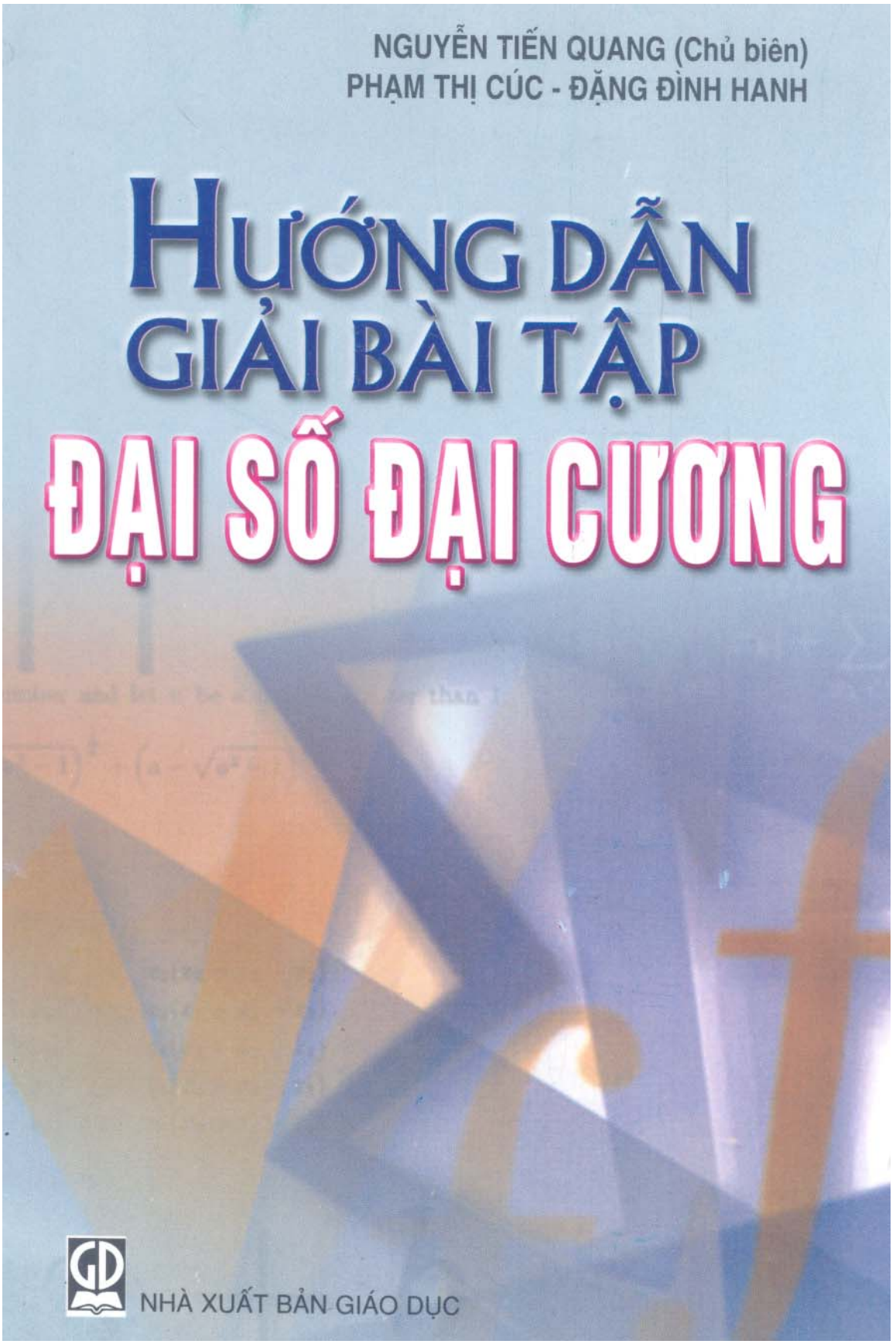
NGUYỄN TIẾN QUANG (Chủ biên)
PHẠM THỊ CÚC - ĐẶNG ĐÌNH HANH

HƯỚNG DẪN GIẢI BÀI TẬP ĐẠI SỐ ĐẠI CƯƠNG



NHÀ XUẤT BẢN GIÁO DỤC

NGUYỄN TIẾN QUANG (Chủ biên)
PHẠM THỊ CÚC – ĐẶNG ĐÌNH HANH

HƯỚNG DẪN GIẢI BÀI TẬP ĐẠI SỐ ĐẠI CƯƠNG

(Tái bản lần thứ nhất)

NHÀ XUẤT BẢN GIÁO DỤC

04 – 2009/CXB/257 – 2117/GD Mã số : 7B720y9 – DAI

LỜI NÓI ĐẦU

Đại số đại cương là một trong những môn học đầu tiên về toán học trừu tượng trong chương trình đào tạo của các trường Đại học Khoa học Tự nhiên, Đại học Sư phạm – Cao đẳng Sư phạm. Nó làm cơ sở cho việc học tập tiếp những môn học khác của chương trình Cử nhân cũng như chương trình Cao học. Ở đây người đọc lần đầu chuyển từ tư duy "toán sơ cấp" sang tư duy "trừu tượng" về đại số. Điều đó gây không ít khó khăn cho người đọc. Thực tế cho thấy, để hình thành kiểu tư duy mới này, chúng ta cần có sự hỗ trợ rất lớn của một hệ thống bài tập. Ngoài một số bài toán có tính chất áp dụng trực tiếp lý thuyết vào các đối tượng cụ thể, còn có những bài toán là sự tìm hiểu sâu nội dung môn học, đòi hỏi chúng ta không chỉ có kỹ năng mà còn phải có phương pháp, thói quen tư duy mới, có sáng tạo.

Các giáo trình về Đại số đại cương có khá nhiều, mỗi cuốn thường có một hệ thống bài tập kèm theo, phù hợp với các vấn đề về lý thuyết đã trình bày. Nhiều bài tập trong cuốn sách này được tuyển chọn từ một số giáo trình như: "Đại số" của G. Birkhoff và S. MacLane, "Đại số" của S. Lang, "Đại số" của T. W. Hungerford, "Đại số với ứng dụng hiện đại" của W. J. Gilbert và W. K. Nichonson, "Bài giảng về đại số đại cương" của A. G. Curos, "Đại số đại cương" của Hoàng Xuân Sính, "Bài tập đại số" của Trần Văn Hạo và Hoàng Kỳ, "Bài tập đại số" của Bùi Huy Hiền... Các bài toán này được sắp xếp và có lời giải phù hợp với cuốn giáo trình "Đại số đại cương" của Nguyễn Tiến Quang. Chúng tôi xin chân thành cảm ơn các tác giả đã dẫn trong sách.

Cuốn sách được chia làm hai phần: Phần thứ nhất trình bày tóm tắt lý thuyết và hệ thống bài toán theo sáu chương. Các bài toán được đánh số theo từng mục trong mỗi chương. Phần thứ hai trình bày lời giải cho một số bài khó, hoặc hướng dẫn, hoặc trả lời cho một số bài đơn giản hơn.

Mức độ khó ở các bài toán là khác nhau, phù hợp với nhiều loại đối tượng. Tuy nhiên, sự đa dạng của các bài toán là có ích cho người đọc. Chúng ta sẽ nắm vững được lý thuyết và hiểu sâu nội dung môn học chỉ sau khi độc lập làm việc với một số lượng lớn các bài tập này.

Bạn đọc phải tự mình hoàn thiện các kỹ năng cũng như phát triển tư duy qua việc giải các bài tập này và có thể đối chiếu lời giải của mình với lời giải hoặc đáp số ở phần hai của cuốn sách.

Một số lời giải được trình bày cô đọng, bạn đọc nên làm rõ hơn, chi tiết hơn cho những lời giải này, cũng như nên tự mình thực hành một cách sáng tạo bằng cách đưa ra những cách lập luận mới.

Những bài toán của cuốn sách đã được tuyển chọn qua thực tế giảng dạy của tác giả cũng như của nhiều bạn đồng nghiệp. Nhiều lời giải thú vị đã được đề xuất từ các bạn sinh viên của chúng tôi. Chúng tôi hy vọng đây là một tài liệu có ích về đại số cho sinh viên không chỉ ở hệ Đại học mà cả ở hệ Cao đẳng Sư phạm.

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

Thư góp ý xin gửi về Công ty Cổ phần Sách Đại học – Dạy nghề, 25 Hàn Thuyên, Hà Nội.

