

b) S là một quan hệ tương đương trong $X' = X - \{O\}$ vì mọi $P \in X'$ ta luôn có O, P, P thẳng hàng hay P S P.

Nếu P S P' nghĩa là O, P, P' thẳng hàng, suy ra ngay P' S P.

Bây giờ giả sử P S P' và P' S P'' nghĩa là O, P, P' thẳng hàng và O, P', P'' thẳng hàng. Vì P, P', P'' khác O nên suy ra P và P'' cùng nằm trên đường thẳng OP'. Vậy P S P''.

Kí hiệu X'/S là tập hợp các lớp tương đương của X' theo quan hệ S ta có mỗi lớp của X'/S là tập hợp các đường thẳng đi qua gốc toạ độ O trừ điểm O.

1.64. a) Hiển nhiên với mọi $x \in X$, $x\ S^{-1}\ x$ vì $x\ S\ x$. Giả sử $x\ S^{-1}\ y$ và $y\ S^{-1}\ x$ khi đó ta có $y\ S\ x$ và $x\ S\ y$, do tính chất phản xứng của S nên suy ra $x = y$. Bây giờ giả sử $x\ S^{-1}\ y$ và $y \in S^{-1}\ z$ có nghĩa $z\ S\ y$ và $y\ S\ x$, do tính chất bắc cầu của S suy ra $z\ S\ x$ vậy $x\ S^{-1}\ z$.

b) Dựa vào kết quả câu a) ta chỉ cần chứng minh nếu S có tính chất đối xứng thì S^{-1} cũng có tính chất đối xứng. Thật vậy giả sử $x\ S^{-1}\ y$ như vậy có $y\ S\ x$ vì S đối xứng nên $x\ S\ y$ do đó $y\ S^{-1}\ x$.

1.65. Vì $S \neq \{(x, x) \mid x \in X\}$ nên $\exists (x, y) \in S, x \neq y$. (*)

Do tính chất đối xứng của S nên $(y, x) \in S$. Nếu S là một quan hệ thứ tự thì ta phải có $x = y$. Điều này trái với (*).

1.66. Hiển nhiên S có tính chất phản xạ.

Giả sử $(a_1, a_2, \ldots, a_n)\ S\ (b_1, b_2, \ldots, b_n)$ (1)

và $(b_1, b_2, \ldots, b_n)\ S\ (a_1, a_2, \ldots, a_n)$. (2)

Nếu $(a_1, a_2, \ldots, a_n) \neq (b_1, b_2, \ldots, b_n)$, theo (1) có một $i\ (i = 1, \ldots, n)$ sao cho $a_1 = b_1, a_2 = b_2, \ldots, a_{i-1} = b_{i-1}, a_i < b_i$, theo (2) có một $j\ (j = 1, \ldots, n)$ sao cho $b_1 = a_1, a_2 = b_2, \ldots, b_{j-1} = a_{j-1}, b_j < a_j$. Nhưng hai điều đó không đồng thời xảy ra được. Vậy $(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$, S có tính chất phản đối xứng.

Giả sử $(a_1, a_2, \ldots, a_n)\ S\ (b_1, b_2, \ldots, b_n)$ và

$$(b_1, b_2, \ldots, b_n)\ S\ (c_1, c_2, \ldots c_n).$$

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

$(b_1, b_2, \ldots, b_n) = (c_1, c_2, \ldots, c_n)$ thì suy ra ngay

$(a_1, a_2, \ldots, a_n)\ S\ (c_1, c_2, \ldots, c_n)$.

Bây giờ giả sử $(a_1, a_2, \ldots, a_n)\ S\ (b_1, b_2, \ldots, b_n)$ và

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

$(b_1, b_2, \ldots, b_n)\ S\ (c_1, c_2, \ldots, c_n)$ và

$(b_1, b_2, \ldots, b_n) \neq (c_1, c_2, \ldots, c_n)$.

Khi đó tồn tại các chỉ số i và j sao cho:

$$a_1 = b_1, \ldots, a_{i-1} = b_{i-1}, a_i < b_i;$$

$$b_1 = c_1, \ldots, b_{j-1} = c_{j-1}, b_j < c_j.$$

nếu $i \leq j$ thì $a_1 = b_1 = c_1, \ldots, a_{i-1} = b_{i-1} = c_{i-1}, a_i < b_i \leq c_i$.

Vậy $(a_1, a_2, \ldots, a_n)\ S\ (c_1, c_2, \ldots, c_n)$.

Nếu $i > j$ thì $a_1 = b_1 = c_1, \ldots, a_{j-1} = b_{j-1} = c_{j-1}, a_j = b_j < c_j$.

Vậy $(a_1, a_2, \ldots, a_n)\ S\ (c_1, c_2, \ldots, c_n)$.

Tóm lại trong cả hai trường hợp ta đều có

$$(a_1, a_2, \ldots, a_n)\ S\ (c_1, c_2, \ldots, c_n),$$

do vậy S có tính chất bắc cầu.

1.67. Để chứng minh S là quan hệ thứ tự toàn phần, ta dựa vào tập $\mathbb{N}$ với quan hệ $\leq$ là tập sắp thứ tự toàn phần.

1.68. a) Theo cách xác định quan hệ S ta thấy ngay S có tính chất phản xạ

Giả sử f S g và g S f như vậy f là mở rộng của g và g là mở rộng của f nên f = g.

Giả sử f S g và g S h. Chẳng hạn có

$$f : X_1 \to Y, g : X_2 \to Y, X_1 \subset X_2 \text{ và } g\big|_{X_1} = f$$

$h: X_3 \to Y, X_2 \subset X_3$ và $h\Big|_{X_2} = g$.

Khi đó ta cũng có $h\Big|_{X_1} = f$ vì với mọi x thuộc X_1,

$$h(x) = g(x) = f(x).$$

Vậy S có tính chất phản đối xứng và bắc cầu. Do đó S là một quan hệ thứ tự.

b) Ta giả sử $X \neq \emptyset$. Nếu Y có một phần tử y thì $\emptyset(X, Y)$ có phần tử lớn nhất là ánh xạ $f: X \to Y = \{y\}$

$$\forall x \in X, y = f(x)$$

và phần tử bé nhất là ánh xạ ϕ.

Nếu Y có nhiều hơn một phần tử thì mỗi ánh xạ $f: X \to Y$ đều là phần tử tối đại và mỗi ánh xạ từ tập $\{x\}$ đến Y đều là phần tử tối tiểu, x là một phần tử tuỳ ý của X, nếu ta loại trừ ánh xạ rỗng trong tập $\emptyset(X, Y)$.

1.69. Giả sử $a \in X$ là phần tử bé nhất của tập sắp thứ tự X, nghĩa là $a \leq x$ với mọi $x \in X$. Giả sử rằng $y \leq a$ (1)

với $y \in X$, ta cũng có $a \leq y$. (2)

từ (1) và (2) suy ra $y = a$. Vậy a là phần tử tối tiểu. Nếu a_1 và a_2 là hai phần tử bé nhất của X thì ta có các quan hệ $a_1 \leq a_2$ và $a_2 \leq a_1$ suy ra $a_1 = a_2$.

1.70. Giả xử X là tập sắp thứ tự tốt. Với hai phần tử bất kì x và y thuộc X; $\{x, y\}$ có phần tử bé nhất, như vậy hoặc x là phần tử bé nhất thì $x \leq y$, hoặc y là phần tử bé nhất thì $y \leq x$. Tức là cặp x, y là so sánh được.

Vậy X là tập sắp thứ tự toàn phần.

1.71. Dựa vào tính chất sắp thứ tự tốt của tập $\mathbb{N}$ để chứng minh.

CHƯƠNG II. NỬA NHÓM VÀ NHÓM

2.1. X là nửa nhóm vì với mọi $x, y, z \in X$

$$x(yz) = xy = x;$$

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

Vậy $x(yz) = (xy)x$.

Nếu X có nhiều hơn một phần tử thì X không giao hoán và cũng không có đơn vị.

2.2. Giả sử trong nửa nhóm X ta có $ab = ba$. Trước hết ta chứng minh với mọi số tự nhiên $n \geq 1$, $ab^n = b^n a$. Chứng minh quy nạp theo n. Thật vậy, với $n = 1$ theo giả thiết ta có $ab = ba$.

Giả sử $m = n - 1$, $ab^m = b^m a$ hay $ab^{n-1} = b^{n-1}a$.

Khi đó $ab^n = a(b^{n-1}b) = (ab^{n-1})b = (b^{n-1}a)b$

$$= b^{n-1}(ab) = b^{n-1}(ba) = (b^{n-1}b)a = b^n a.$$

Bây giờ ta chứng minh $(ab)^n = a^n b^n$ quy nạp theo n. Thật vậy, với $n = 1$ ta có $ab = ba$.

Giả sử với $m = n - 1$ ta có $(ab)^m = a^m b^m$ hay

$$(ab)^{n-1} = a^{n-1}b^{n-1}.$$

Khi đó $(ab)^n = (ab)^{n-1}(ab) = (a^{n-1}b^{n-1})(ab) = a^{n-1}(b^{n-1}a)b$

$$= a^{n-1}(ab^{n-1})b = (a^{n-1}.a)(b^{n-1}.b) = a^n b^n.$$

Nếu $(ab)^2 = a^2b^2$ chưa thể suy ra $ab = ba$.

Chẳng hạn, ta xét nửa nhóm sau: Cho X là một tập tuỳ ý có nhiều hơn một phần tử với phép toán $xy = x$ với mọi x và y thuộc X.

Nếu $a, b \in X$ sao cho $a \neq b$ ta có $a^2 = a$, $b^2 = b$, $ab = a$, $a^2b^2 = a$ nên $(ab)^2 = a^2b^2 = a$, nhưng $ab = a \neq ba = b$.

Tuy nhiên, nếu x là một nhóm thì từ $(ab)^2 = a^2b^2$ ta suy ra được ab = ba. Từ đẳng thức $(ab)^2 = a^2b^2$, nhân cả hai vế với a^{-1} về bên trái và b^{-1} về bên phải thì ta có ba = ab.

2.3. a) Ta chứng minh tương ứng $(\bar{a}, \bar{b}) \mapsto \overline{a+b}$ không phụ thuộc vào các đại diện a và b của các lớp $\bar{a}$, $\bar{b}$. Thật vậy, giả sử $\bar{a} = \overline{a'}$ nghĩa là a − a' chia hết cho n và $\bar{b} = \overline{b'}$ nghĩa là b − b' chia hết cho n khi đó ta cũng có (a + b) − (a' + b') chia hết cho n vậy $\overline{a+b} = \overline{a'+b'}$.

Vậy tương ứng trên là một ánh xạ từ X^2 đến X.

b) Ta kí hiệu phép toán hai ngôi trên là + , ta có $\bar{a} + \bar{b} = \overline{a+b}$. Với phép toán này X là một vị nhóm.

Thật vậy

$$(\bar{a}+\bar{b})+\bar{c} = \overline{a+b}+\bar{c} = \overline{(a+b)+c} =$$

$$= \overline{a+(b+c)} = \bar{a} + \overline{b+c} = \bar{a}+(\bar{b}+\bar{c}),$$

có $\bar{0} \in X$ sao cho $\bar{0}+\bar{a} = \overline{0+a} = \bar{a}$ với mọi $\bar{a}, \bar{b}, \bar{c} \in X$.

c) Giả sử $\bar{a} = \overline{a'}$ và $\bar{b} = \overline{b'}$ nghĩa là a − a' và b − b'; chia hết cho n. Khi đó (a − a')b' + (b − b')a chia hết cho n.

Từ đó suy ra ab − ab' + ab' − a'b' = ab − a'b' chia hết cho n.

Vậy $\bar{a}.\bar{b} = \overline{ab}$ ta cũng có X là một vị nhóm với phép toán này. Thật vậy, với mọi $\bar{a}, \bar{b}, \bar{c} \in X$ ta có

$\bar{a}(\bar{b}\,\bar{c}) = \bar{a}(\overline{bc}) = \overline{a(bc)} = \overline{(ab)c} = \overline{ab}.\bar{c} = (\bar{a}\,\bar{b})\bar{c}$ và

$$\overline{1}.\overline{a} = \overline{1a} = \overline{a}.$$

Ngoài ra ta có $\overline{a}\ \overline{b} = \overline{ab} = \overline{ba} = \overline{b}\ \overline{a}$.

2.4. a) Ta chứng minh tương ứng $(\frac{a}{b},\frac{c}{d}) \mapsto \frac{ad+bc}{bd}$ là một ánh xạ từ X^2 đến X. Thật vậy, nếu $\frac{a}{b} = \frac{a'}{b'}$ và $\frac{c}{d} = \frac{c'}{d'}$ thì ab' = ba' và cd' = dc' suy ra ab'dd' = ba'dd' (1)

$$cd'bb' = dc'bb'. \quad (2)$$

Cộng từ vế của (1) và (2) ta được

$$adb'd' + bcb'd' = bda'd' + bdc'b',$$

do đó $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$.

b) Đặt $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, ta có

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = \frac{cb+da}{db} = \frac{c}{d} + \frac{a}{b}$$

$$(\frac{a}{b} + \frac{c}{d}) + \frac{e}{g} = \frac{ad+bc}{bd} + \frac{e}{g} =$$

$$= \frac{(ad)g+(bc)g+(bd)e}{(bd)g} = \frac{a(dg)+b(cg)+b(de)}{b(dg)}$$

$$= \frac{a(dg)+b(cg+de)}{b(dg)} = \frac{a}{b} + \frac{cg+de}{dg} = \frac{a}{b} + (\frac{c}{d} + \frac{e}{g})$$

và ta có $\frac{0}{1} \in X$ thoả mãn $\frac{0}{1} + \frac{a}{b} = \frac{0b+a}{1.b} = \frac{a}{b}$.

Vậy với phép toán "cộng" này X là một vị nhóm giao hoán.

c) Đặt $\frac{a}{b}.\frac{c}{d}=\frac{ac}{bd}$. Khi đó với $\frac{a}{b}=\frac{a'}{b'}$ và $\frac{c}{d}=\frac{c'}{d'}$

thì ab' = ba' và cd' = dc'

suy ra acb'd' = bda'c' hay $\frac{ac}{bd}=\frac{a'c'}{b'd'}$.

Vậy $\frac{a}{b}.\frac{c}{d}=\frac{a'}{b'}.\frac{c'}{d'}$.

Ta cũng có $\frac{a}{b}.\frac{c}{d}=\frac{ac}{bd}=\frac{ca}{db}=\frac{c}{a}.\frac{d}{b}$;

$$\frac{a}{b}(\frac{c}{d}.\frac{e}{g})=\frac{a}{b}.\frac{ce}{dg}=\frac{a(ce)}{b(dg)}=\frac{(ac)e}{(bd)g}=\frac{ac}{bd}.\frac{e}{g}=(\frac{a}{b}.\frac{c}{d})\frac{e}{g}$$

$\frac{b}{b} \in X$ ($b \in \mathbb{N}^*$) thoả mãn $\frac{b}{b}.\frac{c}{d}=\frac{bc}{bd}=\frac{c}{d}$.

2.5. a) Với mọi $\alpha = (a_1, a_2, ..., a_n)$, $\beta = (b_1 + b_2, ..., b_n)$ và $\gamma = (c_1, c_2, ..., c_n)$ thuộc $\mathbb{N}^n$ ta có

$$\begin{aligned}(\alpha+\beta)+\gamma &= [(a_1, a_2, ..., a_n) + (b_1 + b_2, ..., b_n)] + (c_1 + c_2, ..., c_n)\\ &= ((a_1 + b_1, a_2 + b_2, ..., a_n + b_n) + (c_1 + c_2, ..., c_n))\\ &= ((a_1 + b_1) + c_1, (a_1 + b_2) + c_2, ..., (a_n + b_n) + c_n)\\ &= (a_1 + (b_1 + c_1) + a_2 + (b_2 + c_2), ..., a_n + (b_n + c_n))\\ &= (a_1, a_2, ..., a_n) + (b_1 + c_1, b_2 + c_2, ..., b_n + c_n)\\ &= (a_1, a_2, ..., a_n) + [(b_1 + b_2, ..., b_n) + (c_1 + c_2, ..., c_n)]\\ &= \alpha + (\beta + \gamma).\end{aligned}$$

$$\begin{aligned}\alpha+\beta &= (a_1, a_2, ..., a_n) + (b_1 + b_2, ..., b_n)\\ &= (a_1 + b_1, a_2 + b_2, ..., a_n + b_n)\end{aligned}$$

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

$= (b_1 + b_2, \ldots b_n) + (a_1, a_2, \ldots a_n) = \beta + \alpha$.

Dãy $0 = (0, 0, \ldots, 0) \in \mathbb{N}^n$ thoả mãn

$0 + \alpha = (0, 0, \ldots 0) + (a_1, a_2, \ldots, a_n) = (a_1, a_2, \ldots a_n) = \alpha$.

Vậy $(\mathbb{N}^n, +)$ là một vị nhóm giao hoán.

b) Giả sử $\alpha = (a_1, a_2, \ldots, a_n)$ và $\beta = (b_1 + b_2, \ldots, b_n)$ sao cho $\alpha < \beta$ và $\gamma = (c_1 + c_2, \ldots, c_n)$. Khi đó hoặc $\alpha = \beta$, như vậy $\alpha + \gamma = \beta + \gamma$; hoặc $\alpha \neq \beta$ thì tồn tại i (i = 1, ..., n) sao cho $a_1 = b_1, a_2 = b_2, \ldots a_{i-1} = b_{i-1}, a_i < b_i$. Khi đó $a_1 + c_1 = b_1 + c_1$, $a_2 + c_2 = b_2 + c_2, \ldots, a_{i-1} + c_{i-1} = b_{i-1} + c_{i-1}$ và $a_i + c_i < b_i + c_i$. Vậy $\alpha + \gamma = \beta + \gamma$.

2.6. Đối với tập hợp X = {a, b} gồm hai phần tử có một bảng toán duy nhất sau khi đã chọn phần tử nào của X là phần tử đơn vị để nó lập thành một nhóm

*	a	b
a	a	b
b	b	a

Đối với tập hợp X = {a, b, c} gồm ba phần tử, có một bảng toán duy nhất sau khi đã chọn phần tử đơn vị, để nó thành lập một nhóm

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

2.7. Đây là 21 ví dụ quen thuộc về nhóm và nhóm con.

2.8. Do $X \neq \emptyset$ nên có một phần tử $a \in X$.

Theo giả thiết ta có $aX = Xa = X$ nên suy ra $a \in Xa$, nghĩa là có phần tử $e \in X$ sao cho $a = ea$, ta hãy chứng minh với mọi $x \in X$, $ex = x$. Thật vậy do $aX = X$ nên có $x_0 \in X$ sao cho $x = ax_0$, suy ra $ex = e(ax) = ax_0 = x$. Giả sử $x \in X$ là một phần tử tuỳ ý, do $e \in Xa$ nên có một $x' \in X$ sao cho $e = x'x$. Vậy ta có X là một nhóm (theo một điều kiện tương đương với định nghĩa nhóm).

Đảo lại, nếu X là một nhóm thì hiển nhiên ta có $aX = Xa = X$ với mọi $a \in X$.

2.9. Hom(X, X) là một vị nhóm vì phép nhân ánh xạ có tính chất kết hợp và ánh xạ đồng nhất của X đóng vai trò phần tử đơn vị. Song nếu X có nhiều hơn một phần tử thì Hom(X, X) không là một nhóm vì các ánh xạ không phải là song ánh không có nghịch đảo.

Tích của hai song ánh từ X đến X là một song ánh từ X đến X, và phép nhân ánh xạ có tính chất kết hợp nên S(X) là một nửa nhóm với phép nhân ánh xạ. Ánh xạ đồng nhất 1_X của X là một song ánh nên $1_X \in S(X)$ và cuối cùng nếu $f \in S(X)$ tức là f là một song ánh thì f có ánh xạ ngược $f^{-1} \in S(X)$ và $ff^{-1} = f^{-1}f = 1_X$. Vậy S(X) là một nhóm với phép nhân ánh xạ.

Giả sử $X = \{x_1, x_2, ..., x_n\}$ có n phần tử. Với mỗi hoán vị $(x_{i_1}, x_{i_2}, ..., x_{i_n})$ của X ta có một song ánh $f : X \to X$ xác định bởi $f(x_j) = x_{i_j}$, $j = 1, ..., n$.

Đảo lại, với mỗi song ánh $f: X \to X$, $(f(x_1), f(x_2), ..., f(x_n))$ cho ta một hoán vị của X.

Vậy số phần tử của S(X) bằng số hoán vị của n phần tử, số đó bằng n! hay cấp S(X) bằng n!.

2.10. Ta có $a^2 = e$ với mọi $a \in X$. Vậy $a = a^{-1}$. Với a và b tuỳ ý thuộc X, ta có $(ab)^2 = ab.\ ab = e$, từ đó $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$.

2.11. Đặt $X = \prod x_i = \{(x_i)_{i\in I} \mid x_i \in X_i,\ i \in I\}$.

Giả sử $\alpha = (x_i)_{i\in I}$, $\beta = (y_i)_{i\in I}$, $\gamma = (z_i)_{i\in I}$ ta có

$$(\alpha,\beta)\gamma = [(x_i)_{i\in I}(y_i)_{i\in I}](z_i)_{i\in I}$$
$$= (x_iy_i)_{i\in I}(z_i)_{i\in I} = ((x_iy_i)z_i)_{i\in I}$$
$$= (x_i(y_iz_i)_{i\in I} = (x_i)_{i\in I}(y_iz_i)_{i\in I}$$
$$= (x_i)_{i\in I}[(y_i)_{i\in I}(z_i)_{i\in I}] = \alpha(\beta\gamma).$$

Phép nhân là kết hợp. Gọi e_i là đơn vị của nhóm X_i với mọi $i \in I$ ta có $e = (e_i)_{i\in I}$ thoả mãn

$$e\alpha = (e_i)_{i\in I}(x_i)_{i\in I} = (e_ix_i)_{i\in I} = (x_i)_{i\in I} = \alpha.$$

Giả sử $\alpha = (x_i)_{i\in I} \in X$ khi đó ta có $\alpha' = (x_i^{-1})_{i\in I}$ với x_i^{-1} là nghịch đảo của x_i trong X_i thỏa mãn

$$\alpha'\alpha = (x_i^{-1})_{i\in I}(x_i)_{i\in I} = (x_i^{-1}x_i)_{i\in I} = (e_i)_{i\in I} = e.$$

Vậy X là một nhóm.

2.12. a) p_i là toàn cấu với mọi $(x_j)_{j\in I}$ và $(y_j)_{j\in I}$ thuộc X ta có

$$p_i[(x_j)_{j\in I}(y_j)_{j\in I}] = x_iy_i = p_i[(x_j)_{j\in I}]\ p_i[(y_j)_{j\in I}]$$

và với mọi $x_i \in X$ ta có $(x_j)_{j\in I} \in X$ với $x_j = \begin{cases} x_i & \text{nếu } j = i \\ 0 & \text{nếu } i \neq j \end{cases}$

thoả mãn $p_i[(x_j)_{j\in I}] = x_i$.

b) Ánh xạ $\bar{f} : Y \to X$ được xác định như sau:

với mọi $y \in Y$, $\bar{f}(y) = (f_i(y))_{i\in I}$.

$\bar{f}$ là một đồng cấu vì với mọi y_1 và y_2 thuộc Y ta có :

$\bar{f}(y_1y_2) = (f_i(y_1y_2))_{i\in I} = (f_i(y_1)f_i(y_2))_{i\in I}$

$= (f_i(y_1))_{i\in I}(f_i(y_2))_{i\in I}$

$= \bar{f}(y_1)\bar{f}(y_2)$.

Mặt khác với mọi $y \in Y$ ta có

$(p_i\bar{f})(y) = p_i(\bar{f}(y)) = p_i((f_i(y))_{i\in I}) = f_i(y)$.

Vậy $f_i\bar{f} = f_i$ với mọi $i \in I$.

2.13. Giả sử m và n là hai số nguyên tố cùng nhau.

Khi đó $(\bar{1}, \bar{1}) \in \mathbb{Z}_m \times \mathbb{Z}_n$ có cấp là m.n. Thật vậy.

$$mn(\bar{1}, \bar{1}) = (mn\bar{1}, mn\bar{1})$$
$$= (n(m\bar{1}), m(n\bar{1}))$$
$$= (\bar{0}, \bar{0}).$$

Giả sử $k(\bar{1}, \bar{1}) = (\bar{0}, \bar{0})$ khi đó

$$(k.\bar{1}, k.\bar{1}) = (\bar{0}, \bar{0}) \text{ hay } \begin{cases} k.\bar{1} = (1 + m\mathbb{Z}) = m\mathbb{Z} \\ k.\bar{1} = (1 + n\mathbb{Z}) = n\mathbb{Z} \end{cases}$$

Suy ra k chia hết cho m và k chia hết cho n. Vì (m, n) = 1 nên k chia hết cho mn.

Vậy $\mathbb{Z}_m \times \mathbb{Z}_n$ là nhóm xyclic sinh bởi $(\bar{1}, \bar{1})$.

Đảo lại, giả sử $\mathbb{Z}_m \times \mathbb{Z}_n$ là một nhóm xyclic.

Khi đó tồn tại $\bar{a}.\bar{b}$ thuộc $\mathbb{Z}_m \times \mathbb{Z}_n$ có cấp là mn. Mặt khác nếu [m, n] là bội chung nhỏ nhất của m và n thì

$$[m, n](\bar{a}, \bar{b}) = ([m, n]\bar{a}, [m, n]\bar{b}) = (\bar{0}, \bar{0}).$$

Từ đó suy ra [m, n] chia hết cho mn.

Vậy m, n nguyên tố cùng nhau.

2.14. Áp dụng bài 2.8 ta chỉ cần chứng minh

$$aX = X \text{ và } Xa = X \text{ với mọi } a \in X.$$

Giả sử $X = \{x_1, x_2, ..., x_n\}$ gồm n phần tử. Với mỗi $x_i \in X$ tập hợp $x_iX = \{x_ix_1, x_ix_2, ..., x_ix_n\}$ là một bộ phận của X gồm n tích phân biệt vì nếu $k \neq l$ thì $x_k \neq x_l$ và $x_i x_k \neq x_ix_l$ (do có luật giản ước cho các phần tử của X). Vậy $x_i X = X$. Tương tự ta cũng có $Xx_i = X$ với mọi $x_i \in X$.

2.15. Giả sử A là một bộ phận khác rỗng ổn định của nhóm X. Khi đó A là một nửa nhóm hữu hạn và luật giản ước thực hiện được trong A. Theo bài tập 2.14, A là một nhóm.

2.16. Giả sử $A = m\mathbb{Z}$ (với m là một số nguyên) $A \neq \varnothing$ vì $0 = m$, $0 \in A$. Lấy mk_1 và mk_2 là hai phần tử bất kì của A,

$$mk_1 - mk_2 = m(k_1 - k_2) \in A.$$

Vậy A là một nhóm con của $\mathbb{Z}$.

Đảo lại, giả sử A là một nhóm con của $\mathbb{Z}$.

Nếu $A = \{0\}$ thì ta có $A = 0\mathbb{Z}$ với $m = 0$.

Giả sử $A \neq \{0\}$, khi đó có $a \in A$ là một số nguyên khác 0. Gọi m là số nguyên khác 0 thuộc A sao cho $|m| < |a|$ với mọi $a \neq 0$), $a \in A$. Do đó $A = m\mathbb{Z}$. Thật vậy rõ ràng $m\mathbb{Z} \subset A$(vì $m \in A$). Ngược lại giả sử $a \in A$ là một số nguyên, ta có $a = mq + r$(1) với $r = 0$ hoặc $|r| < |m|$.
Từ đẳng thức (1) suy ra $r = a - mq \in A$ do đó $r = 0$ hay $a = mq \in mA$. Vậy $A \subset m\mathbb{Z}$. Tóm lại có $A = m\mathbb{Z}$.

2.17. Tập hợp $S(X, Y) \neq \varnothing$ vì $1_X(Y) = Y$ nên $1_X \in S(X, Y)$.

Giả sử $f, g \in S(X, Y)$ là hai phần tử bất kì. Khi đó $f(Y) = Y$ và $g(Y) = Y$ kéo theo $gf(Y) = g|f(Y)| = g(Y) = Y$ nên $gf \in S(X, Y)$. Mặt khác $f^{-1}(Y) = f^{-1}(f(Y)) = f^{-1}f(Y) = 1_X(Y) = Y$.

Vậy $f^{-1} \in S(X, Y)$ do đó $S(X, Y)$ là một nhóm con của $S(X)$.

Nếu X có n phần tử và Y có một phần tử thì $S(X, Y)$ có $(n - 1)!$ phần tử, nó ứng với số các hoán vị của $n - 1$ phần tử của tập hợp $X - Y$.

2.18. Ta lập bảng toán của tập

$A = \{e, (12)(34), (13)(24), (14)(23)\}$

*	e	(12) (34)	(13) (24)	(14) (23)
e	e	(12) (34)	(13) (24)	(14) (23)
(12) (34)	(12) (34)	e	(14) (23)	(13) (24)
(13) (24)	(13) (24)	(14) (23)	e	(12) (34)
(14) (23)	(14) (23)	(13) (24)	(12) (34)	e

Nhìn vào bảng toán trên ta có $aA = A$ và $Aa = A$. Theo bài 2.8, A là một nhóm. Các phần tử đối xứng với nhau qua đường chéo chính nên A là một nhóm Aben.

2.19. a) Do tính chất kết hợp của phép toán trong nhóm X.

b) Do tính chất $(a^{-1})^{-1} = a$, với mọi $a \in X$.

c) Do tính chất $(ab)^{-1} = b^{-1}a^{-1}$.

d) Dựa vào một điều kiện tương đương của định nghĩa nhóm con.

2.20. Giả sử A là một nhóm con của nhóm X.

Theo bài 2.19, $A^{-1} \subset A$ do đó $AA^{-1} \subset A$.

Mặt khác, với mọi $a \in A$, $a = ae^{-1} \in AA^{-1}$ nên $A \subset AA^{-1}$ hay $AA^{-1} = A$.

Đảo lại, giả sử $AA^{-1} \subset A$ thế thì với mọi a và b thuộc A ta có $ab^{-1} \in AA^{-1} = A$, suy ra A là một nhóm con của nhóm X.

2.21. Giả sử aA là một nhóm con của X và e là đơn vị của X, khi đó $e = aa' \in aA$ với $a' \in A$. Vậy $a' = a - 1 \in A$, nên $a \in A$. Đảo lại, nếu $a \in A$, theo bài tập 2.8 thì $aA = A$ do đó aA là một nhóm con của nhóm X.

2.22. Nhóm con sinh bởi tập rỗng $\varnothing$ là nhóm con bé nhất (theo quan hệ bao hàm) chứa $\varnothing$. Vậy nhóm đó chính là nhóm con tầm thường {e} chỉ có phần tử đơn vị e.

2.23. Đặt $A = \{x_1, x_2 \ldots x_n \mid x_i \in S \cup S^{-1}\}$.

Khi đó A là một nhóm con của X vì

$$\alpha = x_1 x_2 \ldots x_n, \beta = x'_1 x'_2 \ldots x'_m \in A$$

thì $\alpha\beta = x_1 x_2 \ldots x_n x'_1 x'_2 \ldots x'_m \in A$ và $\alpha^{-1} = x_n^{-1} x_{n-1}^{-1} \ldots x_1^{-1} \in A$.

Mặt khác, nếu $x \in S$ thì $x \in A$ do đó $S \subset A$. Giả sử B là một nhóm con của nhóm X sao cho $S \subset B$.

Như vậy, nếu $\alpha \in A$, $\alpha = x_1 x_2 \ldots x_n$ thì

$x_1, x_2, \ldots, x_n \in S \cup S^{-1}$ hay $x_1, x_2, \ldots, x_n \in B$ do đó tích của chúng $\alpha = x_1 x_2 \ldots x_n \in B$. Hay $A \subset B$. Vậy A là nhóm con bé nhất của X chứa S, tức là A là nhóm con của X sinh bởi tập hợp S.

Nhóm con của nhóm các số hữu tỉ dương sinh bởi các số nguyên tố chính là nhóm $\mathbb{Q}^+$.

2.24. Giả sử $< x >$ là một nhóm xyclic sinh bởi phần tử x, A là một nhóm con của X.

Nếu $A = \{e\}$, e là đơn vị của nhóm X thì $A = < e >$ là nhóm xyclic sinh bởi phần tử e.

Nếu $A \neq \{e\}$ thì có một phần tử x^n ($\neq e$) thuộc A. Khi đó $n \neq 0$. Vì A là nhóm con của X nên $x^{-n} \in A$, giữa n và $-n$ có một số là nguyên dương. Vậy tồn tại các luỹ thừa nguyên dương của x trong A.

Gọi x^m là luỹ thừa nguyên dương bé nhất của x trong A. Khi đó $A = < x^m >$. Thật vậy, vì $x^m \in A$ nên $< x^m > \subset A$. Giả sử x^k là một phần tử tuỳ ý của A. Chia k cho m ta được $k = mq + r$ với $0 \leq r < m$.

Do đó $x^k = x^{mq + r} = (x^m)^q . x^r$ suy ra $x^r = x^k(x^m)^{-q} \in A$, chứng tỏ $r = 0$.

Vậy $x^k = (x^m)^q \in < x^m >$, hay $A \subset < x^m >$.

2.25. Giả sử k là số nguyên sao cho $a^k = e$, vì n là cấp của a nên $n > 0$. Chia k cho n ta được $k = nq + r$ với $o \leq r < n$.

Do đó $a^k = a^{nq + r} = a^{nq}.a^r$, từ đẳng thức đó suy ra $a^r = e$.

Vì n là số nguyên dương bé nhất sao cho $a^n = e$ mà $0 \leq r < n$ nên $r = 0$, do đó $k = nq$, hay k chia hết cho n.

Đảo lại, nếu $k = nq$ thì $a^k = (a^n)^q = e^q = e$.

2.26. Ta có thể giả thiết một trong hai phần tử ab hoặc ba có cấp hữu hạn. Giả sử cấp của ab bằng n, nghĩa là $(ab)^n = e$ và n là số nguyên dương bé nhất sao cho $(ab)^n = e$.

Khi đó ta có $a(ba)^{n-1}b = e$ suy ra $(ba)^{n-1} = a^{-1}b^{-1} = (ba)^{-1}$ hay $(ba)^n = e$, điều này chứng tỏ ba cũng có cấp hữu hạn và cấp của nó chia hết cho n.

Giả sử cấp của ba bằng m, như vậy ta có $(ba)^m = e$ hay

$$b(ab)^{m-1}a = e,\ (ab)^{m-1} = b^{-1}a^{-1} = (ab)^{-1}$$

từ đó suy ra $ab^m = e$, vậy n chia hết cho m. Tóm lại ta được $m = n$.

2.27. Trước hết ta thấy rằng nếu $X = < x >$ là một nhóm xyclic cấp vô hạn thì với mỗi số tự nhiên k ta có $< x^k >$ là một nhóm con xyclic của X và nếu $k \neq l$ thì $< x^k > \neq < x^l >$ do vậy X có vô hạn nhóm con.

Bây giờ giả sử X là một nhóm có cấp vô hạn. Nếu X có một phần tử x_0 có cấp vô hạn thì $A = < x_0 >$ là một nhóm con xyclic cấp vô hạn. Nhóm này có vô hạn nhóm con, mỗi nhóm con của nó lại là một nhóm con của X. Vậy X có vô hạn nhóm con. Nếu mỗi phần tử của X đều có cấp hữu hạn thì số các nhóm con xyclic sinh bởi các phần tử của X là vô hạn vì $\bigcup_{x \in x} < x > = X$ là tập vô hạn mà $< x >$ hữu hạn.

2.28. Giả sử $X = < x >$ có cấp là m và $Y = < y >$ có cấp là n, với m và n nguyên tố cùng nhau.

Ta sẽ chứng minh rằng $X \times Y$ là nhóm xyclic sinh bởi phần tử (x, y). Vì X có m phần tử và Y có n phần tử nên $X \times Y$ có mn phần tử hay cấp $X \times Y = mn$. Ta có

$$(x, y)^{mn} = (x^{mn}, y^{mn}) = (e_X, e_Y).$$

Nếu $(x, y)^k = (e_X, e_Y)$ thì $(x^k, y^k) = (e_X, e_Y)$ suy ra $x^k = e_X$ và $y^k = e_Y$. Theo bài 2.25, k chia hết cho m và k chia hết cho n, vì m và n nguyên tố cùng nhau nên k chia hết cho mn. Do đó cấp (x, y) = mn bằng cấp $X \times Y$.

Vậy $X \times Y$ là một nhóm xyclic sinh bởi (x, y).