CÁC TÁC GIẢ

MỤC LỤC

Phần thứ nhất

TÓM TẮT LÝ THUYẾT VÀ CÁC BÀI TOÁN

Chương I

CƠ SỞ

1. Tập hợp

Khái niệm tập hợp là một trong những khái niệm cơ bản nhất của toán học. Các đối tượng của một tập hợp đã cho nào đó được gọi là các *phần tử* của tập hợp đó. Để ký hiệu phần tử a *thuộc* tập hợp A ta viết $a \in A$; còn nếu phần tử a *không thuộc* tập hợp A ta viết $a \notin A$.

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

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

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

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

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

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

Khi đó, ta cũng nói rằng B *chứa trong* A hay A *chứa* B hay B *bao hàm trong* A. Hai tập hợp A, B được gọi là *bằng nhau* nếu và chỉ nếu chúng có cùng các phần tử. Rõ ràng

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

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

Trên các tập hợp ta thường xét một số phép toán sau:

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

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

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

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

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

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

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

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

Các phép toán tập hợp liên hệ với nhau bởi một số hệ thức cơ bản:

1. Giả sử A, B là những tập hợp con tuỳ ý của tập hợp M. Khi đó các điều sau là tương đương:

$a)$ $A \subset B$ $\qquad$ $d)$ $\overline{B} \subset \overline{A}$

$b)$ $A \cap B = A$ $\qquad$ $e)$ $A \cap \overline{B} = \emptyset$

$c)$ $A \cup B = B$ $\qquad$ $f)$ $M = \overline{A} \cup B$.

2. Giả sử A, B, C, M là những tập hợp tuỳ ý. Khi đó:

a) $A \cup B = B \cup A$; $A \cap B = B \cap A$ $\quad$ (*luật giao hoán*).

b) $A \cap (B \cap C) = (A \cap B) \cap C$;
$A \cup (B \cup C) = (A \cup B) \cup C$ $\quad$ (*luật kết hợp*).

c) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $\quad$ (*luật phân phối*).

d) *Công thức Đờ Moocgăng*

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

2. Ánh xạ

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

$$f : X \to Y$$
$$x \mapsto y = f(x)$$

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

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

Cho ánh xạ $f : X \to Y$. Khi đó với mọi tập con A của X, với mọi tập con B của Y, các tập hợp

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

theo thứ tự được gọi là *ảnh* của A qua f, *tạo ảnh toàn phần* của B qua f. Đặc biệt, ảnh $f(X)$ của X qua f được gọi là *ảnh* của f và ký hiệu bởi $\mathrm{Im}f$, $f(X) = \mathrm{Im}f$.

Ánh xạ $f : X \to Y$ được gọi là một *đơn ánh* nếu

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

với mọi $x, x' \in X$. Ta còn nói f là ánh xạ 1-1 từ X *vào* Y. Ánh xạ $f : X \to Y$ được gọi là một *toàn ánh* nếu với mỗi y thuộc Y đều tồn tại x thuộc X sao cho $f(x) = y$. Ta cũng nói rằng f là một ánh xạ từ X *lên* Y. Ánh xạ $f : X \to Y$ được gọi là một *song ánh* nếu nó đồng thời là đơn ánh và toàn ánh. Khi đó ta còn nói f là một ánh xạ 1-1 *lên*. Hiển nhiên f là song ánh khi và chỉ khi với mỗi $y \in Y$ tồn tại duy nhất $x \in X$ sao cho $f(x) = y$.

Hợp thành (hay *tích*) của các ánh xạ $f : X \to Y$ và $g : Y \to Z$ là ánh xạ $h : X \to Z$ biến x thành $g(f(x))$, ký hiệu bởi $g \circ f$, hoặc đơn giản là gf. Như vậy

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

Phép hợp thành có tính kết hợp, nghĩa là đối với các ánh xạ $f : X \to Y$, $g : Y \to Z$ và $h : Z \to W$ thì $h \circ (g \circ f) = (h \circ g) \circ f$. Một tính chất đơn giản, đáng chú ý của ánh xạ là: với mọi ánh xạ $f : X \to Y$ thì

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

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

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

Một ánh xạ có ngược trái khi và chỉ khi nó là đơn ánh, và một ánh xạ có ngược phải khi và chỉ khi nó là toàn ánh. Một ánh xạ là song ánh khi và chỉ khi nó có ánh xạ ngược.

3. Quan hệ hai ngôi

Tích Dề-các (Descartes) của hai tập hợp A, B dã cho, ký hiệu bởi $A \times B$, là tập hợp tất cả các cặp (a, b) với $a \in A, b \in B$:

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

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

Nếu $(x, y) \in \mathfrak{R}$ ta nói rằng x *nằm trong quan hệ* $\mathfrak{R}$ *với* y và viết $x\mathfrak{R}y$. Nếu (x, y) không thuộc tập hợp đó ta nói rằng x không có quan hệ với y và viết $x\overline{\mathfrak{R}}y$.

Nói cách khác, một quan hệ hai ngôi giữa các tập X, Y là một tập con của tích Đề-các $X \times Y$. Nếu $\mathfrak{R}$ là một quan hệ giữa X và Y thì với $x \in X, y \in Y$ ta luôn có hoặc $x\mathfrak{R}y$ hoặc $x\overline{\mathfrak{R}}y$.

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

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

(i) $a\mathfrak{R}a$ (tính phản xạ);

(ii) Nếu $a\mathfrak{R}b$ thì $b\mathfrak{R}a$ (tính đối xứng);

(iii) Nếu $a\mathfrak{R}b$ và $b\mathfrak{R}c$ thì $a\mathfrak{R}c$ (tính bắc cầu)
với mọi $a, b, c \in S$.

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

$$\overline{a} = \{x \in X \mid a\mathfrak{R}x\}.$$

Khi đó S là hợp rời rạc của tất cả các lớp tương đương phân biệt.

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

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

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

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

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

Quan hệ thứ tự bộ phận như thế thường được ký hiệu bởi $\leq$. Một tập hợp *được sắp thứ tự* là một cặp $(S, \leq)$, trong đó $\leq$ là một thứ tự trên S.

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

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

Phần tử u của tập sắp thứ tự bộ phận $(S, \leq)$ được gọi là *tối tiểu* nếu không tồn tại phần tử $x \in S$ sao cho $x < u$. Phần tử v được gọi là

tối đại nếu không tồn tại phần tử $x \in S$ sao cho $x > v$. (Ta nói rằng $x < u$ có nghĩa là $x \leq u$ nhưng $x \neq u$ và tương tự cho $x > v$).

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

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

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

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

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

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

Cận dưới đúng và cận trên đúng của S được ký hiệu lần lượt bởi $inf S$, $sup S$. Một tập con bất kỳ của tập hợp sắp thứ tự bộ phận có không quá một cận trên đúng và một cận dưới đúng.

4. Số nguyên

Trước hết, tập hợp các số tự nhiên $\mathbb{N}$ thoả mãn hai tiên đề sau:

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

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

(i) $0 \in A$,

(ii) $m \in A$ *với mọi* $0 \leq m < n \Rightarrow n \in A$,

thì $A = \mathbb{N}$.

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

Số nguyên a được gọi là *chia hết cho* số nguyên b nếu $a = bq$ với một số nguyên q nào đó. Khi đó ta nói a là *bội* của b và ký hiệu $a \vdots b$. Ta cũng nói b *chia hết* a hay b là *ước* của a và ký hiệu $b \mid a$.

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

Định lý về phép chia với dư: *Cho hai số nguyên a và $b, b \neq 0$. Khi đó tồn tại duy nhất cặp số nguyên q, r sao cho*

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

Số nguyên d được gọi là *ước chung* của các số nguyên $a_1, a_2, ..., a_n$ nếu nó là ước của mỗi số đó. Ước chung d của các số nguyên $a_1, a_2, ..., a_n$ được gọi là *ước chung lớn nhất* (viết tắt là ƯCLN) nếu d là bội của mọi ước chung của $a_1, a_2, ..., a_n$.

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

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

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

Các số $a_1, a_2, ..., a_n$ được gọi là *nguyên tố cùng nhau* nếu ước chung lớn nhất của chúng bằng 1. Các số nguyên $a_1, a_2, ..., a_n$ nguyên tố cùng nhau khi và chỉ khi tồn tại các số nguyên $x_1, x_2, ..., x_n$ sao cho

$$1 = x_1a_1 + x_2a_2 + ... + x_na_n.$$

Một số tính chất thường gặp của ước chung lớn nhất:

1. Nếu k là một số nguyên dương thì

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

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

3. Nếu a và b là hai số nguyên tố cùng nhau và b là ước của ac thì b là ước của c.

4. Nếu hai số a và b nguyên tố cùng nhau thì

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

với mọi $c \in \mathbb{Z}$.

Để tìm ƯCLN của hai số tự nhiên a và b ta có thuật toán Ơclit, thuật toán đó được tiến hành như sau:

- Nếu $a = bq$ thì $(a, b) = b$.