Đảo lại, giả sử $X \times Y$ là một nhóm xyclic sinh bởi phần tử (x^k, y^l). Gọi M là bội chung nhỏ nhất của m và n ta có

$$(x^k, y')^M = (x^{Mk}, y^{M'}) = (e_X, e_Y),$$

điều này chứng tỏ M chia hết cho cấp của (x^k, y') hay M chia hết cho mn. Vậy m và n nguyên tố cùng nhau.

2.29. Giả sử A là một nhóm con của một nhóm X, A có chỉ số 2 tức là các lớp ghép trái của X theo nhóm con A có hai phần tử và các lớp ghép phải của X theo nhóm con A cũng có hai phần tử. Trong hai lớp ghép có một lớp là A và lớp còn lại là phần bù của A trong X. Do đó, mỗi lớp ghép trái của X theo A là một lớp ghép phải của X theo A và ngược lại. Vậy A là một nhóm con chuẩn tắc của X.

2.30. Do S_n là một nhóm hữu hạn nên để chứng minh A_n là một nhóm con của S_n ta chỉ cần chứng minh A_n ổn định đối với phép nhân ánh xạ. Vì tích của hai phép thế chẵn là một phép thế chẵn cho nên A_n ổn định đối với phép nhân ánh xạ. Theo bài 2.15, A_n là một nhóm con của S_n.

2.31. Vì X là một nhóm xyclic nên nó là một nhóm Aben do đó mỗi nhóm con của X đều là nhóm con chuẩn tắc. Giả sử $A = \langle x^3 \rangle$, như vậy $A = \{x^{3k} \mid k \in \mathbb{Z}\}$. Khi đó tập thương

$$A/X = \{C(x), C(x^2), C(x^0)\}.$$

Thật vậy nếu x^k là một phần tử bất kì của X, chia k cho 3 ta được $k = 3q + r$, $0 \le r < 3$.

Do đó $x^k = x^{3q}.x^r$ suy ra $x^k(x^r)^{-1} = x^{3q} \in A$ cho nên

$$C(x^k) = C(x^r) \in \{C(x), C(x^2), C(x^0)\}.$$

2.32. $C(X) = \{a \in X \mid ax = xa$ với mọi $x \in X\}$, $C(X) \neq \emptyset$ vì $e \in C(X)$. Nếu a và b thuộc C(X) thì $ax = xa$ và $bx = xb$ nên

$$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab).$$

Vậy $ab \in C(X)$.

Từ $ax = xa$ với mọi $x \in X$ ta suy ra $xa^{-1} = a^{-1}x$. Vậy $a^{-1} \in C(X)$. Rõ ràng với mọi a và b thuộc C(X) đều có $ab = ba$. Do đó C(X) là một nhóm giao hoán của X.

Giả sử A là một nhóm con của C(X). Khi đó A cũng là một nhóm con của X. Ngoài ra với mọi $a \in A$, với mọi $x \in X$,

$$x^{-1}ax = ax^{-1}x = a \in A$$

nên A là một nhóm con chuẩn tắc của X.

2.33. S_3 có các nhóm con là {e} (e là ánh xạ đồng nhất);

$\{e, (1\ 2)\} = \langle(12)\rangle$

$\{e, (1\ 3)\} = \langle(1\ 3)\rangle$; $\{e, (2\ 3)\} = \langle(2\ 3)\rangle$

$\{e, (1\ 2\ 3), (1\ 3\ 2)\} = \langle(1\ 2\ 3)\rangle = \langle(1\ 3\ 2)\rangle$ và S_3.

Trong đó có {e}, S_3 và $\langle(1\ 2\ 3)\rangle$ là ba nhóm con chuẩn tắc của S_3.

2.34. Kí hiệu [X, X] là nhóm con sinh bởi các hoán tử. Với mọi $a \in [X, X]$, với mọi $x \in X$ phần tử $b = a^{-1}x^{-1}ax \in [X, X]$. Do đó $x^{-1}ax = ab \in [X, X]$. Vậy [X, X] là một nhóm con chuẩn tắc của X.

Giả sử $\bar{a}$ và $\bar{b}$ thuộc $X/_{[X, X]}$ ta có $\bar{a}.\bar{b} = \overline{ab}$ và $\bar{b}.\bar{a} = \overline{ba}$.

Mặt khác $aba^{-1}b^{-1} = (ab)(ba)^{-1} \in [X, X]$ nên $\overline{ab} = \overline{ba}$ hay $\bar{a}\,\bar{b} = \bar{b}\,\bar{a}$.

2.35. Giả sử $X/_H$ là một nhóm Aben, như vậy với mọi aH và bH thuộc $X/_H$ ta có aHbH = bHaH hay abH = baH.

Do đó $ab(ba)^{-1} = aba^{-1}b^{-1} \in H$. Từ đó suy ra nhóm con các hoán tử của X bị chứa trong H. Đảo lại, nếu nhóm con các hoán

tử của X chứa trong H thì với mọi a, b $\in$ X, $aba^{-1}b^{-1} \in H$. Từ đó suy ra abH = baH, hay aHbH = bHaH tức là X/H là một nhóm Aben.

2.36. Nhóm các hoán tử của S_3 là H = <(1 2 3)>.

2.37. Hiển nhiên nhóm cấp một (nhóm chỉ có một phần tử đơn vị) là một nhóm Aben; nhóm cấp hai, nhóm cấp ba và nhóm cấp năm đều là nhóm cấp nguyên tố nên chúng là những nhóm xyclic do đó chúng là những nhóm Aben.

Giả sử X là một nhóm cấp bốn. Nếu X có một phần tử cấp hai thì nó là một nhóm xyclic nên X là một nhóm Aben. Nếu X không có phần tử nào cấp bốn thì X có ba phần tử cấp hai do đó với mọi a $\in$ X, $a^2 = e$. Theo bài 2.10, X là một nhóm Aben.

2.38. a) $3\mathbb{Z}/15\mathbb{Z} = \{15\mathbb{Z}, 3 + 15\mathbb{Z}, 6 + 15\mathbb{Z}, 9 + 15\mathbb{Z}, 12 + 15\mathbb{Z}\}$

b) $4\mathbb{Z}/24\mathbb{Z} = \{24\mathbb{Z}, 4 + 24\mathbb{Z}, 8 + 24\mathbb{Z}, 12 + 24\mathbb{Z}, 16 + 24\mathbb{Z}, 20 + 24\mathbb{Z}\}$.

c) Gọi $\mathbb{R}^*$ là nhóm nhân các số thực khác 0,

$\mathbb{R}^*_+$ là nhóm nhân các số thực dương,

$\mathbb{R}^*/\mathbb{R}^*_+ = \{\mathbb{R}^*_+, \mathbb{R}^*_-\}$, $\mathbb{R}^*_-$ là tập hợp các số thực âm.

2.39. a) Chứng minh theo định nghĩa của nhóm.

Đơn vị của D là đường thẳng Δ_0 có phương trình y = x. Nghịch đảo của đường thẳng Δ có phương trình y = ax + b là đường thẳng Δ' có phương trình $y = \frac{1}{a}x - b$.

b) Ánh xạ $\varphi : D \to \mathbb{R}^*$

$$\Delta \mapsto a.$$

Với Δ là đường thẳng xác định bởi phương trình $y = ax + b$ là một đồng cấu vì giả sử Δ_1 và Δ_2 là hai đường thẳng xác định bởi $y_1 = a_1x + b_1$ và $y_2 = a_2x + b_2$,

$\varphi(\Delta_1 . \Delta_2) = a_1 a_2 = \varphi(\Delta_1)\, \varphi(\Delta_2)$.

$\text{Ker}\varphi = \{\Delta \in D \mid \Delta$ có phương trình $y = ax + b\}$. $\Delta \in \text{Ker}\varphi$ khi và chỉ khi phương trình của Δ có hệ số của x bằng 1.

2.40. Ta chỉ cần chứng minh tập hợp các phép đối xứng của một hình là nhóm con của nhóm các phép thế của tập hợp các điểm của hình đó.

2.41. Mỗi phép đối xứng của tam giác đều có đỉnh là 1, 2, 3 sẽ chuyển đỉnh 1 thành một trong ba đỉnh 1 hoặc 2 hoặc 3. Do đó, ứng với mỗi phép đối xứng là một phép thế của tập hợp {1, 2, 3}. Số các phép thế của {1, 2, 3} là 6. Mặt khác các phép đối xứng chỉ ra 1, R, R_2, D_1, D_2, D_3 là khác nhau. Vậy $\Delta_3 = \{1, R, R^2, D_1, D_2, D_3\}$ có cấp 6.

Ta có bảng toán sau:

*	1	R	R^2	D_1	D_2	D_3
1	1	R	R^2	D_1	D_2	D_3
R	R	R^2	1	D_3	D_1	D_2
R^2	R^2	1	R	D_2	D_3	D_1
D_1	D_1	D_2	D_3	1	R	R^2
D_2	D_2	D_3	D_1	R^2	1	R
D_3	D_3	D_1	D_2	R	R^2	1

Cho ta thành lập được đẳng cấu $\Delta_3 \cong S_3$.

2.42. a) Ta có $Kerp_1 = \{(e_1, x_2) \mid x_2 \in X_2\} = B$.

Thật vậy, $(x_1\ x_2) \in Kerp_1 \Leftrightarrow p_1(x_1, x_2) = e_1$

$$\Leftrightarrow p_1(x_1, x_2) = x_1 = e_1$$

$$\Leftrightarrow (x_1, x_2) = (e_1, x_2)$$

$$\Leftrightarrow (e_1, x_2) \in B.$$

Tương tự ta có $Kerp_2 = A$.

b) $Imq_1 = A$ theo định nghĩa của q_1 và

$Imq_2 = B$ theo định nghĩa của q_2.

Vì q_1 là đơn cấu và $Imq_1 = A$ nên $G_1 \cong A$ và q_2 là đơn cấu, $Imq_2 = B$ nên $G_2 \cong B$.

c) Vì A và B lần lượt là hạt nhân của p_2 và p_1 nên chúng là những nhóm con chuẩn tắc.

Hơn nữa, với mọi $(x_1, x_2) \in G$ ta có

$$(x_1, x_2) = (x_1, e_2)\ (e_1, x_2) \in AB$$

nên $G \subset AB$, suy ra $AB = G$ (vì luôn có $BA = G$).

2.43. Giả sử $X = < a >$ là một nhóm xyclic sinh bởi phần tử a. Xét ánh xạ $\varphi : \mathbb{Z} \to X$

$$n \mapsto a^n$$

khi đó φ là một toàn cấu từ nhóm cộng các số nguyên $\mathbb{Z}$ đến nhóm xyclic X. Vì mỗi phần tử của X đều là một luỹ thừa nguyên của a và $a^n.a^m = a^{n+m}$ nên $\varphi(n + m) = \varphi(n).\ \varphi(m)$. Ta hãy xác định $Ker\varphi$.

Nếu X là một nhóm hữu hạn cấp n thì $\text{Ker}\varphi = n\mathbb{Z}$. Thật vậy với $k = nq \in n\mathbb{Z}$ ta có $\varphi(k) = \varphi(nq) = a^{nq} = e^x$. Suy ra $n\mathbb{Z} \subset \text{Ker}\varphi$.

Giả sử $k \in \text{Ker}\varphi$ thì $\varphi(k) = a^k = e$ suy ra k chia hết cho n, hay $k = nq \in n\mathbb{Z}$, hay $\text{Ker}\varphi \subset n\mathbb{Z}$.

Nếu X là một nhóm xyclic cấp vô hạn thì với $n \neq m$, $a^n \neq a^m$ nên φ là một đơn cấu và do đó $\text{Ker}\varphi = \{0\}$.

Theo định lí đồng cấu ta có $\mathbb{Z}/\text{Ker}\varphi = X$.

Như vậy nếu X có cấp n thì $X \cong \mathbb{Z}/n\mathbb{Z}$.

Nếu X có cấp vô hạn thì $X \cong \mathbb{Z}$.

2.44. Làm tương tự như bài 2.43.

2.45. Giả sử $X = < a >$ là nhóm xyclic cấp vô hạn với phép nhân. Khi đó X có hai phần tử sinh là a và a^{-1}. Hơn nữa, x cũng chỉ có hai tự đẳng cấu là $id_x : X \to X$ và $\varphi : X \to X$.

$x \mapsto x$ $\qquad$ $x \mapsto x^{-1}$

Thật vậy, giả sử X có phần tử sinh là b, khi đó $b = a^n$, $n \in \mathbb{Z}$.

Vì $a \in X$ nên có $m \in \mathbb{Z}$ để $a = b^m = a^{mn}$. Do X là nhóm có cấp vô hạn nên $mn = 1$. Từ đó có hai trường hợp: $n = 1$ thì $b = a$; hoặc $n = -1$ thì $b = a^{-1}$. Mặt khác có $< a^{-1} > = < a >$.

Nếu $f : X \to X$ là một đồng cấu thì f sẽ biến phần tử sinh của X thành một phần tử sinh của X. Vậy chỉ có hai khả năng $f(a) = a$, khi đó $f = id_x$. Hoặc $f(a) = a^{-1}$, khi đó $f = \varphi$.

2.46. Kiểm tra lại theo định nghĩa của nhóm và nhóm Aben.

2.47. a) Giả sử φ: $X \to Y$

$$x^n \mapsto (y^k)^n$$

là một đồng cấu với x là phần tử sinh của X có cấp s và y là phần tử sinh của Y có cấp t. Như vậy, ta phải có

$$\varphi(x^n . x^m) = \varphi(x^n)\varphi(x^m) \text{ hay}$$

$$(y^k)^{n+m} = (y^k)^n (y^k)^m \text{ và}$$

$$\varphi(e_x) = \varphi(x^s) = (y^k)^s = y^{ks} = e_Y.$$

Do đó ks phải chia hết cho t (cấp của Y) (theo bài 2.25). Đảo lại, nếu ks chia hết cho t thì ks = tr. Giả sử $x^m = x^n$ thì $x^{m-n} = e^x$ hay m − n = su. Khi đó $\varphi(x^m) = y^{km}$ và $\varphi(x^n) = y^{kn}$, suy ra $\varphi(x^m)|\varphi(x^n)|^{-1} = y^{km} . y^{-kn} = y^{k(m-n)} = y^{ksu} = y^{tru} = e_Y$.

Do đó $\varphi(x^m) = \varphi(x^n)$, do đó φ là một ánh xạ. Hơn nữa

$$\varphi(x^m . x^n) = \varphi(x^{m+n}) = y^{k(m+n)} = y^{km} . y^{kn} = \varphi(x^m)\varphi(x^n).$$

Vậy φ là một đồng cấu.

b) Nếu φ là một đẳng cấu và sk = mt thì do X và Y là hữu hạn nên s = t và suy ra m = k. Mặt khác do φ là đẳng cấu nên y^k phải là một phần tử sinh của Y do đó theo bài 2.25, k và t nguyên tố cùng nhau hay k và s nguyên tố cùng nhau.

2.48. Ta có $\varphi(ab) = (ab)^k = a^k b^k$ (vì X là một nhóm Aben) nên

$$\varphi(ab) = \varphi(a)\varphi(b).$$

$$\text{Ker}\varphi = \{x \in X \mid x^k = e\} = \{x \in X \mid \text{cấp } x \text{ là ước của } k\}.$$

2.49. Giả sử X là một nhóm Aben thì theo bài tập 2.48, φ là một đồng cấu $\text{Ker}\varphi = \{x \in X \mid x \text{ có cấp là ước của } -1\}$

hay $x \in \text{Ker}\varphi \Leftrightarrow$ cấp của x là ước của $-1 \Leftrightarrow x = e$.

Do đó φ là một đơn cấu, hơn nữa hiển nhiên φ là một toàn cấu vì $(x^{-1})^{-1} = x$. Do đó φ là một đẳng cấu. Đảo lại, giả sử φ là một đẳng cấu. với mọi a và b thuộc X ta có

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

Mặt khác $\varphi(ab) = (ab)^{-1}$ nên suy ra $(ab)^{-1} = a^{-1}b^{-1} = (ba)^{-1}$ hay ab = ba. Vậy X là một nhóm Aben.

2.50. Kí hiệu Aut(X) là tập hợp các tự đẳng cấu của nhóm X. Khi đó $Aut(X) \subset S(X)$ với S(X) là nhóm các song ánh của tập X với phép nhân ánh xạ. $1_X \in Aut(X)$ nên $Aut(X) \neq \emptyset$. Ngoài ra ta còn có tích của hai tự đẳng cấu của X là một tự đẳng cấu của X và nghịch đảo của một tự đẳng cấu của X là một tự đẳng cấu của X. Do đó Aut(X) là một nhóm con của S(X).

2.51. Giả sử $h : X \to G$

$$x \mapsto h(x) = (f(x), g(x))$$

là một đồng cấu. Khi đó với x_1 và x_2 thuộc X ta có

$$h(x_1x_2) = h(x_1)h(x_2) = (f(x_1), g(x_1))(f(x_2), g(x_2))$$

$$= (f(x_1).f(x_2), g(x_1).g(x_2)).$$

Mặt khác $h(x_1x_2) = (f(x_1, x_2), g(x_1, x_2))$. Như vậy có đẳng thức

$$(f(x_1, x_2). g(x_1x_2)) = (f(x_1)f(x_2), g(x_1)g(x_2)).$$

Suy ra $f(x_1x_2) = f(x_1)f(x_2)$ và $g(x_1x_2) = g(x_1)g(x_2)$ nghĩa là f và g là những đồng cấu.

Đảo lại, giả sử f và g là những đồng cấu. Khi đó

$$h(x_1.x_2) = (f(x_1x_2), g(x_1x_2))$$

$$= (f(x_1)f(x_2). g(x_1)g(x_2))$$

$$= (f(x_1), g(x_1), (f(x_2), g(x_2))$$

$= h(x_1)h(x_2)$

Vậy h là một đồng cấu.

2.52. a) Ta có X là một nhóm với phần tử trung lập là (0, 0, 0). Phần tử đối xứng của $\alpha = (k_1, k_2, k_3)$ là

$$((-1)^{k_2+1}k_1, -k_2, -k_3).$$

b) Nhóm con A được xác định như sau:

$$(1, 0, 0)^1 = (1, 0, 0)$$

$$(1, 0, 0)^2 = (2, 0, 0).$$

Bằng quy nạp ta có với $n \geq 0$

$$(1, 0, 0)^n = (n, 0, 0) \text{ và do đó}$$

$$(1, 0, 0)^{-n} = (-n, 0, 0).$$

Vậy $A = \{(k, 0, 0) \mid k \in \mathbb{Z}\}$.

Giả sử $\alpha = (k_1, k_2, k_3) \in X$ và $a = (k, 0, 0) \in A$ khi đó

$$\alpha^{-1}a\alpha = ((-1)^{k_2+1}k_1, -k_2, -k_3).\ (k, 0, 0).\ (k_1, k_2, k_3)$$

$$= (k, 0. 0) \in A$$

nên A là một nhóm con chuẩn tắc của X.

c) Xét ánh xạ $X \xrightarrow{\varphi} X[i]$

$$(k_1, k_2, k_3) \mapsto k_1 + k_3 i$$

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

φ là một toàn cấu và $\text{Ker}\varphi = A$ nên theo định lí đồng cấu ta suy ra $X/A \cong \mathbb{Z}[i]$.

2.53. Gọi $\mathbb{R}$ là nhóm cộng các số thực và $\mathbb{R}_+^*$ là nhóm nhân các số thực dương. Ta xét ánh xạ lg: $\mathbb{R}_+^* \to \mathbb{R}$

$$x \mapsto \lg x.$$

(lgx là logarit thập phân của x).

Do tính chất của hàm lg ta có $\lg(xy) = \lg x + \lg y$ nên lg là một đồng cấu, nếu $x \neq y$ thì $\lg x \neq \lg y$ nên lg là một đơn cấu. Ngoài ra với mỗi $a \in \mathbb{R}$, $10^a \in \mathbb{R}_+^*$ thoả mãn $\lg 10^a = a$. Vậy lg là một đẳng cấu.

2.54. Xét ánh xạ $\varphi : \mathbb{Z} \to \mathbb{Z}[i]$

$$(a, b) \mapsto a + bi$$

Ta có φ là một đẳng cấu.

2.55. a) Giả sử $X = < a >$ có cấp n, $b = a^k \in X$. Gọi d là ước chung lớn nhất của k và n khi đó $n = n_1 d$ và $k = k_1 d$ với n_1 và k_1 nguyên tố cùng nhau. Ta có

$$b^{n_1} = (a^k)^{n_1} = a^{kn_1} = a^{k_1 d n_1} = e^{k_1} = e$$

Thêm nữa, nếu $b^t = e$ hay $a^{kt} = e$ thì kt chia hết cho n. Như vậy có $kt = k_1 dt = n_1 ds$ hay $k_1 t = n_1 s$ nghĩa là $k_1 t$ chia hết cho n_1. Vì k_1 và n_1 nguyên tố cùng nhau nên t chia hết cho n_1. Vậy $n_1 = \frac{n}{d}$ là cấp của $b = a^k$.

b) Phần tử $b = a^k$ là phần tử sinh của nhóm X nếu và chỉ nếu cấp của b bằng cấp của X và bằng n. Theo câu a), cấp b là $\frac{n}{d}$. Như vậy, phần tử b là phần tử sinh của X khi và chỉ khi $d = 1$ hay n và k nguyên tố cùng nhau. Vậy số các phần tử

sinh của X bằng số các số nguyên dương bé hơn n và nguyên tố với n.

2.56. Do $ab = ba$ nên $(ab)^{rs} = a^{rs}b^{rs} = e.e = e$.

Giả sử $(ab)^t = e$ hay $a^tb^t = e$, suy ra $a^t = b^{-t}$. Nâng cả hai vế lên luỹ thừa r và s ta được $a^{ts} = b^{-ts} = e$ (1)

$$a^{tr} = b^{-tr} = e\,. \qquad (2)$$

Từ (1) và (2) suy ra ts chia hết cho r và tr chia hết cho s. Vì r và s nguyên tố cùng nhau nên t chia hết cho cả r lẫn s và do đó t chia hết cho tích rs. Vậy rs là cấp của phần tử ab.

2.57. a) Giả sử X là một nhóm cấp bốn. Nếu trong X có một phần tử cấp bốn thì X là một nhóm xyclic sinh bởi phần tử có cấp bốn đó. Nếu X không có phần tử nào có cấp bốn thì X có ba phần tử cấp hai. Trong trường hợp này X đẳng cấu với $\mathbb{Z}_2 \times \mathbb{Z}_2$.

b) Giả sử X là một nhóm có cấp sáu. Khi đó X chứa một phần tử cấp hai và một phần tử cấp ba. Chẳng hạn $a \in X$ có cấp hai và $b \in X$ có cấp ba. Nếu $ab = ba$ thì ab có cấp sáu do đó X là một nhóm xyclic. Nếu $ab \neq ba$ thì X đẳng cấu với S_3.

2.58. Giả sử X là một nhóm xyclic với phần tử sinh là a. Ánh xạ $f: X \to Y$ là một đồng cấu từ X đến Y. Như vậy $f(a) \in \mathrm{Im}f$ và do đó $\mathrm{Im}f = \{f(a)^n = f(a^n) \mid n \in \mathbb{Z}\}$ là một nhóm xyclic sinh bởi phần tử f(a).

Bây giờ giả sử H là một nhóm con của nhóm xyclic X. Ta xét phép chiếu chính tắc

$$p : X \to X/H$$
$$x \mapsto xH.$$

p là một toàn cấu, Imp = X/H H theo chứng minh trên thì Imp là một nhóm xyclic. Vậy nhóm thương X/H là một nhóm xyclic.

2.59. a) Gọi b là bội chung nhỏ nhất của m và n. Ta có:

$$m \setminus b \Rightarrow m\mathbb{Z} \supset b\mathbb{Z};$$

$$n \setminus b \Rightarrow n\mathbb{Z} \supset b\mathbb{Z}.$$

Suy ra $m\mathbb{Z} \cap n\mathbb{Z} \supset b\mathbb{Z}$. (1)

Mặt khác nếu $a \in m\mathbb{Z} \cap n\mathbb{Z}$ thì tồn tại k_1 và k_2 thuộc $\mathbb{Z}$ sao cho $a = mk_1$ và $a = nk_2$. Do đó a chia hết cho b hay tồn tại $k \in \mathbb{Z}$ sao cho $a = bk$. Vậy $a \in b\mathbb{Z}$. Suy ra $m\mathbb{Z} \cap n\mathbb{Z} \subset b\mathbb{Z}$. (2)

Từ (1) và (2) suy ra $m\mathbb{Z} \cap n\mathbb{Z} = b\mathbb{Z}$.

b) Gọi d là ước chung lớn nhất của m và n. Khi đó tồn tại hai số nguyên u và v sao cho $d = mu + nv$. Vậy $d \in m\mathbb{Z} + n\mathbb{Z}$. Suy ra $d\mathbb{Z} \subset m\mathbb{Z} + n\mathbb{Z}$. Giả sử $a \in m\mathbb{Z} + n\mathbb{Z}$, khi đó tồn tại k_1 và k_2 thuộc $\mathbb{Z}$ sao cho $a = mk_1 + nk_2$. Vì d là ước chung lớn nhất của m và n nên tồn tại m_1 và n_1 thuộc $\mathbb{Z}$ sao cho $m = dm_1$ và $n = dn_1$. Suy ra $a = d(m_1k_1 + n_1k_2) \in d\mathbb{Z}$.

Như vậy ta có $m\mathbb{Z} + n\mathbb{Z} \subset d\mathbb{Z}$. Hay $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$.

c) Xét ánh xạ $\varphi : m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$

$$mk \mapsto k + n\mathbb{Z}.$$

φ là một đồng cấu vì với mọi mk và ml thuộc $m\mathbb{Z}$ có

$$\varphi(mk + ml) = \varphi(m(k + l)) = (k + l) + n\mathbb{Z}$$

$$= (k + n\mathbb{Z}) + (l + n\mathbb{Z}) = \varphi(mk) + \varphi(ml).$$

φ là một toàn ánh vì nếu $k + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ thì $mk \in m\mathbb{Z}$ thoả mãn $\varphi(mk) = k + n\mathbb{Z}$.

Tìm $\text{Ker}\varphi$:

$$a = mk \in \text{Ker}\varphi \Leftrightarrow k + n\mathbb{Z} = n\mathbb{Z} \Leftrightarrow k \text{ chia hết cho } n$$

$$\Leftrightarrow k = nk_1, \text{ với } k_1 \in \mathbb{Z}$$

$$\Leftrightarrow a = mnk_1.$$

Vậy $\text{Ker}\varphi = mn\mathbb{Z}$.

Theo định lí đồng cấu ta có $m\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$.

2.60. Do $AB = X$ nên mỗi phần tử x của X viết được dưới dạng $x = ab$ với $a \in A$ và $b \in B$. Giả sử có $x = ab = a'b'$ với $a, a' \in A$ và $b, b' \in B$ thì $a'^{-1}a = b'b^{-1} \in A \cap B$. Vì $A \cap B = \{e\}$ nên $a'^{-1}.a = b'^{-1}b = e$, do đó $a' = a$ và $b' = b$. Vậy mỗi phần tử $x \in X$ viết được một cách duy nhất dưới dạng $x = ab$ với $a \in A$ và $b \in B$. Mặt khác các phần tử của A giao hoán được với các phần tử của B. Thật vậy, với a và b tuỳ ý thuộc A và B, xét tích $a^{-1}b^{-1}ab$. Vì A và B là những nhóm con chuẩn tắc của X

nên $b^{-1}ab \in A$ và $a^{-1}b^{-1}a \in B$. Vậy $a^{-1}b^{-1}ab \in A \cap B = \{e\}$.

nên $a^{-1}b^{-1}ab = e$, hay $ab = ba$.

Ánh xạ $A \times B \to X$

$$(a, b) \mapsto ab$$

là một đồng cấu do $ab = ba$, là đơn cấu do $A \cap B = \{e\}$, là toàn cấu do $X = AB$. Vậy ta có đẳng cấu.

2.61. a) Giả sử A và B là hai nhóm con chuẩn tắc của nhóm X. Khi đó $AB = \{ab \mid a \in A, b \in B\}$ cũng là một nhóm con chuẩn tắc của X. Thật vậy, $e \in A$ và $e \in B$ nên $e = e.e \in AB$ nên $AB \neq \varnothing$. Hơn nữa với mọi $a \in A$, $a = ae \in AB$ và với mọi $b \in B$, $b = eb \in AB$.

Giả sử $a_1b_1 \in AB$ và $a_2b_2 \in AB$,

$$(a_1b_1)(a_2b_2) = a_1(b_1a_2)b_2 = a_1a_2b'_1b_2 \in AB$$

(vì B là nhóm con chuẩn tắc của X nên $a_2B = Ba_2$);

$$(a_1b_1)^{-1} = b_1^{-1}a_1^{-1} = a_1^{-1}b' \in AB$$

(vì B là nhóm con chuẩn tắc của X).

Ngoài ra, với mọi $x \in X$ có

$$x(AB) = (xA)B = (Ax)B = A(Bx) = ABx.$$

b) Ta biết rằng giao của hai nhóm con của một nhóm X là một nhóm con của nhóm X. Giả sử $a \in A \cap B$ và $x \in X$. Khi đó $a \in A$ và $a \in B$ nên $x^{-1}ax \in A$ và $x^{-1}ax \in B$ hay

$$x^{-1}ax \in A \cap B.$$

Vậy $A \cap B$ là một nhóm con chuẩn tắc của X.

c) Xét ánh xạ $\varphi : X \to \left(X/A\right) \times \left(X/B\right)$

$$x \mapsto (xA, xB).$$

φ là một đồng cấu vì với mọi x_1 và x_2 thuộc X

$$\varphi(x_1x_2) = (x_1x_2A, x_1x_2B) = (x_1Ax_2A, x_1Bx_2B)$$

$$= (x_1A, x_1B)(x_2a, x_2B) = \varphi(x_1)\varphi(x_2).$$

$A \cap B = \text{Ker}\varphi$ vì với mọi $x \in A \cap B$ thì $x \in A$ và $x \in B$ nên $xA = A$ và $xB = B$, do đó $\varphi(x) = (xA, xB) = (A, B)$ là đơn vị của X/A và X/B và nếu $x \in \text{Ker}\varphi$ thì $\varphi(x) = (A, B) = (xA, xB)$ suy ra $x \in A$ và $x \in B$ hay $x \in A \cap B$. Vậy theo định lí đồng cấu có một đơn ánh $\overline{\varphi} : X/(A \cap B) \to (X/A) \times (X/B)$.

d) Xét ánh xạ $\sigma : A \to (AB)/B$

$$a \mapsto a.eB = aB.$$

$\sigma(a_1a_2) = a_1a_2eB = a_1e.a_2eB = a_1eB.a_2eB = \sigma(a_1)\sigma(a_2)$.

Với mọi $abB \in (AB)/B$ ta có $a \in A$ thoả mãn

$\sigma(a) = aeB = abB$ (vì $b \in B$) do đó σ là một toàn cấu.

Giả sử $x \in \text{Ker}\sigma$, $\sigma(x) = B = xeB$ như vậy $x \in B$, đương nhiên $x \in A$, do đó $x \in A \cap B$.

Nếu $x \in A \cap B$ thì $\sigma(x) = B$. Vậy ta có $\text{Ker}\sigma = A \cap B$. Theo định lí đồng cấu $A/(A \cap B) \cong (AB)/B$.

2.62. Giả sử H là một nhóm con chuẩn tắc của nhóm G.

Khi đó f(H) là một nhóm con của G'. Mặt khác, nếu $h' \in f(H)$ và $x' \in G'$, khi đó tồn tại $h \in H$ sao cho $f(h) = h'$ và vì f là toàn ánh nên tồn tại $x \in G$ sao cho $f(x) = x'$. Do đó

$$x'h'x'^{-1} = f(x)f(h)f(x)^{-1} = f(xhx^{-1}) \in f(H).$$

Vậy f(H) là nhóm con chuẩn tắc của G'.

Ví dụ sau chứng to H là nhóm con chuẩn tắc của G, nhưng f(H) không là nhóm con chuẩn tắc của G' khi f không là toàn cấu.

$G = \mathbb{Z}_2$, $G' = S_3 = \{(1), (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\}$

$$\begin{aligned} f : \mathbb{Z}_2 &\to S_3 \\ \bar{0} &\mapsto (1) \\ \bar{1} &\mapsto (1\ 2) \end{aligned}$$

f là một đồng cấu. Ta có $\mathbb{Z}_2$ là nhóm con chuẩn tắc của $\mathbb{Z}_2$ nhưng $f(\mathbb{Z}_2) = \{(1), (1\ 2)\}$ không là nhóm con chuẩn tắc của S_3.

2.63. Trước hết ta chứng minh rằng nếu $f : X \to Y$ là một toàn cấu và A là một nhóm con chuẩn tắc của X thì f(A) cũng là một nhóm con chuẩn tắc của Y. Ta đã biết nếu A là một nhóm con của X thì f(A) là một nhóm con của Y (tính chất của đồng cấu nhóm). Giả sử $y \in Y$ và $b \in f(A)$, tồn tại $a \in A$ sao cho $b = f(a)$ vì f là toàn cấu nên tồn tại $x \in X$ sao cho $f(x) = y$. Xét phần tử

$$y^{-1}by = f(x^{-1})f(a)f(x) = f(x^{-1}ax) \in f(A) \text{ vì } x^{-1}ax \in A.$$

Bây giờ ta xét ánh xạ $p : X \to X/A$

$$x \mapsto xA,$$

p là một toàn cấu. Do đó, với mỗi nhóm con chuẩn tắc H của X mà $H \supset A$ thì ta có một nhóm con chuẩn tắc p(H) của X/A. Đảo lại, nếu K là một nhóm con chuẩn tắc của X/A thì $p^{-1}(K)$ là một nhóm con chuẩn tắc của X chứa A. Như vậy, tồn tại một tương ứng 1 – 1 hay một song ánh từ tập các

nhóm con chuẩn tắc của X chứa A đến tập các nhóm con chuẩn tắc của X/A.

2.64. Áp dụng kết quả bài 2.63. Giả sử H là nhóm con chuẩn tắc tối đại của G. Khi đó, giữa H và G chỉ có hai nhóm con chuẩn tắc là H và G. Do đó nhóm thương G/H cũng chỉ có hai nhóm con chuẩn tắc. Vậy G/H là một nhóm đơn. Đảo lại, nếu G/H là một nhóm đơn thì giữa G và H không còn một nhóm con chuẩn tắc nào khác. Như vậy H là nhóm con chuẩn tắc tối đại của G.

2.65. a) Ta có H và K là hai nhóm con chuẩn tắc của G nên HK là một nhóm con chuẩn tắc của G. Hơn nữa, ta có $H \subset HK$ và $K \subset HK$. Vì $H \neq K$ nên suy ra $H \neq HK$ và $K \neq HK$. Mặt khác, H và K là hai nhóm con chuẩn tắc tối đại của G nên $HK = G$.

b) Theo đẳng cấu Noether ta có

$$G/H = (HK/H) \cong (K/H \cap K) \text{ và}$$

$$G/H = (HK/H) \cong (H/H \cap K).$$

Vì G/H là nhóm đơn nên $K/H \cap K$ và $H/H \cap K$ là những nhóm đơn từ đó suy ra $H \cap K$ là nhóm con chuẩn tắc tối đại của H và của K.

2.66. Giả sử $f : \mathbb{Q} \to \mathbb{Z}$ là một đồng cấu từ nhóm cộng $\mathbb{Q}$ đến nhóm cộng $\mathbb{Z}$. Nếu $f \neq 0$ nghĩa là tồn tại một số hữu tỉ q ($q \neq 0$) sao cho $f(q) \neq 0$. Giả sử $q = \frac{r}{s} \in \mathbb{Q}$ với $s > 0$. Khi đó $s.f(\frac{r}{s}) = f(r) \neq 0$.

Mặt khác $f(r) = f(r.1) = rf(1)$, từ đó $f(1) = n_1 \neq 0$. Vậy với mọi số nguyên $n \neq 0$, $f(n) = nf(1) \neq 0$.

Giả sử $n > 1$, $n \in \mathbb{Z}$ và $(n, n_1) = 1$. Ta có

$$f(1) = f(n.\frac{1}{n}) = nf(\frac{1}{n}) = nn_0 = n_1 \text{ với } f(\frac{1}{n}) = n_0.$$

Như vậy, n lại là ước của n_1. Vô lí.

Vậy chỉ có một đồng cấu duy nhất là đồng cấu không từ $\mathbb{Q}$ vào $\mathbb{Z}$; $\mathbb{Q}$ không đẳng cấu với $\mathbb{Z}$ nên $\mathbb{Q}$ không là một nhóm xyclic.

2.67. a) Có thể chứng minh Aut(X) là nhóm con của nhóm S(X) (S(X) là nhóm các song ánh từ X đến X với phép nhân ánh xạ).

b) $\mathbb{Z}$ là nhóm xyclic có cấp vô hạn sinh bởi 1 và -1 vậy Aut($\mathbb{Z}$) gồm hai ánh xạ

$$id_{\mathbb{Z}} : \mathbb{Z} \to X \qquad \text{và} \quad \varphi: \mathbb{Z} \to \mathbb{Z}$$

$$x \mapsto x. \qquad\qquad n \mapsto -n.$$

Vậy $\text{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

2.68. a) Với mọi a và b thuộc A ta có

$$\begin{aligned}(f + g)(a + b) &= f(a + b) + g(a + b)\\ &= [f(a) + f(b)] + [g(a) + g(b)]\\ &= [f(a) + g(a)] + [f(b) + g(b)]\\ &= (f + g)(a) + (f + g)(b).\end{aligned}$$

Vậy f + g là một đồng cấu.

Phép cộng trong End(A) có tính chất giao hoán và kết hợp được suy từ tính chất giao hoán và kết hợp của phép cộng trong A.

Ánh xạ không $0 : A \to A$

$$a \mapsto 0$$

thuộc End(A) thoả mãn $f + 0 = f$ với mọi $f \in End(A)$ với mỗi $f \in End(A)$ ánh xạ $g: A \to A$

$$a \mapsto g(a) = -f(a)$$

thoả mãn $f + g = 0$.

Vậy End(A) là một nhóm Aben.

b) Ánh xạ $F : End(\mathbb{Z}) \to \mathbb{Z}$

$$f \mapsto F(f) = f(1)$$

là một đẳng cấu.

Thật vậy, với mọi f và g thuộc $End(\mathbb{Z})$ ta có

$$F(f + g) = (f + g)(1) = f(1) + g(1) = F(f) + F(g).$$

$F(f) = F(g)$ nên $f(1) = g(1)$ hay $\forall n \in \mathbb{Z}$,

$$f(n) = nf(1) = n(1) = g(n)$$

nghĩa là $f = g$.

$\forall n \in \mathbb{Z}$, ánh xạ $f : \mathbb{Z} \to \mathbb{Z}$

$$1 \mapsto n$$

$$a \mapsto na$$

là một tự đồng cấu của X.

Vậy $End(\mathbb{Z}) \cong X$.

c) Tương tự câu b) ánh xạ $F : End(\mathbb{Q}) \to \mathbb{Q}$

$$f \mapsto f(1)$$

là một đẳng cấu.

2.69. a) Giả sử x và y thuộc X ta có

$$f_a(xy) = axya^{-1} = (axa^{-1})(aya^{-1}) = f_a(x) \cdot f_a(y).$$

Nếu $f_a(x) = f_a(y)$ tức là $axa^{-1} = aya^{-1}$ thì sau khi giản ước ta được $x = y$. Với mỗi $y \in Y$ ta có $a^{-1}ya \in X$ thoả mãn

$$f_a(x) = f_a(a^{-1}ya)\ a(a^{-1}ya)a^{-1} = y.$$

Vậy f_a là một đẳng cấu.

b) Ta sẽ chứng minh với mọi a và b thuộc X có $f_a \cdot f_b = f_{ab}$. Thật vậy, với mọi $x \in X$,

$$f_a \cdot f_b(x) = f_a[f_b(x)] = f_a(bxb^{-1}) = abx(ab)^{-1} = f_{ab}(x).$$

Như vậy, tập hợp các tự đẳng cấu trong của nhóm X là một tập con ổn định của Aut(X). Hơn nữa với mọi $a \in X$ ta có

$$f_{a^{-1}} \cdot f_a = f_{a^{-1}a} = f_e = 1_X.$$

Do đó, tập hợp các tự đẳng cấu trong X là nhóm con của Aut(X).

c) Giả sử H là một nhóm con chuẩn tắc của X và f_a là một tự đẳng cấu trong của X. Ta có $f_a(H) = aHa^{-1} = H$.

Đảo lại, giả sử $f_a(H) = aHa^{-1} = H$ với mọi $a \in X$. Khi đó H là chuẩn tắc (theo định nghĩa).

d) Xét ánh xạ $X \xrightarrow{f} A$

$$a \mapsto f(a) = f_a$$

với A là nhóm các tự đẳng cấu trong của X.

f là đồng cấu vì $f(ab) = f_{ab} = f_a f_b = f(a)f(b)$. Hiển nhiên f là toàn ánh.

Ta có $a \in \text{Kerf} \Leftrightarrow f_a = 1_X \Leftrightarrow axa^{-1} = x$ với mọi $x \in X$

$\Leftrightarrow ax = xa$ với mọi $x \in X \Leftrightarrow a \in C(X)$.

Vậy Kerf = C(X). Theo định lí đồng cấu ta có $\left(X/_{C(X)}\right) \cong A$.

2.70. a) Giả sử cấp của a là m, nghĩa là $a^m = e_X$ và $a^t = e$ thì t chia hết cho m. Khi đó $[f(a)]^m = f(a^m) = f(e_X) = e_Y$. Vậy cấp của f(a) là ước của m.

b) Theo định lí đồng cấu ta có

$$X/_{\text{Kerf}} \cong f(X).$$

Nếu X là hữu hạn thì cấp của $X/_{\text{Kerf}}$ bằng chỉ số của Kerf là một ước của cấp của X. Vậy cấp của f(X) là một ước của cấp của X.

2.71. Ứng dụng bài tập 2.58 và bài tập 2.70.

2.72. a) Giả sử $X = < a >$ là một nhóm xyclic cấp n. Mỗi tự đồng cấu của X cho ta một giá trị xác định của $f(a) \in X$. Đảo lại với mỗi $b \in X$, ánh xạ $f : X \to X$

$$a^k \mapsto b^k, k = 1, 2, ..., n$$

là một tự đồng cấu của X. Như vậy mỗi tự đồng cấu f của X hoàn toàn xác định bởi $f(a) \in X$. Do đó có đúng n tự đồng cấu của X.

b) Mỗi đồng cấu $f : \mathbb{Z}_m \to \mathbb{Z}_n$ cho một giá trị xác định $f(\bar{1}) \in \mathbb{Z}$. Cấp của $f(\bar{1})$ là ước của n. Vì $\bar{1}$ có cấp m nên theo

bài 2.70, cấp của $f(\bar{1})$ là ước của m. Do đó cấp của $f(\bar{1})$ là ước chung của m và n.

Đảo lại, phần tử $\bar{b} \in \mathbb{Z}_n$ có cấp là ước chung của m và n, ánh xạ $\bar{k} \mapsto \overline{kb}$ cho ta một đồng cấu $f : \mathbb{Z}_m \to \mathbb{Z}_n$.

Từ đó suy ra có sáu đồng cấu từ $\mathbb{Z}_6$ đến $\mathbb{Z}_{18}$. Đó là các ánh xạ $f : \mathbb{Z}_6 \to \mathbb{Z}_{18}$ sao cho $f(\bar{1}) = \bar{0}$; $f(\bar{1}) = \bar{3}$; $f(\bar{1}) = \bar{6}$; $f(\bar{1}) = \bar{9}$; $f(\bar{1}) = \overline{12}$; $f(\bar{1}) = \overline{15}$.

c) Theo câu b) ta có sáu đồng cấu từ $\mathbb{Z}_{18}$ đến $\mathbb{Z}_6$, đó là các đồng cấu $f(\bar{1}) = \bar{0}$; $f(\bar{1}) = \bar{2}$; $f(\bar{1}) = \bar{3}$; $f(\bar{1}) = \bar{4}$; $f(\bar{1}) = \bar{5}$; $f(\bar{1}) = \bar{1}$.

2.73. Mỗi số phức thuộc H (nằm trên trục thực hoặc trục ảo) viết dưới dạng lượng giác là

$$r(\cos\frac{k\pi}{2} + i\sin\frac{k\pi}{2}) \text{ với } k \in \mathbb{Z}, r \in \mathbb{R}_+.$$

Vậy $H = \{ r(\cos\frac{k\pi}{2} + i\sin\frac{k\pi}{2}) \mid k \in \mathbb{Z}, r \in \mathbb{R}_+ \}$.

Dễ kiểm nghiệm H là nhóm con của $\mathbb{C}^*$.

Xét ánh xạ $F : \mathbb{C}^* \to U$

$$r(\cos\varphi + i\sin\varphi) \mapsto \cos 4\varphi + i\sin 4\varphi.$$

F là một đồng cấu vì

$$F(r(\cos\varphi + i\sin\varphi).r(\cos\varphi' + i\sin\varphi')) =$$

$$= F(rr'(\cos(\varphi + \varphi') + i\sin(\varphi + \varphi')))$$

$$= (\cos 4(\varphi + \varphi') + i\sin 4(\varphi + \varphi')$$

$$= (\cos 4\varphi + i\sin 4\varphi).(\cos 4\varphi' + i\sin 4\varphi')$$

$$= F(r(\cos\varphi + i\sin\varphi)).F(r(\cos\varphi' + i\sin\varphi')).$$

Với mọi $\cos\varphi + i\sin\varphi \in U$ ta có $\cos\frac{\varphi}{4} + i\sin\frac{\varphi}{4} \in \mathbb{C}^*$ thoả mãn $F(\cos\frac{\varphi}{4} + i\sin\frac{\varphi}{4}) = \cos\varphi + i\sin\varphi$.

Vậy F là toàn cấu.

Ta hãy tìm KerF. Ta có

$$z = r(\cos\varphi + i\sin\varphi) \in \text{KerF} \Leftrightarrow F(z) = \cos 4\varphi + i\sin 4\varphi = 1$$

$$\Leftrightarrow 4\varphi = 2k\pi \Leftrightarrow \varphi = \frac{k\pi}{2} \Leftrightarrow z \in H.$$

Ta suy ra $\mathbb{C}/H \cong U$.

2.74. Xét ánh xạ $G : \mathbb{R} \to U$

$$r \mapsto \cos 2\pi r + i\sin 2\pi r.$$

Dễ kiểm tra được G là một toàn cấu và $\text{Ker}G = \mathbb{Z}$. Suy ra $\mathbb{R}/\mathbb{Z} \cong U$.

2.75. Đặt X_1 là nhóm nhân các ma trận vuông có định thức bằng 1.

X_2 là nhóm nhân các ma trận vuông có định thức bằng ± 1.

X_3 là nhóm nhân các ma trận vuông có định thức dương.

a) Xét ánh xạ $f_1 : X \to \mathbb{R}^*$

$$A \mapsto |A|$$

($|A|$ là định thức của A).

f_1 là một toàn cấu và $\text{Ker}f_1 = X_1$.

b) Xét ánh xạ $f_2 : X \to \mathbb{R}_+$

$$A \mapsto \|A\|$$

($\|A\|$ là giá trị tuyệt đối của định thức của A) từ nhóm nhân các ma trận vuông cấp n không suy biến đến nhóm nhân các số thực dương. f_2 là một toàn cấu và $\text{Ker}f_2 = X_2$.

c) Ta có $Y = \{-1, 1\}$ là một nhóm xyclic với phép nhân thông thường.

Xét ánh xạ $f_3 : X \to Y$

$$f_3(A) = \begin{cases} 1 & \text{nếu } |A| > 0 \\ -1 & \text{nếu } |A| < 0 \end{cases}$$

f_3 là một toàn cấu và $\text{Ker}f_3 = X_3$.

2.76. Xét nhóm cộng các lớp thặng dư theo modun p, với p là một số nguyên tố:

$$\mathbb{Z}_p = \{\bar{0}, \bar{1}, ..., \overline{p-1}\}.$$

Tập hợp, $\mathbb{Z}_p^* = \{\bar{1}, \bar{2}, ..., \overline{p-1}\}$ là một nhóm với phép nhân $\bar{a}.\bar{b} = \overline{ab}$.

Nhóm này có cấp là $p-1$. Do đó mọi phần tử của nó có cấp là ước của $p-1$. Giả sử $a \in \mathbb{Z}$ là một số nguyên tuỳ ý.

Nếu a chia hết cho p thì ta có $a \equiv 0 (\text{mod} p)$ và $a^p \equiv 0 (\text{mod} p)$. Vậy $a^p \equiv a \ (\text{mod} p)$.

Nếu a không chia hết cho p thì $\bar{a} \in \mathbb{Z}_p^*$ do đó $\overline{a^{p-1}} = \bar{1}$, suy ra $a^{p-1} \equiv 1 \pmod{p}$ hay $a^p \equiv a \pmod{p}$.

2.77. a) Với mọi $x \in K = \text{Ker}f$

$fi(x) = f(i(x)) = f(x) = e_Y$. vậy fi là ánh xạ đơn vị từ K vào Y.

b) Vì fg là ánh xạ đơn vị từ G đến Y nên với mỗi $a \in G$,

$$fg(a) = f(g(a)) = e_Y.$$

điều đó chứng tỏ $g(a) \in \text{Ker}f$ hay $g(G) \subset K$.

Khi đó hiển nhiên ta có đồng cấu $\bar{g} : G \to K$

$$a \mapsto \bar{g}(a) = g(a)$$

và $i\bar{g} = g$.

Giả sử $g' : G \to K$ là đồng cấu sao cho $ig' = g = i\bar{g}$. Vì i là đơn cấu nên $g' = \bar{g}$. Vậy $\bar{g}$ được xác định một cách duy nhất.

2.78. Ta có ánh xạ $g : X \to G$

$$x \mapsto g(x) = (g_1(x), g_2(x))$$

(vì $g_1 : X \to G_1$ nên $g_1(x) \in G_1$ và

$g_2 : X \to G_2$ nên $g_2(x) \in G_2$, do đó

$$(g_1(x), g_2(x)) \in G = G_1 \times G_2.$$

Với mọi $x, y \in X$, có

$g(x.y) = (g_1(x.y), g_2(x.y)) = (g_1(x).g_1(y), g_2(x).g_2(y)) =$

$= (g_1(x), g_2(x).(g_1(y), g_2(y)) = g(x)\, g(y)$

suy ra g là đồng cấu.

Với mọi $x \in X$, có

$$p_1g(x) = p_1(g(x)) = p_1(g_1(x), g_2(x)) = g_1(x).$$

Tương tự $p_2g(x) = g_2(x)$. Vậy ta có $p_1g = g_1$ và $p_2g = g_2$.

Giả sử có $g' : X \to G$ sao cho $p_1g' = p_1g$ và $p_2g' = p_2g$.

Từ đó suy ra $g'(x) = (a_1, a_2) = (g_1(x), g_2(x)) = g(x)$ hay $g' = g$.

2.79. Vì $h_1 : G_1 \to Y$ và $h_2 : G_2 \to Y$ nên với mọi cặp $(x_1, x_2) \in G$ tổng $h_1(x_1) + h_2(x_2) \in Y$.

Khi đó ta có ánh xạ $h : G \to Y$

$$(x_1, x_2) \mapsto h_1(x_1) + h_2(x_2).$$

Với mọi $(x_1, x_2) \in G$, $(x'_1, x'_2) \in G$

$$h((x_1, x_2) + (x'_1, x'_2)) = h((x_1 + x'_1, x_2 + x'_2))$$

$$= h_1(x_1 + x'_1) + h_2(x_2 + x'_2)$$

$$= [h_1(x_1) + h_1(x'_1)] + [h_1(x_2) + h_2(x'_2)]$$

$$= [h_1(x_1) + h_2(x_2)] + [h_1(x'_1) + h_2(x'_2)] \text{ (vì Y là Aben)}$$

$$= h((x_1, x_2)) + h((x'_1, x'_2)).$$

Vậy h là một đồng cấu. Với mọi $x_1 \in G$,

$$hq_1(x_1) = h(q_1(x_1)) = h((x_1, 0)) = h_1(x_1) + h_2(0)$$

$$= h_1(x_1) + 0 = h_1(x_1).$$

Vậy $hq_1 = h_1$. Tương tự, chứng minh được $hq_2 = h_2$. Giả sử có $h' : G \to Y$ sao cho $h'q_1 = hq_1$ và $h'q_2 = hq_2$. Từ đó suy ra

$$h'(x_1, x_2) = h'((x_1, 0) + (0, x_2)) = h'(x_1, 0) + h'(0, x_2)$$

$$= h_1(x) + h_2(x) = h(x_1, x_2),$$

nghĩa là $h' = h$.

2.80. Ta hãy chứng minh a) $\Rightarrow$ b).

Giả sử tồn tại một đồng cấu h : H $\to$ K sao cho g = hf. Nếu $x \in G$ sao cho $f(x) = e_H$ như vậy $g(x) = hf(x) = h(f(x)) = h(e_H) = e_K$, nghĩa là Kerf $\subset$ Kerg.

Đảo lại, giả sử Kerf $\subset$ Kerg. Vì f là toàn ánh nên với mỗi $y \in H$ tồn tại $x \in G$ sao cho f(x) = y. Khi đó ta có tương ứng h từ H đến K cho bởi quy tắc h(y) = g(x), với f(x) = y. Quy tắc h là một ánh xạ vì nếu có x_1 và x_2 thuộc G sao cho

$$f(x_1) = f(x_2)$$

nghĩa là $f(x_1x_2^{-1}) = e_H$ hay $x_1x_2^{-1} \in$ Kerf $\subset$ Kerg, thì

$$g(x_1x_2^{-1}) = e_K \text{ hay } g(x_1) = g(x_2);$$

h là đồng cấu vì $h(y_1y_2) = g(x_1x_2)$ với

$$(f(x_1) = y_1, f(x_2) = y_2) = g(x_1)g(x_2) = h(y_1)h(y_2).$$

Do cách xây dựng h, ta có g = hf.

c) Tính chất duy nhất của h được suy ra từ tính chất f là toàn cấu.

d) Ta hãy tìm Kerh. Ta có

$$\text{Kerh} = \{y \in H \mid h(y) = e_K\}$$
$$= \{f(x) \mid hf(x) = g(x) = e_K\} = f(\text{Kerg}).$$

Vậy nếu h là đơn cấu thì Kerh = f(Kerg) = $\{e_H\}$, suy ra Kerg $\subseteq$ Kerf. Vậy Kerg = Kerf.

Đảo lại nếu Kerg = Kerf thì Kerh = $\{e_H\}$, do đó h là đơn cấu.

e) Ta có Imh = hf(G) = g(G).

Vậy h(H) = Imh = K $\Leftrightarrow$ g(G) = K hay h là toàn ánh khi và chỉ khi g là toàn ánh.

2.81. a) Giả sử a và b thuộc X, $a \neq b$. Khi đó với G là một nhóm nhiều hơn một phần tử và ta có ánh xạ $g : X \to G$ sao cho $g(a) \neq g(b)$. Ánh xạ $\bar{g} : F \to G$ thoả mãn $g = \bar{g} f$ suy ra

$$g(a) = \bar{g} f(a) = \bar{g}(f(a))$$

$$g(b) = \bar{g} f(b) = \bar{g}(f(b)).$$

Vì $g(a) \neq g(b)$ nên $\bar{g}(f(a)) \neq \bar{g}(f(b))$ hay $f(a) \neq f(b)$.

Vậy f là một đơn ánh.

b) Giả sử G là nhóm con của F, sinh ra bởi f(X). $G = \langle f(x) \rangle$.

Ánh xạ $g : X \to G$

$$x \mapsto f(x)$$

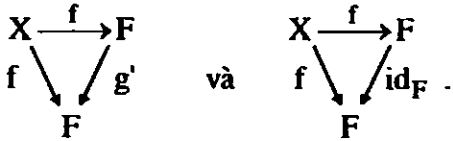
"cảm sinh" một ánh xạ $\bar{i} : F \to G$ sao cho $g = \bar{g}.f$.

Mặt khác ta có ánh xạ $i: G \to F$

$$x \mapsto x$$

là một đơn cấu suy ra ánh xạ $g' = ig: F \to F$.

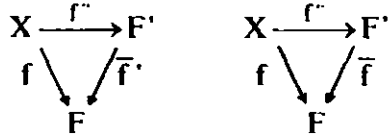
Ngoài ra $id_F : F \to F$ là ánh xạ đồng nhất của F cho ta các biểu đồ sau giao hoán



Tức là ta có $g'f = f = id_F f$. Suy ra $g' = id_F$.

Vậy $F = G = \langle f(x) \rangle$.

b) Giả sử (F, f) và (F ', f ') đều là các nhóm tự do trên tập X. Khi đó ta có các ánh xạ $\bar{f} : F' \to F$ và $\bar{f}' : F \to F'$ là những đồng cấu sao cho các tam giác sau giao hoán:



Tức là $f = \bar{f}'f'$ hay $\bar{f}'.f' = id_F$

và $f' = \bar{f}f$ hay $\bar{f}f = id_{F'}$.

Suy ra $\bar{f}$ và $\bar{f}'$ là những đẳng cấu. Vậy $F \cong F'$.

2.82. Đặt F bao gồm các tích hình thức (gọi là các từ)

$$u = a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_n^{\varepsilon_n},$$

trong đó $a_i \in X$, $\varepsilon_i = \pm 1$, $i = 1, 2, \dots, n$ và không có hai nhân tử nào kề nhau có dạng a^1 và a^{-1} hoặc a^{-1} và a^1, kí hiệu e là tích rỗng.

Nếu u và v thuộc F, ta định nghĩa tích uv như sau:

$uv = u$ nếu $v = e$.

$uv = v$ nếu $u = e$.

Nếu $u \neq e$, $v \neq e$ thì uv được xác định bằng cách "ghép" hai từ u và v với nhau rồi giản ước tất cả các cặp có dạng $a^{-1}a^1$ hoặc a^1a^{-1}.

Với phép toán như vậy, F là một nhóm. Cùng với ánh xạ

$$f : X \to F$$

$$a \mapsto a^{-1}$$

F là nhóm tự do trên tập X.

2.83. a) nếu $X = \varnothing$ thì nhóm tự do trên tập X chính là nhóm đơn vị, đó là $F = \{0\}$ và $f: \varnothing \to F$ là ánh xạ rỗng.

b) Nếu $X = \{a\}$ thì $F = \{a^n \mid n \in \mathbb{Z}\}$ và $f : \{a\} \to F$

$$a \mapsto a^1.$$

Trong trường hợp này X là một nhóm xyclic có cấp vô hạn.

c) Nếu $x = \{a, b\}$ thì

$$F = \{a^{m_1}b^{n_1}a^{m_2}b^{n_2}...a^{m_k}b^{n_k} \mid m_i \in \mathbb{Z}, n_i \in \mathbb{Z}, c = 1, ..., k\}.$$

$$\begin{aligned} f : X &\to F \\ a &\mapsto a^1 \\ b &\mapsto b^1. \end{aligned}$$

2.84. Theo bài 2.82. Nhóm tự do trên tập $X = \{a\}$ là một nhóm xyclic có cấp vô hạn nên $X \cong \mathbb{Z}$.

2.85. Cho G là một nhóm tuỳ ý. Gọi (F, f) là nhóm tự do sinh bởi tập G. Với ánh xạ đồng nhất của G là $id_G : G \to G$ tồn tại duy nhất đồng cấu $h : F \to G$ sao cho $id_G = hf$. Vì id_G là toàn ánh nên h là toàn cấu, vì vậy $G = h(F)$. Theo định lí đồng cấu ta có $G \cong H/\text{Ker}h$.

2.86. Làm tương tự bài 2.81.

2.87. Đặt $F = \{(a_i)_{i \in X} \in \mathbb{Z}^X \mid (a_i)_{i \in X}$ có giá hữu hạn$\}$.

Trong F ta định nghĩa phép cộng như sau :

Với mọi u và v thuộc F,

$$u = (a_i)_{i \in X}, v = (b_i)_{i \in X}, u + v = ((a_i + b_i)_{i \in X}.$$

Với phép toán này F là một nhóm Aben.

Cùng với ánh xạ $f : X \to F$

$$x \mapsto (a_i)_{i \in X} \text{ với } a_i = \begin{cases} 0 & \text{nếu } i \neq x \\ 1 & \text{nếu } i = x \end{cases}$$

F là một nhóm tự do.

Thật vậy, giả sử g: X $\to$ A là một ánh xạ tuỳ ý từ X đến nhóm Aben A. Khi đó ta có ánh xạ $\bar{g}: F \to A$

$$(a_i)_{i\in X} \mapsto \sum_{i\in X} a_i(g_{(i)}).$$

(Tổng $\sum_{i\in X} a_i(g_{(i)})$ có nghĩa vì chỉ có hữu hạn a_i khác 0).

$\bar{g}$ là một đẳng cấu và thoả mãn $\bar{g}f = g$.

Do tính chất f là đơn ánh nên suy ra $\bar{g}$ là duy nhất thoả mãn đẳng thức trên. Vậy (F, f) là nhóm Aben tự do trên tập X.

(Có thể chứng minh điều này dựa vào bài 2.82 và bài 2.90).

2.88. Theo kết quả bài 2.87 ta có

a) Khi X = {a} thì $F \cong \mathbb{Z}^1 = \mathbb{Z}$.

b) Khi $X = \{a_1, a_2, ..., a_n\}$ thì $F \cong \mathbb{Z}^n$.

c) Khi X tuỳ ý ta có F đẳng cấu với một nhóm con của $\mathbb{Z}^X$.

2.89. a) Giả sử A là một nhóm Aben đã cho. Đặt (F, f) là nhóm Aben tự do trên tập A. Khi đó ánh xạ $id_A : A \to A$ cảm sinh một đồng cấu h: F $\to$ A, h còn là một toàn cấu và do đó $F/\text{Ker}h \cong A$.

b) Chứng minh dựa vào bài 2.87.

2.90. Giả sử (F, f) là một nhóm tự do trên tập X; [F, F] là nhóm con hoán tử của F và p: $F \to F/[F, F]$ là phép chiếu chính tắc.

Đặt $j = pf : X \to F/[F, F]$, khi đó ta có $F/[F, F]$ cùng với ánh xạ j là một nhóm Aben tự do trên tập X.

CHƯƠNG III. VÀNH VÀ TRƯỜNG

3.1. a) Chỉ cần chứng minh

$$A = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\right\}$$

là một vành con của vành các số thực $\mathbb{R}$.

Có $n \in \mathbb{Z}, n = n + 0\sqrt{2} \in A$. Vậy $\mathbb{Z} \subset A$ nên $A \neq \varnothing$.

Giả sử $a + b\sqrt{2}$, $c + d\sqrt{2} \in A$.

$$\left(a + b\sqrt{2}\right) - \left(c + d\sqrt{2}\right) = (a - c) + (b - d)\sqrt{2} \in A;$$

$$\left(a + b\sqrt{2}\right)\left(c + d\sqrt{2}\right) = (ac + 2bd) + (ad + bc)\sqrt{2} \in A.$$

Vậy A là một vành con của $\mathbb{R}$. Vì $\mathbb{R}$ là giao hoán nên A cũng giao hoán. Đơn vị của A là $1 + 0.\sqrt{2}$.

b) Chứng minh tương tự câu a).

3.2. Tổng và hiệu của hai ma trận vuông cấp n với các phần tử là những số nguyên là một ma trận vuông cấp n với các phần tử là những số nguyên. Tích của hai ma trận vuông cấp n với các phần tử nguyên là một ma trận vuông cấp n với các phần tử nguyên. Do đó tập hợp các ma trận vuông cấp n với các phần tử là những số nguyên là một vành con của vành các ma trận vuông cấp n.

3.3. Chứng minh tương tự như bài 3.2

3.4. Chứng minh dựa vào định nghĩa của vành.

3.5. Chứng minh dựa vào định nghĩa của vành.

3.6. Xem chứng minh bài 2.75 (chương II).

3.7. Vành số nguyên $\mathbb{Z}$ có đặc số 0, vì với mọi $n > 0$ có $n.1 = n > 0$.

Tương tự với các trường số hữu tỉ $\mathbb{Q}$, trường số thực $\mathbb{R}$ và trường số phức $\mathbb{C}$ ta đều có $\forall n > 0, n.1 = n > 0$.

3.8. Giả sử F_n là trường hữu hạn gồm n phần tử. Khi đó nhóm cộng F_n có cấp là n. Do $1 \in F_n$ nên cấp của 1 là một ước của n. Vậy F_n có đặc số khác 0.

3.9. Giả sử X là một miền nguyên, có đặc số $m \neq 0$ và $m > 1$. Nếu m không là số nguyên tố thì $m = pq$, trong đó p và q là hai số nguyên lớn hơn 1. Do đó $me = (pq)e = (pe)(qe) = 0$ (e là đơn vị của x).

Vì p và q đều bé hơn m nên $pe \neq 0$ và $qe \neq 0$. Như vậy X có ước của không, trái với giả thiết. Vậy m phải là số nguyên tố.

3.10. Giả sử X là một trường tuỳ ý. Xét ánh xạ φ sau đây:

$$\varphi : \mathbb{Z} \to X$$
$$n \mapsto n.1$$

($\mathbb{Z}$ là vành số nguyên, 1 là đơn vị của trường X).

φ là một đồng cấu vì:

$\forall m, n \in \mathbb{Z}, \varphi(m + n) = (m + r).1 = m.1 + n.1 = \varphi(m) + \varphi(n)$

và $\varphi(mn) = (mn) = m.1.n.1 = \varphi(m)\varphi(n)$.

– Nếu X có đặc số 0 thì φ còn là một đơn cấu, do đó X chứa vành con $\varphi(\mathbb{Z})$ đẳng cấu với $\mathbb{Z}$. Từ đó suy ra X chứa một trường con đẳng cấu với trường số hữu tỉ $\mathbb{Q}$.

– Nếu X có đặc số $p \neq 0$ thì p là một số nguyên tố (theo bài 3.9). Trong trường hợp này $\text{Ker}\varphi = p\mathbb{Z}$. Mặt khác, p là số nguyên tố nên $\mathbb{Z}_p$ là một trường. Theo định lí đồng cấu, X chứa một vành con là $\varphi(\mathbb{Z})$ đẳng cấu với $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$.

3.11. Để chứng minh X là một vành ta chỉ còn phải chứng minh phép cộng trong X là giao hoán.

Với mọi $x, y \in Y$ ta có

$$(x + y).(1 + 1) = (x + y).1 + (x + y).1 = x + y + x + y.$$

Mặt khác ta có

$$(x + y)(1 + 1) = x(1 + 1) + y(1 + 1) = x + x + y + y$$

do đó $x + y + x + y = x + x + y + y$.

Giản ước bên trái cho x và bên phải cho y ta được

$$y + x = x + y.$$

Suy ra phép cộng là giao hoán.

Vậy đối với một vành có đơn vị tiên đề về tính giao hoán của phép cộng được suy ra từ các tiên đề khác.

3.12. Các ước của $\bar{0}$ trong vành $\mathbb{Z}/6\mathbb{Z}$ là $\bar{2}$, $\bar{4}$ và $\bar{3}$ vì

$$\bar{2}.\bar{3} = \bar{0},\ \bar{4}.\bar{3} = \bar{0}.$$

3.13. Giả sử $\mathbb{Z}/n\mathbb{Z}\ (n \neq 0)$ là một miền nguyên do đó $n \neq \pm 1$.

Vì $n\mathbb{Z} = -n\mathbb{Z}$ nên ta có thể lấy $n > 0$. Nếu n không phải là một số nguyên tố thì có hai số nguyên p_1 và p_2 khác 1 sao cho $n = p_1p_2$.

Như vậy $\bar{0} = \bar{p}_1 \bar{p}_2$ mà $\bar{p}_1 \neq \bar{0}$ và $\bar{p}_2 \neq \bar{0}$, điều đó chứng tỏ $\mathbb{Z}/n\mathbb{Z}$ có ước của $\bar{0}$, trái với giả thiết $\mathbb{Z}/n\mathbb{Z}$ là một miền nguyên.

Đảo lại, nếu n là một số nguyên tố thì $\mathbb{Z}/n\mathbb{Z}$ là một miền nguyên, hơn nữa ta còn chứng minh được nó là một trường. Giả sử $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$, $\bar{a} \neq \bar{0}$, như vậy a không chia hết cho n. Vì n nguyên tố nên a và n nguyên tố cùng nhau do đó tồn tại u và v thuộc $\mathbb{Z}$ sao cho $au + nv = 1$.

Suy ra

$$\overline{au + nv} = \bar{1} \text{ hay } \bar{a}\bar{u} + \bar{n}\bar{v} = \bar{1} \text{ hay } \bar{a}\bar{u} = 1.$$

Chứng tỏ $\bar{u}$ là nghịch đảo của $\bar{a}$.

3.14. Ta có

$$[(a_1, b_1) + (a_2, b_2)] + (a_3, b_3) = (a_1 + a_2, b_1 + b_2) + (a_3, b_3)$$
$$= ((a_1 + a_2) + a_3, (b_1 + b_2) + b_3) = (a_1 + (a_2 + a_3), b_1 + (b_2 + b_3))$$
$$= (a_1, b_1) + (a_2 + a_3, b_2 + b_3) = (a_1, b_1) + [(a_2, b_2) + (a_3, b_3)].$$

Chứng tỏ phép cộng là kết hợp.

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$
$$= (a_2 + a_1, b_2 + b_1) = (a_2, b_2) + (a_1, b_1).$$

Vậy phép cộng là giao hoán.

Phần tử không là (0, 0) vì

$$(0, 0) + (a, b) = (0 + a, 0 + b) = (a, b);$$

tương tự (a, b) + (0, 0) = (a, b);

$(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$

$= (a_2a_1, b_2b_1) = (a_2, b_2)(a_1, b_1).$

Vậy phép nhân là giao hoán.

$[(a_1, b_1)(a_2, b_2)](a_3, b_3) = (a_1a_2, b_1b_2)(a_3b_3)$

$= ((a_1a_2)a_3, (b_1b_2)b_3) = (a_1(a_2a_3), b_1(b_2b_3))$

$= (a_1, b_1)(a_2a_3, b_2b_3) = (a_1, b_1)[(a_2, b_2)(a_3, b_3)].$

Vậy phép nhân là kết hợp.

$(a_1, b_1)[(a_2, b_2) + (a_3, b_3)] =$

$= (a_1, b_1)(a_2 + a_3, b_2 + b_3)(a_1(a_2 + a_3), b_1(b_2 + b_3)) =$

$= (a_1a_2 + a_1a_3, b_1b_2 + b_1b_3) =$

$= (a_1a_2, b_1b_2) + (a_1a_3, b_1b_3) =$

$= (a_1, b_1)(a_2, b_2) + (a_1, b_1)(a_3, b_3).$

Vậy phép nhân phân phối đối với phép cộng.

Phần tử đơn vị là (1, 1) vì (1, 1)(a, b) = (1.a, 1.b) = (a, b).

Các ước của không trong vành $X = \mathbb{Z} \times \mathbb{Z}$ là

$$A = \{(0,b) \mid b \in \mathbb{Z}\} \cup \{(a,0) \mid a \in \mathbb{Z}\}.$$

3.15. a) Với mọi $x \in X$ ta có

$$-x = (-x)^2 = x^2 = x.$$

b) Với mọi $x, y \in X$ ta có

$$x + y = (x + y)^2 = x^2 + xy + yx + y^2$$

$$= x + y + xy + yx,$$

hay $xy + yx = 0$ suy ra $xy = yx$. Vậy X là vành giao hoán.

c) Giả sử $x \in X$ sao cho $x \neq 0$ và $y \in X$ là một phần tử tuỳ ý ta có $xy = x^2y = x(xy)$. Vì X không có ước của không nên ta có thể giản ước cho x ở đẳng thức trên và ta được $xy = y$.

Vậy x là phần tử đơn vị của X. Trong trường hợp này vành X chỉ có hai phần tử là 0 và đơn vị e.

3.16. Các vành đã cho trong các bài tập 3.1 , 3.2, 3.3 không vành nào là vành con của vành còn lại.

3.17. Giả sử A và B là hai iđêan của một vành X.

Đặt $C = A + B = \{a + b \mid a \in A, b \in B\}$.

$C \neq \emptyset$ vì $0 \in A$ và $0 \in B$ nên $0 = 0 + 0 \in A + B$.

Giả sử $c_1 = a_1 + b_1 \in C$ và $c_2 = a_2 + b_2 \in C$.

Khi đó $c_1 - c_2 = (a_1 - a_2) + (b_1 - b_2) \in C$.

Giả sử $x \in X$, ta có

$$x(a_1 + b_1) = xa_1 + xb_1 \in C$$

và $(a_1 + b_1)x = a_1x + b_1x \in C$.

Vậy C là một iđêan của X.

3.18. Giả sử $A = \{x \in X \mid nx = 0\}$.

Ta có $n.0 = 0$ nên $0 \in A$, vậy $A \neq \emptyset$.