- Nếu a không chia hết cho b thực hiện liên tiếp các phép chia với dư ta được

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

Dãy phép chia này phải là hữu hạn, với phép chia cuối cùng là một phép chia hết. Từ đó ta được

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

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

Việc tìm UCLN của n số $(n > 2)$ sẽ được tính theo công thức truy hồi:

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

Số nguyên m được gọi là *bội chung* của các số nguyên khác không $a_1, a_2, ..., a_n (n \geq 2)$ nếu nó chia hết cho mỗi số nguyên đó. Bội chung m của các số nguyên $a_1, a_2, ..., a_n$ được gọi là *bội chung nhỏ nhất* của các số này (viết tắt là BCNN) nếu nó là ước của mọi bội chung của $a_1, a_2, ..., a_n$. Nếu m và m' là những BCNN của các số $a_1, a_2, ..., a_n$ thì $m = \pm m'$. Trong trường hợp $m > 0$ ta ký hiệu

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

và quy ước gọi nó là BCNN của $a_1, a_2, ..., a_n$.

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

Giữa ước chung lớn nhất và bội chung nhỏ nhất của hai số nguyên a, b có mối quan hệ sau:

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

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

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

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

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

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

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

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

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

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

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

Sự phân tích

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

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

Bài tập

1. Tập hợp

1.1. Chứng tỏ rằng từ mỗi một trong các hệ thức:

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

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

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

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

1.3. Giả sử A, B là những tập hợp con tuỳ ý của tập hợp M. Khi đó các điều sau là tương đương:

$a)$ $A \subset B$ $\qquad$ $d)$ $\overline{B} \subset \overline{A}$

$b)$ $A \cap B = A$ $\qquad$ $e)$ $A \cap \overline{B} = \emptyset$

$c)$ $A \cup B = B$ $\qquad$ $f)$ $M = \overline{A} \cup B$.

1.4. Giả sử A, B, C, M là những tập hợp tuỳ ý. Chứng minh rằng:

a) $A \cup B = B \cup A$; $A \cap B = B \cap A$ (*luật giao hoán*).

b) $A \cap (B \cap C) = (A \cap B) \cap C$;
$A \cup (B \cup C) = (A \cup B) \cup C$ (*luật kết hợp*).

c) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (*luật phân phối*).

d) *Công thức Đờ Moocgăng*
$M \setminus (A \cup B) = (M \setminus A) \cap (M \setminus B)$;
$M \setminus (A \cap B) = (M \setminus A) \cup (M \setminus B)$.

1.5. Chứng minh rằng nếu $A \subset B$ thì $A \cup C \subset B \cup C$ và $A \cap C \subset B \cap C$.

1.6. Chứng minh rằng nếu $X \subset Y$ thì $P(X) \subset P(Y)$.

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

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

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

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

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

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

e) $C_X(\bigcup\limits_{i \in I} A_i) = \bigcap\limits_{i \in I} C_X(A_i)$;

f) $C_X(\bigcap\limits_{i \in I} A_i) = \bigcup\limits_{i \in I} C_X(A_i)$.

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

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

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

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

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

1.10. 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.

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

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

Hãy chứng minh rằng:

a) $A \triangle B = (A - B) \cup (B - A)$.

b) $A \triangle B = B \triangle A$.

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

2. Ánh xạ

2.1. Xét các ánh xạ $f(n) = 3n$; $g(n) = 3n + 1$ và $h(n) = 3n + 2$ từ $\mathbb{Z}$ vào $\mathbb{Z}$. Hãy tìm ánh xạ là ngược trái đồng thời của f, g và h.

2.2. Cho các ánh xạ $g : X \to Y$, $f : Y \to Z$. Chứng minh rằng:

a) Nếu $f \circ g$ được xác định và cả hai hàm f, g đều có ngược trái thì $f \circ g$ cũng có ngược trái.

b) Chứng tỏ bằng ví dụ mệnh đề đảo nói chung không đúng, tức là, $f \circ g$ có ngược trái cả khi f không có ngược trái.

2.3. a) Có bao nhiêu toàn ánh từ tập có ba phần tử lên tập có hai phần tử.

b) Có bao nhiêu đơn ánh từ tập có bốn phần tử đến tập có ba phần tử.

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

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

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

2.5. Chứng minh rằng ánh xạ:

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

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

2.6. 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 không?

2.7. Giả sử X là một tập hợp hữu hạn. Chứng minh rằng đối với ánh xạ $f : X \to X$ thì tính đơn ánh, tính toàn ánh và tính song ánh là trùng nhau. Tìm một đơn ánh từ $\mathbb{N}$ vào $\mathbb{N}$ mà không phải là toàn ánh và một toàn ánh từ $\mathbb{N}$ vào $\mathbb{N}$ mà không phải là đơn ánh.

2.8. Cho ánh xạ $f : X \to Y$, A và B là hai tập con tuỳ ý của X. Chứng minh rằng:

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

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

b) Nếu f là đơn ánh thì

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

2.9. 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) $f(X \setminus A) \supset f(X) \setminus f(A)$;

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

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

a) $A \subset f^{-1}(f(A))$.

b) $C \supset f(f^{-1}(C))$.

c) Nếu $A \subset B$ thì $f(A) \subset f(B)$.

d) Nếu $C \subset D$ thì $f^{-1}(C) \subset f^{-1}(D)$.

2.11. Chứng minh rằng ánh xạ $f : X \to Y$ là đơn ánh khi và chỉ khi f thoả mãn một trong các điều kiện dưới đây:

a) $A = f^{-1}(f(A))$ với mọi $A \subset X$.

b) $f(A \cap B) = f(A) \cap f(B)$ với mọi $A, B \subset X$.

2.12. Giả sử $f : X \to Y$ và $g : Y \to Z$ 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 giả thiết f là toàn ánh thì g là đơn ánh.

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

2.13. Giả sử $f : X \to Y$ và $g : Y \to X$ là hai ánh xạ sao cho fgf là một song ánh. Chứng minh rằng f và g đều là song ánh.

2.14. Cho $X = \{a, b, c\}$, $P(X)$ là tập hợp các tập con của X; $Y = \{0, 1\}$ và $\mathrm{Hom}(X, Y)$ là tập hợp các ánh xạ từ X đến Y. Hãy thiết lập một song ánh giữa $P(X)$ và $\mathrm{Hom}(X, Y)$.

2.15. Cho ba ánh xạ $f : X \to Y$; $g, g' : V \to X$. Chứng minh hai điều kiện sau là tương đương:

a) f là đơn ánh.

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

2.16. Cho ba ánh xạ $f : X \to Y$; $h, h' : Y \to Z$. Chứng minh hai điều sau là tương đương:

a) f là một toàn ánh.

b) Với mọi h, h' và với mọi Z, từ $hf = h'f$ suy ra $h = h'$.

2.17. 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) $f(\bigcup\limits_{i \in I} A_i) = \bigcup\limits_{i \in I} f(A_i)$;

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

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

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

3. Quan hệ hai ngôi

3.1. Hãy xác định các tính chất phản xạ, đối xứng, phản đối xứng, bắc cầu của những quan hệ sau trên tập $\mathbb{N}^*$. Với $m, n \in \mathbb{N}^*$ thì $m\mathfrak{R}n$ khi và chỉ khi:

a) $m + n$ chẵn;

b) $m + n \leq 100$;

c) m/n là luỹ thừa của 2;

d) m/n chẵn;

e) mn lẻ.

3.2. Trong những quan hệ trên $\mathbb{Z}$ sau đây, quan hệ nào là đối xứng:

a) $m\rho n$ có nghĩa $m + n$ chia hết cho 3;

b) $m\delta n$ có nghĩa $m - n$ chia hết cho 3.

Quan hệ nào trong chúng là bắc cầu?

3.3. Trên tập $\mathbb{R}^2$, xét quan hệ S như sau: $(x, y)S(z, t) \Leftrightarrow x = z$.

a) Chứng tỏ rằng S là một quan hệ tương đương. Mô tả các lớp tương đương theo quan hệ S.

b) Lập một song ánh từ $\mathbb{R}^2/S$ vào $\mathbb{R}$.

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

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

Chứng minh:

a) $\mathfrak{R}$ là một quan hệ tương đương;

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

3.5. Cho quan hệ tương đương E trên S. Chứng minh rằng tập con A của S là một lớp tương đương của S theo quan hệ tương đương E nếu và chỉ nếu với $y \in A, z \in A \Rightarrow yEz$.