Giả sử $x_1, x_2 \in X$, mà $nx_1 = 0$ và $nx_2 = 0$, suy ra

$$n(x_1 - x_2) = nx_1 - nx_2 = 0,$$

vậy $x_1 - x_2 \in A$.

Giả sử $x \in X$ và $a \in A$ ta có $na = 0$.

Từ đó $n(xa) = x(na) = x.0 = 0$, $n(ax) = (na)x = 0x = 0$.

Suy ra $ax \in A$ và $xa \in A$.

Vậy A là một iđêan của X.

3.19. Với $aX = \{ax \mid x \in X\}$, ta có $0 = a.0 \in aX$. Vậy $aX \neq \varnothing$. Giả sử $ax_1, ax_2 \in aX$ và $x \in X$ ta có

$$ax_1 - ax_2 = a(x_1 - x_2) \in aX$$

$$(ax_1)x = a(x_1x) \in aX.$$

Vậy aX là iđêan phải của X.

Tương tự có Xa là iđêan trái của X.

3.20. a) Rõ ràng $0 \in I J$.

Giả sử $u = \sum_{i=1}^{n} a_i b_i \in I J$ và $v = \sum_{j=1}^{m} a'_j b'_j \in I J$.

Khi đó

$$u - v = \sum_{a_i=1}^{n} a_i b_i - \sum_{j=1}^{m} a'_i b'_i = \sum_{i=1}^{n} a_i b_i + \sum_{j=1}^{m} \left(-a'_j\right) b_j \in I J.$$

Với $x \in X$ ta có

$$xu = x\sum_{i=1}^{n} a_i b_i = \sum_{i=1}^{n} x\left(a_i b_i\right) = \sum_{i=1}^{n} \left(xa_i\right) b_i \in I J.$$

Vậy I J là một iđêan của X.

b) Ta luôn có $I J \subset I$ và $I J \subset J$ nên $I J \subset I \cap J$.

Bây giờ giả sử $a \in I \cap J$, vì $I + J = X$ và $1 \in X$ nên $1 = u + v$ với $u \in I$. $v \in J$.

Từ đó suy ra $a = a.1 = a(u + v) = au + av. \in I J$.

Vậy ta có $I J = I \cap J$.

3.21. Giả sử m và n là hai số nguyên tố cùng nhau. Khi đó tồn tại hai số nguyên u, v sao cho $mu + nv = 1$. Do đó $1 \in m\mathbb{Z} + n\mathbb{Z}$.

Vậy $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$. Đảo lại. nếu $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$ thì

$$1 \in m\mathbb{Z} + n\mathbb{Z} \text{ hay } 1 = mu + nv, \text{ với u và v thuộc } \mathbb{Z}.$$

Vậy m và n nguyên tố cùng nhau.

3.22. a) Chứng minh theo định nghĩa đồng cấu.

b) Giả sử p là toàn cấu. Khi đó với mỗi x thuộc X thì

$(x + I, (1-x) + J) \in \left(X/I\right) \times \left(X/J\right)$ nên tồn tại $a \in X$ sao cho

$$p(a) = (x + I, (1-x) + J)$$

$$\text{hay } (x + J), (1 + x) + J) = (a + I, a + J).$$

Từ đó suy ra $a + I = x + I$ và $a + J = (1 + x) + J$, do đó

$$a - x + u \in I \text{ và } (1 + x) - a = 1 - (a - x) = 1 - u = v \in J.$$

Vậy $1 = u + v \in I + J$. Vậy $X = I + J$.

Đảo lại, nếu $I + J = X$ thì $1 = u + v$ với $u \in I$ và $v \in J$. Giả sử $(a + I, b + J)$ là phần tử tuỳ ý của $I + J$. Đặt $x = va + ub \in X$. Khi đó ta có $p(x) = (a + I, b + J)$. Vậy p là một toàn cấu.

3.23. Gọi n là cấp của phần tử đơn vị e của vành X, nghĩa là n là số nguyên dương bé nhất cho cho $ne = 0$.

a) Nếu n là hợp số, nghĩa là $n = n_1n_2$ với $0 < n_1, n_2 < n$ thì $ne = n_1e\ n_2e = 0$. Như vậy, vì X là miền nguyên, nên $n_1e = 0$ hoặc $n_2e = 0$ trái với giả thiết về n. Vậy n phải là một số nguyên tố. (Đương nhiên $n \neq 1$ vì nếu $n = 1$ thì $1e = e = 0$, X không phải là một miền nguyên).

b) Với mọi x ta có $x = ex$, do đó $nx = n(ex) = (ne)x = 0$.

Vậy cấp của x là ước của n. Vì n nguyên tố nên cấp của x bằng n.

c) $mX = \{mx \mid x \in X\} \neq \varnothing$ vì $0 = m0 \in mX$.

Giả sử $x \in X$, mx_1 và $mx_2 \in mX$, ta có

$$mx_1 - mx_2 = m(x_1 - x_2) \in mX,$$

$$x(mx_1) = m(xx_1) \in mX$$

và $(mx_1)x = m(x_1x) \in mX$.

Vậy mX là một iđêan của X.

d) Ta hãy xác định mX.

– Nếu m chia hết cho n thì $m = nq$, $q \in \mathbb{Z}$

$$mX = \{mx = n(qx) = 0\}.$$

Vậy $mX = \{0\}$.

– Nếu m không chia hết cho n thì m và n nguyên tố cùng nhau, do đó có u, $v \in \mathbb{Z}$ sao cho $nu + mv = 1$.

Vậy với mọi $x \in X$ có

$$x = 1x = (nu + mv)x = n(ux) + m(vx) = m(vx) \in mX,$$

do đó $mX = X$.

Tóm lại

– Nếu m chia hết cho n thì $X/mX = X/\{0\} \cong X$.

– Nếu m không chia hết cho n thì $X/mX = X/X \cong \{0\}$.

3.24. a) Giả sử P là một iđêan nguyên tố của một vành X; $X/P = \{x + P \mid x \in X\}$ là vành thương của vành X trên P. Vì P nguyên tố nên $P \neq X$ do đó X/P có nhiều hơn một phần tử. Đơn vị của X/P là $e + P$ với e là đơn vị của X. Do X là vành

giao hoán nên X/P cũng là vành giao hoán. Bây giờ giả sử $x + P$ và $y + P$ là hai phần tử tuỳ ý của X/P nếu

$$(x + P)(y + P) = 0 + P = P$$

thì $xy + P = P$ hay $xy \in P$. Vì P là nguyên tố nên hoặc $x \in P$ suy ra $x + P = P = 0 + P$ hoặc $y \in P$ suy ra $y + P = P = 0 + P$.

Vậy X/P không có ước của không, do đó X/P là một miền nguyên.

Giả sử X/P là một miền nguyên. Khi đó X/P có nhiều hơn một phần tử, do đó $P \neq X$. Giả sử x, y là hai phần tử thuộc X sao cho $xy \in P$ như vậy $xy + P = (x + P)(y + P) = P = 0 + P$.

Vì X/P không có ước của $\bar{0}$ nên suy ra hoặc $x + P = P$ hay $x \in P$ hoặc $y + P = P$ hay $y \in P$. Vậy P là iđêan nguyên tố.

b) Giả sử X/A là một trường khi đó X/A có nhiều hơn một phần tử do đó $A \neq X$. Giả sử I là một iđêan của X sao cho $I \supset A$ như vậy có một phần tử $x_0 \in I - A$. Ta xét

$$x_0 + A \in X/A.$$

Vì $x_0 \notin A$ nên $x_0 + A$ khả nghịch, nghĩa là có một phần tử $x'_0 + A$ sao cho $(x'_0 + A)(x_0 + A) = x'_0x_0 + A = e + A$, hay $e = x'_0x_0 + a$, $a \in A$. Vì $x_0 \in I$ và $e \in A \subset I$ nên $e \in I$ do đó $I = X$. Vậy A là iđêan tối đại của X.

Đảo lại, giả sử A là iđêan tối đại của X thì $A \neq X$ do đó X/A có nhiều hơn một phần tử. Vì X là một vành giao hoán có đơn

vị nên X/A cũng là một vành giao hoán có đơn vị. Bây giờ giả sử $x + A$ là một phần tử khác không hay $x + A \neq A$, vậy $x \notin A$. Xét iđêan I của X mà $I = A + xX$. Khi đó $I \supset A$ và $x \in I$. Vì A là tối đại nên $I = X$ suy ra $e \in I$.

Do đó $e = a + xx_1$ với $a \in A$ và $x_1 \in X$ hay

$$e + A = (a + xx_1) + A = xx_1 + A = (x + A)(x_1 + A).$$

Điều đó chứng tỏ $x_1 + A$ là nghịch đảo của $x + A$. Do đó X/A là một trường.

Từ hai kết quả trên ta có nhận xét :

Mọi iđêan tối đại đều là iđêan nguyên tố.

3.25. a) Trước hết ta có $0 = f(0) \in f(I)$.

Giả sử $a', b' \in f(I)$ khi đó tồn tại $a, b \in Y$ sao cho $f(a) = a'$, $f(b) = b'$. Như vậy $a' - b' = f(a) - f(b) = f(a - b) \in I$.

Giả sử $a' \in f(I)$, $y \in Y$, $a' = f(a)$, $a \in I$. Vì f là toàn cấu nên $\exists x \in X$ sao cho $f(x) = y$. Khi đó $a'y = f(a)f(x) = f(ax) \in I$.

Vậy f(I) là một iđêan của Y.

Nếu f không là toàn cấu thì khẳng định trên không còn đúng. Chẳng hạn $f : \mathbb{Z} \to \mathbb{Q}$

$$n \mapsto n$$

là ánh xạ nhúng tự nhiên từ vành số nguyên $\mathbb{Z}$ vào trường số hữu tỉ $\mathbb{Q}$. Tuy nhiên $\mathbb{Z}$ là iđêan của $\mathbb{Z}$ nhưng $f(\mathbb{Z})$ không là iđêan của $\mathbb{Q}$.

b) Ta đã biết nếu P là iđêan của Y thì $f^{-1}(P)$ là một iđêan của X. Giả sử hai phần tử x_1, x_2 thuộc X sao cho

$x_1x_2 \in f^{-1}(P)$ như vậy ta có $f(x_1x_2) \in P$ hay $f(x_1)f(x_2) \in P$. Vì P là idêan nguyên tố nên hoặc $f(x_1) \in P$ hoặc $f(x_2) \in P$. Nếu $f(x_1) \in P$ thì $x_1 \in f^{-1}(P)$, nếu $f(x_2) \in P$ thì $x_2 \in f^{-1}(P)$. Vậy $f^{-1}(P)$ là idêan nguyên tố của X.

Nếu P là idêan tối đại của Y thì không thể kết luận $f^{-1}(P)$ là idêan tối đại của X. Chẳng hạn, $f : \mathbb{Z} \to \mathbb{Q}$

$$n \mapsto n$$

là phép nhúng tự nhiên từ vành $\mathbb{Z}$ vào $\mathbb{Q}$. Tuy nhiên $\{0\}$ là idêan tối đại của $\mathbb{Q}$ nhưng $f^{-1}(0) = \{0\}$ không là idêan tối đại của $\mathbb{Z}$.

3.26. Đặt $\sum$ là tập hợp tất cả các idêan thực sự của X, chứa I. Khi đó $\sum \neq \varnothing$ vì $I \in \sum$. Theo Bổ đề Zorn, $\sum$ có phần tử tối đại là M. M chính là idêan tối đại của X chứa I. ($\sum$ được sắp thứ tự theo quan hệ bao hàm).

3.27. Áp dụng bài 3.26 với $I = \dot{X}a$.

3.28. $(i) \Rightarrow (ii)$. Giả sử X chỉ có một idêan tối đại duy nhất là M. Khi đó idêan M là tập các phần tử không khả nghịch của M (Áp dụng bài 3.26).

$(ii) \Rightarrow (i)$ Giả sử tập M các phần tử không khả nghịch của X là một idêan của X. Rõ ràng M là idêan tối đại của X. Giả sử M' là một idêan tối đại bất kì của X khi đó (theo bài 3.26) $M' \subset M$. Vậy suy ra $M' = M$ tức là X chỉ có một idêan tối đại duy nhất.

3.29. a) $N(X)=\left\{x\in X \mid \exists n\in \mathbb{N}^*.nx=0\right\}$ là một iđêan của X vì

$$0=1.0\Rightarrow 0\in N(X).$$

Giả sử a, $b\in N(X)$. Khi đó $\exists n,m\in N^*$ sao cho ma = 0, nb = 0 khi đó mn(a–b) = 0 tức là $a-b\in N(X)$.

Giả sử $x\in X$, $a\in N(X)$, khi đó $\exists m\in N^*$ sao cho ma = 0 suy ra m(ax) = (ma)x = 0 do đó $ax\in N(X)$.

b) Giả sử $a\in N(X)$, khi đó $\exists n\geq 1$ sao cho $a^n=0\in P$ với mọi iđêan nguyên tố P của X. Vì P là iđêan nguyên tố nên suy ra $a\in P$. Vậy N(X) là tập con của giao của tất cả các iđêan nguyên tố của X. Đảo lại, nếu $a\notin N(X)$ ta có một iđêan nguyên tố P_0 mà $a\notin P_0$.

Đặt $S=\left\{a^n \mid n\geq 0\right\}$ và gọi $\sum$ là tập các iđêan của X mà không giao với S. Vì $a\in N(X)$ nên $a^n\neq 0$, $\forall n\geq 1$ nên $\{0\}\in\sum$. Vậy $\sum\neq\varnothing$ Theo bổ đề Zorn ($\sum$ được sắp thứ tự theo quan hệ bao hàm), $\sum$ có phần tử tối đại là P_0. Ta có thể chứng minh được P_0 là một iđêan nguyên tố của X và $a\notin P_0$. Vậy N(X) là giao của họ tất cả các iđêan nguyên tố của X.

3.30. Hiển nhiên.

3.31. Trước hết ta có các ánh xạ $0:\mathbb{Z}\to\mathbb{Z}$ và $1_{\mathbb{Z}}:\mathbb{Z}\to\mathbb{Z}$

$$n\mapsto 0 \qquad\qquad n\mapsto n$$

là hai tự đồng cấu của vành số nguyên $\mathbb{Z}$.

Giả sử $f:\mathbb{Z}\to\mathbb{Z}$ là một tự đồng cấu của $\mathbb{Z}$ và $f\neq 0$. Như vậy tồn tại $a\in\mathbb{Z}$ sao cho $f(a)\neq 0$.

Mặt khác ta có $f(a) = f(a.1) = f(a)f(1)$. Vì $f(a)\neq 0$ nên suy ra $f(1) = 1$. Với n là một số nguyên tuỳ ý $f(n) = nf(1) = n$. Vậy $f = 1_{\mathbb{Z}}$.

Do đó tập hợp các tự đồng cấu của $\mathbb{Z}$ là $\{0, 1_{\mathbb{Z}}\}$.

3.32. Làm tương tự như bài 3.31. Giả sử $f:\mathbb{Z}\left[\sqrt{2}\right]\to\mathbb{Z}\left[\sqrt{2}\right]$ là một tự đồng cấu của vành $\mathbb{Z}\left[\sqrt{2}\right]$ mà $f\neq 0$. Khi đó ta suy ra

$$f(n) = n,\ \forall n\in\mathbb{Z}.$$

$$\left[f\left(\sqrt{2}\right)\right]^2 = f(2) = 2 \text{ hay } f\left(\sqrt{2}\right) = \begin{bmatrix}\sqrt{2}\\ -\sqrt{2}\end{bmatrix}.$$

Nếu $f\left(\sqrt{2}\right) = \sqrt{2}$ thì $\forall u = a + b\sqrt{2}\in\mathbb{Z}\left[\sqrt{2}\right]$, $f(u) = u$ trong trường hợp này f là ánh xạ đồng nhất.

Nếu $f\left(\sqrt{2}\right) = -\sqrt{2}$ thì

$$\forall u = a + b\sqrt{2}\in\mathbb{Z}\left[\sqrt{2}\right], f(u) = a - b\sqrt{2}.$$

Ta cũng chứng minh được trong trường hợp này, f còn là ánh xạ đẳng cấu. Vậy ngoài đồng cấu không, $\mathbb{Z}\left[\sqrt{2}\right]$ còn có hai tự đẳng cấu nữa là $id_{\mathbb{Z}\left[\sqrt{2}\right]}$ và $f:\mathbb{Z}\left[\sqrt{2}\right]\to\mathbb{Z}\left[\sqrt{2}\right]$

$$a + b\sqrt{2}\mapsto a - b\sqrt{2}.$$

3.33. Làm tương tự bài 3.32, ngoài tự đồng cấu không, $\mathbb{Z}[i]$ còn có hai tự đẳng cấu nữa là $id_{\mathbb{Z}[i]}$ và $f : \mathbb{Z}[i] \to \mathbb{Z}[i]$

$a + bi \mapsto a - bi.$

3.34. Vì $f(0) = 0$ nên $A \neq \varnothing$.

Giả sử $x_1, x_2 \in A$, như vậy $f(x_1) = x_1$, $f(x_2) = x_2$ do đó

$$f(x_1 - x_2) = f(x_1) - f(x_2) = x_1 - x_2$$

và $f(x_1x_2) = f(x_1)f(x_2) = x_1x_2$.

Vậy A là một vành con của X.

3.35. a) Chứng minh như đối với bài tập 3.1. Phần tử đơn vị là $(0, 1)$.

b) Ánh xạ $f : X \to X \times \mathbb{Z}$

$x \mapsto (x, 0)$

hiển nhiên là một đơn ánh. Nó là một đồng cấu vì:

$f(x + y) = (x + y, 0) = (x, 0) + (y, 0) = f(x) + f(y)$;

$f(xy) = (xy, 0) = (x, 0)(y, 0) = f(x)\, f(y)$.

3.36. a) Chứng minh dựa vào định nghĩa của vành.

b) $\overline{A} = \{(a,0) \mid a \in A\}$ là một vành con của X vì $\overline{A} \ni (0, 0)$ nên $\overline{A} \neq \varnothing$. Giả sử $(a, 0)$ và $(b, 0)$ thuộc $\overline{A}$,

$$(a, 0) - (b, 0) = (a - b, 0 - 0) = (a - b, 0) \in \overline{A},$$

$$(a, 0)(b, 0) = (ab, 0.0) = (ab, 0) \in \overline{A}.$$

Tương tự ta có $\overline{B} = \{(0,b) \mid b \in B\}$ là một vành con của X.

Các ánh xạ $f_1 : A \to X$ và $f_2 : B \to X$

$a \mapsto (a,0)$ $\quad$ $b \mapsto (0.b)$

là những đơn cấu và lần lượt ta có $\mathrm{Im}f_1 = \overline{A}$. $\mathrm{Im}f_2 = \overline{B}$ nên suy ra $A \cong \overline{A}$, $B \cong \overline{B}$.

c) Giả sử $x = (a_1, b_1) \in X$ và $\alpha = (a_2, 0) \in \overline{A}$ ta có

$$x\alpha = (a_1, b_1)(a_2, 0) = (a_1a_2, 0) \in \overline{A},$$

$$\alpha x = (a_2, 0)(a_1, b_1) = (a_2a_1, 0) \in \overline{A}.$$

Vậy $\overline{A}$ là iđêan của X.

Tương tự ta có $\overline{B}$ là iđêan của X.

d) Theo định nghĩa ta có $\overline{A} \cap \overline{B} = \{(0, 0)\}$.

Ngoài ra, nếu $x \in X$, $x = (a_1, b_1)$ thì

$$x = (a_1, b_1) = (a_1, 0) + (0, b_1) \in \overline{A} + \overline{B}.$$

Vậy $X = \overline{A} + \overline{B}$.

d) Giả sử e_A là đơn vị của A, e_B là đơn vị của B khi đó

$$e = (e_A, e_B) \text{ là đơn vị của X.}$$

3.37. a) Với mọi $x \in X$ ta có $h_a(x) = ax$, do đó với mọi $x_1, x_2 \in X$ có $h_a(x_1 + x_2) = a(x_1 + x_2) = ax_1 + ax_2 = h_a(x_1) + h_a(x_2)$. Vậy h_a là đồng cấu từ nhóm cộng X đến nhóm cộng X.

Gọi $E = \mathrm{End}(X)$ là vành các tự đồng cấu của nhóm cộng Aben X. Khi đó $h : X \to E$

$$a \mapsto h(a) = h_a$$

là một đồng cấu (vành) vì với mọi $a, b \in X$,

$$h(a + b) = h_{a+b} \text{ và } h(ab) = h_a h_b.$$

Thật vậy, với mọi $x \in X$ ta có

$h_{a+b}(x) = (a + b)x = ax + bx = h_a(x) + h_b(x) = (h_a + h_b)(x)$

và $h_{ab}(x) = (ab)x = a(bx) = h_a(bx) = h_a(h_b(x)) = h_a h_b(x)$.

c) $\text{Kerh} = \{a \in X \mid h_a(x) = 0 \text{ với mọi } x \in X\}$

$= \{a \in X \mid ax = 0 \text{ với mọi } x\}$.

Nếu X là vành có đơn vị thì $a \in$ Kerh khi và chỉ khi $ae = a = 0$.

Vậy $\text{Kerh} = \{0\}$ hay h là một đơn cấu.

Từ bài tập 3.35 và bài tập 3.37 ta suy ra rằng mọi vành đều đẳng cấu với một vành con của vành các tự đồng cấu của một nhóm Aben .

3.38. Ta cho tương ứng mỗi $x + A$ thuộc X/A, lớp $f(x) + B \in Y/B$.

Ký hiệu tương ứng đó là $\bar{f}$, nghĩa là $\bar{f}(x + A) = f(x) + B$.

Giả sử $x + A = x' + A$ nghĩa là có $x - x' \in A$. Khi đó $\bar{f}(x + A) = f(x) + B$ và $\bar{f}(x' + A) = f(x') + B$ bằng nhau. Vì $x - x' \in A$ nên $f(x) - f(x') = f(x - x') \in f(A) \subset B$. Vậy tương ứng $\bar{f}$ là một ánh xạ từ X/A đến Y/B.

Với mọi $x_1 + A$, $x_2 + A$ ta có

$\bar{f}((x_1 + A) + (x_2 + A)) = \bar{f}((x_1 + x_2) + A) = f(x_1 + x_2) + B$

$= (f(x_1) + f(x_2)) + B = (f(x_1) + B) + (f(x_2) + B)$

$= \bar{f}(x_1 + A) + \bar{f}(x_2 + A)$;

$\bar{f}((x_1) + A)(x_2 + A)) = \bar{f}(x_1 x_2 + A) = f(x_1 x_2) + B$

$= f(x_1)f(x_2) + B = [f(x_1) + B][f(x_2) + B]$.

Mặt khác

$$\bar{f}\,p(x) = \bar{f}\,(p(x)) = \bar{f}\,(x + A) = f(x) + B = p'(f(x)) = p'f(x)$$

Vậy $\bar{f}$ là một đồng cấu thỏa mãn $\bar{f}p = p'f$.

Giả sử có f_1: $X/A \to Y/B$ là đồng cấu sao cho $f_1p = p'f$ thì ta có đẳng thức $\bar{f}p = f_1p$. Vì p là toàn ánh nên giản ước cho p ta được $\bar{f} = f_1$.

Điều đó nói lên tính chất duy nhất của $\bar{f}$.

Nếu f là một toàn ánh thì p'f là một toàn ánh.

Như vậy ta có $\bar{f}p$ là một toàn ánh từ đó suy ra $\bar{f}$ là một toàn ánh và do đó $\bar{f}$ là một toàn cấu (bài tập 1.49 chương I).

3.39. Giả sử $X = \{0, e, x_2, ..., x_n\}$ là một miền nguyên. Để chứng minh X là một trường ta chỉ cần chứng tỏ mỗi phần tử của X khác 0 đều có nghịch đảo. Giả sử $x_1 \in X$, $x_1 \neq 0$. Xét $x_iX = \{x_i0, x_1x_2, ..., x_ix_n\}$. Do trong X có luật giản ước nên tập hợp x_iX có đúng n phần tử bằng số phần tử của X, do đó $x_iX = X$; $e \in X$ nên tồn tại $x_j \in X$ sao cho $e = x_ix_j$ (e là đơn vị của vành X).

Vậy x_j là nghịch đảo của x_i.

3.40. Xét vành $\mathbb{Z}_n = \{\bar{0}, \bar{1}, ..., \overline{n-1}\}$.

Theo bài 3.13, $\mathbb{Z}_n$ là một miền nguyên khi và chỉ khi n là nguyên tố. Kết hợp với 3.39 ta có điều khẳng định.

3.41. Giả sử A là một trường con của trường các số hữu tỉ $\mathbb{Q}$, cần chứng minh $A = \mathbb{Q}$. Ta luôn có $A \subset \mathbb{Q}$. Đảo lại, vì $1 \in A$ (do A là trường con của $\mathbb{Q}$) nên với mọi số nguyên $n > 0$, đều có

$$n = \underbrace{1+1+...+1}_{n \text{ lần}} \in A,\ -n \in A \text{ và } \frac{1}{n} \in A$$

Từ đó suy ra nếu $\frac{p}{q}(q \neq 0)$ là một số hữu tỉ bất kì thì ta có $\frac{p}{q} = p\left(\frac{1}{q}\right) \in A$. Vậy $\mathbb{Q} \subset A$ do đó $\mathbb{Q} = A$.

3.42. Ta có $\mathbb{Q} \subset A$ vì với mọi $a \in \mathbb{Q}$, $a = a + 0\sqrt{2}$. Giả sử $a + b\sqrt{2}$ và $c + d\sqrt{2} \in A$. Ta có

$$\left(a + b\sqrt{2}\right) - \left(c + d\sqrt{2}\right) = (a - c) + (b - d)\sqrt{2} \in A;$$

nếu $c + d\sqrt{2} \neq 0$ thì

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{\left(a + b\sqrt{2}\right)\left(c - d\sqrt{2}\right)}{c^2 - 2d^2} = \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2}\sqrt{2} \in A.$$

Trong đó $\frac{ac - 2bd}{c^2 - 2d^2}$ và $\frac{bc - ad}{c^2 - 2d^2} \in \mathbb{Q}$.

Vậy A là một trường con của trường số thực $\mathbb{R}$.

3.43. Chứng minh giống như đối với bài 3.42 hoặc dựa vào kết quả chứng minh bài tập 5.31 chương V.

3.44. $A \neq \varnothing$ vì $0 = 0.e \in A$, $e = 1.e \in A$. (1)

với mọi $n_1e, n_2e \in A$ ta có $n_1e - n_2e = (n_1 - n_2)e \in A$

$(n_1e)(n_2e) = (n_1n_2)e \in A$ do phép nhân phân phối đối với phép cộng và $e^2 = e$.

Vậy A là vành con của X. Vì X là một trường nên A không có ước của 0 và theo (1), suy ra A là một miền nguyên.

b) Xét ánh xạ $\varphi : \mathbb{Z} \to X$

$$n \mapsto ne.$$

Dễ thấy φ là một đồng cấu và $Im\varphi = A$.

Tìm $Ker\varphi$

• e có cấp vô hạn thì với hai số nguyên n, $m \in \mathbb{Z}$, $n \neq m$ kéo theo $ne \neq me$, do đó φ là một đơn cấu và ta có $\mathbb{Z} \cong A$.

• e có cấp p thì vì X là một trường nên vành $A = \varphi(\mathbb{Z})$ là một miền nguyên có p phần tử e, 2e, ..., (p–1)e, pe = 0. Lúc đó $Ker\varphi = p\mathbb{Z}$ với p nguyên tố và $A \cong \mathbb{Z}/p\mathbb{Z}$.

c) Theo kết quả bài tập 3.40 ta có $\mathbb{Z}/p\mathbb{Z}$ là một trường, do đó A là một trường.

3.45. Hiển nhiên.

3.46. a) Giả sử $f: \mathbb{Q} \to \mathbb{Q}$ là một tự đồng cấu của $\mathbb{Q}$. Nếu $f \neq 0$, chứng minh giống như bài tập 3.31, ta có

$f(1) = 1$;

$f(n) = n$ với mọi $n \in \mathbb{Z}$.

Với $q \in \mathbb{Z}, q \neq 0$, $f(1) = f\left(q.\frac{1}{q}\right) = f(q)f\left(\frac{1}{q}\right) = qf\left(\frac{1}{q}\right)$,

suy ra $f\left(\frac{1}{q}\right)=\frac{1}{q}$. Do đó với mọi số hữu tỉ $\frac{p}{q}\in\mathbb{Q}$, $q\neq 0$ ta có $f\left(\frac{p}{q}\right)=f.\left(p.\frac{1}{q}\right)=pf\left(\frac{1}{q}\right)=p.\frac{1}{q}=\frac{p}{q}$.

Vậy f là ánh xạ đồng nhất của $\mathbb{Q}$.

Tóm lại, các tự đồng cấu của trường số hữu tỉ $\mathbb{Q}$ chỉ là đồng cấu 0 và đồng cấu đồng nhất.

b) Chứng minh như câu a) nếu $f: \mathbb{R}\to\mathbb{R}$ là một tự đồng cấu, $f\neq 0$ thì $f(a)=a$ với mọi số hữu tỉ $a\in\mathbb{Q}$. Ta hãy chứng minh nếu $r\in\mathbb{R}$ là một số thực dương thì $f(r)\geq 0$. Thật vậy, r có thể viết $r=\left(\sqrt{r}\right)^2$ do đó $f(r)=f\left(\sqrt{r^2}\right)=\left[f\left(\sqrt{r}\right)\right]^2\geq 0$.

Bây giờ giả sử $r\in\mathbb{R}$ là một số thực tùy ý mà $f(r)\neq r$. Do tính chất trù mật khắp nơi của trường số hữu tỉ $\mathbb{Q}$ trong $\mathbb{R}$ nên có số hữu tỉ q sao cho $r<q<f(r)$ (1) hoặc $f(r)<q<r$. Khi đó $q-r>0$ do đó $f(q-r)=f(q)-f(r)\geq 0$ hay $q\geq f(r)$ mâu thuẫn với (1). Hoặc $r-q>0$ do đó $f(r-q)=f(r)-f(q)=f(r)-q\geq 0$ mâu thuẫn với $f(r)<q<r$.

Vậy $f(r)=r$ hay f phải là một ánh xạ đồng nhất.

Do đó tập hợp các tự đồng cấu của $\mathbb{R}$ là $\{0, 1_{\mathbb{R}}\}$.

c) Giả sử $f : \mathbb{C} \to \mathbb{C}$ là một tự đồng cấu của trường số phức $\mathbb{C}$ sao cho $f(a) = a$ với mọi $a \in \mathbb{R}$.

Như vậy với số phức bất kì $\alpha = a + bi \in \mathbb{C}$ ta có

$$f(\varphi) = f(a + bi) = f(a) + f(b)f(i) = (a + b)f(i).$$

Hãy tìm $f(i)$. Vì $i^2 = -1$ nên $[f(i)]^2 = f(i^2) = f(-1) = -1$.

Vậy $f(i) = i$ hoặc $f(i) = -i$. Do đó f phải là tự đẳng cấu đồng nhất hay tự đẳng cấu đặt tương ứng mỗi số phức $a + bi$ với số phức liên hợp $a - bi$.

3.47. $\mathbb{Q}(\sqrt{2})$ có hai tự đẳng cấu là:

$$Id_{\mathbb{Q}(\sqrt{2})} \text{ và } f: \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$$

$$a + b\sqrt{2} \mapsto a - b\sqrt{2}.$$

3.48. $\mathbb{Q}(i)$ có hai tự đẳng cấu là: $Id_{\mathbb{Q}(i)}$ và $f : \mathbb{Q}(i) \to \mathbb{Q}(i)$

$$a + b \mapsto a - bi.$$

3.49. $\mathbb{Q}(\sqrt[3]{2})$ chỉ có một tự đẳng cấu duy nhất là ánh xạ đồng nhất.

3.50. Đặt $M = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle| a, b \in \mathbb{R} \right\}$.

Xét ánh xạ $f : \mathbb{C} \to M$

$$a + bi \mapsto \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

f là một song ánh vì nếu $a + bi \neq c + di$ nghĩa là $a \neq c$ hoặc $b \neq d$ thì

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \neq \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$$

do đó $f(a + bi) \neq f(c + di)$, với mỗi ma trận $\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in M$ ta có ngay $a + bi \in \mathbb{C}$ (vì a, b thực), $f(a + bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$.

Giả sử $a + bi, c + di \in \mathbb{C}$, khi đó

$$(a + bi) + (c + di) = (a + c) + (b + d)i \text{ và}$$

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

Tương ứng ta có

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ -(b+d) & a+c \end{bmatrix}$$

và

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{bmatrix}$$

Như vậy suy ra $f((a + bi) + (c + di)) = f(a + bi) + f(c + di)$ và $f((a + bi)(c + di)) = f(a + bi) f(c + di)$ Vì $\mathbb{C}$ là một trường nên theo kết quả bài 3.45 ta có M là một trường.

3.51. Chứng minh tương tự bài 3.50. Bằng cách đặt

$$M = \left\{ \begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \middle| a, b \in \mathbb{Q} \right\} \text{ và xét ánh xạ}$$

$$f: A \to M$$

$$a + b\sqrt{2} \mapsto \begin{bmatrix} a & b \\ 2b & a \end{bmatrix}.$$

3.52. Theo kết quả của bài 3.44 ta có: Nếu e có cấp vô hạn thì $A = \{ne | n \in \mathbb{Z}\}$ đẳng cấu với vành số nguyên $\mathbb{Z}$. Khi đó trường các thương của A đẳng cấu với trường số hữu tỉ $\mathbb{Q}$ là trường của các thương của $\mathbb{Z}$.

Nếu e có cấp p thì A đẳng cấu với $\mathbb{Z}_p$, nó là một trường nên trường các thương của A chính là A.

3.53. Xét ánh xạ $f : \mathbb{Z} \to T$

$$n \mapsto ne.$$

Với T là một trường và e là phần tử đơn vị của trường T. Khi đó f là một đồng cấu vì với n và m thuộc $\mathbb{Z}$ ta có

$$f(n + m) = ne + me = f(n) = f(m),$$
$$f(nm) = (nm)e = ne.me = f(n)\, f(m).$$

Nếu T là trường có đặc số 0 (tức là cấp của e là vô hạn) thì f là một đơn cấu. Khi đó $\mathbb{Z}$ đẳng cấu với vành con A của T. Trường các thương của A rõ ràng là một trường con của T. Nó đẳng cấu với $\mathbb{Q}$ (theo bài 3.52). Nếu T là trường có đặc số p ($\neq 0$) thì A đẳng cấu với $\mathbb{Z}_p$, nó là một trường.

3.55. Đặt $A = \left\{ \frac{m}{n} \in \mathbb{Q} \middle| (n, p) = 1 \right\}$, $A \neq \varnothing$ vì $\mathbb{Z} \subset A$.

Nếu $\frac{m_1}{n_1}, \frac{m_2}{n_2} \in A$ thì $\frac{m_1}{n_1} - \frac{m_2}{n_2} = \frac{m_1n_2 - m_2n_1}{n_1n_2}$.

Vì $(n_1, p) = 1$ và $(n_2, p) = 1$ nên $(n_1n_2, p) = 1$,

do đó $\frac{m_1n_2 - m_2n_1}{n_1n_2} \in A$.

Tương tự có $\frac{m_1}{n_1}.\frac{m_2}{n_2} = \frac{m_1m_2}{n_1n_2} \in A$.

Vậy A là một vành con của $\mathbb{Q}$, nó chứa 1 nên A là một miền nguyên. Gọi $\overline{A}$ là trường các thương của A thì vì $A \supset \mathbb{Z}$ nên $\overline{A} \supset \mathbb{Q}$, mặt khác vì $A \subset \mathbb{Q}$ nên $\overline{A} \subset \mathbb{Q}$. Vậy $\overline{A} = \mathbb{Q}$

3.56. a) Ta có $A + B = \{a + b \mid a \in A, b \in B\}$ khác rỗng vì

$$0 = 0 + 0 \in A + B.$$

Giả sử $a_1 + b_1, a_2 + b_2 \in A + B$. Ta có

$$(a_1 + b_1) - (a_2 + b_2) = (a_1 - b_1) + (b_1 - b_2) \in A + B,$$

$$(a_1 + b_1)(a_2 + b_2) = a_1a_2 + a_1b_2 + b_1a_2 + b_1b_2 \in A + B,$$

vì $a_1a_2 + a_1b_2 + b_1a_2 \in A$ và $b_1b_2 \in B$.