3.6. Cho E là một quan hệ tương đương trên tập X và cho $f : X \to S$ là một ánh xạ thoả mãn điều kiện $f(x) = f(y) \Leftrightarrow xEy$. Chứng

minh rằng khi đó tồn tại duy nhất ánh xạ $g : X/E \to S$ sao cho $f = g \circ p$, trong đó $p : X \to X/E$ là phép chiếu tự nhiên. Hơn nữa, nếu f là toàn ánh thì g là song ánh.

3.7. Giả sử S là một tập hợp, T là một quan hệ hai ngôi có tính chất phản xạ, đối xứng trong S. Ta xác định quan hệ hai ngôi $\mathfrak{R}$ trong S như sau: $x\mathfrak{R}y$ khi và chỉ khi có $x_1 = x, x_2, ..., x_n = y$ sao cho

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

Chứng minh:

a) $\mathfrak{R}$ là một quan hệ tương đương và $T \subset \mathfrak{R}$;

b) Với mọi quan hệ tương đương H sao cho $T \subset H$ thì $\mathfrak{R} \subset H$.

3.8. Chứng tỏ rằng trên tập hợp X khác rỗng bất kỳ tồn tại duy nhất một quan hệ vừa là quan hệ tương đương vừa là quan hệ thứ tự.

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

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

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

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

3.11. Đối với hai tập con $A \subset B$ của tập hợp S, ta gọi ánh xạ $g : B \to Y$ là kéo dài của ánh xạ $f : A \to Y$ nếu $g(x) = f(x)$ với mọi $x \in A$. Gọi $\Phi(S, Y)$ là tập hợp các ánh xạ từ các tập con của S đến Y. Xét quan hệ $\mathfrak{R}$ trong $\Phi(S, Y)$ được xác định như sau:

$$f\ \mathfrak{R}\ g \text{ khi và chỉ khi } g \text{ là kéo dài của } f.$$

a) Chứng minh $\mathfrak{R}$ là một quan hệ thứ tự.

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

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

3.13. Chứng minh rằng nếu tập S sắp thứ tự tốt thì S sắp thứ tự toàn phần.

4. Số nguyên

4.1. Chứng minh rằng nếu $m-n$ chia hết $mp+nq$ thì $m-n$ chia hết $mq+np$ (ở đó $m,n,p,q \in \mathbb{Z}$).

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

4.3. Chứng minh rằng nếu $(a^3+b^3+c^3) \vdots 9$ thì một trong ba số a,b,c chia hết cho 3.

4.4. Chứng minh rằng không có cặp số nguyên x,y nào thoả mãn đẳng thức:
a) $x^2+1=3y$.
b) $x^2+2=5y$.

4.5. Chứng minh rằng với mọi số tự nhiên $n \geq 1$, tích

$$(n+1)(n+2)...(n+n)$$

chia hết cho 2^n.

4.6. Chứng minh rằng tồn tại vô số số nguyên dương n sao cho 2^n+1 chia hết cho n.

4.7. Cho đa thức $P(x)$ với các hệ số nguyên, biết rằng tồn tại số nguyên dương a sao cho không có số nào trong các số $P(1),P(2),...,P(a)$ chia hết cho a. Chứng minh rằng với mọi số nguyên z ta có $P(z) \neq 0$.

4.8. Chứng minh rằng nếu a và c là hai số nguyên tố cùng nhau thì $a \mid m$ và $c \mid m$ kéo theo $ac \mid m$.

4.9. Cho $a>0$. Chứng minh rằng $(ab,ac)=a(b,c)$.

4.10. Chứng minh rằng với hai số nguyên dương a và b tập hợp tất cả các số dạng $am+bn$ (m,n nguyên dương) chứa tất cả các bội của (a,b) lớn hơn ab.

4.11. Chứng minh rằng với mọi số nguyên a và b ta có:

$$(3a+5b, 8a+13b)=(a,b).$$

4.12. Tìm $(a+b, a-b)$ biết $(a,b)=d$.

4.13. Chứng minh rằng $(a,b)=1$ với:

a) $a=21m+4,\ b=14m+3$;

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

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

trong đó $m\in\mathbb{Z}, n\in\mathbb{Z}$.

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

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

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

4.16. Cho a, b là hai số nguyên dương sao cho $(a,b)=1$. Tìm

$$(5^a+7^a, 5^b+7^b).$$

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

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

4.18. Tìm bội chung nhỏ nhất của ba số nguyên liên tiếp khác không.

4.19. Đặt $[a,b]=m$. Chứng minh rằng:

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

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

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

Chứng minh rằng:

$$[a_1, a_2, ..., a_n]=\frac{M}{D}.$$

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

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

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

4.22. Cho p và $2p+1$ là hai số nguyên tố lớn hơn 3. Chứng minh rằng $4p+1$ là một hợp số.

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

4.24. Chứng minh rằng tồn tại vô số số nguyên dương a sao cho n^4+a là hợp số với mọi số nguyên dương n.

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

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

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

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

Chương II

NHÓM - ĐỒNG CẤU NHÓM

1. Đại số hai ngôi

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

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

Như vậy, phép toán hai ngôi là một quy tắc cho tương ứng hai phần tử $x, y \in S$ với một phần tử của S là ảnh của (x, y) qua φ. Tập hợp S cùng với phép toán hai ngôi $\circ$ cho trên nó được gọi là một *đại số hai ngôi*, ký hiệu bởi $(S, \circ)$.

Đại số hai ngôi $(S, \circ)$ được gọi là một *nửa nhóm* nếu phép toán trên S thoả mãn luật kết hợp, nghĩa là

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

với mọi $a, b, c \in S$. Nửa nhóm S được gọi là *vị nhóm* nếu trong S có phần tử e, gọi là *phần tử đơn vị*, sao cho

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

với mọi $a \in S$. Phần tử đơn vị còn được gọi là *phần tử trung hoà*. Trong trường hợp phép toán được ký hiệu bởi *phép cộng* thì phần tử này ký hiệu bởi 0.

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

Vị nhóm M được gọi là *xyclic* nếu nó chỉ gồm các luỹ thừa c^n của phần tử c nào đó. Khi đó ta nói rằng vị nhóm M được *sinh* bởi c. Trong vị nhóm bất kỳ M thì $a^m a^n = a^{m+n}$ đối với $a \in M$ và với mọi số tự nhiên m, n. Nửa nhóm M được gọi là *giao hoán* (hay *aben*) nếu $ab = ba$ với mọi $a, b \in M$. Hiển nhiên mọi vị nhóm xyclic đều giao hoán.

Tập con H của nửa nhóm $(N, \circ)$ được gọi là *đóng* (hay *ổn định*) đối với phép toán trong N nếu với mọi $a, b \in H$ ta đều có $ab \in H$. Nếu tập con H đóng thì H là nửa nhóm với phép toán $H \times H \to H$, thu hẹp của phép toán trong N. Khi đó ta nói rằng phép toán trong H là *cảm sinh* bởi phép toán trong N và H là *nửa nhóm con* của N.

Ánh xạ $f : N \to N'$ từ nửa nhóm N tới nửa nhóm N' được gọi là *đồng cấu nửa nhóm* nếu

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

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

Nếu $f : N \to N'$ là đồng cấu nửa nhóm và N có đơn vị e thì $f(e)$ là đơn vị của $\mathrm{Im}f$. Chú ý rằng nếu $f : N \to N'$ là một đồng cấu của các nửa nhóm và N có đơn vị e thì có thể $f(e)$ không phải là đơn vị của N'.

Cấu trúc của một vị nhóm xyclic bất kỳ C sinh bởi phần tử c được mô tả như sau: Nếu tất cả các luỹ thừa của c đều khác nhau thì ta có ánh xạ

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

là một đẳng cấu. Trong trường hợp ngược lại, sẽ tồn tại số nguyên dương bé nhất s sao cho $c^s = c^m$ đối với m nào đó, $m < s$. Khi đó $C = \{1, c, \ldots, c^s\}$ và

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

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

Trong mỗi vị nhóm xyclic kiểu (m, n), $m \neq 0$, có đúng một phần tử $a \neq 1$ sao cho $a^2 = a$. Ta gọi a là phần tử *luỹ đẳng*.

2. Nhóm

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

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

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

(i) Phép toán kết hợp:

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

với mọi a, b, c thuộc G.

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

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

với mọi $a \in G$.

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

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

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

Phần tử a' có tính chất $aa' = a'a = e$ là duy nhất đối với mỗi $a \in G$, được gọi là *nghịch đảo* của a và ký hiệu bởi a^{-1}. Đối với mọi phần tử a, b của nhóm G các tính chất sau luôn được thoả mãn:

(i) $(a^{-1})^{-1} = a$;

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

Trong nhóm G luật giản ước luôn luôn thực hiện được, nghĩa là $ax = ay$ kéo theo $x = y$ và $xb = yb$ kéo theo $x = y$, với mọi $a, b \in G$. Khái niệm nhóm thường được đặc trưng bởi những điều kiện sau:

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

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

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

2. Nửa nhóm G là nhóm nếu và chỉ nếu các phương trình $ax = b$ và $ya = b$ có nghiệm trong G với mọi $a, b \in G$.

Tập hợp $S(X)$ tất cả các song ánh từ tập hợp X tới chính nó lập thành một nhóm với phép toán hai ngôi là phép hợp thành các ánh xạ. Phần tử đơn vị của $S(X)$ là ánh xạ đồng nhất id_X và đối với song ánh $f \in S(X)$ thì phần tử nghịch đảo f' ở đây chính là ánh xạ ngược của f. Mỗi phần tử $f \in S(X)$ được gọi là một *phép thế* của X và $S(X)$ được gọi là *nhóm tất cả các phép thế* của X, hay *nhóm đối xứng* của X. Khi tập hợp X có hữu hạn phần tử ta ký hiệu nhóm đối xứng của tập $X = \{1, 2, \ldots, n\}$ là S_n, và gọi là *nhóm đối xứng của* n *phần tử*. Mỗi song ánh từ X lên chính nó được gọi là một *phép thế* bậc n và được ký hiệu bởi

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

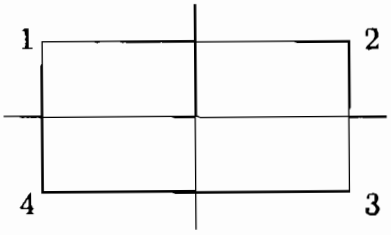
trong đó mỗi phần tử ở dòng dưới là ảnh của phần tử tương ứng ở dòng trên. Một cách tổng quát, mỗi phép thế f có thể viết dưới dạng

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

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

Nếu f, g là hai phép thế thì tích $g \circ f$ là phép thế thu được bởi việc thực hiện liên tiếp phép thế f rồi tới phép thế g (Cũng có tác giả quy ước tích $g \circ f$ được thực hiện bởi g trước rồi đến f). Nếu $a_1, a_2, \ldots, a_m, 1 \leq m \leq n$, là các phần tử phân biệt của tập hợp $\{1, 2, \ldots, n\}$ thì phép thế f cho bởi $f(a_1) = a_2$, $f(a_2) = a_3, \ldots, f(a_{m-1}) = a_m, f(a_m) = a_1$, và $f(x) = x$ nếu $x \notin \{a_1, a_2, \ldots, a_m\}$, được gọi là một vòng xích độ dài m, hay một m - xích. Ta ký hiệu vòng xích này bởi $(a_1 a_2 \ldots a_m)$.

4-*nhóm Klein* hay nhóm đối xứng của hình chữ nhật không là hình vuông: Ta đánh dấu các đỉnh của hình chữ nhật bởi các số 1, 2, 3, 4 như ở hình vẽ sau:



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

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

Tương tự b là phép đối xứng qua trục tung. Phép đối xứng thứ ba c là phép quay 180^0 quanh tâm của hình chữ nhật. Phép đối xứng cuối cùng là phép đồng nhất e. Nhóm các phép đối xứng của hình chữ nhật được cho bởi bảng sau:

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

3. Nhóm con

Ta nhắc lại rằng tập con khác rỗng H của nửa nhóm nhân G được gọi là *đóng* (hay *ổn định*) nếu $a, b \in H$ kéo theo $ab \in H$, và khi đó H là nửa nhóm con của G với phép toán cảm sinh bởi phép toán trong G. Tập con đóng H của nhóm nhân G được gọi là *nhóm con* của G nếu nó là một nhóm đối với phép toán cảm sinh bởi phép nhân trong G. Nhóm con được đặc trưng bởi các điều kiện sau:

1. Tập con H của nhóm G là nhóm con khi và chỉ khi các điều kiện sau được thoả mãn:

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

Nói riêng, nếu H là một tập con hữu hạn khác rỗng của nhóm G và $ab \in H$ với mọi $a, b \in H$, thì H là nhóm con của G.

2. Giả sử H là tập con khác rỗng của nhóm G. Khi đó các điều kiện sau là tương dương:

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

Nói riêng, trong nhóm G tập hợp tất cả các luỹ thừa a^n ($n \in \mathbb{Z}$) của $a \in G$ lập thành một nhóm con, được gọi là nhóm xyclic sinh bởi a.

Phần tử a của nhóm G gọi là có *cấp vô hạn* nếu không tồn tại số nguyên dương n nào sao cho $a^n = e$, và được gọi là có *cấp hữu hạn* m nếu m là số nguyên dương bé nhất sao cho $a^m = e$. Lực lượng của nhóm G, ký hiệu bởi $|G|$, được gọi là *cấp* của nhóm. G được gọi là nhóm hữu hạn hoặc vô hạn nếu $|G|$ tương ứng là hữu hạn hoặc vô hạn.

Nhóm các phép quay của một đa giác đều n đỉnh trong mặt phẳng là nhóm xyclic cấp n, sinh bởi phép quay góc $2\pi/n$ radian. Nhóm này ký hiệu bởi C_n.

Nếu e là phần tử đơn vị của nhóm G và $a \in G$ là phần tử có cấp n thì $a^k = e$ khi và chỉ khi k chia hết cho n.

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

Rõ ràng nhóm con H là xyclic khi nó được sinh bởi tập gồm một phần tử. Nhóm con của một nhóm xyclic là xyclic, và mọi nhóm con của nhóm $(\mathbb{Z}, +)$ đều có dạng $A = m\mathbb{Z}$ với $m \in \mathbb{Z}$.

Nhóm các phép tự trùng D_n *của đa giác đều trong không gian*: Xét nhóm tất cả các phép dời hình trong không gian ba chiều biến một đa giác đều n đỉnh thành chính nó. Ngoài n phép quay trong mặt phẳng còn có n phép *lật* đa giác trong không gian quanh trục đối xứng (có n trục đối xứng). Gọi g là phép quay góc $2\pi/n$ radian và h là một phép

lật, thế thì h là một phần tử cấp 2 và nhóm D_n sinh bởi hai phần tử g, h :

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

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

4. Nhóm con chuẩn tắc - nhóm thương

Cho H là một nhóm con của nhóm G. Khi đó các tập hợp $gH = \{ga \mid a \in H\}$, $Hg = \{ag \mid a \in H\}$ với $g \in G$ lần lượt được gọi là *lớp ghép trái, lớp ghép phải* của nhóm G theo nhóm con H. Với $a, b \in G$, khi đó:

$$\begin{aligned} aH = bH &\Leftrightarrow a^{-1}b \in H, \\ Ha = Hb &\Leftrightarrow ab^{-1} \in H. \end{aligned}$$

Quan hệ hai ngôi $\sim$:

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

là một *quan hệ tương đương* trên G; do đó nó cho *một phân hoạch nhóm G theo các lớp không giao nhau và mỗi lớp như vậy là một lớp ghép trái theo H*. Tương tự, quan hệ hai ngôi $a \sim b \Leftrightarrow ab^{-1} \in H$ là một quan hệ tương đương trên G mà mỗi lớp tương đương là một lớp ghép phải theo H. Tập

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

các lớp ghép trái của H trong nhóm G được gọi là *tập thương* của nhóm G theo H. Lực lượng của tập các lớp ghép trái của G theo nhóm con H được gọi là *chỉ số* của H trong G, và ký hiệu bởi $[G : H]$.

Định lý Lagrange: *Nếu G là một nhóm hữu hạn và H là nhóm con của G thì cấp của H chia hết cấp của G*. Đặc biệt suy ra rằng mọi nhóm cấp nguyên tố p là xyclic.

Định lý Lagrange có thể mở rộng cho trường hợp các nhóm xyclic hữu hạn. *Nếu G là một nhóm xyclic cấp n, và k chia hết n thì G có*

đúng một nhóm con H cấp k. Hơn nữa, nếu g sinh ra G, thì H được sinh bởi $g^{n/k}$.

Nhóm con H của nhóm G được gọi là *nhóm con chuẩn tắc* nếu $gH = Hg$ với mọi $g \in G$. Khi đó ta cũng nói rằng H là nhóm con chuẩn tắc trong G. Đối với nhóm con H của nhóm G các điều sau là tương đương:

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

Phần tử gag^{-1} được gọi là *liên hợp* của a bởi g. Nếu H là nhóm con chuẩn tắc trong nhóm G thì tương ứng

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

là một ánh xạ. Và bởi vậy, tập thương G/H là một nhóm với phép toán $(aH)(bH) = (ab)H$. Nhóm này được gọi là *nhóm thương* của G theo H. Nhờ khái niệm nhóm thương ta chứng minh được rằng: *Nếu G là nhóm aben hữu hạn và p là số nguyên tố chia hết cấp của nhóm G thì G chứa phần tử cấp p và do đó chứa nhóm con cấp p.*

5. Đồng cấu nhóm

Một trong những kết quả cơ bản của lý thuyết nhóm là định lý đồng cấu nhóm. Nó mô tả mối quan hệ sâu sắc giữa những đồng cấu với các nhóm con chuẩn tắc và các nhóm thương. Những kết quả tương tự cũng được phát biểu cho các vành, các không gian vectơ, cũng như cho phần lớn các hệ đại số khác.