Vậy A + B là một vành con của vành X.

b) Rõ ràng $A \cap B \subset B$ và $A \cap B \neq \varnothing$ vì $0 \in A \cap B$. Giả sử a_1, a_2 là hai phần tử tùy ý của $A \cap B$ và b là phần tử tùy ý của B. Khi đó $a_1, a_2 \in A$ và $a_1, a_2 \in B$ nên $a_1 - a_2 \in A \cap B$, đồng thời $a_1b \in A \cap B$ và $ba_1 \in A \cap B$. Vậy $A \cap B$ là một iđêan của B.

c) Vì $A \subset A + B$ và A là iđêan của X nên A cũng là iđêan của $A + B \subset X$.

d) Xét ánh xạ $f: B \to {A(A+B)}/{A}$

$$b \mapsto (0 + b) + A = b + A.$$

Với mọi $b_1, b_2 \in B$,

$f(b_1 + b_2) = (b_1 + b_2) + A = (b_1 + A) + (b_2 + A) = f(b_1) + f(b_2)$

$f(b_1 b_2) = b_1 b_2 + A = (b_1 + A)(b_2 + A) = f(b_1) f(b_2)$

Ta hãy tìm Kerf, có $b \in \text{Kerf} \Leftrightarrow b + A = A$

$$\Leftrightarrow b \in A$$

$$\Leftrightarrow b \in A \cap B.$$

Theo định lí đồng cấu suy ra $\left({B}/{A}\right) \cap B \cong {A + B}/{A}$.

3.57. Hiển nhiên ${B}/{A} \neq \emptyset$

Giả sử $x_1 + A, x_2 + A \in {B}/{A}$, khi đó $x_1, x_2 \in B$ và vì B là iđêan của X nên $x_1 - x_2 \in B$ do đó

$$(x_1 + A) - (x_2 + A) = (x_1 - x_2) + A \in {B}/{A}.$$

Giả sử $x + A \in {B}/{A}$ và $x' + A \in {X}/{A}$. Khi đó $x \in B$ vì B là iđêan của X nên $x'x \in B$, do đó

$$(x' + A)(x + A) = x'x + A \in {B}/{A}.$$

Tương tự $(x + A)(x' + A) \in {B}/{A}$. Vậy ${B}/{A}$ là một iđêan của ${X}/{A}$.

Với mỗi $x + A \in X/A$ ta đặt tương ứng với $x + B \in X/B$.

Nếu $x + A = x' + A$ thì $x - x' \in A \subset B$ nên $x + B = x' + B$.

Vậy ta có một ánh xạ $\varphi : X/A \to X/B$

$$x + A \mapsto x + B.$$

Dễ thấy φ là một toàn cấu, và bây giờ tìm $\mathrm{Ker}\varphi$

$$x + A \in \mathrm{Ker}\varphi \Leftrightarrow \varphi(x + A) = x + B = B$$

$$\Leftrightarrow x \in B$$

$$\Leftrightarrow x + A \in B/A.$$

Vậy $\mathrm{Ker}\varphi = B/A$.

Theo định lí đồng cấu $\left(X/A\right)\Big/\left(B/A\right) \cong X/B$.

3.58. Xét ánh xạ $f : X \to \left(X/A\right) \times \left(X/B\right)$

$$x \mapsto (x + A, x + B).$$

Rõ ràng f là một đồng cấu.

Ta có $1 = e_1 + e_2$ với $e_1 \in A$ và $e_2 \in B$. Như vậy, với mọi $x_1, x_2 \in X$ đặt $x = e_2x_1 + e_1x_2 \in X$, từ đó

$$x - x_1 = (e_2 - 1)x_1 + e_1x_2 = e_1(-x_1 + x_2) \in A,$$

$$x - x_2 = e_2x_1 + (e_1 - 1)x_2 = e_2(x_1 - x_2) \in B,$$

do đó $x + A = x_1 + A$ và $x + B = x_2 + B$, suy ra f là một toàn ánh.

Mặt khác, $x \in \mathrm{Ker}f \Leftrightarrow (x + A, x + B = (A, B)$

$$\Leftrightarrow x \in A \cap B.$$

Vậy Kerf = A ∩ B.

Vì A và B là những iđêan, nên AB là một iđêan luôn luôn chứa trong A ∩ B. Bao hàm thức A ∩ B ⊂ AB suy ra từ

$$X = A + B.$$

Vậy A ∩ B = AB.

Theo định lí đồng cấu suy ra $X/_{AB} \cong \left(X/_{A}\right) \times \left(X/_{B}\right)$.

3.59. Do m và n là nguyên tố cùng nhau nên $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$.

$$m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z}.$$

Áp dụng bài 3.58 ta có $\mathbb{Z}/_{mn\mathbb{Z}} \cong \left(\mathbb{Z}/_{m\mathbb{Z}}\right) \times \left(\mathbb{Z}/_{n\mathbb{Z}}\right)$.

3.60. Đặt $U = \left\{a \in X \mid \exists a' \in X, a'a = aa' = 1\right\}$.

$U \neq \varnothing$ vì $1 \in U$. Giả sử $a, b \in U$, khi đó tồn tại $a', b' \in X$ sao cho $aa' = a'a = 1$ và $bb' = b'b = 1$ suy $abb'a' = 1$; $b'a'ab = 1$.

Vậy $ab \in U$.

Nếu $a \in U$ thì a' là phần tử sao cho $a'a = aa' = 1$, chứng tỏ $a' \in U$ và là nghịch đảo của a trong U.

3.61. Các ước của đơn vị trong vành $\mathbb{Z}/_{m\mathbb{Z}}$ là và chỉ là các lớp $\bar{a}$ sao cho a và m nguyên tố cùng nhau.

Trong vành $\mathbb{Z}/_{p\mathbb{Z}}$, các ước của đơn vị là $\bar{1}, \bar{2}, \ldots, \overline{p-1}$.

Chúng lập thành một nhóm cấp p − 1 với phép nhân.

Do đó nếu a là một số nguyên mà a không chia hết cho p thì $\bar{a}$ là một ước của đơn vị và $\overline{a^{p-1}} = \bar{1}$, vậy $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.

3.62. Chứng minh tương tự bài 2.77 (chương II).

3.63. Chứng minh tương tự bài 2.78 (chương II).

3.64. Chứng minh tương tự bài 2.80 (chương II).

3.65. a) Chứng minh tương tự bài 3.42 (chương III).

b) Giả sử có một đẳng cấu f từ $\mathbb{Q}(\sqrt{7})$ đến $\mathbb{Q}(\sqrt{11})$.

Làm như bài 3.46 ta có f (a) = a với mọi $a \in \mathbb{Q}$ do đó

$$\left[f\left(\sqrt{7}\right)\right]^2 = f\left(\sqrt{7^2}\right) = f(7) = 7.$$

Vậy $f(\sqrt{7}) = \sqrt{7}$. Nhưng $\sqrt{7} \notin \mathbb{Q}\left(\sqrt{11}\right)$, mâu thuẫn !

3.66. Ta biết rằng một trường chỉ có hai iđêan tầm thường. Bây giờ giả sử X là một miền nguyên và X chỉ có hai iđêan tầm thường là $\{0\}$ và X. Giả sử $a \neq 0$ là một phần tử của X. Ta xét iđêan I = (a) của X sinh ra bởi phần tử a. Vì $a \neq 0$ nên $I \neq \{0\}$ do đó I = X. Ta có $1 \in X$ nên $1 \in I$ hay tồn tại một phần tử $a' \in X$ sao cho $1 = a\,a'$. Vậy X là một trường.

3.67. Giả sử $(X, \leq)$ là một vành sắp thứ tự. Khi đó ta đặt

$$P = \{x \in X \mid x \geq 0\}.$$

Đảo lại, nếu có P là tập con dương của X thỏa mãn các tính chất: $a \in P$ và $b \in P \Rightarrow a + b \in P$

$a \in P$ và $b \in P \Rightarrow ab \in P$

$P \cap (-P) = \{0\}$

$P \cup (-P) = X$

thì với quan hệ $a \leq b \Leftrightarrow b - a \in P$, X là một vành sắp thứ tự.

3.68. (i) $a + x < a + y \Rightarrow -a + a + x < -a + a + y$.

$\Rightarrow 0 + x < 0 + y \Rightarrow x < y.$

$a - x < a - y \Rightarrow (a - y) - (a - x) > 0$

$\Rightarrow x - y > 0$ hay $x > y$.

Với $c > 0$ và $a \le b$ ta có $0 \le b - a \Leftrightarrow$

$\Leftrightarrow 0 \le c(b - a)$

$\Leftrightarrow 0 \le cb - ca$

$\Leftrightarrow ca \le cb$.

Với $a < 0$, $ax < ay \Leftrightarrow 0 < ay - ax$

$\Leftrightarrow 0 < a(y - x)$

$\Leftrightarrow 0 < -a(x - y)$

$\Leftrightarrow 0 < x - y \Leftrightarrow y < x$.

Nếu $a > 0$ thì $ax < ay \Leftrightarrow$

$0 < ay - ax \Leftrightarrow a(y - x) > 0$

$\Leftrightarrow y - x > 0 \Leftrightarrow x < y$.

$a > 0 \Rightarrow a^2 > 0$,

$a < 0 \Rightarrow -a > 0 \Rightarrow (-a)^2 = a^2 > 0$.

ii) Giả sử $a, b \in X$. Nếu $a - b \in P$ thì $a \ge b$; nếu $a = b \in -P$ thì $a - b \le 0$ do đó $b - a \ge 0$ hay $b \ge a$.

Vậy X sắp thứ tự toàn phần.

3.69. a) Theo bài 3.68 ta có $1 = 1^2 > 0$ (1 là đơn vị của vành A). Lần lượt áp dụng tính chất $a > b \Rightarrow a + c > b + c$ ta có

$1 > 0$

$1 + 1 > 1$

$1 + 1 + 1 > 1 + 1$

...

$\underbrace{1 + 1 + ... + 1}_{\text{n lần}} > \underbrace{1 + 1 + ... + 1}_{\text{n-1 lần}}$.

Do tính chất bắc cầu của quan hệ $\geq$ nên suy ra $n.1 > 0$ với mọi $n > 0$, $n \in \mathbb{Z}$ vậy vành A có đặc số 0.

b) Đặt $P_1 = A \cap P$. Khi đó P_1 thỏa mãn các tính chất sau: với mọi $a, b \in P_1$, $a, b \in A$ và $a, b \in P$ nên

$$a + b \in A \cap P = P_1$$

$$ab \in A \cap P = P_1$$

$$\begin{aligned} P_1 \cap (-P_1) &= (A \cap P) \cap (A \cap -P) \\ &= A \cap (P \cap -P) = \{0\} \end{aligned}$$

$$\begin{aligned} P_1 \cup (-P_1) &= (A \cap P) \cup (A \cap -P) \\ &= A \cap (P \cup -P) = A \cap X = A. \end{aligned}$$

Vậy A là một vành sắp thứ tự với tập con dương là

$$P_1 = A \cap P.$$

3.70. Chứng minh dựa vào định nghĩa của $|a|$.

3.71. Giả sử A là một miền nguyên sắp thứ tự với tập con dương là P; $\bar{A}$ là trường các thương của A. Khi đó trong $\bar{A}$ ta xây dựng tập con dương như sau $\bar{P} = \left\{ \frac{a}{b} \in \bar{A} \mid ab \in P \right\}$.

Ta có thể chứng minh được với tập con dương $\bar{P}$, $\bar{\lambda}$ là một trường sắp thứ tự và $\bar{P} \cap A = P$.

3.72. Giả sử 1 là đơn vị của trường sắp thứ tự X. Khi đó với hai phần tử x, y thuộc X sao cho $x < y$, ta xét $z = \frac{x + y}{2}$. Phần tử z thỏa mãn $x < z < y$. Thật vậy, $x < y$ nên $\frac{x}{2} < \frac{y}{2}$, từ đó

$$x = \frac{x}{2} + \frac{x}{2} < z = \frac{x}{2} + \frac{y}{2} \text{ và } z = \frac{x}{2} + \frac{y}{2} < \frac{y}{2} + \frac{y}{2} = y.$$

3.73. a) Giả sử $\frac{a}{b}, \frac{c}{d}$ là hai số hữu tỉ, với $\frac{c}{d} > 0$.

– Nếu $\frac{a}{b} < 0$, ta có $\frac{a}{b} < 1.\frac{c}{d} = \frac{c}{d}$.

– Nếu $\frac{a}{b} > 0$, ta lấy số tự nhiên $n \in \mathbb{N}$ sao cho $nbc > ad$ thì sẽ được $\frac{a}{b} < n\frac{c}{d}$.

Vậy $\mathbb{Q}$ là trường sắp thứ tự Ac-si-met.

Giả sử a, b là hai số thực, $a > 0$.

– Nếu $b < 0$ thì ta có $b < 1.a = a$.

– Nếu $b > 0$, đặt $[b]$ là phần nguyên của b.

Ta luôn có $[b] + 1 > b$.

Nếu $a < 1$ thì $\frac{1}{a} > 1, \left[\frac{1}{a}\right] + 1 > \frac{1}{a}$ do đó

$$b < [b] + 1 = \frac{[b]+1}{a}a < ([b]+1)\left(\left[\frac{1}{a}\right]+1\right)a.$$

Nếu $a > 1$ thì $b < ([b]+1)a$.

b) Giả sử X là một trường sắp thứ tự Ac-si-met, $x, y \in X$ sao cho $a < y$. Như vậy $y - x > 0$, vì X sắp thứ tự Ac-si-met nên tồn tại số tự nhiên m sao cho $1 < m(y - x) = my - mx$ (1 là đơn vị của X) hay $mx + 1 < my$. Cũng vì lí do X sắp thứ tự Ac-si-met nên tồn tại số tự nhiên m sao cho $|my| < n1 = n$.

Xét tập hợp $M = \{k \in \mathbb{Z} \mid k < my\}$; M bị chặn trên vì với mọi $k \in M$, $k < my < n$. Mặt khác $M \neq \{0\}$ vì $-n1 < -|my| \leq my$, tức là $-n \in M$.

Vậy M có phần tử lớn nhất là p. Ta có $p < my$. Và ta cũng có $mx < p$ (vì nếu $mx \geq p$ thì $p + 1 \leq mx + 1 < my$, do đó $p + 1 \in M$, mâu thuẫn với giả thiết về p).

Vậy ta có $mx < p < my$. Từ đó suy ra $x < \frac{p}{m} < y$.

3.74. Ta biết rằng nếu $(X, \leq)$ là một trường sắp thứ tự thì

$\forall a \in X, a \neq 0: 0 \leq a^2$ và $0 < 1$, suy ra $-1 < 0$.

Nếu trong $\mathbb{C}$ có một quan hệ thứ tự $\leq$ sao cho $(\mathbb{C}, \leq)$ là một trường sắp thứ tự thì ta phải có $0 \leq i^2$. Nhưng $i^2 = -1 < 0$ (mâu thuẫn).

Vậy không có một quan hệ thứ tự nào trong $\mathbb{C}$ để $\mathbb{C}$ trở thành một trường sắp thứ tự.

4.1. a) Có 18 đa thức bậc hai trong $\mathbb{Z}_3[x]$, đó là

$x^2; x^2 + \bar{1}; x^2 + x$

$x^2 + x + \bar{1}; x^2 + \bar{2}; x^2 + \bar{2}x$

$x^2 + \bar{2}x + \bar{1}; x^2 + \bar{2}x + \bar{2};$

$x^2 + x + \bar{2};$

$\bar{2}x^2; \bar{2}x^2 + \bar{1}; \bar{2}x^2 + x$

$\bar{2}x^2 + x + \bar{1}; \bar{2}x^2 + \bar{2}; \bar{2}x^2 + \bar{2}x$

$\bar{2}x^2 + \bar{2}x + \bar{1}; \bar{2}x^2 + \bar{2}x + 2; \bar{2}x^2 + x + \bar{2}$

b) Có $2.3.3.3 = 54$ đa thức bậc ba trong $\mathbb{Z}_3[x]$.

c) Có 2.3^n đa thức bậc n. Thật vậy, giả sử

$$f(x) = a_0x^n + a_1x^{n-1} + ... + a^n \in \mathbb{Z}_3[x]$$

là một đa thức bậc n. Có bao nhiêu bộ $(a_0, a_1, ..., a_n)$ phần tử của $\mathbb{Z}_3^* \times \mathbb{Z}_3 \times ... \times \mathbb{Z}_3$ thì có bấy nhiêu đa thức $f(x)$. Số phần tử của $\mathbb{Z}_3^* \times \mathbb{Z}_3 \times ... \times \mathbb{Z}_3 = \mathbb{Z}_3^* \times \mathbb{Z}_3^n$ là 2.3^n.

Vậy số đa thức bậc n trong $\mathbb{Z}_3[x]$ là 2.3^n.

với $n = 2$ ta có $2.3^2 = 18$ đa thức

$n = 3$ ta có $2.3^3 = 54$ đa thức.

4.2. a) Trong vành $\mathbb{Z}[x]$ các ước của 1 là ± 1.

b) Khi A là một trường, tập các ước của 1 trong A[x] là tập các phần tử khác 0 của A.

c) Khi A là một miền nguyên thì tập các ước của 1 trong A[n] là tập các ước của 1 trong A.

4.3. Giả sử a là một phần tử luỹ linh của vành A. Theo định nghĩa tồn tại số nguyên dương n sao cho $a^n = 0$. Giả sử m là số mũ bé nhất sao cho $a^m = 0$.

Ta có $1 = 1 + a^m.x^m = 1 + (ax)^m$

$$\Leftrightarrow 1 = (1+ax)\left[(ax)^{m-1} - (ax)^{m-2} + ... + (-1)^{m-1}\right]$$

$$\Leftrightarrow 1 = (1 + ax)\left(a^{m-1}.x^{m-1} - a^{m-2}.x^{m-2} + ... + (-1)^{m-1}\right)$$

Vậy 1 + ax khả nghịch.

Một cách tổng quát ta có:

Cho $f(x) = a_0 + a_1x + ... + a_nx^n \in A[x]$ (A là một vành giao hoán, có đơn vị 1), f(x) là ước của đơn vị khi và chỉ khi a_0 là ước của 1 và a_i (i = 1, 2, ..., n) là những phần tử luỹ linh. Độc giả tự chứng minh.

4.4. Chứng minh $\bar{\varphi}$ là đẳng cấu bằng cách cho f(x) và g(x) là những biểu thức xác định của chúng.

4.5. Trong vành $\mathbb{Z}_8[x]$ ta có

$(1 + 4x)(1 + 4x) = 1;$

$(1 + 4x + 4x^2)(1+ 4x + 4x^2) = 1.$

Một cách tổng quát $(1 + 4x + ... + 4x^n)^2 = 1$ $(n \in \mathbb{Z}^*)$

Do đó suy ra các kết quả của a), b) và c).

4.6. a) Đặt $p = \{f(x) \in A[x] \mid f(x)$ có hệ tử cao nhất dương$\}$ là tập các phần tử dương của A[x].

Với mọi f(x) và g(x) thuộc P ta có $f(x) + g(x) \in P$

$f(x)\,g(x) \in P.$

Đặt $-P = \{f(x) \in A[x] \mid f(x)$ có hệ tử cao nhất âm$\}$,

khi đó $P \cap \{-P\} = \varnothing$

$$P \cup \{0\} \cup (-P) = A[x].$$

Vậy, ta đã chỉ ra được tập các phần tử dương của $A[x]$ làm cho $A[x]$ trở thành một vành sắp thứ tự.

b) Làm tương tự câu a)

Đặt $P = \{f(x) \in A[x] \mid f(x)$ có hạng tử tự do dương$\}$

4.7. Chứng minh bằng cách cho $f(x)$ và $g(x)$ bởi biểu thức cụ thể và dựa vào định nghĩa của đạo hàm hình thức.

4.8. $(\overline{2}x^2 + \overline{4}x + \overline{1})(\overline{3}x^2 + \overline{1}x + \overline{2}) =$

$$\overline{1}x^4 + (\overline{2} + \overline{2})x^3 + (\overline{4} + \overline{3} + \overline{4})x^2 + (\overline{3} + \overline{1})x + \overline{2}$$

$$= \overline{1}x^4 + \overline{4}x^3 + \overline{1}x^2 + \overline{4}x + \overline{2}$$

$$= -\overline{2}x^2 + \overline{4}x + \overline{3})^2 = \overline{4}x^4 + \overline{4}x^3 + \overline{4}x + \overline{4}$$

4.9. $(\overline{2}x^3 + \overline{4}x^2 + \overline{1}x)(\overline{3}x^2 + \overline{3}x + \overline{2}) = \overline{1}x^3 + \overline{5}x^2 + \overline{2}x$.

Vành $\mathbb{Z}_6[x]$ có ước của không, chẳng hạn $\overline{2}x$ và $3x^2 + \overline{3}$ là hai đa thức khác $\overline{0}$ nhưng $\overline{2}x.(\overline{3}x^2 + \overline{3}) = 0$.

4.10. Ta có thể viết $f(x) = \overline{4}x^3 + \overline{2}x^2 + \overline{2}x + \overline{1}$

$g(x) = \overline{3}x^2 + \overline{2}x + \overline{4}$.

(vì $-\overline{1} = \overline{4}$ và $-\overline{2} = 3$). Ta thực hiện phép chia theo sơ đồ sau:

$\overline{4}x^3 + \overline{2}x^2 + \overline{2}x + \overline{1}$	$\overline{3}x^2 + \overline{2}x + \overline{4}$
$\overline{4}x^3 + \overline{1}x^2 + \overline{2}x$	$\overline{3}x + \overline{2}$
$\overline{1}x^2 \quad + \overline{1}$	
$\overline{1}x^2 + \overline{4}x + \overline{3}$	
$\overline{1}x + \overline{3}$	

Vậy $f(x) = g(x)(\bar{3}x + \bar{2}) + \bar{1}x + \bar{3}$.

4.11. Ta có

$$\begin{array}{l|l}
\bar{1}x^3 + \bar{p}x + \bar{5} & \bar{1}x^2 + \bar{5}x + \bar{6} \\
\hline
\bar{1}x^3 + \bar{5}x^2 + \bar{6}x & \bar{1}x + \bar{2} \\
\hline
\bar{2}x^2 + \overline{(p-6)}x + \bar{5} & \\
\bar{2}x^2 + \bar{3}x + \bar{5} & \\
\hline
\overline{(p-6-3)}x &
\end{array}$$

Để cho $(\overline{p-6-3}) = \bar{0}$ ta phải có $p \equiv 2 \pmod 7$.

p có dạng $7k + 2$ với $k \in \mathbb{Z}$.

4.12. a) $2x + 1$ có thể viết thành

$$2x + 1 = 2(x + \frac{1}{2})$$

Ta có $f\left(-\frac{1}{2}\right) = \left(-\frac{1}{2}+1\right)^{2n} - \left(-\frac{1}{2}\right)^{2n} - 2\left(-\frac{1}{2}\right) - 1 = 0$.

Vậy f(x) chia hết cho $\left(x + \frac{1}{2}\right)$, do đó f(x) chia hết cho $2\left(x + \frac{1}{2}\right)$ trong $\mathbb{Q}[x]$.

b) Ta cũng có $f(-1) = 0$, do đó f(x) chia hết cho $(x + 1)$.

c) $f(0) = 0$ nên f(x) chia hết cho x.

4.13. a) Đa thức $f(x) = \bar{1}x^2 + \overline{14} \in \mathbb{Z}_{15}[x]$

có bốn nghiệm trong $\mathbb{Z}_{15}$ là $\overline{1}$, $\overline{14} = -\overline{1}$, $\overline{4}$ và $\overline{11} = -\overline{4}$

ngoài ra không còn nghiệm nào khác.

b) Các nghiệm của $f(x) = \overline{1}x^2 + \overline{20} \in \mathbb{Z}_{21}[x]$ trong $\mathbb{Z}_{21}$ là

$\overline{1}$, $\overline{20}$, $\overline{8}$ và $\overline{13}$.

4.14. Giả sử $f(x) = a_0x^n + a_1x^{n-1} + ... + a_n$ và

$$g(x) = x^m + b_1x^{m-1} + ... + b_m.$$

Trong trường hợp hệ tử cao nhất của g(x) bằng 1, ta vẫn thực hiện được thuật toán Óclit trong A[x] để tìm q(x) và r(x).

Bây giờ giả sử

$f(x) = g(x)\,q_1(x) + r_1(x)$ với bậc $r_1(r)$ < bậc g(x) nếu $r_1(x) \neq 0$ và

$f(x) = g(x)q_2(x) + r_2(x)$ với bậc $r_2(x)$ < bậc g(x) nếu $r_2(x) \neq 0$.

Từ hai đẳng thức này suy ra

$$g(x)\,(q_1(x) - q_2(x)) = r_2(x) - r_1(x). \qquad (*)$$

Nếu $r_1(x) \neq r_2(x)$ thì $q_1(x) \neq q_2(x)$ và có bậc của vế phải của đẳng thức (*) bé hơn m (bậc g(x)) còn bậc của vế trái của (*) lớn hơn hay bằng m (vì hệ số cao nhất của g(x) bằng 1) điều này không thể sảy ra. Vậy $r_1(x) = r_2(x)$ và do đó $q_1(x) = q_2(x)$, tức là các đa thức q(x) và r(x) được xác định một cách duy nhất.

4.15. a) Theo kết quả bài 4.14 ta có

$f(x) = (x - u)\,g(x) + r(x)$ với bậc r(x) < 1 nếu $r(x) \neq 0$.

Như vậy $f(x) = (x - u)\,q(x) + a$ với $a \in A$.

Ta có $0 = f(u) = (u - u)\,q(u) + a$

từ đó suy ra $a = 0$ hay f(x) chia hết cho $x - u$.

b) Giả sử $u_1, u_2, \ldots, u_m$ là m nghiệm phân biệt của f(x) trong A. Theo a) ta có

$$f(x) = (x - u_1)\, q_1(x) \text{ với } q_1(x) \in A[x].$$

$$f(u_2) = (u_2 - u_1)\, q_1(u_2) = 0$$

$u_2 - u_1 \neq 0$ nên $q_1(u_2) = 0$ nghĩa là u_2 là một nghiệm của $q_1(x)$. Lại theo a) ta có

$$q_1(x) = (x - u_2)\, q_2(x).$$

do đó $f(x) = (x - u_2)(x - u_2)\, q_2(x)$. Lặp lại tương tự như trên đối với u_3 và $q_2(x)$... Sau m bước ta có

$$f(x) = (x - u_1)(x - u_2)\ldots(x - u_m)\, q_m(x) \text{ với } q_m(x) \in A[x].$$

4.16. Giả sử $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \in A[x]$, $a_0 \neq 0$ có nhiều hơn n nghiệm phân biệt trong A. Theo bài tập 4.15 ta có

$$f(x) = (x - x_1)(x - x_2)\ldots(x - x_m)\, g(x) \qquad (1)$$

trong đó $x_1, x_2, \ldots, x_m$ là m nghiệm phân biệt của f(x) với $m > n$.

Vì A là một trường nên bậc của đa thức vế phải của (1) bằng m + bậc $g(x) \geq m$ lớn hơn bậc của đa thức f(x) ở vế trái.

Điều đó dẫn đến mâu thuẫn. Vậy f(x) có không quá n nghiệm phân biệt trong A.

Nếu A là một miền nguyên thì tính chất này vẫn còn đúng.

Còn nếu A là một vành tuỳ ý thì tính chất này không còn đúng nữa. Xem bài 4.13.

4.17. a) Trước hết ta chứng minh rằng nếu $p(x) = q(x)\, g(x)$ với q(x) và g(x) thuộc A[x] thì bậc q(x) = 0 và bậc g(x) = bậc p(x) hoặc bậc g(x) = 0 và bậc q(x) = bậc p(x). Thật vậy, nếu bậc $g(x) \neq 0$ và bậc $q(x) \neq 0$, giả sử bậc $g(x) = m_1$ và bậc $q(x) = m_2$, thế thì $m_1 + m_2 =$ bậc p(x), $0 < m_1, m_2 <$ bậc p(x).

Khi đó ta có $p(\alpha) = g(\alpha)q(\alpha) = 0$.

Vì A là một trường nên $g(\alpha) = 0$ hoặc $q(\alpha) = 0$.

Điều này trái với giả thiết về $p(x)$.

(Khi đó ta nói rằng đa thức $p(x)$ bất khả quy trong $A[x]$).

Ngoài ra, giả sử $f(x) \in A[x]$ sao cho $f(\alpha) = 0$ thì $f(x)$ chia hết cho $p(x)$ hay $f(x) \in (p(x))$. Thật vậy ta có

$f(x) = p(x)q(x) + r(x)$ nếu $r(x) \neq 0$ thì

$$\text{bậc } r(x) < \text{bậc } p(x). \qquad (*)$$

$f(\alpha) = p(\alpha)\, q(\alpha) + r(\alpha) = 0$ kéo theo $r(x) = 0$. Do (*) nên suy ra $r(x) = 0$.

Vậy $f(x) = p(x)\, q(x)$. Bây giờ giả sử $f(x) \in A[x]$ sao cho $f(x)$ không chia hết cho $p(x)$. Dùng thuật toán Óclit ta chứng minh được ước chung lớn nhất của $f(x)$ và $p(x)$ là một đa thức bậc 0 nghĩa là một phần tử của trường A và có các đa thức $u(x)$ và $v(x)$ sao cho

$$p(x)\, u(x) + f(x)\, v(x) = 1 \qquad (**)$$

(1 là đơn vị của trường A). Dựa vào các kết quả trên ta chứng minh $I = (p(x))$ là iđêan tối đại trong $A[x]$. Thật vậy, giả sử B là một iđêan của $A[x]$ sao cho $I \subset B$, và giả sử $B \neq I$, như vậy tồn tại $f(x) \in B$ sao cho $f(x) \notin I$. Khi đó $f(x)$ không chia hết cho $p(x)$. Theo (**), tồn tại các đa thức $u(x)$ và $v(x)$ thuộc $A[x]$ sao cho $p(x)\, u(x) + f(x)\, v(x) = 1$. Do đó $1 \in B$, hay $b = A[x]$. Vậy I là iđêan tối đại.

b) Xét ánh xạ φ: $A[x] \to A[\alpha]$

$$f(x) \mapsto f(\alpha).$$

Rõ ràng φ là một toàn cấu từ vành $A[x]$ đến vành $A[\alpha]$. Hơn nữa $\text{Ker}\varphi = I$ (dựa vào kết quả đã chứng minh trong câu a). Do đó $f(x) \in \text{Ker}\varphi$ khi và chỉ khi $\varphi(f(x)) = 0$ hay $f(\alpha) = 0$ hay $f(x) \in I$.

Theo định lí đồng cấu ta có $A[x]/I \cong A[\alpha]$

4.18. Chứng minh theo định nghĩa của đa thức bất khả quy.

4.19. Giả sử $\varphi: A \to V$ là một đồng cấu từ vành A đến vành V sao cho $\varphi(1) = 1$ và $u \in V$ là một phần tử cho trước. Khi đó có ánh xạ $\bar{\varphi}: A[x] \to V$ được xác định như sau

$$\bar{\varphi}(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} \varphi(a_i)u^i)$$

với mọi $f(x) = \sum_{i=0}^{n} a_i x^i \in A[x]$, $\bar{\varphi}$ là một đồng cấu. Thật vậy, ta có

$$\bar{\varphi}(\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i) = \bar{\varphi}(\sum_{i=0}^{n} (a_i + b_i)x^i$$

$$= \sum_{i=0}^{n} \varphi(a_i + b_i)u^i$$

$$= \sum_{i=0}^{n} (\varphi(a_i)u^i + \varphi(b^i)u^i$$

$$= \sum_{i=0}^{n} \varphi(a_i)u^i + \sum_{i=0}^{n} (\varphi(b_i)u^i$$

$$= \bar{\varphi}(\sum_{i=0}^{n} a_i x^i) + \bar{\varphi}(\sum_{i=0}^{n} b_i x^i).$$

Giả sử $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{j=0}^{m} b_j x^j$.

$f(x).g(x) = h(x) = \sum_{i=0}^{n+m} c_i x^i$ với $c_i = \sum_{k+l=i} a_k b_l$

$i = 0, \ldots n + m.$

Khi đó $\bar{\varphi}(f(x).g(x)) = \sum_{i=0}^{m+n} (\varphi(c_i))u^i =$

$$= \sum_{i=0}^{m+n} \varphi(\sum_{k+l=i} a_k b_l)u^i = \sum_{i=0}^{m+n} (\sum_{k+l=i} \varphi(a_k)\varphi(b_l))u^i . \quad (*)$$

Mặt khác $\bar{\varphi}(f(x)) = \bar{\varphi}(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} \varphi(a_i)u^i$

$$\bar{\varphi}(g(x)) = \bar{\varphi}(\sum_{j=0}^{m} b_j x^j) = \sum_{j=0}^{m} \varphi(b_i)u$$

do đó $\bar{\varphi}(f(x))\varphi(g(x)) = \sum_{i=0}^{n} \varphi(a_i)u_i . \sum_{j=0}^{m} \varphi(b_j)u^j$

$$= \sum_{i=0}^{n+m} (\sum_{k+l=i} \varphi(a_k)\varphi(b_l))u^i . \quad (**)$$

So sánh (*) với (**) ta thấy $\bar{\varphi}(f(x)g(x)) = \bar{\varphi}(f(x)).\bar{\varphi}(g(x))$.

Hơn nữa $\bar{\varphi}(x) = \bar{\varphi}(1.x) = \varphi(1).u = 1.u = u$;

và với mọi $a \in A$ ta có $\bar{\varphi}(a) = \varphi(a)$, nghĩa là $\bar{\varphi}|_A = \varphi$.

Bây giờ giả sử $\psi : A[x] \to A$ là một đồng cấu sao cho

$\psi(x) = u$ và $\psi|_A = \varphi$ thì với mọi $f(x) = \sum_{i=0}^{n} a_i x^i \in A[x]$ có

$$\psi(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} \psi(a_i)\psi(x^i) = \sum_{i=0}^{n} \varphi(a_i)u^i) = \bar{\varphi}\sum_{i=0}^{n} a_i x^i .$$

Vậy $\psi = \bar{\varphi}$. Tức là $\bar{\varphi}$ được xác định một cách duy nhất.

4.20. Xét ánh xạ φ: $A[x] \to \left(A/I\right)[x]$

$$f(x) = \sum_{i=0}^{n} a_i x^i \mapsto \bar{f}(x) = \sum_{i=0}^{n} (a_i + I)x^i$$

Ta có ngay φ là toàn cấu và $\text{Ker}\varphi = I[x]$.

Vậy theo định lí đẳng cấu suy ra:

a) $I[x]$ là iđêan của $A[x]$.

b) $A[x]/I[x] \cong \left(A/I\right)[x]$.

c) I là iđêan nguyên tố của A $\Leftrightarrow$ A/I là miền nguyên

$\Leftrightarrow \left(A/I\right)[x]$ là miền nguyên

$\Leftrightarrow A[x]/I[x]$ là miền nguyên

$\Leftrightarrow$ $I[x]$ là iđêan nguyên tố của $A[x]$.

d) Nếu I là iđêan tối đại của A thì $I[x]$ không là iđêan tối đại của $A[x]$ vì $A[x]/I[x] \cong \left(A/I\right)[x]$ không là trường.

4.21. Xét ánh xạ φ: $A[x] \to A$

$$f(x) = \sum_{i=0}^{n} a_i x^i \mapsto f(0) = a_0.$$

là một toàn cấu và

$$\text{Ker}\varphi = I = \{ \sum_{i=1}^{n} a_i x^i \mid a_i \in A,\ i = 1, \ldots n,\ n \geq 1 \}.$$

Từ đó suy ra I là một iđêan của A[x] đồng thời $A[x]/I \cong A$, vì A là một miền nguyên nên suy ra I là một iđêan nguyên tố của A[x].

Nếu A là một trường thì ta cũng có I là một iđêan tối đại của A[x].

4.22. Ta dùng phương pháp hệ số bất định để biểu diễn đa thức $x_1^4 + x_2^4 + x_3^4$ qua các đa thức đối xứng cơ bản.

Hệ thống số mũ là

$$M = \{(4, 0, 0), (3, 1, 0), (2, 2, 0), (2, 1, 1)\}.$$

Do đó $x_1^4 + x_2^4 + x_3^4 = \delta_1^4 + a\delta_1^2\delta_2 + b\delta_2^2 + c\delta_1\delta_3$

x_1	x_2	x_3	a	b	c
1	−1	0		2	
1	1	0	−4		
1	1	−1			4

Vậy $x_1^4 + x_2^4 + x_3^4 = \delta_1^4 - 4\delta_1^2\delta_2 + 2\delta_2^2 + 4\delta_1\delta_3$

4.23. Trong vành $\mathbb{Z}_2[x_1, x_2, x_3]$ ta có

$$(x_1 + x_2 + x_3)^4 = x_1^4 + x_2^4 + x_3^4$$

nên đa thức $x_1^4 + x_2^4 + x_3^4$ biểu diễn được qua các đa thức đối xứng cơ bản là

$$x_1^4 + x_2^4 + x_3^4 = \delta_1^4$$

4.24. Đặt $S_k = x^k + y^k$ ta có

$$S_1 = \delta_1$$

$$S_2 = x^2 + y^2 = \delta_1^2 - 2\delta_2 = \delta_1.S_1 - \delta_2.S_0$$

...

Tổng quát ta có

$(x + y + (x^{k-1} + y^{k-1}) = (x^k + y^k) + xy(x^{k-2} + y^{k-2})$

$x^k + y^k = \delta_1.S_{k-1} - \delta_2.S_{k-2}$.

Suy ra $S_3 = \delta_1^3 - 3\delta_1\delta_2$

$$S_4 = \delta_1^4 - 4\delta_1^2\delta_2 + 2\delta_2^2$$

$$S_5 = \delta_1^5 - 5\delta_1^3\delta_2 + 5\delta_1\delta_2^2.$$

b) Ta có $x^5 + 2x^3y^2 + 3x^2y^2 - x^4y - xy^4 + 2x^2y^3 + y^5$

$= (x^5 + y^5) + 2x^2y^2(x + y) + 3x^2y^2 - xy(x^3 + y^3)$

$= (\delta_1^5 - 5\delta_1^3\delta_2 + 5\delta_1\delta_2^2) + 2\delta_1\delta_2^2 + 3\delta_2^2 - \delta_2(\delta_1^3 - 3\delta_1\delta_2)$

$= \delta_1^5 - 6\delta_1^3\delta_2 + 10\delta_1\delta_2 + 3\delta_2^2$.

4.25. Đặt $\delta_1 = x + y + z$

$$\delta_2 = xy + yz + zx$$

$$\delta_3 = xyz.$$

Ta có hệ phương trình

$$\begin{cases} \delta_1 = 6 \\ \delta_3 = 6 \\ \delta_1^3 - 3\delta_1\delta_2 + 3\delta_3 = 36. \end{cases}$$

Từ hệ này tìm được $\delta_2 = 11$. Vậy x, y, z là ba nghiệm của phương trình bậc ba

$$f(X) = X^3 - 6X^2 + 11X - 6 = 0.$$

Phương trình này có một nghiệm là 1 (vì tổng các hệ số bằng 0).

Khi đó vế trái của phương trình có dạng

$$f(X) = (X - 1)(X^2 - 5X + 6).$$

Đa thức $X^2 - 5X + 6$ có nghiệm là 2 và 3. Vậy các số nguyên cần tìm là 1; 2 và 3.

4.26. Đặt $\delta_1 = x + y$

$\delta_2 = xy$ khi đó hệ đã cho trở thành

$$\begin{cases} \delta_1^3 - 3\delta_1\delta_2 = 8 \\ \delta_1^2 - 2\delta_2 = 4. \end{cases}$$

Từ hệ phương trình này suy ra

$$-\frac{1}{2}\delta_1^3 + 6\delta_1 - 8 = 0 \text{ hay}$$

$$\delta_1^3 + 12\delta_1 - 16 = 0.$$

Phương trình này có một nghiệm là 2. Vậy vế trái có dạng

$$(\delta_1 - 2)(\delta_1^2 + 2\delta_1 - 8).$$

Phương trình $\delta_1^2 + 2\delta_1 - 8 = 0$ có hai nghiệm là 2 và –4.

Với $\delta_1 = 2$ ta có $\delta_2 = 0$

$\delta_1 = -4$ ta có $\delta_2 = 6$.

Suy ra x và y là nghiệm của các hệ phương trình sau:

$$\begin{cases} x + y = 2 \\ xy = 0 \end{cases} \quad \text{và} \quad \begin{cases} x + y = -4 \\ xy = 6. \end{cases}$$

Các hệ phương trình này cho ta các nghiệm là

$$\begin{cases} x_1 = 2 \\ y_1 = 0 \end{cases} \qquad \begin{cases} x_2 = 0 \\ y_2 = 2 \end{cases}$$

$$\begin{cases} x_3 = -2 + i\sqrt{2} \\ y_3 = -2 - i\sqrt{2} \end{cases} \qquad \begin{cases} x_4 = -2 - i\sqrt{2} \\ y_4 = -2 + i\sqrt{2}. \end{cases}$$

4.27. Đặt $\delta_1 = x + y + z$

$$\delta_2 = xy + yz + zx$$

$$\delta_3 = xyz$$

khi đó hệ phương trình đã cho trở thành

$$\begin{cases} \delta_1 = a \\ \delta_1^2 - 2\delta_2 = b^2 \\ \delta_1^3 - 3\delta_1\delta_2 + 3\delta_3 = a^3. \end{cases}$$

Từ hệ này suy ra

$$\delta_1 = a$$

$$\delta_2 = \frac{1}{2}(a^2 - b^2)$$

$$\delta_3 = \frac{1}{2}a(a^2 - b^2).$$

Vậy x, y, z là nghiệm của phương trình bậc ba

$$f(X) = X^3 - aX^2 + \frac{1}{2}(a^2 - b^2)X - \frac{1}{2}a(a^2 - b^2) = 0.$$

Vế trái của phương trình phân tích được thành

$$f(X) = (X - a)\left[X^2 + \frac{1}{2}(a^2 - b^2)\right].$$

Vậy phương trình $f(x) = 0$ có các nghiệm là

$$X_1 = a, X_2 = \sqrt{\frac{b^2 - a^2}{2}}, X_3 = -\sqrt{\frac{b^2 - a^2}{2}}.$$

Khi kết hợp lại ta được sáu nghiệm của hệ phương trình đã cho.

4.28. Đặt $\delta_1 = x + y$

$\delta_2 = xy.$

Từ phương trình đã cho ta có phương trình $\delta_1 = \delta_1^2 - 3\delta_2$.

Vì x, y nguyên nên cũng là những số thực, vậy phải có $\delta_1^2 - 4\delta_2 \geq 0$ tức là $\delta_1^2 \geq 4\delta_2$, vì vậy

$$\delta_1^2 - \delta_1 = 3\delta_2 \leq \frac{3}{4}\delta_1^2$$

hay $\frac{1}{4}\delta_1^2 - \delta_1 \leq 0$ tức là $\delta_1(\delta_1 - 4) \leq 0$.

Từ đó suy ra $\begin{cases} 0 \leq \delta_1 \leq 4 \\ 3\delta_2 = \delta_1^2 - \delta_1 \end{cases}$,

ta có các hệ

$$\begin{cases} \delta_1 = 0 \\ \delta_2 = 0 \end{cases} \quad \begin{cases} \delta_1 = 1 \\ \delta_2 = 0 \end{cases} \quad \begin{cases} \delta_1 = 3 \\ \delta_2 = 2 \end{cases} \quad \begin{cases} \delta_1 = 4 \\ \delta_2 = 4 \end{cases}.$$

Từ đó suy ra

$$\begin{cases} x_1 = 0 \\ y_2 = 0 \end{cases} \quad \begin{cases} x_2 = 1 \\ y_2 = 0 \end{cases} \quad \begin{cases} x_3 = 0 \\ y_3 = 1 \end{cases} \quad \begin{cases} x_4 = 2 \\ y_4 = 1 \end{cases}$$

$$\begin{cases} x_5 = 1 \\ y_5 = 2 \end{cases} \quad \begin{cases} x_6 = 2 \\ y_6 = 2 \end{cases}.$$

4.29. Đặt $\delta_1 = x + y$

$\delta_2 = xy$.

Phương trình đã cho trở thành

$$\delta_1^3 - 3\delta_1\delta_2 - 1 = 3\delta_2$$

hay $(\delta_1 + 1)(\delta_1^2 - \delta_1 + 1 - 3\delta_2) = 0$.

Vì $x > 0, y > 0$ nên $\delta_1 = x + y > 0$, do đó $\delta_1 + 1 \neq 0$.

Vậy ta có $\delta_1^2 - \delta_1 - 3\delta_2 + 1 = 0$,

từ đó suy ra $\delta_2 = \frac{1}{3}(\delta_1^2 - \delta_1 + 1)$.

Vậy x và y thoả mãn

$$\begin{cases} x + y = \delta_1 \\ xy = \frac{1}{3}(\delta_1^2 - \delta_1 + 1) \end{cases}$$

Chúng là nghiệm của phương trình bậc hai

$$z^2 - \delta_1 z + \frac{1}{3}(\delta_1^2 - \delta_1 + 1) = 0. \qquad (1)$$

Phương trình (1) vô nghiệm nếu $\delta_1 \neq 2$.

Vậy phải có $\delta_1 = 2$ hay $x = y = 1$.

4.30. Gọi x_1, x_2, x_3, x_4 là bốn nghiệm của đa thức f(x). Khi đó

$$S = x_1^3 + x_2^3 + x_3^3 + x_4^3 = \delta_1^3 - 3\delta_1\delta_2 + 3\delta_3 \qquad (1)$$

với $\delta_1 = x_1 + x_2 + x_3 + x_4 = -1$

$$\delta_2 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 = 2$$

$\delta_3 = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 = -1.$

Thay vào (1) ta có S = 2.

4.31. a) Ta có $f(x, y) = 6(x^4 + y^4) - 11xy(x^2 + y^2) - 18x^2y^2 =$

$= 6(\delta_1^4 - 4\delta_1^2\delta_2 + 2\delta_2^2) - 11\delta_2(\delta_1^2 - 2\delta_2) - 18\delta_2^2$

$= 6\delta_1^4 - 35\delta_1^2\delta_2 + 16\delta_2^2.$

Vế phải là một tam thức bậc hai đối với δ_2. Nó có nghiệm là

$\delta_2 = 2\delta_1^2$ và $\delta_2 = \frac{3}{16}\delta_1^2.$

Vì vậy ta có

$f(x, y) = 16(\delta_2 - 2\delta_1^2)(\delta_2 - \frac{3}{16}\delta_1^2)$

$= (2\delta_1^2 - \delta_2)(3\delta_1^2 - 16\delta_2).$

$f(x, y) = (2x^2 + 3xy + 2y^2)\ (3x^2 - 10xy + 3y^2)$

$= (2x^2 + 3xy + 2y^2)\ (x - 3y)\ (3x - y).$

b) $g(x, y, z) = 2(x^2y^2 + x^2z^2 + y^2z^2) - (x^4 + y^4 + z^4)$

$= 2(\delta_2^2 - 2\delta_1\delta_3) - (\delta_1^4 - 4\delta_1^2\delta_2 + 2\delta_2^2 + 4\delta_1\delta_3)$

$= -\delta_1^4 + 4\delta_1^2\delta_2 - 8\delta_1\delta_3$

$= \delta_1(4\delta_1\delta_2 - \delta_1^3 - 8\delta_3).$

Vậy $g(x, y, z)$ chia hết cho $\delta_1 = x + y + z$.

$g(x, y, z)$ chỉ chứa các lũy thừa chẵn của x, y, z nên $g(x, y, z)$ cũng chia hết cho $x - y + z$, $-x + y + z$ và $x + y - z$. Vậy $g(x, y, z) =$

$(x + y + z)\ (x - y + z)\ (-x + y + z)\ (x + y - z).h(x, y, z).$

So sánh bậc của hai vế ta có bậc của h(x, y, z) bằng 0 đối với x, y, z tức là h là một số. Cho x = y = z = 1 ta được

$$3 = 3.\ h(x, y, z).$$

Suy ra h(x, y, z) = 1.

Vậy ta có g(x, y, z) =

$$(x + y + z)\,.\,(x - y + z)\,.\,(-x + y + z)\,.\,(x + y - z).$$

4.32. Ta có (x + y) (x + z) (y + z) =

$$= x^2y + x^2z + y^2z + y^2x + xz^2 + yz^2 + 2xyz$$

$$= \delta_1\delta_2 - 3\delta_3 + 2\delta_3$$

$$= \delta_1\delta_2 - \delta_3$$

$$= (x + y + z)\,(xy + yz + zx) - xyz.$$

4.33. Ta có $x^4 + y^4 + z^4 = \delta_1^4 - 4\delta_1^2\delta_2 + 2\delta_2^2 + 4\delta_1\delta_3$

Vì $\delta_1 = x + y + z = 0$ nên

$x^4 + y^4 + z^4 = 2\delta_2^2 = 2(xy + yz + zx)^2$.

4.34. Đặt $\delta_1 = a + b$, $\delta_2 = ab$

$$\Delta = \delta_1^2 - 4\delta_2$$

$$a^2 + b^2 = \delta_1^2 - 2\delta_2 = \delta_1^2 - 2.\frac{1}{4}(\delta_2^2 - \Delta)$$

$$= \frac{1}{2}\delta_1^2 + \frac{1}{2}\Delta.$$

Vì $\Delta \geq 0$ và $\delta_1 = a + b \geq c$ nên

$$a^2 + b^2 \geq \frac{1}{2}c^2.$$

4.35. Ta luôn có

$$(x-y)^2+(y-z)^2+(z-x)^2 \geq 0$$

$$\Leftrightarrow 2(x^2+y^2+z^2)-2(xy+yz+zx) \geq 0$$

$$\Leftrightarrow 2(\delta_1^2-2\delta_2)-2\delta_2 \geq 0$$

$$\Leftrightarrow 2\delta_1^2-6\delta_2 \geq 0$$

$$\Leftrightarrow 2\delta_1^2 \geq 6\delta_2$$

$$\Leftrightarrow \delta_1^2 \geq 3\delta_2$$

$$\Leftrightarrow (x+y+z)^2 \geq 3(xy+yz+zx).$$

Nếu $x = y = z$ thì đẳng thức xảy ra.

4.36. Theo kết quả bài 4.35, ta có

$$(x+y+z)^2 \geq 3(xy+yz+zx).$$

Thay $x = ab$, $y = ac$, $z = bc$ ta được

$$(ab+ac+bc)^2 \geq 3(a^2bc+ab^2c+abc^2) \text{ hay}$$

$$(ab+ac+bc)^2 \geq 3abc(a+b+c).$$

4.37. Vì x, y, z dương nên $\delta_1 > 0$, $\delta_2 > 0$, $\delta_3 > 0$. Theo kết quả bài 4.35 và 4.36 ta có

$$\delta_1^2 \geq 3\delta_2$$

$$\delta_2^2 \geq 3\delta_1\delta_3.$$

Từ đó suy ra

$$\delta_1^2\delta_2^2 \geq 9\delta_1\delta_2\delta_3.$$

Giản ước cho $\delta_1\delta_2$ ta được

$$\delta_1\delta_2 \geq 9\delta_3.$$

Vậy $(x+y+z)(xy+xz+yz) \geq 9xyz$.

4.38. $f(x, y) = (x^3 + y^3) + 3xy(x^2 + y^2) + 2xy(x + y) + 3x^2y^2$

$= \delta_1(\delta_1^2 - 3\delta_2) + 3\delta_2(\delta_1^2 - 2\delta_2) + 2\delta_1\delta_2 + 3\delta_2^2$

$= \delta_1^3 - \delta_1\delta_2 + 3\delta_1^2\delta_2 - 3\delta_2^2$

$= (\delta_1 - 3\delta_2)(\delta_1^2 - \delta_2)$

$= (x + y - 3xy)(x^2 + y^2 + xy).$

Các đa thức $g(x, y) = x + y - 3xy$ và $h(x, y) = x^2 + y^2 + xy$ bất khả quy trong $\mathbb{R}[x,y]$.

4.39. $f(x, y, z) = -x^4 - y^4 - z^4 + 2x^2y^2 + 2x^2z^2 + 2y^2z^2$

$= -(x^4 + y^4 + z^4) + 2(x^2y^2 + x^2z^2 + y^2z^2)$

$= -(\delta_1^4 - 4\delta_1^2\delta_2 + 2\delta_2^2 + 4\delta_1\delta_3) + 2(\delta_2^2 - \delta_1\delta_3)$

$= \delta_1(-\delta_1^3 + 4\delta_1\delta_2 - 8\delta_3),$

$f(x, y, z) = (x + y + z)(x + y - z)(x - y + z)(-x + y + z).$

4.40. $A = a(b^2 - 1)(c^2 - 1) + b(a^2 - 1)(c^2 - 1) + c(a^2 - 1)(b^2 - 1)$

$= abc(ab + ac + bc) - (ab^2 + ac^2 + ba^2 + bc^2 + ca^2 + cb^2) + (a + b + c)$

$= \delta_2\delta_3 - (\delta_1\delta_2 - 3\delta_3) + \delta_1.$

Theo giả thiết $\delta_1 = a + b + c = abc = \delta_3$.

Vậy $A = 4\delta_3 = 4abc$.

4.41. Ta có $A = x^4 + y^4 + z^4 = \delta_1^4 - 4\delta_1^2\delta_2 + 2\delta_2^2 + 4\delta_1\delta_3$

Do $\delta_1 = x + y + z = 0$ nên

$$A = 2\delta_2^2 = 2(xy + xz + yz)^2.$$

5.1. Cho đa thức $f(x) = ax^2 + bx + c \in \mathbb{R}[x]$, $a \neq 0$ với $\Delta = b^2 - 4ac < 0$. Do $\Delta < 0$ nên $f(x)$ không có nghiệm thực mà nó có hai nghiệm phức liên hợp. Nếu $f(x)$ khả quy, thì $f(x) = g(x)\ h(x)$ với $g(x)$ và $h(x)$ thuộc $\mathbb{R}[x]$ và bậc $g(x)$ = bậc $h(x) = 1$. Khi đó $g(x)$ và $h(x)$ lại có nghiệm thực. Các nghiệm này đồng thời cũng là nghiệm của $f(x)$, điều này mâu thuẫn với $\Delta < 0$. Vậy $f(x)$ là bất khả quy trong $\mathbb{R}[x]$.

Điều này không còn đúng khi thay trường số phức $\mathbb{C}$ cho trường số thực $\mathbb{R}$, vì đa thức bất khả quy trong $\mathbb{C}[x]$ là và chỉ là các đa thức bậc nhất.

5.2. (i) Giả sử a là ước của b, khi đó $\exists c \in X$ sao cho $b = ac \in aX$ suy ra $bX \subset aX$.

Đảo lại, nếu $bX \subset aX$ thì $b \in bX$ nên $b' \in aX$ do $b = ax$, $x \in X$ vậy a là ước của b.

ii) Áp dụng kết quả (i), a liên kết với b khi và chỉ khi $a \setminus b$ và $b \setminus a$ từ đó suy ra $bX \subset aX$ và $aX \subset bX$ vậy $aX = bX$.

5.3. (i) $\rightarrow$(ii)

Xét dãy giảm những ước thực sự $a_1, a_2, ..., a_n...$ (1)

trong đó a_i là ước thực sự của a_{i-1}. Ứng với dãy này ta có dãy tăng những iđêan chính của X là $(a_1) \underset{\neq}{\subset} (a_2) \underset{\neq}{\subset} ... \underset{\neq}{\subset} ...$ (2)

Dãy này dừng (theo (i)) nên dãy (1) dừng.

(ii) $\rightarrow$(i) Giả sử có dãy (2) là dãy tăng những iđêan chính, ta có dãy giảm những ước thực sự (1). Theo (i) dãy (1) dừng, vậy dãy (2) dừng.

(i) $\rightarrow$(iii) Giả sử Σ là một họ khác rỗng những iđêan chính của vành $\mathbb{R}$. Một iđêan I_1 của Σ. Nếu I_1 là phần tử tối đại của Σ (tức là I_1 không bị chứa thực sự trong một iđêan nào thuộc Σ) thì Σ có iđêan tối đại là I_1. Nếu I_1 không là phần tử tối đại của Σ thì có $I_2 \in \Sigma$ sao cho $I_1 \subset I_2$. Xét I_2 tương tự I_1 ta có dãy tăng những iđêan $I_1 \subset I_2 \subset ... \subset I_n ...$.

Dãy này dừng (theo (i)) tức là cuối cùng ta có I_m là phần tử tối đại của Σ.

(iii). Giả sử có dãy tăng những iđêan chính của vành X.

$$(a_1) \subset (a_2) \subset ... \subset (a_n) \subset ... \qquad (*)$$

Gọi $\Sigma = \{(a_i) \mid i = 1, 2, ...\}$ theo (iii), Σ có phần tử tối đại là (a_m) như vậy $\forall\ n > m$ đều có $a_m = a_n$.

Vậy dãy $(a_1, a_2, ..., a_m, ...)$ dừng.

5.4. a) Giả sử $f(x) = ax + b \in K[x]$, $a \neq 0$ có sự phân tích trong $K[x]$ là

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

với $g(x)$ và $h(x)$ thuộc $K[x]$, bậc $g(x) \leq$ bậc $f(x)$ và bậc $h(x) \leq$ bậc $f(x)$ đồng thời bậc $g(x)$ + bậc $h(x) = 1$.

Khi đó ta có nếu bậc $g(x) = 1$ thì bậc $h(x) = 0$ hay $h(x) \in K$ và $h(x) = d \neq 0$. Như vậy

$$g(x) = d^{-1} f(x)$$

tức là g(x) và f(x) liên kết với nhau. Nếu bậc g(x) = 0 thì g(x) $\in$ K và g(x) = d' $\neq$ 0 do đó h(x) = d'^{-1}f(x) hay f(x) và h(x) liên kết với nhau. Vậy trong cả hai trường hợp suy ra f(x) là đa thức bất khả quy.

Điều trên đây không còn đúng nữa nếu A không là một trường. Chẳng hạn đa thức

$$f(x) = 2x + 4 \in X[x]$$

có f(x) = 2(x + 2) cả 2 và x + 2 đều không là ước của 1 trong $\mathbb{Z}[x]$.Chứng tỏ f(x) không bất khả quy.

b) Giả sử f(x) $\in$ K[x], bậc f(x) = 2 hoặc bậc f(x) = 3.

f(x) khả quy $\Leftrightarrow$ f(x) = g(x) h(x);

g(x) và h(x) thuộc K[x] và hoặc g(x) hoặc h(x) có bậc một nghĩa là f(x) có nghiệm trong K.

Vậy f(x) bất khả quy khi và chỉ khi f(x) không có nghiệm trong K.

5.5. f(x) = 2x + 8 = 2(x + 4) do đó f(x) không là bất khả quy trong $\mathbb{Z}[x]$.

$g(x) = x^2 + 1$ là một đa thức nguyên bản không có nghiệm hữu tỉ.

Vậy g(x) là đa thức bất khả quy trong $\mathbb{Z}[x]$.

$$h(x) = x^2 + 2x - 2$$

h(x) có sự phân tích duy nhất trong $\mathbb{R}[x]$ là

$$h(x) = (x + 1 - \sqrt{3})(x + 1 + \sqrt{3})$$

và h(x) là một đa thức nguyên bản nên ta cũng suy ra h(x) bất khả quy trong $\mathbb{Z}[x]$.

5.6. Giả sử a, b $\in$ A với a và b nguyên tố cùng nhau trong vành chính A. Vì A là một vành chính nên tồn tại u và v thuộc A sao cho

$$au + bv = 1.$$

Như vậy ta có 1 thuộc vào iđêan sinh bởi a và b do đó iđêan này trùng với A.

5.7. Giả sử p là phần tử bất khả quy trong vành chính A; I là một iđêan của A sao cho Ap $\subset$ I, và Ap $\neq$ I. Như vậy có một phần tử a $\in$ I – Ap. Vì a $\notin$ Ap nên a không chia hết cho p, nên a và p là nguyên tố cùng nhau. Từ đó suy ra tồn tại u và v thuộc A sao cho

$$au + pv = 1.$$

Vì a $\in$ I và p $\in$ Ap $\subset$ I nên 1 = au + pv $\in$ I, vậy I = A. Điều đó chứng tỏ Ap là một iđêan tối đại của A.

Đảo lại, giả sử Ap là một iđêan tối đại của A, khi đó Ap $\neq$ A và do đó p không là ước của 1. Giả sử p không là bất khả quy, nghĩa là p có một ước thực sự là a $\in$ A để a.1 = p. Vì thế Aa $\neq$ A (do a không là ước của 1), Aa $\supset$ Ap và Aa $\neq$ Ap (do a không liên kết với p). Như vậy có iđêan Aa mà $Ap \subset_{\neq} Aa \subset_{\neq} A$, trái với giả thiết về tính tối đại của iđêan Ap.

Vậy p phải là phần tử bất khả quy trong A.

5.8. Do các tính chất A/I là một trường khi và chỉ khi I là iđêan tối đại và A/I là một miền nguyên khi và chỉ khi I là một

idêan nguyên tố của A, nên mọi idêan tối đại đều là idêan nguyên tố.

Bây giờ ta chứng minh rằng nếu A là một vành chính thì mọi idêan nguyên tố khác $\{0\}$ đều là tối đại. Thật vậy. Giả sử $I \neq \{0\}$ là một idêan nguyên tố của vành chính A. Vì A là vành chính nên tồn tại $a \in A$ sao cho $I = (a)$, vì I là nguyên tố nên $I \neq A$ do đó a không là ước của 1. Dựa vào kết quả bài 5.7, ta chỉ cần chứng minh a là phần tử bất khả quy trong A. Thật vậy, giả sử $a = uv$ với u và v thuộc A thì ta sẽ có $(a) \subset (u)$ và $(a) \subset (v)$.

Mặt khác vì $uv = a \in (a)$ nên hoặc $u \in (a)$ hoặc $v \in (a)$ hay $(u) \subset (a)$ hoặc $(v) \subset (a)$.

Từ các bao hàm thức trên ta suy ra hoặc $(a) = (u)$ hoặc $(a) = (v)$, nghĩa là hoặc a liên kết với u hoặc a liên kết với v. Vậy a là phần tử bất khả quy.

5.9. Nếu K là một trường thì K là một miền nguyên và K chỉ có hai idêan là K và $\{0\}$. Khi đó ta có K là idêan chính sinh bởi 1 và $\{0\}$ là idêan chính sinh bởi 0. Vậy K là một vành chính.

5.10. Vành thương của một vành chính có thể không phải là một vành chính. Chẳng hạn, vành số nguyên $\mathbb{Z}$ là một vành chính nhưng vành thương $\mathbb{Z}/4\mathbb{Z}$; $\mathbb{Z}/6\mathbb{Z}$ tổng quát hơn $\mathbb{Z}/m\mathbb{Z}$ (với $m > 1$, m không phải là một số nguyên tố) là những vành có ước của 0, do đó chúng không là vành chính.

5.11. Vành con của một vành chính có thể không phải là một vành chính. Chẳng hạn $m\mathbb{Z}$, $m > 1$ là một vành con của vành chính

$\mathbb{Z}$, nhưng nó không phải là một vành chính vì $m\mathbb{Z}$ không có đơn vị.

5.12. Ta chứng minh rằng vành $\mathbb{Z}[x]$ không phải là vành chính.

Thật vậy. Trong $\mathbb{Z}[x]$ ta xét iđêan I sinh bởi x và 2

$$I = \{f(x).x + 2.g(x) \mid f(x), g(x) \in \mathbb{Z}[x]\}.$$

$h(x) \in I$ nghĩa là hạng tử tự do của h(x) là một số chẵn. Hiển nhiên $I \neq \{0\}$ và $I \neq \mathbb{Z}[x]$. Giả sử I là một iđêan chính, nghĩa là tồn tại đa thức $g(x) \in \mathbb{Z}[x]$ sao cho $I = (g(x))$. Ta có

$$x = 1.x + 2.0 \text{ và } 2 = 0.x + 2.1$$

nên x và 2 thuộc I và do đó g(x) là ước của 2 và là ước của x. Nếu g(x) là ước của 2 thì g(x) chỉ có thể là ± 1 và ± 2. Nếu g(x) là ước của x thì g(x) chỉ là ± 1 và $\pm x$. Kết hợp lại g(x) bằng -1 hoặc $+1$. Nhưng vì $I \neq \mathbb{Z}[x]$ nên g(x) không thể là -1 hoặc 1 được. Vậy I không phải là một iđêan chính. Do đó $\mathbb{Z}[x]$ không phải là một vành chính.

5.13. a) Để chứng minh $A = \{a + b\sqrt{3}\,i \mid a, b \in \mathbb{Z}\}$ là một miền nguyên ta chỉ cần chứng minh A là một vành con chứa đơn vị của trường số phức $\mathbb{C}$. Thật vậy, $1 = 1 + 0\sqrt{3}\,i \in A$.

Giả sử $a + b\sqrt{3}\,i$ và $c + d\sqrt{3}\,i$ là hai phần tử của A. Khi đó

$$(a + b\sqrt{3}\,i) - (c + d\sqrt{3}\,i) = (a - c + (b - d)\sqrt{3}\,i) \in A$$

$(a + b\sqrt{3}\,i)(c + d\sqrt{3}\,i) = (ac - 3bd) + (ad + bc)\sqrt{3}\,i \in A.$

b) Với mỗi số phức $\alpha = a + bi$ ta gọi chuẩn của nó là $N(\alpha) = \alpha\overline{\alpha} = a^2 + b^2$. Khi đó nếu α và β là hai số phức thì ta có $N(\alpha\beta) = N(\alpha)N(\beta)$.

Thật vậy, $N(\alpha\beta) = (\alpha\beta)(\overline{\alpha\beta}) = \alpha\beta\overline{\alpha}\,\overline{\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = N(\alpha)N(\beta)$

Như vậy nếu $\alpha \in A$ mà α là ước của 1 thì $N(\alpha) = 1$. Ta có

$$N(2) = 4;\ N(1+\sqrt{3}\,i) = 4 \text{ và } N(1-\sqrt{3}\,i) = 4$$

nên các số 2 ; $1 + \sqrt{3}\,i$ và $1-\sqrt{3}\,i$ không là ước của 1. Bây giờ ta hãy chứng minh 2 không có ước thực sự trong A. Giả sử $\beta = x + y\sqrt{3}\,i$ là một ước của 2 khi đó $N(\beta) = x^2 + 3y^2$ phải là ước của 4.

Tức là hoặc $N(\beta) = 1$ hoặc $N(\beta) = 2$ hoặc $N(\beta) = 4$.

Nếu $N(\beta) = 1$ thì $\beta = 1 + 0\sqrt{3}i$ hoặc $\beta = -1 + 0\sqrt{3}i$ nên β là ước của 1.

Nếu $N(\beta) = 2$ thì ta có $x^2 + 3y^2 = 2$, điều này không thể xảy ra.

Nếu $N(\beta) = 4$ thì ta có $2 = \beta\gamma$ với $N(\gamma) = 1$ do đó $\gamma = \pm 1$ nên 2 và β liên kết với nhau. Vậy 2 không có ước thực sự trong A.

Tương tự ta chứng minh được $1 + \sqrt{3}i$ và $1 - \sqrt{3}i$ là những phần tử bất khả quy trong A.

A không phải là một vành chính vì trong A, 4 có hai sự phân tích thành một tích những phần tử khả quy:

$$4 = 2.\ 2 = (1 + \sqrt{3}i)(1 - \sqrt{3}i).$$

5.14. Xét vành $A = \{a + b\sqrt{2}\,i \mid a, b \in \mathbb{Z}\}$. Ta hãy chứng minh A là vành chính.

Ta thấy ngay $\mathbb{Q}(i\sqrt{2}) = \{\alpha + \beta\sqrt{2}i \mid \alpha, \beta \in \mathbb{Q}\}$ là một trường chứa miền A. Trên trục số, ta cũng thấy ngay cho một số hữu tỉ α, bao giờ cũng tìm thấy một số nguyên a sao cho $|\alpha - a| \le \frac{1}{2}$. Do đó ta có thể khẳng định được rằng: Với mọi $x \in \mathbb{Q}(i\sqrt{2})$, tồn tại $z \in A$ sao cho $|x - z|^2 \le \frac{3}{4} < 1$. (*)

Bây giờ hãy lấy một idêan I không tầm thường của A. Tập hợp $X = \left\{ |z|^2 \;\middle|\; 0 \ne z \in I \right\}$ là một bộ phận khác rỗng của $\mathbb{N}$ và không chứa). Vì $\mathbb{N}$ 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 tuỳ ý $v \in I$. Hiển nhiên $\frac{v}{u} \in \mathbb{Q}(i\sqrt{2})$.

Theo khẳng định (*), tồn tại $z \in A$ sao cho $\left|\frac{v}{u} - z\right|^2 < 1$ hay $|v - uz|^2 < |u|^2$. 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.

5.15. Theo bài $\mathbb{Z}[x]$ không là vành chính. Vì $x^2 + 2$ là đa thức bất khả quy trong $\mathbb{Z}[x]$. Do đó $(x^2 + 2)$ là một iđêan tối đại của $\mathbb{Z}[x]$ cho nên $\mathbb{Z}[x]/(x^2 + 2)$ là một trường.

Vậy $\mathbb{Z}[x]/(x^2 + 2)$ là một vành chính.

5.16. Làm tương tự bài 5.21.

5.17. Làm tương tự bài 5.15.

5.18. Có $d = p_1^{\gamma_1} p_2^{\gamma_2} ... p_n^{\gamma_n}$ với $\gamma_i = \min(\alpha_i, \beta_i)$ $i = 1, ..., n$, trong đó

$$a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_n^{\alpha_n}, \ \alpha_i \in \mathbb{N}, i = 1, ..., n$$

và $$b = p_1^{\beta_1} p_2^{\beta_2} ... p_n^{\beta_n}, \ \beta_i \in \mathbb{N}, i = 1, ..., n$$

là sự phân tích của a và b thành một tích những nhân tử bất khả quy trong một vành chính. Rõ ràng d là ước chung của a và b. Bây giờ giả sử c là một ước chung của a và b, và c có sự phân tích là

$$c = p_1^{\delta_1} p_2^{\delta_2} ... p_n^{\delta_n}.$$

Khi đó phải có $\delta_i \leq \alpha_i$ và $\delta_i \leq \beta_i$; $i = 1, ..., n$ do đó $\delta_i \leq \min(\alpha_i, \beta_i)$ *với* $i = 1, 2, ..., n$. Từ đó suy ra c là ước của d. Vậy d là ước chung lớn nhất của a và b.

5.19. Trước hết nếu A là một trường thì A[x] là một vành Ơclit, do đó A[x] là một vành chính.

Đảo lại, giả sử A[x] là một vành chính. Giả sử $a \in A$ là một phần tử khác 0. Ta xét tập hợp

$$I = \{xf(x) + ag(x) \mid f(x), g(x) \in A[x]\}.$$

I là một iđêan của A[x] sinh bởi a và x. Theo giả thiết A[x] là một vành chính nên I là một iđêan chính sinh bởi đa thức p(x), I = (p(x)). Khi đó p(x) phải là ước của a và do đó $p(x) \in A$ và p(x) là ước của x nên p(x) phải là ước của 1. Vậy I = A[x]. Suy ra $1 \in I$ và $1 = 0x + a.b$.

Điều đó chứng tỏ b là nghịch đảo của a. Vậy a khả nghịch, do đó A là một trường.

5.20. a) Hiển nhiên.

b) Giả sử a và b là hai phần tử bất kì của vành Gao-xơ A.

Nếu a = 0 hoặc b = 0 thì ước chung lớn nhất của a và b sẽ là phần tử khác 0 trong hai phần tử a và b. Nếu một trong hai phần tử là ước của đơn vị, chẳng hạn a là ước của đơn vị thì ta cũng có ngay a là ước chung lớn nhất của a và b. Bây giờ giả sử cả a và b có sự phân tích thành một tích những nhân tử bất khả quy trong A. Gọi $\{p_1, p_2, \ldots, p_n\}$ là tập hợp tất cả các nhân tử bất khả quy khác nhau của a và b. Khi đó ta có

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n} \text{ với } \alpha_i \geq 0, i = 1, \ldots, n$$

và $$b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n}, \beta_i \geq 0, i = 1, \ldots, n.$$

Khi đó ta sẽ có

$$d = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_n^{\gamma_n} \text{ với } \gamma_i = \min(\alpha_i, \beta_i); i = 1, \ldots, n,$$

là ước chung lớn nhất của a và b.

c) Giả sử $a \in A$ là một phần tử khác 0, khác ước của 1 có sự phân tích thành một tích những nhân tử bất khả quy trong A là $a = p_1p_2...p_k$, trong đó các p_i không nhất thiết là phân biệt thì ta nói rằng a có độ dài bằng k. Nếu a = bc với b và c là những ước thực sự của a thì ta sẽ được sự phân tích của a thành một tích những nhân tử bất khả quy bằng cách nhân các sự phân tích tương ứng của b và c với nhau. Như vậy độ dài của a bằng độ dài của b cộng với độ dài của c. Bây giờ giả sử trong A có một dãy tuỳ ý những ước thực sự :

$$a_1, a_2, ..., a_n \qquad (1)$$

trong đó a_{i+1} là ước thực sự của a_i với i = 1, 2, 3, ..., n − 1. Tương ứng với dãy này ta sẽ có một dãy giảm các độ dài của các phần tử a_i. Dãy các độ dài này dừng do đó dãy (1) dừng.

d) Giả sử A là miền nguyên thoả mãn tính chất b) và c) thì A là một vành Gao-xơ.