Ánh xạ $f : G \to H$ từ nhóm G đến nhóm H được gọi là *đồng cấu nhóm* (hay một cách ngắn gọn là *đồng cấu*) nếu:

$$f(ab) = f(a)f(b) \text{ với mọi } a, b \in G.$$

Đồng cấu f được gọi là một *đơn cấu* (tương ứng *toàn cấu, đẳng cấu*) nếu f là một đơn ánh (tương ứng toàn ánh, song ánh).

Khái niệm đồng cấu có một số tính chất cơ bản sau:

1. Nếu $f : G \to H$ là một đồng cấu nhóm thì:

(i) $f(e_G) = e_H$, với e_G, e_H lần lượt là các phần tử đơn vị của G, H.

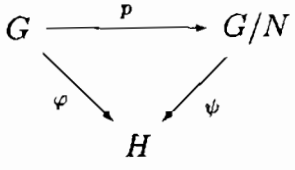
(ii) $f(a^{-1}) = [f(a)]^{-1}$, với mọi $a \in G$.

2. Hợp thành của hai đồng cấu $\alpha : A \to B, \beta : B \to C$ là một đồng cấu.

3. Đồng cấu $f : G \to H$ là đơn cấu khi và chỉ khi $\mathrm{Ker} f = \{e\}$.

4. Nhóm con N của G là chuẩn tắc khi và chỉ khi N là hạt nhân của một đồng cấu $f : G \to H$ nào đó.

5. Định lý đồng cấu: *Giả sử N là nhóm con chuẩn tắc của G. Khi đó với mỗi đồng cấu $\varphi : G \to H$ sao cho $N \subset \mathrm{Ker}\ \varphi$ đều tồn tại duy nhất một đồng cấu $\psi : G/N \to H$ sao cho biểu đồ sau giao hoán*



nghĩa là $\varphi = \psi \circ p$, trong đó p là phép chiếu tự nhiên. Hơn nữa, ψ đơn cấu khi và chỉ khi $N = \mathrm{Ker}\varphi$. Nói riêng, ta luôn có

$$G/Ker\varphi \cong Im\varphi.$$

Khái niệm đẳng cấu cho phép phân loại các nhóm xyclic: *mỗi nhóm xyclic cấp vô hạn đẳng cấu với nhóm cộng các số nguyên $\mathbb{Z}$, và mỗi nhóm xyclic cấp n đẳng cấu với nhóm cộng $\mathbb{Z}_n$ các lớp đồng dư theo môđun n.* Trong cuốn sách này chúng ta thường nói tới hai nhóm xyclic $(\mathbb{Z}_n, +)$ và $(C_n, \circ)$ với số nguyên dương n nào đó, chúng là đẳng cấu.

Định lý đồng cấu có hai hệ quả quan trọng:

1. *Giả sử A, B là hai nhóm con chuẩn tắc của nhóm G và $A \subset B$. Khi đó có đẳng cấu chính tắc*

$$(G/A)(B/A) \cong G/B.$$

2. *Nếu A là nhóm con chuẩn tắc của nhóm G và B là một nhóm con của G thì tập $AB = \{ab \mid a \in A, b \in B\}$ là một nhóm con của G và ta có đẳng cấu*

$$AB/B \cong B/(A \cap B).$$

Bài tập

1. Đại số hai ngôi

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

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

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

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

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

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

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

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

1.8. Cho tập hợp $A = \{a, b\}$. Có bao nhiêu phép toán hai ngôi trên A, hãy chỉ rõ tất cả các phép toán đó.

1.9. Giả thiết rằng phép toán hai ngôi $*$ trên tập X có đơn vị và thoả mãn đẳng thức sau với mọi x, y, z thuộc X:

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

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

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

a) $m * n = m - n$;

b) $m * n = m^2 + n^2$;

c) $m * n = 2(m + n)$.

1.11. Cho tập hợp $A = \{a, b, c\}$. Hãy xây dựng phép toán hai ngôi trên A sao cho:

a) A có đúng một đơn vị trái.

b) A có đúng hai đơn vị trái.

c) A có đúng ba đơn vị trái.

1.12. Trên tập hợp X xét phép toán hai ngôi sau: $ab = b$ với mọi $a, b \in X$.

a) Chứng tỏ rằng X cùng với phép toán trên là nửa nhóm.
b) Chứng tỏ rằng mọi phần tử của X đều là đơn vị trái.
c) Khi nào thì X có đơn vị? Khi nào thì phép toán hai ngôi đã cho là giao hoán?

1.13. Trên tập hợp M tất cả các ma trận thực vuông cấp hai cho phép toán hai ngôi xác định bởi: $a \circ b = ab + ba$. Chứng tỏ rằng phép toán đó có tính chất giao hoán nhưng không có tính chất kết hợp.

1.14. Cho $f : X \to Y$ là một đồng cấu của các nửa nhóm. Chứng minh rằng:
a) Nếu A là một nửa nhóm con của X thì ảnh $f(A)$ là nửa nhóm con của Y.
b) Nếu B là nửa nhóm con của Y thì tạo ảnh toàn phần $f^{-1}(B)$ là nửa nhóm con của X.

1.15. Cho các đồng cấu nửa nhóm $\alpha : A \to B; \beta : B \to C$. Chứng minh rằng:
a) Nếu $\beta \circ \alpha$ là toàn cấu thì β là toàn cấu.
b) Nếu $\beta \circ \alpha$ là đơn cấu thì α là đơn cấu.

1.16. Cho A, B là những vị nhóm và $f : A \to B$ là đồng cấu nửa nhóm. Chứng minh rằng các điều sau tương đương:
a) $f(e_A) = e_B$, trong đó e_A, e_B lần lượt là các phần tử đơn vị của A, B.
b) Ảnh $f(A)$ là vị nhóm con của B.
c) Tạo ảnh $f^{-1}(e_B)$ là vị nhóm con của A.
Ngoài ra, nếu $f^{-1}(e_B) = \{e_A\}$ thì f có là đơn cấu hay không?

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

2. Nhóm

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

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

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

2.3. $(\mathbb{R}^*, \circ)$, trong đó $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ và $x \circ y$ là xy nếu $x > 0$, là x/y nếu $x < 0$.

2.4. $(\mathbb{Z}, *)$, trong đó $m * n$ là $m + n$ nếu m chẵn, và là $m - n$ nếu m lẻ.

2.5. Chứng minh rằng $\mathbb{Z}_6^* = \mathbb{Z}_6 \setminus \{\overline{0}\}$ không là nhóm đối với phép nhân $\overline{r}.\overline{s} = \overline{rs}$.

2.6. Hãy trang bị phép toán hai ngôi cho tập hợp A để A trở thành nhóm trong trường hợp A có 2, 3, 4 phần tử.

2.7. Cho $A = \{0, 1, 2, ..., n-1\}$, với $n \in \mathbb{Z}$. Trên A cho phép toán hai ngôi: $a * b$ là dư của phép chia ab cho n. Chứng minh rằng
a) A là một vị nhóm.
b) A là nhóm khi và chỉ khi n là số nguyên tố.

2.8. Cho G là tập tất cả các các cặp số thực (a, b), trong đó $a \neq 0$. Trên G xác định phép toán hai ngôi cho bởi công thức

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

Chứng tỏ rằng khi đó G là một nhóm.

2.9. Chứng minh rằng trong nhóm G:

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

2.10. Chứng minh rằng trong nhóm G, $(a^{-1}ba)^k = a^{-1}b^k a$ đối với mỗi số nguyên k.

2.11. Cho G là một nhóm và $a, b \in G$ sao cho $bab^{-1} = a^r$, với $r \in \mathbb{N}$. Chứng minh rằng $b^i ab^{-i} = a^{r^i}$ $\forall i \in \mathbb{N}$.