Trước hết ta chứng minh nếu miền nguyên A thoả mãn tính chất b) thì mọi phần tử bất khả quy đều là nguyên tố. Thật vậy, giả sử p là phần tử bất khả quy trong A, và p là ước của tích ab với $a, b \in A$. Do A có tính chất b) nên a và p có ước chung lớn nhất d. Vì p bất khả quy nên d liên kết với p hoặc d là ước của 1. Nếu d liên kết với p thì p là ước của a. Nếu d là ước của 1 thì b là ước chung lớn nhất của ab và pb. Vì $p \setminus ab$ và $p \setminus pb$ nên p chia hết ước chung lớn nhất b. Vậy chứng minh được rằng nếu $p \setminus ab$ thì $p \setminus a$ hoặc $p \setminus b$ hay p là phần tử nguyên tố.

Nếu A là vành thoả mãn tính chất c) thì mọi phần tử khác 0, khác ước của đơn vị đều có một ước bất khả quy. Thật vậy, giả sử $a \in A$ là một phần tử khác 0 và khác ước của 1. Nếu a

bất khả quy thì việc chứng minh xong. Nếu a không bất khả quy thì a có một ước thực sự là a_1. Nếu a_1 bất khả quy thì chứng minh xong. Nếu a_1 không bất khả quy thì a_1 có một ước thực sự là a_2. Hoặc a_2 bất khả quy hoặc a_2 có ước thực sự là a_3. Quá trình tiếp tục ta sẽ được một dãy những ước thực sự $a_1, a_2, ..., a_n...$ Theo giả thiết dãy này dừng nên cuối cùng phải có một ước của a là bất khả quy.

Bây giờ giả sử a là một phần tử khác 0, khác ước của 1. Nếu a bất khả quy thì xong. Nếu không, theo trên a có một ước bất khả quy thực sự p_1, $a = p_1a_1$. Nếu a_1 là bất khả quy thì xong. Nếu không, a_1 lại có sự phân tích $a_1 = p_2a_2$, trong đó p_2 là ước bất khả quy thực sự của a_1. Lặp lại quá trình trên ta sẽ được một dãy những ước thực sự:

$$a_1, a_2, ..., a_n.$$

Dãy này dừng. Như vậy cuối cùng ta sẽ được

$$a = p_1p_2...p_k$$

với các p_i là bất khả quy.

Ta hãy chứng minh tính chất duy nhất của dãy trên. Giả sử a có hai sự phân tích là:

$a = p_1p_2...p_k$; $p_1, p_2, ..., p_k$ là bất khả quy và

$a = q_1q_2...q_l$; $q_1, q_2, ..., q_l$ là bất khả quy.

Từ đó $p_1p_2...p_k = = q_1q_2...q_l$.

p_1 là ước của vế trái nên cũng là ước của vế phải. Và vì p_1 là bất khả quy nên p_1 phải là ước của một nhân tử q_i nào đó,

chẳng hạn p_1 là ước của q_1. Vì q_1 là bất khả quy nên $q_1 = p_1u_1$ với u_1 là ước của 1.

Vậy có $p_1p_2...p_k = u_1p_1q_2...q_l$.

Giản ước cho p_1 ta được $p_2p_3...p_k = u_1q...q_l$. Tiếp tục lập luận như trên nếu $k < l$ thì sau k lần giản ước ta được:

$$1 = u_1u_2...u_kq_{k+1}...q_l$$

Điều này không thể xảy ra vì q_i bất khả quy do đó $k \geq 1$.

Lập luận tương tự ta có $l \geq k$.

Vậy $k = l$ và $p_iu_i = q_i$; $i = 1, ..., k$.

Do đó A là một vành Gao-xơ.

5.21. Xét ánh xạ $\delta : A^* \to \mathbb{N}$

$$\alpha = a + b\sqrt{2}i \mapsto \delta(a) = a^2 + 2b^2 = N(\alpha) = |\alpha|^2.$$

Ta phải chứng minh δ là một ánh xạ Óclit.

Trong bài 5.13 ta đã chứng minh $N(\alpha\beta) = N(\alpha)N(\beta)$ nên nếu α là ước của β thì $N(\alpha) \leq N(\beta)$.

Cuối cùng cho $x, y \in A^*$ ta phải tìm q và r thuộc A sao cho $x = yq + r$; nếu $r \neq 0$ thì $\delta(r) < \delta(y)$.

Muốn vậy xét $\frac{x}{y} = \alpha + \beta i \in \mathbb{Q}(i\sqrt{2})$. Ta biết rằng cho một số hữu tỉ α bao giờ cũng tìm được một số nguyên a sao cho

$$|\alpha - a| \leq \frac{1}{2} \text{ hay } |\alpha - a|^2 \leq \frac{1}{4}.$$

Cũng làm như vậy đối với số hữu tỉ β, ta có $b \in \mathbb{Z}$ sao cho

$|\beta - b|^2 \le \frac{1}{4}$ hay $2|\beta - b|^2 \le \frac{1}{2}$: Đặt $q = a + b\sqrt{2}i$, ta có

$$\left|\frac{x - yq}{y}\right|^2 = \left|\frac{x}{y} - q\right|^2 = \left|(\alpha + \beta\sqrt{2}i) - (a + b\sqrt{2}i)\right|^2$$

$$= \left|(\alpha - a) + i\sqrt{2}(\beta - b)\right|^2$$

$$= (\alpha - a)^2 + 2(\beta - a)^2$$

$$\le \frac{1}{4} + \frac{1}{2} = \frac{3}{4} < 1.$$

Vậy $\left|\frac{x - yq}{y}\right|^2 < 1$ hay $|x - yq|^2 < |y|^2$.

Đặt $r = x - yq$, ta được $x = yq + r$ với $\delta(r) < \delta(y)$ nếu $r \neq 0$.

Chú ý. Cách chứng minh giống bài 5.14.

5.22. Giả sử A là một trường, khi đó A cùng với ánh xạ

$$\delta : A^* \to \mathbb{N}$$
$$a \mapsto \delta(a) = n_0$$

với n_0 là một số tự nhiên cho trước, là một vành Ơclit.

5.23. Giả sử A là một vành Ơclit với ánh xạ Ơclit:

$$\delta : A^* \to \mathbb{N}.$$

Nếu A là một trường thì với mọi $x \in A^*$ ta có $1 = xx^{-1}$.

Vậy $\delta(1) \ge \delta(x)$; mặt khác $x = 1.x$ vậy $\delta(x) \ge \delta(1)$. Kết luận $\delta(x) = \delta(1)$ với mọi $x \in A^*$.

Đảo lại, nếu δ là một ánh xạ hằng ; với $x = 1$ và $y \neq 0$ ta có q và r thuộc A sao cho

$$1 = yq + r.$$

Nếu $r \neq 0$ ta phải có $\delta(r) < \delta(y)$ nhưng δ là ánh xạ hằng. Vậy $r = 0$, nghĩa là mọi $y \neq 0$ đều có nghịch đảo.

5.24. Giả sử vành A với ánh xạ $\delta : A^* \to \mathbb{N}$ là một vành Oclit. Khi đó hoặc $\delta(A^*)$ là hữu hạn, hoặc $\delta(A^*)$ là vô hạn. Vì $\mathbb{N}$ là tập sắp thứ tự tốt và $\delta(A^*)$ là một tập con khác $\varnothing$ của $\mathbb{N}$ nên $\delta(A^*)$ có phần tử bé nhất và thừa hưởng thứ tự của $\mathbb{N}$.

Nếu $\delta(A^*)$ hữu hạn gồm m phần tử

$$\delta(A^*) = \{n_0, n_2, ..., n_{m-1}\} \text{ với } n_0 < n_2 < ... < n_{m-1};$$

khi đó ta lập ánh xạ

$\delta' : A^* \to \mathbb{N}$ như sau: $\delta'(a) = i$ nếu $\delta(a) = n_i$.

Nếu $\delta(A^*)$ là tập vô hạn, do mọi bộ phận khác rỗng của $\mathbb{N}$ đều có phần tử bé nhất nên $\delta(A^*)$ là dãy các số tự nhiên tăng sau đây $\delta(A^*) = \{n_0, n_1, ..., n_k, n_{k+1}, ...\}$ với $n_k < n_{k+1}$ và $k = 0, 1, 2, ...$ khi đó ta lập ánh xạ

$$\delta' : A^* \to \mathbb{N}$$

$\delta'(a) = i$ nếu $\delta(a) = n_i$.

Ta hãy chứng minh δ' là ánh xạ Óclit. Giả sử $a \setminus b$ với a và b thuộc A, khi đó $\delta(a) \leq \delta(b)$ chẳng hạn $\delta(a) = n_i$ và $\delta(b) = n_k$, với $n_i \leq n_k$ như vậy $i \leq k$ do đó $\delta'(a) \leq \delta'(b)$.

Giả sử $a \in A$ và $b \in A^*$ khi đó tồn tại q và r thuộc A sao cho $a = bq + r$ với $\delta(r) < \delta(b)$ nếu $r \neq 0$. Giả sử $\delta(b) = n_k$ và nếu $r \neq 0$ có $\delta(r) = n_l$ thì $n_l < n_k$, nên $l < k$ hay $\delta'(r) < \delta'(b)$.

5.25. Vì 1 là ước của mọi phần tử trong A* nên $\delta(1) \leq \delta(a)$ với mọi $a \in A^*$ do đó $\delta(1)$ là phần tử bé nhất trong $\delta(A^*)$. Giả sử $u \setminus 1$, nên $\delta(u) \leq \delta(1)$, suy ra $\delta(u) = \delta(1)$ là phần tử bé nhất trong $\delta(A^*)$.

Đảo lại, giả sử $u \in A^*$ sao cho $\delta(u) = \delta(a)$ với mọi $a \in A^*$. Vì A là vành Óclit nên cho 1 và u ta có v và r thuộc A sao cho $1 = uv + r$; nếu $r \neq 0$ thì $\delta(r) = \delta(u)$. Nhưng điều cuối cùng này không xảy ra được, vậy $r = 0$ và do đó u là ước của 1.

5.26. Giả sử A là một vành Óclit. áp dụng bài 5.24 ta có thể lấy ánh xạ Óclit δ của A sao cho $\delta(A^*)$ là dãy 0, 1, 2, ... (*) hữu hạn hay vô hạn. Theo giả thiết của bài toán, A không phải là một trường, nên dãy (*) có ít nhất hai phần tử. Lấy $x \in A^*$ sao cho $\delta(x) = 1$, áp dụng bài 5.25, x không khả nghịch. Giả sử y là một phần tử tuỳ ý của A. Lấy y chia cho x ta được

$$y = xq + r,\ \delta(r) < \delta(x) = 1 \text{ nếu } r \neq 0$$

nghĩa là $\delta(r) = 0$ nếu $r \neq 0$, hay r khả nghịch nếu $r \neq 0$ theo bài 5.25.

Vậy mọi phần tử y của A có dạng

$$y = xq$$

hay

$$y = xq + r,\ r \text{ khả nghịch.}$$

Nói cách khác mọi lớp của $A/(x)$ có một đại diện hoặc bằng 0 hoặc khả nghịch.

5.27. Trước hết ta đưa hai nhận xét sau:

1) Nếu $y = a + b\dfrac{1+i\sqrt{19}}{2}$ với a và b thuộc $\mathbb{Z}$ là một phần tử tuỳ ý thuộc $\mathbb{Z}\left[\dfrac{1+i\sqrt{19}}{2}\right]$ thì chuẩn của y, $N(y) = |y|^2$, là một số tự nhiên. Thật vậy

$$N(y) = |y|^2 = \left(a + \frac{b}{2}\right)^2 + \frac{19b^2}{4} \quad (\geq 0)$$

$$= a^2 + ab + 5b^2 \in \mathbb{N}$$

Mặt khác, nếy y có phần ảo, thì theo các đẳng thức trên $N(y) \geq 5$.

2) Các phần tử khả nghịch của $\mathbb{Z}\left[\dfrac{1+i\sqrt{19}}{2}\right]$ là ± 1.

Thật vậy, giả sử $u = a + b\dfrac{1+i\sqrt{19}}{2}$ sao cho có v để $uv = 1$.

Thế thì $N(u)N(v) = N(uv) = N(1) = 1$. Theo nhận xét 1), $N(u) = 1 = (a + \frac{b}{2})^2 + \frac{19b^2}{4}$ hay $(2a + b)^2 + 19b^2 = 4$. Vậy $b = 0$ và $4a^2 = 4$ hay $a = \pm 1$.

Áp dụng vào bài toán, ta hãy chứng minh bằng phản chứng. Giả sử $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ là một vành Ơclit, ta phải có

$$x = a + b\frac{1+i\sqrt{19}}{2} \text{ (theo bài 5.26)}$$

sao cho mọi y của vành có dạng $y = xq$ hay $y = xq \pm 1$ (theo nhận xét 2).

Trước hết x không thể không có phần ảo, vì nếu không có phần ảo, x sẽ có dạng $x = m \in \mathbb{Z}$, và mỗi y của vành sẽ có dạng $ma + mb\frac{1+i\sqrt{19}}{2}$, hay $ma \pm 1 + mb\frac{1+i\sqrt{19}}{2}$.

Như vậy y không chạy khắp $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ (vì x không khả nghịch nên $m \neq \pm 1$).

Vậy x phải có phần ảo, và do đó theo nhận xét 1) thì $N(x) \geq 5$. Bây giờ ta hãy lấy $y = 2$ thế thì $2 = xq$ hay $2 = xq \pm 1$. Nếu $2 = xq \pm 1$ thì $3 = xq$. ($1 = xq$ không xảy ra vì x không khả nghịch).

Nếu $xq = 2$ thì $N(x)N(q) = 4$. Nhưng $N(x) \geq 5$ nên $N(x) = 9$ và $N(q) = 1$. Theo nhận xét 1) thì $q = \pm 1$, vậy $x = \pm 3$, mâu thuẫn với việc x phải có phần ảo.

5.28. Dùng thuật toán Ơclit

$$x^5 + x^3 + x^2 + x + 1 \;\Big|\; x^3 + 2x^2 + x + 1$$
$$x^5 + 2x^4 + x^3 + x^2 \qquad\qquad x^2 - 2x + 4$$
$$-2x^4 + x + 1$$
$$-2x^4 - 4x^3 - 2x^2 - 2x$$
$$4x^3 + 2x^2 + 3x + 1$$
$$4x^3 + 8x^2 + 4x + 4$$

$$6x^3 + 12x^2 + 6x + 6 \;\Big|\; -6x^2 - x - 3$$
$$6x^3 + x^2 + 3x \qquad\qquad -x - \frac{11}{6}$$
$$11x^2 + 3x + 6$$
$$11x^2 + \frac{11}{6}x + \frac{11}{2}$$

$$6x^2 + x + 3 \;\Big|\; \frac{7}{6}x + \frac{1}{2}$$
$$6x^2 + \frac{18}{7}x + 3 \;\Big|\; \frac{36}{7}x - \frac{66}{7}$$
$$-\frac{11}{7}x + 3$$
$$-\frac{11}{7}x - \frac{33}{7}$$
$$7\frac{5}{7}$$

Vậy ước chung lớn nhất của f(x) và g(x) là 1.

Có thể nhận xét như sau: Đa thức $g(x) = x^3 + 2x^2 + x + \bar{1}$ bậc ba không có nghiệm hữu tỉ do đó g(x) bất khả quy trong $\mathbb{Q}[x]$ (bài tập 2.28) và f(x) không chia hết cho g(x) nên ước chung lớn nhất của f(x) và g(x) bằng 1.

5.29. Dùng thuật toán Ơclit

$$\begin{array}{r|l} x^5 + x^3 + x^2 + x + \bar{1} & x^3 + \bar{2}x^2 + x + \bar{1} \\ \hline x^5 + \bar{2}x^4 + x^3 + x^2 & x^2 + x + \bar{1} \\ \hline x^4 + x + \bar{1} & \end{array}$$

$$\begin{array}{r|l} x^4 + \bar{2}x^3 + x^2 + x & x^3 + \bar{2}x^2 + x + \bar{1} \\ \hline x^3 + \bar{2}x^2 + \bar{1} & \bar{2}x \\ \hline \bar{2}x^2 + x + \bar{2} & \end{array}$$

$$\begin{array}{r|l} x^3 + \bar{2}x^2 + x + \bar{1} & \bar{2}x^2 + x + \bar{1} \\ \hline x^3 & x \\ \hline \bar{2}x^2 + x + \bar{1} & \\ \hline \bar{2}x^2 & \\ \hline x + \bar{1} & \\ \hline x & \\ \hline \bar{1} & \end{array}$$

Vậy ước chung lớn nhất của f(x) và g(x) bằng 1. Cũng nhận xét như bài 5.28, bậc g(x) bằng 3 và g(x) không có nghiệm trong $\mathbb{Z}_3$ nên g(x) là bất khả quy trong $\mathbb{Z}_3[x]$ và f(x) không chia hết cho g(x), nên ước chung lớn nhất của chúng bằng 1.

5.30. a) Ta chỉ cần chứng minh $\mathbb{R}(\sqrt{-3})$ là một trường con của trường số phức $\mathbb{C}$.

Ta có $0 = 0 + 0.\sqrt{3}\,i \in \mathbb{R}(\sqrt{-3})$ và

$1 = 1 + 0.\sqrt{3}\,i \in \mathbb{R}(\sqrt{-3})$ nên $\mathbb{R}(\sqrt{-3})$ có nhiều hơn một phần tử. Giả sử $a + b\sqrt{3}\,i$ và $c + d\sqrt{3}\,i$ là hai phần tử thuộc $\mathbb{R}(\sqrt{-3})$ ta có

$$(a + b\sqrt{3}\,i) - c + d\sqrt{3}\,i) - (a - c) + (b - d)\sqrt{3}\,i \in \mathbb{R}(\sqrt{-3}).$$

Nếu $c + d\sqrt{3}\,i \neq 0$ thì

$$\frac{a + b\sqrt{3}i}{c + d\sqrt{3}i} = \frac{(a + b\sqrt{3}i)(c - d\sqrt{3}i)}{c^2 + 3d^2}$$

$$= \frac{ac + 3bd}{c^2 + 3d^2} + \frac{bc - ad}{c^2 + 3d^2}\sqrt{3}i \in \mathbb{R}(\sqrt{3}).$$

Vậy $\mathbb{R}(\sqrt{-3})$ là một trường con của $\mathbb{C}$.

Tương tự ta chứng minh được $\mathbb{Q}(\sqrt{-3})$ và $\mathbb{Q}(\sqrt{2})$ lần lượt là trường con của $\mathbb{C}$ và $\mathbb{R}$.

b) Xét ánh xạ $\varphi : \mathbb{R}[x] \to \mathbb{C}$

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n \mapsto f(\sqrt{-3}) =$$

$$= a_0 + a_1\sqrt{3}i + \ldots + a_n(\sqrt{3}i)^n.$$

Ta có φ là một đồng cấu từ vành $\mathbb{R}[x]$ đến $\mathbb{C}$ và $\text{Im}\varphi = \mathbb{R}(\sqrt{-3})$. Ngoài ra ta có $\text{Ker}\varphi = (x^2 + 3)$ là iđêan sinh bởi $x^2 + 3$. Theo định lí đồng cấu

$$\mathbb{R}[x]/(x^2 + 3) \cong \mathbb{R}(\sqrt{-3}).$$

c) Xét ánh xạ $\varphi : \mathbb{Q}[x] \to \mathbb{R}$

$$f(x) \mapsto f(\sqrt{2}).$$

Ta cũng có φ là một đồng cấu, $\text{Im}\varphi = \mathbb{Q}(\sqrt{2})$ và $\text{Ker}\varphi = (x^2 - 2)$ là iđêan sinh bởi đa thức $x^2 - 2$ trong $\mathbb{Q}[x]$.

Vậy $\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}(\sqrt{2})$.

5.31. $f(x)$ là một đa thức bất khả quy của $K[x]$ nên mọi đa thức $g(x) \in K[x]$ hoặc nguyên tố với $f(x)$ hoặc chia hết cho $f(x)$. Nếu $f(x)$ và $g(x)$ cùng nhận $u \in E$ làm nghiệm thì chúng cùng nhận ước chung là $x - u$, vậy chúng không nguyên tố cùng nhau (khái niệm bất khả quy phụ thuộc vào trường mà ta đang xét nhưng khái niệm nguyên tố cùng nhau không như vậy) cho nên $g(x)$ chia hết cho $f(x)$, nghĩa là có $q(x) \in K[x]$ để $g(x) = f(x)q(d)$. Từ đó suy ra a) và b).

c) Xét ánh xạ $\varphi : K[x] \to E$

$$g(x) \mapsto g(u).$$

Rõ ràng φ là một đồng cấu và $\text{Im}\varphi = K[u]$.

Ngoài ra, dựa vào câu b) ta có $\text{Ker}\varphi = (f(x))$.

Theo định lí đồng cấu $K[x]/(f(x)) \cong K[u]$.

Theo bài 5.5 ta có K[u] là một trường.

5.32. Theo bài 5.31 c) K[u] là một trường. Mặt khác, K[u] là một trường chứa trường K và chứa trong trường E. Hiển nhiên với phép cộng và phép nhân trong E, K[u] là một không gian vectơ trên K.

Cũng theo bài 5.31 c) mỗi phần tử của $K[x]/(f(x))$ có đại diện là một đa thức có bậc $\leq n-1$ hay đa thức 0. Vậy các phần tử của K[u] có dạng $a_0 + a_1u + ... + a_{n-1}u^{n-1}$, $a_i \in K$, $i = 0, ..., n-1$.

Vậy $\{1, u, ..., u^{n-1}\}$ là một hệ sinh của không gian véctơ K[u]. Hệ sinh đó là độc lập tuyến tính. Thật vậy, giả sử có $a_0, a_1, ..., a_{n-1} \in K$ không bằng 0 tất cả, sao cho

$$a_0 + a_1u + ... + a_{n-1}u^{n-1} = 0$$

thế thì đa thức $r(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1}$ có bậc bé hơn n, nhận u làm nghiệm, trái với kết quả của bài 5.31.

Do $\{1, u, ..., u^{n-1}\}$ là một cơ sở của K[u], nên K[u] có số chiều bằng n.

5.33. Trước hết ta chứng minh nếu

$$\varphi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$$

là một tự đẳng cấu của $\mathbb{Q}(\sqrt{2})$ thì $\varphi(a) = a$ với mọi $a \in \mathbb{Q}$.

Thật vậy, vì φ là một tự đẳng cấu của $\mathbb{Q}(\sqrt{2})$ nên φ là một tự đẳng cấu của nhóm nhân các số khác 0 của $\mathbb{Q}(\sqrt{2})$, mà một đẳng cấu của nhóm nhân đến một nhóm nhân thì biến đơn vị thành đơn vị. Cho nên với mỗi số nguyên n có $\varphi(n) = \varphi(n.1) = n.1 = n$ và nếu $n \neq 0$ thì

$$\varphi(1) = \varphi\left(n.\frac{1}{n}\right) = n\varphi\left(\frac{1}{n}\right) = 1.$$

Vậy $\varphi\left(\frac{1}{n}\right) = \frac{1}{n}$. Từ đó suy ra $\varphi\left(\frac{p}{q}\right) = p\varphi\left(\frac{1}{q}\right) = \frac{p}{q}$ với $\frac{p}{q}$ là phân số bất kì thuộc $\mathbb{Q}$.

Cuối cùng ta có $\left[\varphi(\sqrt{2})\right]^2 = \varphi(\sqrt{2^2}) = \varphi(2) = 2$.

Vậy $\varphi(\sqrt{2}) = \sqrt{2}$ hoặc $\varphi(\sqrt{2}) = -\sqrt{2}$.

Như vậy, nếu φ là tự đẳng cấu của $\mathbb{Q}(\sqrt{2})$ thì với mọi $a + b\sqrt{2}$ thuộc $\mathbb{Q}(\sqrt{2})$

$$\varphi(a + b\sqrt{2}) = \varphi(a) + \varphi(b)\varphi(\sqrt{2}) = a + b\varphi(\sqrt{2})$$

Vậy hoặc $\varphi(a + b\sqrt{2}) = a + b\sqrt{2}$

hoặc $\varphi(a + b\sqrt{2}) = a - b\sqrt{2}$.

5.34. a) Xét ánh xạ

$$\varphi : \mathbb{Q}(\sqrt{2}) \to X = \mathbb{Q}^2$$
$$a + b\sqrt{2} \mapsto (a, b)$$

Ta có φ là một song ánh và

$$\begin{aligned}\varphi((a + b\sqrt{2}) + (c + d\sqrt{2})) &= \varphi(a + c + (b + d)\sqrt{2}) \\ &= (a + c, b + d) \\ &= (a, b) + (c, d) \\ &= \varphi(a + b\sqrt{2}) + \varphi(c + d\sqrt{2});\end{aligned}$$

$$\varphi((a+b\sqrt{2})(c+d\sqrt{2})) = \varphi(ac+2bd+(ad+bc)\sqrt{2})$$
$$= (ac+2bd, ad+bc)$$
$$= (a, b)(c, d)$$
$$= \varphi(a+b\sqrt{2})\varphi(c+d\sqrt{2}).$$

Vậy φ là một đẳng cấu. Theo bài 5.30a), $\mathbb{Q}(\sqrt{2})$ là một trường nên X cũng là một trường.

b) Theo bài 5.33, $\mathbb{Q}(\sqrt{2})$ có hai tự đẳng cấu và theo câu a) $\mathbb{Q}(\sqrt{2}) \cong X$ nên X có hai tự đẳng cấu, đó là tự đẳng cấu đồng nhất và tự đẳng cấu xác định bởi:

$$X \to X$$
$$(a,b) \mapsto (a,-b)$$

Do đó tập hợp các tự đẳng cấu của X là một nhóm xyclic cấp hai.

5.35. Xét phép chiếu chính tắc $\varphi : \mathbb{Z} \to \mathbb{Z}_p$

$$a \mapsto \varphi(a) = a + p\mathbb{Z} = \bar{a}$$

φ là một toàn cấu. φ mở rộng được thành một đồng cấu $\bar{\varphi}$ từ $\mathbb{Z}[n]$ đến $\mathbb{Z}_p[x]$:

$$\bar{\varphi} : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$$

$$f(x) = a_0 + a_1 + \ldots + a_n x^n \mapsto \varphi(a_0) + \varphi(a_i)x + \ldots + \varphi(a_n)x^n$$

Nếu $f(x) \in \mathbb{Z}[x]$, $f(x)$ không bất khả quy trong $\mathbb{Q}[x]$ thì $f(x) = g(x)h(x)$ với $g(x)$ và $h(x)$ thuộc $\mathbb{Z}[x]$ mà $1 < \deg g(x)$ $\deg h(x) < \deg f(x)$.

Khi đó $\overline{\varphi}(f(x)) = \overline{\varphi}(g(x))\overline{\varphi}(h(x))$ với $\overline{\varphi}(f(x))$, $\overline{\varphi}(g(x))$ và $\overline{\varphi}(h(x))$ đều thuộc $\mathbb{Z}[x]$ thỏa mãn

$$\deg \overline{\varphi}(g(x)) = \deg g(x) > 1$$
$$\deg \overline{\varphi}(h(x)) = \deg h(x) > 1.$$

Do đó $\overline{\varphi}(f(x))$ không bất khả quy trong $\mathbb{Z}_p[x]$.

Vậy nếu $f(x)$ bất khả quy trong $\mathbb{Z}[x]$ thì nó bất khả quy trong $\mathbb{Q}[x]$.

5.36. (Chứng minh theo định nghĩa của đồng cấu)

Dễ dàng kiểm tra được $\varphi : A[x] \to A[x]$

$$f(x) \mapsto f(ax + b)$$

là một đồng cấu.

Nếu a khả nghịch thì φ có ánh xạ ngược là

$$\overline{\varphi} : A[x] \to A[x]$$
$$f(x) \mapsto f(a^{-1}x - a^{-1}b).$$

5.37. $f(x) = x^5 - x^4 - 3x^3 + 2x + 4$.

a) Trong $\mathbb{Q}[x]$ ta có $f(x) = (x^2 - 2)(x - 2)(x^2 + x + 1)$

b) Trong $\mathbb{Q}(\sqrt{2})[x]$ ta có

$$f(x) = (x - \sqrt{2})(x + \sqrt{2})(x^2 + x + 1)$$

c) Trong $\mathbb{R}[x]$ ta có $f(x) = (x - \sqrt{2})(x + \sqrt{2})(x^2 + x + 1)$

d) Trong $\mathbb{C}[x]$ ta có

$$f(x) = (x - \sqrt{2})(x + \sqrt{2})\left(x + \frac{1}{2} - \frac{i\sqrt{3}}{2}\right)\left(x + \frac{1}{2} + \frac{i\sqrt{3}}{2}\right).$$

5.38. a) Giả sử $f(x) = a_0 + a_1x + ... + a_nx_n \in A[x]$ và

$$g(x) = b_0 + b_1x + ... + b_mx_m \in A[x]$$

là hai đa thức nguyên bản. Khi đó ước chung lớn nhất của các hệ số a, a_1,..., a_n và ước chung lớn nhất của các hệ số b_0, b_1,..., b_m đều bằng 1.

Đặt $h(x) = f(x)g(x) = c_0 + c_1x + ... + c_{m+n}x^{m+n}$

trong đó $c_i = \sum_{k+l=i} a_k b_l$, $i = 0, m + n$

Nếu h(x) không là đa thức nguyên bản, tức là các hệ số c_0, c_1, ..., c_{m+n} có một ước chung là phần tử nguyên tố p. Vì các a_i nguyên tố cùng nhau nên tồn tại a_k mà a_k không chia hết cho p

Giả sử r là chỉ số bé nhất sao cho a_r không chia hết cho p.

Tương tự, giả sử s là chỉ số bé nhất sao cho b_s không chia hết cho p.

Từ đây lại suy ra C_{r+s} không chia hết cho p (mâu thuẫn).

Vậy h(x) phải là đa thức nguyên bản.

b) Giả sử $f(x) \in A[x]$, f(x) khả quy trong $\overline{A}[x]$. Tức là trong A[x], f(x) = g(x)h(x) với g(x) và h(x) thuộc $\overline{A}[x]$

$$1 < \deg g(x), \deg h(x) < \deg f(x).$$

Đặt $\frac{a_1}{b_1}g_1(x) = g(x)$ trong đó $\frac{a_1}{b_1} \in \overline{A}$, $g_1(x) \in A[x]$ và $g_1(x)$ nguyên bản ;

$\frac{a_2}{b_2} h_1(x) = h(x)$ với $\frac{a_2}{b_2} \in \bar{A}$, $h_2(x) \in A[x]$, $h_1(x)$ nguyên bản khi đó

$$f(x) = \frac{a_1 a_2}{b_1 b_2} g_1(x) h_1(x).$$

Đặt $\frac{a}{b} = \frac{a_1 a_2}{b_1 b_2}$ với a và b nguyên tố cùng nhau, ta có $f(x) = \frac{a}{b} g_1(x) h_1(x)$. Vì $h_1(x)$ và $g_1(x)$ là hai đa thức nguyên bản nên $g_1(x)h_1(x)$ là đa thức nguyên bản.

Do $f(x) \in A[x]$ nên ta cũng suy ra $\frac{a}{b} \in A$. Vậy $f(x)$ cũng không bất khả quy trong $A[x]$.

5.39. Làm tương tự bài 6.20 (chương 6). Khi thay $\mathbb{Z}$ bằng một vành Gao-xơ bất kì.

Kết quả sẽ không còn đúng nếu thay giả thiết "vành Gao-xơ" bằng "vành chính" hoặc "vành Ơclit". Khi A là vành chính không suy ra được A[x] là vành chính. Khi A là vành Ơclit thì cũng không suy ra được A[x] là vành chính. Kết quả chỉ đúng khi A là một trường thì A[x] là một vành Ơclit và do đó cũng là vành chính.

5.40. a) $f(x) = x^4 - 10x^2 + 1$;

b) $f(x) = x^4 - 10x^2 + 1$;

c) $f(x) = x^4 + 2x^2 + 25$.

5.41. Trong cả ba trường hợp, số chiều của $\mathbb{Q}[u]$ đều bằng 4.

6.1. a) $x^2 + i = x^2 - (\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2})^2 =$

$$= \left[x - (\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2})\right]\left[x + (\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2})\right].$$

b) Đổi ra dạng lượng giác ta có

$$1 + i = \sqrt{2}(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4})$$

đặt $\alpha_1 = \sqrt[4]{\sqrt{2}(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4})} = \sqrt[8]{2}(\cos\frac{\pi}{16} + i\sin\frac{\pi}{16})$

là một giá trị của $\sqrt[4]{1+i}$ ta có

$\alpha_2 = \alpha_1 i$, $\alpha_3 = \alpha_1 i^2$, $\alpha_4 = \alpha_1 i^3$. Do $x^4 - 1 - i = x^4 - \alpha^4$ nên ta có

$$x^4 - 1 - i = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4)$$

c) Ta có căn bậc hai của số phức $4i - 3$ là $1 + 2i$ và $-1 - 2i$, do đó $x^2 - 4i + 3 = x^2 - (1 + 2i)^2$

$$= (x - 1 - 2i)(x + 1 + 2i).$$

d) Viết $1 + i\sqrt{3}$ dưới dạng lượng giác

$$1 + i\sqrt{3} = 2(\frac{1}{2} + i\frac{\sqrt{3}}{2}) = 2(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3})$$

Gọi α là một giá trị của căn bậc bảy của $1 + i\sqrt{3}$,

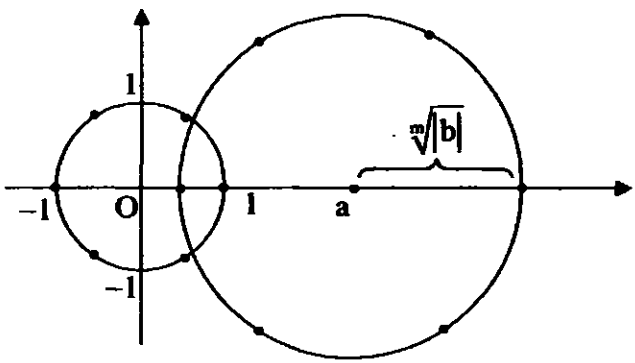
$\alpha = \sqrt[7]{2}(\cos\frac{\pi}{21} + i\sin\frac{\pi}{21})$, các giá trị còn lại của căn bậc bảy của $1+i\sqrt{3}$ là $\alpha_1 = \alpha\varepsilon$, $\alpha_2 = \alpha\varepsilon^2$, $\alpha_3 = \alpha\varepsilon^3$, $\alpha_4 = \alpha\varepsilon^4$, $\alpha_5 = \alpha\varepsilon^5$, $\alpha_6 = \alpha\varepsilon^6$, $\alpha_7 = \alpha\varepsilon^7 = \alpha$ với ε là một căn nguyên thuỷ bậc bảy của 1.

Ta có $x^7 - 1 - i\sqrt{3} = (x-\alpha_1)(x-\alpha_2)...(x-\alpha_7)$.

6.2. Biểu diễn hình học nghiệm của đa thức

$f(x) = x^p - 1$

$g(x) = (x-a)^m - b$ $(a \neq 0)$.



Hình 14

Nghiệm của đa thức $x^p - 1$ là các giá trị của căn bậc p của đơn vị.

Gọi α là một giá trị của căn bậc m của b và $\alpha\varepsilon$, $\alpha\varepsilon^2$, ..., $\alpha\varepsilon^{m-1}$ là các giá trị còn lại của căn bậc m của b, với ε là một căn nguyên thuỷ bậc m của đơn vị. Khi đó các nghiệm của đa thức g(x) là $\alpha+a$, $\alpha\varepsilon+a$, ..., $\alpha\varepsilon^{m-1}+a$. Vậy các nghiệm của đa thức f(x) là các điểm nằm trên đường tròn đơn vị tâm (0, 0). Các nghiệm của đa thức g(x) là các

điểm nằm trên đường tròn tâm (a, 0) bán kính bằng $\sqrt[m]{|b|}$. Hai đường tròn này cắt nhau không quá hai điểm vì chúng không đồng tâm (a, 0) $\neq$ (0, 0). Vậy hai đa thức này chỉ có nhiều nhất là hai nghiệm chung.