2.12. Chứng minh rằng nếu $a^2 = e$ với mọi phần tử a của nhóm G thì G là nhóm aben.

2.13. Nếu a không là đơn vị của nhóm và $a^4 b = ba^5$, hãy chứng minh $ab \neq ba$.

2.14. Cho G là nửa nhóm. Với mỗi $a \in G$ ký hiệu

$$\begin{aligned} aG &= \{ax \mid x \in G\} \\ Ga &= \{xa \mid x \in G\}. \end{aligned}$$

Chứng minh rằng G là nhóm khi và chỉ khi với mỗi a thì

$$aG = Ga = G.$$

2.15. Cho X là một tập hợp khác rỗng. Chứng minh rằng ba mệnh đề sau là tương đương:

a) X là một nhóm.

b) Tồn tại một phép toán hai ngôi $(a, b) \mapsto ab$ trên X và một phép toán một ngôi $a \mapsto a^{-1}$ trên X sao cho:

i) $a(bc) = (ab)c$ với mọi $a, b, c \in X$.

ii) $a^{-1}(ab) = b = (ba)a^{-1}$ với mọi $a, b \in X$.

c) Tồn tại một phép toán hai ngôi $(a, b) \mapsto a/b$ trên X sao cho:

i) $a/a = b/b$.

ii) $a/(b/b) = a$.

iii) $(a/a)/(b/c) = c/b$.

iv) $(a/c)/(b/c) = a/b$.

với mọi $a, b, c \in X$.

2.16. Chứng minh rằng G là một nhóm aben khi và chỉ khi G thoả mãn các điều kiện sau:

(i) $(ab)c = a(cb)$,

(ii) Tồn tại $e \in G$ sao cho $ea = a$ với mọi $a \in G$,

(iii) Với mỗi $a \in G$ tồn tại $a' \in G$ để $a'a = e$.

2.17. Chứng minh rằng các tính chất sau trong nhóm G là tương đương :

(i) G là aben.

(ii) $(ab)^2 = a^2b^2$ đối với mọi $a, b \in G$.

(iii) $(ab)^{-1} = a^{-1}b^{-1}$ đối với mọi $a, b \in G$.

(iv) $(ab)^n = a^nb^n$ đối với mọi $a, b \in G$ và $n \in \mathbb{Z}$.

(v) $(ab)^n = a^nb^n$ đối với mọi $a, b \in G$ và ba số nguyên n liên tiếp.

Chứng minh rằng (v)⇒(i) là không đúng nếu thay giả thiết "ba" bởi "hai".

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

3. Nhóm con

3.1. Chứng minh rằng trong một nhóm thì:

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

b) Cấp của phần tử ab chính là cấp của ba.

3.2. Trong nhóm nhân các ma trận vuông cấp n trên $\mathbb{R}$ với định thức khác không, hãy tìm cấp của ma trận sau theo a:

$$A_a = \begin{bmatrix} a & 0 & \cdots & 0 \\ 0 & a & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & a \end{bmatrix}$$

3.3. Tìm cấp của tất cả các phần tử của nhóm $A = \{e, a, b, c\}$ với phép toán hai ngôi được cho như sau:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	a
b	b	c	e	a
c	c	b	a	e

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

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

3.6. Trong nhóm các phép thế S_4 chứng minh rằng các phép thế sau:

$$e, a = (12)(34), b = (13)(24) \text{ và } c = (14)(23)$$

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

3.7. Chứng minh rằng tập hợp các phần tử có cấp hữu hạn của một nhóm aben A là một nhóm con của A. Nếu A không là nhóm aben thì kết quả này còn đúng hay không?

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

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

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

trong đó

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

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

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

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

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

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

3.12. Chứng minh các phát biểu sau là tương đương:
a) Nhóm G có nhiều hơn một phần tử và không có nhóm con thực sự.
b) G là nhóm xyclic cấp nguyên tố.

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

3.14. Chứng minh rằng mọi nhóm có cấp bé hơn hoặc bằng 5 đều giao hoán.

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

3.16. Cho A là một nhóm xyclic cấp n và d là một ước của n. Chứng minh rằng A có đúng một nhóm con cấp d và nhóm con này là xyclic.

3.17. Chứng minh rằng mọi nhóm xyclic vô hạn đều có đúng hai phần tử sinh.

3.18. Các số nguyên Gauss là các phần tử thuộc tập hợp

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

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

3.19. Chứng minh rằng $(\mathbb{Z}_6^*, \times)$ và $(\mathbb{Z}_{17}^*, \times)$, trong đó $(\mathbb{Z}_n^*$ là nhóm nhân các phần tử khả nghịch của $\mathbb{Z}_n)$, là nhóm xyclic. Tìm các phần tử sinh của chúng.

3.20. Cho A là một nhóm aben. Với mỗi số tự nhiên n, ta ký hiệu:

$$A_n = \{a \in A \mid a^n = e\}.$$

a) Chứng minh rằng A_n là một nhóm con của A.

b) Chứng minh rằng nếu $(m, n) = 1$ thì $A_m \cap A_n = \{e\}$.

c) Giả sử $(m, n) = 1$ và $A = A_{mn}$. Chứng minh rằng mỗi phần tử $a \in A$ đều viết được dưới dạng $a = xy, x \in A_m, y \in A_n$.

3.21. Chứng minh rằng hai nhóm con khác không bất kỳ của nhóm $(\mathbb{Q}, +)$ có giao khác không.

3.22. Giả sử p là số nguyên tố , $\mathbb{Z}(p^\infty)$ là tập con của nhóm $\mathbb{Q}/\mathbb{Z}$:

$$\mathbb{Z}(p^\infty) = \left\{ \left[\frac{a}{b}\right] \in \mathbb{Q}/\mathbb{Z} \mid a, b \in \mathbb{Z}, b = p^i, i \geq 0 \right\},$$

trong đó $\left[\frac{a}{b}\right] = \frac{a}{b} + \mathbb{Z}$. Chứng minh rằng $\mathbb{Z}(p^\infty)$ là nhóm vô hạn đối với phép cộng trong $\mathbb{Q}/\mathbb{Z}$.

3.23. Chứng minh rằng nhóm chỉ có một số hữu hạn nhóm con là nhóm hữu hạn.

3.24. Nếu H, K là hai nhóm con có chỉ số hữu hạn trong nhóm G sao cho $[G : H]$ và $[G : K]$ nguyên tố cùng nhau thì $G = HK$.

3.25. Cho H và K là các nhóm con của nhóm G, chứng minh rằng HK là nhóm con của nhóm G khi và chỉ khi $HK = KH$.

3.26. Cho A là một nhóm con của nhóm G và $a \in G$. Chứng minh rằng tập hợp $aA = \{ax \mid x \in A\}$ là một nhóm con của G khi và chỉ khi $a \in A$.

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

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

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

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

3.29. Giả sử a, b là hai phần tử của một nhóm lần lượt có cấp là r và s, ngoài ra $(r, s) = 1$ và $ab = ba$. Chứng minh rằng cấp của ab bằng rs.

3.30. Chứng minh rằng nhóm có cấp là số chẵn có ít nhất một phần tử cấp 2.

4. Nhóm con chuẩn tắc - nhóm thương

4.1. Trên nhóm G cho quan hệ C xác định bởi aCb nếu và chỉ nếu $ab = ba$. Đó có phải là quan hệ tương đương hay không? Nếu đó là quan hệ tương đương hãy mô tả các lớp tương đương của nó.

4.2. Nếu H là nhóm con duy nhất với cấp cho trước của nhóm G, chứng minh rằng H là chuẩn tắc.

4.3. Cho H là một nhóm con của nhóm G. Chứng minh rằng có tương ứng 1-1 giữa tập các lớp ghép trái của H trong G và tập các lớp ghép phải của H trong G.

4.4. Tìm các lớp ghép trái và lớp ghép phải của

$$H = \{(1), (12), (34), (12) \circ (34)\}$$

trong S_4.

4.5. Nhóm con xyclic $\{(1), (123), (132)\}$ có là chuẩn tắc trong S_4 không?

4.6. Nhóm con

$$\{(1), (1234), (13) \circ (24), (1432), (13), (24), (14) \circ (23), (12) \circ (34)\}$$

có là chuẩn tắc trong S_4 không?

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

4.8. Giả sử S là một tập con của nhóm G. Chứng minh rằng tập con

$$C(S) = \{g \in G \mid gs = sg, \forall s \in S\}$$

là một nhóm con của G. Nhóm con $C(S)$ được gọi là *cái tâm hoá* của S; trường hợp đặc biệt $C(G)$ gọi là *tâm* của G. Chứng minh rằng $C(G)$ là nhóm con chuẩn tắc của G.

4.9. Giả sử A là một nhóm con của nhóm G có chỉ số 2. Chứng minh rằng A là chuẩn tắc.

4.10. Hai nhóm con A và B của nhóm G được gọi là *liên hợp* nếu tồn tại $a \in G$ sao cho $B = a^{-1}Aa$. Chứng minh rằng giao của các

liên hợp của nhóm con A của G là một nhóm con chuẩn tắc của G.