6.3. Xét phương trình

$$f(x) = (1 - x^2)^3 - (-2x)^3 = 0 \text{ hay } (1 - x^2)^3 = (-2x)^3. \quad (1)$$

Gọi ε là một căn nguyên thuỷ bậc ba của 1 thì phương trình (1) tương đương với tuyển ba phương trình sau:

$$\begin{cases} 1 - x^2 = -2x \\ 1 - x^2 = -2\varepsilon x \\ 1 - x^2 = -2\varepsilon^2 x \end{cases} \Leftrightarrow \begin{cases} 1 - x^2 + 2x = 0 & (2a) \\ 1 - x^2 = 2\varepsilon x = 0 & (2b) \\ 1 - x^2 + 2\varepsilon^2 x = 0 & (2c) \end{cases}$$

Phương trình (2a) có hai nghiệm là

$$x_1 = 1 + \sqrt{2}$$

$$x_2 = 1 - \sqrt{2}.$$

Phương trình (2b) có hai nghiệm là

$$x_3 = \varepsilon + \sqrt{\varepsilon^2 + 1} = \varepsilon + \sqrt{-\varepsilon}$$

$$x_4 = \varepsilon - \sqrt{\varepsilon^2 + 1} = \varepsilon - \sqrt{-\varepsilon}.$$

Phương trình (2c) ta có hai nghiệm là

$$x_5 = \varepsilon^2 + \sqrt{1 + \varepsilon} = \varepsilon^2 + \sqrt{-\varepsilon^2}$$

$$x_6 = \varepsilon^2 - \sqrt{1 + \varepsilon} = \varepsilon^2 - \sqrt{-\varepsilon^2}$$

Ta có $x_5 = \overline{x}_3$ vì $\varepsilon^2 = \overline{\varepsilon}$;

$x_6 = \overline{x}_4$ vì $\varepsilon^2 = \overline{\varepsilon}$.

Vậy $f(x) = (x - x_1)(x - x_2)(x - x_3)(x - x_4)(x - x_5)(x - x_6)$

$=(x-x_1)(x-x_2)[(x-x_3)(x-x_5)][(x-x_4)(x-x_6)]$.

Đặt $\varepsilon = -\frac{1}{2}+i\frac{\sqrt{3}}{2}$ ta có $\varepsilon^2 = -\frac{1}{2}-i\frac{\sqrt{3}}{2}$ và

$$x_3 = \frac{\sqrt{3}-1}{2}+i\frac{\sqrt{3}-1}{2},\ x_4 = \frac{-\sqrt{3}-1}{2}+i\frac{\sqrt{3}+1}{2}$$

$$x_5 = \frac{\sqrt{3}-1}{2}-i\frac{\sqrt{3}-1}{2},\ x_6 = \frac{-\sqrt{3}-1}{2}-i\frac{\sqrt{3}+1}{2}$$

là các nghiệm phức của đa thức f(x).

Vậy

$$f(x) = (x-1-\sqrt{2})(x-1+\sqrt{2}).[x^2+(1-\sqrt{3})x+(2-\sqrt{3})]$$
$$.[x^2+(1+\sqrt{3})x+(2+\sqrt{3})]$$

là sự phân tích f(x) thành một tích những đa thức bất khả quy trong $\mathbb{R}[x]$.

6.4. Ước chung lớn nhất của f(x) và g(x) trong $\mathbb{Q}[x]$ là:

a) 1; b)1; c)1; d) $(x-1)^2(x+2) = x^3-3x+2$.

6.6. a)

$$\begin{array}{l|l} x^4+2x^3-x^2-4x-2 & x^4+x^3-x^2-2x-2 \\ \hline x^4+x^3-x^2-2x-2 & 1 \end{array}$$

$$\begin{array}{l|l} x^4+x^3-x^2-2x-2 & x^3-2x \\ \hline x^4-2x^2 & x+1 \end{array}$$

$$\begin{array}{l|l} x^3+x^2-2x-2 & \\ \hline x^3-2x & \end{array}$$

$$\begin{array}{l|l} x^3-2x & x^2-2x \\ \hline x^3-2x & x \\ \hline 0 & \end{array}$$

Ta có ước chung lớn nhất của f(x) và g(x) là d(x) = $x^2 - 2$.

Do đó $x^2 - 2 = g(x) - (x^3 - 2x)(x + 1)$

$= g(x) - [f(x) - g(x).1](x + 1)$

$= f(x)[-(x + 1)] + g(x)[1 + (x + 1)]$

$= f(x)[-(x + 1)] + g(x)$

Vậy ta tìm được p(x) = $-(x + 1)$

q(x) = x + 2.

b) Cách làm tương tự câu a).

6.7. Giả sử f(x) chia hết cho g(x) trong $\mathbb{C}[x]$,

$f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in \mathbb{Z}[x]$.

a) Ta có

$$f\left(\frac{p}{q}\right) = a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + ... + \left(\frac{p}{q}\right) + a_0 = 0$$

Suy ra $a_n \frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^n}.q + ... + a_1\frac{p}{q^n}.q^{n-1} + a_0 = 0$

hay $a_n p^n + a_{n-1}p^{n-1}q + ... + a_1 pq^{n-1} + a_0 q^n = 0$ (1)

Từ (1) ta có hai đẳng thức sau:

$$a_n p^n + a_{n-1}p^{n-1} + ... + a_1 pq^{n-1} = -a_0 q^n$$

suy ra $p(a_n p^{n-1} + a_{n-1}p^{n-2}q + ... + a_1 q^{n-1}) = -a_0 q^n$ (2)

và $a_{n-1}p^{n-1}q + ... + a_0 q^n = -a_n p^n$.

Do đó $q(a_{n-1}p^{n-1} + ... + a_0 q^{n-1}) = -a_n p^n$. (3)

Vì p, q nguyên tố cùng nhau nên p, q^n cũng nguyên tố cùng nhau và p^n, q cũng nguyên tố cùng nhau. Từ các đẳng thức (2) và (3) suy ra $p \setminus a_0$ và $q \setminus a_n$.

b) Chia f(x) cho x – m, ta được

$$f(x) = (x - m)\, g(x) + f(m).$$

Vì $m \in \mathbb{Z}$ và $f(x) \in [x]$ nên theo sơ đồ Hoocne ta cũng có $g(x) \in \mathbb{Z}[x]$.

$$f\left(\frac{p}{q}\right) = \left(\frac{p}{q} - m\right) g\left(\frac{p}{q}\right) + f(m) = 0$$

do vậy $f(m) = (p - mq).\ \frac{A}{q^t}$ trong đó $A \in \mathbb{Z}$ (vì các hệ số của g(x) là nguyên).

hay $q^t f(m) = (p - mq)\, A.$ (*)

Vì p và q nguyên tố cùng nhau nên q^t và p cũng nguyên tố cùng nhau và do đó q^t và p – mq cũng nguyên tố cùng nhau.

$f(x) = g(x)q(x)$.

$\alpha \in \mathbb{C}$ là một nghiệm của g(x) tức là $g(\alpha) = 0$ suy ra $f(\alpha) = 0$, và nếu α là nghiệm bội cấp k ($k \geq 1$) của g(x) thì $g(x) = (x - \alpha)^k . h(x)$, do đó $f(x) = (x - \alpha)^k h(x)q(x)$ điều này chứng tỏ α là nghiệm bội cấp không nhỏ hơn k của f(x). Đảo lại, nếu mọi nghiệm bội cấp k_i ($k_i \geq 1$) của g(x) (kể cả nghiệm đơn của g(x)) đều là nghiệm bội có cấp không nhỏ hơn k_i của f(x) thì ta có sự phân tích f(x) và g(x) như sau:

$$g(x) = (x - \alpha_1)^{k_1} (x - \alpha_2)^{k_2} \ldots (x - \alpha_t)^{k_t}$$

và $f(x) = (x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}...(x-\alpha_t)^{k_t}.\ k(x)$, với α_i là nghiệm bội cấp k_i của đa thức g(x), i = 1, ..., t. Điều này cho ta đẳng thức

$$f(x) = g(x)k(x).$$

Vậy f(x) chia hết cho g(x).

6.8. Đa thức $g(x) = x^2 + x + 1$ là một đa thức bậc hai không có nghiệm hữu tỉ nên nó là bất khả quy trong $\mathbb{Q}[x]$. Đa thức này có nghiệm phức là ε (và ε^2), là hai căn nguyên thuỷ bậc ba của đơn vị (ta có $x^3 - 1 = (x-1)g(x)$). Ta cũng có

$$f(x) = x^{3k} + x^{3l+1} + x^{3n+2}$$

có nghiệm là ε (và cả ε^2)

$$f(\varepsilon) = \varepsilon^{3k} + \varepsilon^{3l+1} + \varepsilon^{3n+2} = \varepsilon^0 + \varepsilon + \varepsilon^2 = 0$$

Theo bài 6.7 có $h(x) \in \mathbb{C}[x]$ sao cho

$$g(x) = g(x)h(x).$$

Nhưng f(x) và $g(x) \in \mathbb{Q}[x]$ nên ta suy ra $h(x) \in \mathbb{Q}[x]$.

6.9. Đa thức $f(x) = x^3 - 3n^2x + n^3$, $n \neq 0$ có bậc ba. Do vậy f(x) bất khả quy trong $\mathbb{Q}[x]$ khi và chỉ khi f(x) không có nghiệm hữu tỉ. Giả sử f(x) có nghiệm hữu tỉ là q và $q^3 - 3n^2q + n^3 = 0$

suy ra $\left(\frac{q}{n}\right)^3 - 3\left(\frac{q}{n}\right) + 1 = 0$.

Như vậy thì $\frac{q}{n}$ là nghiệm của đa thức $g(x) = x^3 - 3x + 1$.

Nhưng đa thức g(x) là đa thức bất khả quy trong $\mathbb{Q}[x]$ (xem

bài tập 6.21) nên không thể nhận $\frac{q}{n}$ làm nghiệm. Vậy đa thức f(x) không có nghiệm hữu tỉ và do đó là bất khả quy trong $\mathbb{Q}[x]$.

6.10. a) Giải phương trình

$$4y^3 - 36y^2 + 84y - 20 = 0 \quad (1)$$

$$\Leftrightarrow \quad y^3 - 9y^2 + 21y - 5 = 0. \quad (2)$$

Đặt $x = y - 3$ ta có

$$(x+3)^3 - 9(x+3)^2 + 21(x+3) - 5 = 0$$

$$x^3 - 6x + 4 = 0 \quad (3)$$

áp dụng công thức Cac-đa-nô ta có

$$u_1 = \sqrt[3]{-29 + \sqrt{29^2 - 2^3}} = \sqrt[3]{-29 + \sqrt{833}}.$$

Gọi u_1 là một giá trị thực của $\sqrt[3]{-29 + \sqrt{833}}$ và có v_1 là giá trị tương ứng với u_1 sẽ là giá trị thực của $\sqrt[3]{-29 - \sqrt{833}}$. Vậy ta sẽ có nghiệm của phương trình (3) là

$$x_1 = u_1 + v_1 = \sqrt[3]{-29 + \sqrt{833}} + \sqrt[3]{-29 - \sqrt{833}}$$

$$x_2 = u_1\varepsilon + v_1\varepsilon^2 \text{ và}$$

$$x_3 = u_1\varepsilon^2 + v_1\varepsilon$$

từ đó suy ra ba nghiệm của phương trình (2) và (1).

b) Giải phương trình

$$x^3 - x - 6 = 0.$$

Phương trình này có một nghiệm là $x_1 = 2$, do đó vế trái của phương trình có dạng

$$x^3 - x - 6 = (x-2)(x^2 + 2x + 3).$$

Phương trình $x^2 + 2x + 3 = 0$ có hai nghiệm là

$$x_2 = -1 + i\sqrt{2}$$

$$x_3 = -1 - i\sqrt{2}.$$

Chú ý: Nếu giải phương trình này bằng công thức Cac-đa-nô thì nghiệm thực của x_1 của nó sẽ viết dưới dạng tổng của hai số phức rất cồng kềnh.

6.11. Đặt $\delta_1 = x_1 + x_2 + x_3$

$$\delta_2 = x_1x_2 + x_1x_3 + x_2x_3$$

$$\delta_3 = x_1x_2x_3$$

với x_1, x_2, x_3 là ba nghiệm của phương trình

$$x^3 + px + q = 0.$$

Theo công thức Vi-et ta có $\delta_1 = 0$, $\delta_2 = p$, $\delta_3 = -q$.

Bây giờ ta biểu diễn đa thức

$$f(x_1, x_2, x_3) = (x_1 - x_2)^2(x_1 - x_3)^2 \times (x_2 - x_3)^2$$

qua các đa thức đối xứng cơ bản. Đây là đa thức đối xứng thuần nhất có hạng tử cao nhất $x_1^4x_2^2$. Do đó ta có hệ thống số mũ, và $f(x_1, x_2, x_3) = \delta_1^2\delta_2^2 + a\delta_1^3\delta_3 + b\delta_2^3 + c\delta_1\delta_2\delta_3 + d\delta_3^2$.

Bằng phương pháp hệ số bất định ta được

$$f(x_1, x_2, x_3) = \delta_1^2\delta_2^2 - 4\delta_1^3\delta_3 - 4\delta_2^3 - 18\delta_1\delta_2\delta_3 - 27\delta_3^2$$

Thay các giá trị của δ_1, δ_2, δ_3 ta được

$$f(x_1, x_2, x_3) = -4p^3 - 27q^2.$$

d) Giải phương trình

$$x^4 + 6x^3 + 6x^2 - 8 = 0 \qquad (1)$$

$$\Leftrightarrow \qquad x^4 + 6x^3 = -6x^2 + 8$$

$$\Leftrightarrow \quad x^4 + 6x^3 + 9x^2 = 9x^2 - 6x^2 + 8$$

$$\Leftrightarrow \quad (x^2 + 3x)^2 = 3x^2 + 8. \qquad (2)$$

Cộng vào hai vế của (2) với $(x^2 + 3x)y + \frac{y^2}{4}$ ta được

$$(x^2 + 3x + \frac{y}{2})^2 = (y+3)x^2 + 3yx + (\frac{y^2}{4} + 8) \qquad (3)$$

Để cho vế phải là một bình phương của biểu thức, y phải thoả mãn điều kiện

$$\Delta = 9y^2 - 4(y+3)\,(\frac{y^2}{4} + 8) = 0$$

$$\Leftrightarrow \quad y^3 - 6y^2 + 32y + 96 = 0. \qquad (4)$$

Phương trình này tương đương với

$$\Leftrightarrow \begin{cases} x^2 + 3x - 1 = x - 3 \\ x^2 + 3x - 1 = -x + 3 \end{cases}$$

$$\Leftrightarrow \begin{cases} x^2 + 2x + 2 = 0 & (*) \\ x^2 + 4x - 4 = 0 & (**) \end{cases}$$

Phương trình (*) có nghiệm là

$$x_1 = -1 + i; \qquad x_2 = -1 - i.$$

Phương trình (**) có nghiệm là

$$x_3 = -2 + \sqrt{8}; \qquad x_4 = -2 - \sqrt{8}.$$

Vậy phương trình (1) có bốn nghiệm là x_1, x_2, x_3, x_4 trên đây.

6.13. $\alpha = 1 + i$ có $|\alpha| = \sqrt{2}$, $\arg\alpha = \frac{\pi}{4} + 2k\pi$.

Vậy $\alpha = \sqrt{2}(\cos = \frac{\pi}{4} + i\sin\frac{\pi}{4})$

a) Ta có $\alpha^n = \sqrt{2}^n(\cos\frac{n\pi}{4} + i\sin\frac{n\pi}{4})$

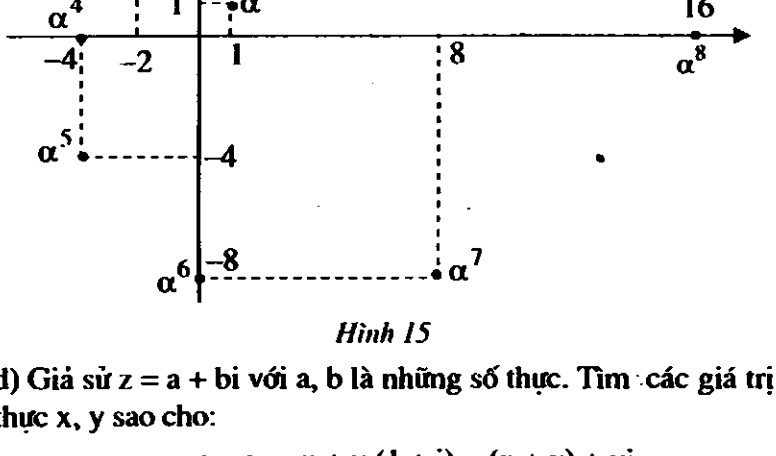
$$\alpha^{-n} = \frac{1}{(\sqrt{2})^n}(\cos\frac{-n\pi}{4} + i\sin\frac{-n\pi}{4})$$

b) $\alpha^n = (1+i)^n$. Theo nhị thức Niutơn ta có

$$\alpha^n = (1+i)^n$$
$$= 1 + C_n^1 i + C_n^2 i^2 + C_n^3 i^3 + ... + C_n^k i^k + ... + C_n^n i^n$$
$$= 1 - C_n^2 + C_n^4 - C_n^6 + ...) + (C_1^n - C_n^3 + C_n^5 - C_n^7 + ...)i .$$

Với $C_n^k = \frac{n!}{(n-k)!k!}$ là số tổ hợp chập k của n, $0 \le k \le n$.

c) Biểu diễn hình học α^n và α^{-n} với $n < 8$



Hình 15

d) Giả sử z = a + bi với a, b là những số thực. Tìm các giá trị thực x, y sao cho:

$$z = x + y\alpha = x + y(1 + i) = (x + y) + yi.$$

Từ điều kiện trên suy ra $\begin{cases} x + y = a \\ y = b \end{cases}$ (*)

hệ phương trình (*) là một hệ cramer (có định thức $\begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix} = 1 \neq 0$).

Nó có nghiệm duy nhất là

$$y = b \text{ và } x = a - b$$

Vậy $z = (a - b) + b\alpha$.

e) Chứng minh ánh xạ

$$f : \mathbb{C} \to M$$

$$z = x + y\alpha \mapsto \begin{bmatrix} x & y \\ -2y & x + 2y \end{bmatrix}$$

là một đẳng cấu. Thật vậy, giả sử $z = x + y\alpha$ và $z' = x' + y'\alpha$ ta có

$$z + z' = (x + y\alpha) + (x' + y'\alpha) = (x + x') + (y + y')\alpha$$

do đó

$$f(z + z') = \begin{bmatrix} x + x' & y + y' \\ -2(y + y') & (x + x') + 2(y + y') \end{bmatrix}$$

$$= \begin{bmatrix} x & y \\ -2y & x + 2y \end{bmatrix} + \begin{bmatrix} x' & y' \\ -2y' & x' + 2y' \end{bmatrix} = f(z) + f(z');$$

$$z.z' = (x + y\alpha)(x' + y'\alpha) = (x + y + yi)(x' + y' + y'i)$$

$$= (x + y)(x' + y') - yy' + [(x + y)y' + (x' + y')y]i$$

$$= (xx' + xy' + yx') + (yx' + xy' + 2yy')i$$

$$= (xx' - 2yy') + (2yy' + xy' + yx') + (yx' + xy' + 2yy')i$$

$$= (xx' - 2yy' + (2yy' + xy' + yx')\alpha$$

do đó

$$\varphi(z.z') = \begin{bmatrix} xx' - 2yy' & xy' + yx' + 2yy' \\ -2(xy' + yx' + 2yy') & xx' - 2yy' + 2(xy' + yx' + 2yy') \end{bmatrix} \quad (1)$$

Mặt khác ta cũng có

$$\begin{bmatrix} x & y \\ -2y & x + 2y \end{bmatrix} \begin{bmatrix} x' & y' \\ -2y' & x' + 2y' \end{bmatrix} =$$

$$= \begin{bmatrix} xx' - 2yy' & xy' + yx' + 2yy' \\ -2(xy' + yx' + 2yy') & -2yy' + xx' + 2xy' + 2yx' + 4yy' \end{bmatrix} \quad (2)$$

So sánh (1) và (2) ta có hai ma trận này bằng nhau, vậy f là một đồng cấu.

f là toàn ánh và là đơn ánh hiển nhiên. Vậy M đẳng cấu với $\mathbb{C}$, do đó M là một trường

6.14. a) Giả sử $f(x) = (x - 1)^2 p(x) + 2x$ và

$$f(x) = (x - 2)^3 q(x) + 3x.$$

Trừ vế với vế ta có

$$0 = (x - 1)^2 p(x) - (x - 2)^3 q(x) - x.$$

Do đó $(x - 1)^2 p(x) = (x - 2)^3 q(x) + x$.

Từ kết quả trên ta thấy rằng $\deg p(x) = \deg q(x) + 1$.

Giả sử $\deg q(x) = 0$ và $\deg p(x) = 1$. Khi đó $p(x) = ax + b$ và $q(x) = c$. Ta có đẳng thức

$$(x^2 - 2x + 1)(ax + b) = (x^3 - 6x + 12x^2 - 8)c + x$$

hay

$$ax^3 + (b - 2a)x^2 + (a - 2b)x + b = cx^3 + 12cx^2 + (1 - 6c)x - 8c.$$

$$\begin{cases} a = c \\ b - 2a = 12c \\ a - 2b = 1 - 6c \\ b = -8c \end{cases} \Leftrightarrow \begin{cases} a = c \\ b - 2c = 12c \\ c - 2b = 1 - 6c \\ b = -8c \end{cases} \Leftrightarrow \begin{cases} a = c \\ b = 10c \\ b = -8c. \end{cases}$$

Hệ phương trình này vô nghiệm.

Giả sử $\deg q(x) = 1$ và $\deg p(x) = 2$ khi đó

$$q(x) = ax + b \text{ và } p(x) = cx^2 + dx + e.$$

Ta có đẳng thức

$$(x^2 - 2x + 1)(cx^2 + dx + e) = (x^3 - 6x + 12x^2 - 8)(ax + b) + x$$

$$\Leftrightarrow cx^4 + (d - 2c)x^3 + (c - 2d + e)x^2 + (d - 2c)x + e =$$

$$= ax^4 + (12a + b)x^3 + (12b - 6a)x^2 - (6b + 8a - 1)x - 8b.$$

Suy ra $\begin{cases} c = a \\ d - 2c = 12a + b \\ c - 2d + e = 12b - 6a \\ d - 2e = 1 - 6b - 8a \\ c = -8b \end{cases} \Leftrightarrow \begin{cases} a - c = 0 \\ 10a + b - d = 0 \\ c - 2d + e = 12b - 6a \\ 7a - 20b - 2d = 0 \\ 8a + 22b + d = 1. \end{cases}$

Giải hệ phương trình này ta tìm được :

$a = 4, b = -3$

$c = 4, d = -19, e = 24.$

Vậy ta có $p(x) = 4x^2 - 19x + 24$

$$q(x) = 4x - 3$$

và $f(x) = 4x^4 - 27x^3 + 66x^2 - 65x + 24.$

6.15. a) Tìm nghiệm hữu tỉ của đa thức

$$f(x) = x3 - 6x2 + 15x - 14.$$

Các ước của 14 là $\pm 1, \pm 2, \pm 14$.

$f(1) = -4 \neq 0$,

$f(-1) = -36 \neq 0$,

$f(2) = 0$.

	1	–6	15	–14
2	1	–4	7	0
7	1	3	$28 \neq 0$	
–7	1	–11	$84 \neq 0$	

Vậy f(x) có một nghiệm hữu tỉ là 2.

6.16. Giả sử $\frac{p}{q} \in \mathbb{Q}$, $q > 0$, $(p, q) = 1$ là nghiệm của đa thức.

Từ đẳng thức (*) ta suy ra $p - mq$ là ước của f(m). Với $m = 1$, ta có $p - 1q = p - q$ là ước của f(1) và với $m = -1$ ta có $p - (-1q) = p + q$ là ước của f(–1).

6.17. Theo bài 6.16 nếu phân số tối giản $\frac{p}{q} \in \mathbb{Q}$ là nghiệm của đa thức

$f(x) = 10x^5 - 81x^4 + 90x^3 - 102x^2 + 80x - 21$

thì $p \setminus 21$ và $q \setminus 10$.

Ngoài ra $(p - q) \setminus f(1)$ và $(p + q) \setminus f(-1)$.

Ta có $f(1) = -24$

$f(-1) = -384$.

Các giá trị của p có thể là $\pm 1, \pm 3, \pm 7, \pm 21$

Các giá trị của q có thể là 1, 2, 5, 10.

Ta lần lượt xét các phân số ± 3, ± 7, ± 21; $\pm\frac{1}{2}$; $\pm\frac{1}{5}$; $\pm\frac{3}{2}$; $\pm\frac{3}{5}$; $\pm\frac{7}{5}$; $\pm\frac{7}{2}$; $\pm\frac{21}{2}$; $\pm\frac{21}{5}$.

Trước hết ta loại trừ các phân số không thoả mãn điều kiện cần đã nêu trong bài 6.16.

$21 - 1 = 20$ không chia hết cho $24 = f(1)$,

$-21 - 1 = -22$ không chia hết $24 = f(1)$,

$21 - 2 = 19$ không chia hết $24 = f(1)$,

$-21 - 2 = -23$ không chia hết $24 = f(1)$.

Vậy ± 21, $\pm\frac{21}{2}$ không là nghiệm của đa thức f(x). Tương tự ± 3, $\pm\frac{21}{5}$ cũng không là nghiệm của f(x).

Còn lại dùng sơ đồ để tìm nghiệm của f(x):

	10	−81	+90	−102	+80	−21
7	10	−11	13	−11	3	0
$\frac{1}{2}$	10	−6	10	−6	0	
$\frac{3}{5}$	10	0	10	0		

Đa thức $10x^2 + 10$ không có nghiệm hữu tỉ. Vậy f(x) có ba nghiệm hữu tỉ là: 7, $\frac{1}{2}$ và $\frac{3}{5}$.

6.18. Giả sử $f(x) \in \mathbb{Z}[x]$ với f(0) và f(1) đều lẻ mà f(x) có nghiệm nguyên là a. Do f(0) là số hạng tự do cho nên a là ước của

f(0) phải là một số lẻ. Lại theo điều kiện cần trong bài 6.16, a −1 phải là ước của f(1). Nhưng a − 1 chẵn và f(1) lẻ nên a − 1 không thể là ước của f(1) được. Điều vô lí này chứng tỏ f(x) không có nghiệm nguyên.

6.19. Ta xét hai trường hợp:

a) $p(x) \in \mathbb{Z}$. Như vậy p(x) là một số nguyên tố. Hiển nhiên nếu $p(x) \setminus f(x)g(x)$ thì $p(x) \setminus f(x)$ hoặc $p(x) \setminus g(x)$.

b) $p(x) \notin \mathbb{Z}$. Như vậy p(x) phải là một đa thức nguyên bản. Ta coi p(x) như một đa thức thuộc $\mathbb{Q}[x]$. Khi đó tính chất bất khả quy của p(x) trong $\mathbb{Q}[x]$ tương đương với tính chất bất khả quy của p(x) trong $\mathbb{Z}[x]$. Vì $\mathbb{Q}[x]$ là một vành chính nên p(x) là một phần tử nguyên tố trong $\mathbb{Q}[x]$. Điều này nói lên rằng nếu $p(x) \setminus f(x)g(x)$ với f(x) và g(x) thuộc $\mathbb{Z}[x]$ thì $p(x) \setminus f(x)$ hoặc $p(x) \setminus g(x)$.

6.20. Việc chứng minh bài toán được dựa trên bổ đề sau đây (xem Đại số đại cương, Hoàng Xuân Sính):

Nếu $f(x) \in \mathbb{Z}[x]$ có bậc lớn hơn 0 và f(x) không bất khả quy trong $\mathbb{Q}[x]$ thì f(x) phân tích được thành một tích những đa thức bậc khác 0 với hệ số nguyên.

Bây giờ ta hãy đi vào bài toán. Nếu f(x) có bậc 0 thì f(x) là một số nguyên. Nếu số nguyên đó khác ±1, nó sẽ phân tích thành một tích những thừa số nguyên tố. Nếu f(x) có bậc lớn hơn 0, áp dụng bổ đề trên f(x) sẽ viết được dưới dạng:

$$f(x) = p_1(x)\, p_2(x) \ldots p_k(x) \qquad (*)$$

trong đó có những $p_i(x)$ có thể có bậc 0, vậy là những số nguyên tố, còn đối với các $p_i(x)$ có bậc khác 0 thì chúng là những đa thức với hệ số nguyên, nguyên bản và bất khả quy trong $\mathbb{Q}[x]$.

Áp dụng bài 6.19, ta có thể chứng minh sự phân tích (*) là duy nhất sai khác ± 1 với mỗi nhân tử.

6.21. a) Đặt $y = x - 3$ ta có

$$x^4 - 8x^3 + 12x^2 - 6x + 3 = y^4 + 4y^3 - 6y^2 - 42y - 42 = g(y).$$

Đa thức $g(y)$ bất khả quy trong $\mathbb{Q}[x]$ vì theo tiêu chuẩn Aidenstainơ với $p = 2$, do đó suy ra đa thức

$$f(x) = x^4 - 8x^3 + 12x^2 - 6x + 3$$

bất khả quy trong $\mathbb{Q}[x]$.

b) Độc giả tự giải.

c) Đặt $y = x - 1$

$$f(x) = x^{p-1} + x^{p-2} + ... + x + 1 = y^{p-1} + C_p^1 y^{p-2} + ... + C_p^{p-1}$$

$$= y^{p-1} + y^{p-2} + ... + p = g(y)$$

Theo tiêu chuẩn Aidenstainơ đa thức vế phải $g(y)$ là bất khả quy trong $\mathbb{Q}[x]$. Vậy $f(x)$ bất khả quy trong $\mathbb{Q}[x]$.

d) Đặt $x = y + 2$. Rồi áp dụng tiêu chuẩn Aidenstainơ.

6.22. Giả sử $f(x) = x^4 + px^2 + q \in \mathbb{Q}[x]$ khả quy trong $\mathbb{Q}[x]$ thì $f(x)$ có thể phân tích được thành tích của hai đa thức bậc hai

$$x^4 + px^2 + q = (x^2 + ax + m)(x^2 + bx + n).$$

So sánh hệ số ở hai vế suy ra

$$\begin{cases} a + b = 0 \\ m + n + ab = p \\ an + bm = 0 \\ mn = q. \end{cases}$$

Nếu $a = 0$ thì $b = 0$ và

$$\begin{cases} m + n = p \\ mn = q. \end{cases}$$

Khi đó m và n là nghiệm của phương trình

$$X^2 - pX + q = 0.$$

Phương trình này có nghiệm hữu tỉ khi và chỉ khi $\Delta = p^2 - 4q$ là bình phương của một số hữu tỉ.

Nếu $a \neq 0$ thì $m = n$ và $\begin{cases} a = -b \\ 2n - a^2 = p \\ n^2 = q. \end{cases}$

Vì a và n là những số hữu tỉ nên q, $2\sqrt{q} - p\ (=a^2)$ phải là bình phương của những số hữu tỉ.

Từ các kết quả trên suy ra rằng đa thức $x^4 + px^2 + q$ là bất khả quy trong $\mathbb{Q}[x]$ khi và chỉ khi q, $p^2 - 4q$ và $2\sqrt{q} - p$, không phải là bình phương của những số hữu tỉ.

6.23. Giả sử $f(x) = (x - a_1)(x - a_2)...(x - a_n) - 1$, với a_i là những số nguyên phân biệt, $i = 1, 2, ..., n$, không phải là đa thức bất khả quy trong $\mathbb{Q}[x]$. Nghĩa là tồn tại hai đa thức h(x) và g(x) của $\mathbb{Z}[x]$ sao cho

$$f(x) = g(x)\, h(x) \qquad (1)$$

với 0 < bậc g(x), bậc h(x) < bậc f(x).

Từ đẳng thức (1) suy ra

$t(a_i) = g(a_i) = -1$ với $i = q, 2, ..., n$.

vì $g(a_i)$ và $h(a_i)$ thuộc $\mathbb{Z}$ nên $g(a_i) = -h(a_i)$ với $i = 1, 2, ..., n$.

Đặt $k(x) = g(x) + h(x)$. Nếu $k(x) = 0$ thì ta có $g(x) = -h(x)$, như vậy $f(x) = -[g(x)]^2$. Hệ số cao nhất của $-[g(x)]^2$ âm, còn hệ số của f(x) bằng $1 > 0$. Điều này không thể xảy ra. Nếu $k(x) \neq 0$ thì bậc k(x) nhỏ hơn n, nhưng

$$k(a_i) = g(a_i) + h(a_i) = 0, i = 1, 2, ..., n.$$

Vậy k(x) có n nghiệm phân biệt, mâu thuẫn với điều đã chứng minh trong bài 4.16.

TÀI LIỆU THAM KHẢO

[1] Hoàng Xuân Sính: Đại số đại cương
Nhà xuất bản Giáo dục 1995.

[2] Ngô Thúc Lanh: Đại số và Số học Tập 1, Tập 2
Nhà xuất bản Giáo dục 1985.

[3] Bùi Huy Hiền, Nguyễn Hữu Hoan.
Bài tập Đại số và Số học Tập 1
Nhà xuất bản Giáo dục 1986.

[4] Bùi Huy Hiền, Nguyễn Hữu Hoan, Phan Doãn Thoại
Bài tập Đại số và Số học Tập 2.
Nhà xuất bản Giáo dục 1986.

MỤC LỤC

Chịu trách nhiệm xuất bản :

Chủ tịch HĐQT kiêm Tổng Giám đốc NGÔ TRẦN ÁI

Phó Tổng Giám đốc kiêm Tổng Biên tập NGUYỄN QUÝ THAO

Biên tập nội dung :

TRẦN PHƯƠNG DUNG

Biên tập tái bản :

TRẦN PHƯƠNG DUNG

LÊ THỊ THANH HẰNG

Trình bày bìa :

BÙI QUANG TUẤN

Sửa bản in :

LÊ THỊ THANH HẰNG

Chế bản :

NGUYỄN THỊ THANH XUÂN

BÀI TẬP ĐẠI SỐ ĐẠI CƯƠNG

Mã số: 7K150T7-DAI

In 2.000 bản, khổ 14,5 x 20,5cm. Tại Nhà in Hà Nam
Số 29 - QL 1A - P. Quang Trung - TX. Phủ Lý - Hà Nam
Số in: 47. Giấy phép xuất bản số: 11-2007/CXB/203-2119/GD
In xong và nộp lưu chiểu tháng 2 năm 2007.

CÔNG TY CỔ PHẦN SÁCH ĐẠI HỌC - HEVOBCO
25 HÀN THUYÊN – HÀ NỘI
Website : www.hevobco.com.vn

TÌM ĐỌC SÁCH CĐSP BỘ MÔN TOÁN
CỦA NHÀ XUẤT BẢN GIÁO DỤC

1.	**Đại số đại cương (GTCĐSP)**	*Hoàng Xuân Sính*
2.	**Xác suất thống kê (GTCĐSP)**	*Phạm Văn Kiều* *Lê Thiên Hương*
3.	**Quy hoạch tuyến tính (GTCĐSP)**	*Phí Mạnh Ban*
4.	**Phương pháp dạy học môn Toán – Tập 1, 2 (GTCĐSP)**	*Phạm Gia Đức*
5.	**Thực hành giải toán (GTCĐSP)**	*Vũ Dương Thuỵ*
6.	**Bài tập đại số đại cương**	*Bùi Duy Hiển*
7.	**Bài tập đại số tuyến tính**	*Hoàng Xuân Sính* *Trần Phương Dung*
8.	**Bài tập số học**	*Nguyễn Tiến Quang*
9.	**Bài tập giải tích – tập 1, 2**	*Nguyễn Thuỷ Thanh*

Bạn đọc có thể mua tại các Công ti Sách - Thiết bị trường học ở các địa phương hoặc các Cửa hàng của Nhà xuất bản Giáo dục :

Tại Hà Nội : 25 Hàn Thuyên; 187B Giảng Võ; 232 Tây Sơn; 23 Tràng Tiền.

Tại Đà Nẵng : Số 15 Nguyễn Chí Thanh; Số 62 Nguyễn Chí Thanh.

Tại Thành phố Hồ Chí Minh : 104 Mai Thị Lựu, Quận 1; Cửa hàng 451 - 453, Hai Bà Trưng, Quận 3; 240 Trần Bình Trọng – Quận 5.

Tại Thành phố Cần Thơ : Số 5/5, đường 30/4.

Website : www.nxbgd.com.vn

8 934980 759011

Giá :22.000 đ