4.11. Giả sử A, B là hai nhóm con chuẩn tắc của nhóm G sao cho $A \cap B = \{e\}$. Chứng minh rằng $ab = ba$ với mọi $a \in A$ và $b \in B$.

4.12. Hãy chứng tỏ rằng tính chất chuẩn tắc không bắc cầu. Nghĩa là tồn tại ba nhóm con A, B, C của nhóm G sao cho A chuẩn tắc trong B, B chuẩn tắc trong C nhưng A không chuẩn tắc trong C.

4.13. Giả sử A, B là hai nhóm con chuẩn tắc của G. Chứng minh rằng $A \cap B$, AB và BA là những nhóm con chuẩn tắc của G. Hơn nữa, $AB = BA$.

4.14. Cho G là nhóm cấp $p^k m$, với p nguyên tố và $(p, m) = 1$. Giả sử H là nhóm con cấp p^k và K là nhóm con cấp p^d với $0 < d \leq k$ nhưng K không là nhóm con của H. Chứng minh rằng HK không là nhóm con của G.

4.15. Tìm tâm của các nhóm D_3, D_4.

4.16. Với hai phần tử a, b của nhóm G, ta gọi $aba^{-1}b^{-1}$ là *giao hoán tử* của a và b. Chứng minh rằng:

a) Nhóm con G' sinh bởi mọi giao hoán tử của G là một nhóm con chuẩn tắc của G (nhóm con này được gọi là *nhóm con giao hoán tử* của G).

b) Nhóm thương G/G' là nhóm aben.

c) Nếu A là nhóm con chuẩn tắc trong G thì nhóm thương G/A là aben khi và chỉ khi $G' \subset A$.

4.17. Hãy xác định các phần tử của các nhóm thương:

a) Nhóm cộng $3\mathbb{Z}$ trên nhóm con $15\mathbb{Z}$.

b) Nhóm cộng $4\mathbb{Z}$ trên nhóm con $24\mathbb{Z}$.

c) Nhóm xyclic vô hạn sinh bởi phần tử a trên nhóm con sinh bởi phần tử a^5.

d) Nhóm nhân các số thực khác không trên nhóm nhân các số thực dương.

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

4.19. Chứng minh rằng mọi nhóm cấp p^m, trong đó p là số nguyên tố, đều chứa một nhóm con cấp p.

4.20. Cho G là một nhóm con cấp n và $(n, m) = 1$. Chứng minh rằng

mọi phần tử h của G có một căn bậc m, nghĩa là $h = g^m$ với một $g \in G$ nào đó.

4.21. Chứng minh rằng:

a) Nếu M là một nhóm con của nhóm G, N là nhóm con chuẩn tắc của G thì tập hợp

$$MN = \{xy \mid x \in M, y \in N\}$$

là một nhóm con của G.

b) Nếu M cũng là nhóm con chuẩn tắc của G thì MN là nhóm con chuẩn tắc của G.

4.22. Cho S là một tập con của nhóm G và

$$N_S = \{g \in G \mid gSg^{-1} = S\}$$

a) Chứng tỏ rằng N_S là nhóm con của G (N_S được gọi là *cái chuẩn hoá* của S).

b) Nếu K là một nhóm con của G và H là một nhóm con chuẩn tắc của K thì $K \subset N_H$.

c) Nếu K là một nhóm con của N_H thì

$$KH = \{ab \mid a \in K, b \in H\}$$

là một nhóm và H là nhóm con chuẩn tắc của $K{\cdot}H$.

d) Cái chuẩn hoá N_H của nhóm con H là nhóm con lớn nhất của nhóm G nhận H làm nhóm con chuẩn tắc của nó.

4.23. Cho tập hợp $A = \{(x, y) \in \mathbb{R}^2, x \neq 0\}$ với $\mathbb{R}$ là tập các số thực.

Trên A xác định một phép toán hai ngôi $\circ$ như sau:

$$(x, y) \circ (u, v) = (xu, yu + v).$$

Chứng minh rằng tập hợp $H = \{(1, y) \mid y \in \mathbb{R}\}$ là một nhóm con chuẩn tắc trong A.

4.24. Gọi $\mathbb{C}^*$ là nhóm các số phức khác không dưới phép nhân và W là nhóm nhân các số phức theo môđun đơn vị. Mô tả $\mathbb{C}^*/W$.

4.25. Nhóm G được gọi là *mêta aben* nếu nó có một nhóm con chuẩn tắc K sao cho cả K và G/K đều giao hoán.

a) Chứng minh rằng mọi nhóm con và nhóm thương của một nhóm mêta aben là mêta aben.
b) Chứng minh rằng G là mêta aben nếu và chỉ nếu nhóm giao hoán tử G' là giao hoán.

4.26. Nhắc lại rằng, tâm $Z(G)$ của một nhóm G được định nghĩa bởi

$$Z(G) = \{z \in G \mid zg = gz \text{ với mọi } g \in G\}.$$

Cho $K \subset Z(G)$ là một nhóm con. Chứng minh rằng
a) K là chuẩn tắc trong G.
b) Nếu G/K là xyclic thì G là giao hoán.

5. Đồng cấu nhóm

Trong các bài tập từ 5.1 đến 5.4, hãy kiểm tra định nghĩa của mỗi ánh xạ là hợp lý. Xác định trong số đó đâu là đồng cấu nhóm, và khi đó hãy tìm hạt nhân và ảnh của nó. Phần tử của $\mathbb{Z}_n$ chứa x được ký hiệu là $[x]_n$.

5.1. $f : \mathbb{Z}_{12} \to \mathbb{Z}_{12}$, trong đó $f([x]_{12}) = [x+1]_{12}$.

5.2. $f : C_{12} \to C_{12}$, trong đó $f(g) = g^3$.

5.3. $f : \mathbb{Z} \to \mathbb{Z}_2 \times \mathbb{Z}_4$, ở đó $f(x) = ([x]_2, [x]_4)$.

5.4. $f : \mathbb{Z}_8 \to \mathbb{Z}_2$, ở đó $f([x]_8) = [x]_2$.

5.5. Chứng minh rằng mỗi ảnh toàn cấu của một nhóm xyclic là xyclic.

5.6. Cho vị nhóm cộng $\mathbb{N}$, nhóm cộng $\mathbb{Z}$ và phép nhúng tự nhiên $i : \mathbb{N} \to \mathbb{Z}$. Nếu A là một nhóm và $f : \mathbb{N} \to A$ là đồng cấu của các vị nhóm thì tồn tại duy nhất đồng cấu nhóm $f' : \mathbb{Z} \to A$ sao cho $f = f' \circ i$.

5.7. Cho A là nhóm con chỉ số hữu hạn trong nhóm G. Chứng minh rằng tồn tại một nhóm con chuẩn tắc B của G chứa trong A sao cho chỉ số của B trong G là hữu hạn.

5.8. Cho đồng cấu nhóm

$$\begin{aligned} \varphi : \mathbb{Z} &\to \mathbb{Z} \\ x &\mapsto 6x. \end{aligned}$$

Hãy tìm $\mathrm{Ker}\varphi$ và $\varphi^{-1}(12\mathbb{Z})$.

5.9. Trong nhóm cộng các số nguyên $\mathbb{Z}$, chứng minh rằng:
a) $m\mathbb{Z} \cap n\mathbb{Z} = b\mathbb{Z}$, trong đó b là bội chung nhỏ nhất của m và n.
b) $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$, trong đó d là ước chung lớn nhất của m và n.
c) $m\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$.

5.10. Tìm mọi đồng cấu từ $(\mathbb{Z}, +)$ đến $(\mathbb{Q}, +)$.

5.11. $(\mathbb{Z}, +)$ có đẳng cấu với $(\mathbb{Q}^*, \cdot)$ hay không, trong đó $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$. Hãy giải thích.

5.12. $(\mathbb{R}, +)$ có đẳng cấu với $(\mathbb{R}^+, \times)$ hay không, trong đó $\mathbb{R}^+$ là tập các số thực dương? Cho giải thích.

5.13. $\mathbb{C}^*$ là nhóm nhân các số phức khác không, H là tập hợp các số phức của $\mathbb{C}^*$ nằm trên trục thực hoặc 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 môđun bằng 1.

5.14. Chứng minh rằng nhóm thương $(\mathbb{R}/\mathbb{Z}, +)$ đẳng cấu với nhóm nhân U các số phức có môđun bằng 1.

5.15. Cho hai nhóm xyclic $A = \langle a \rangle, B = \langle b \rangle$ lần lượt sinh bởi các phần tử a, b có cấp tương ứng là m, n. Cho $f : A \to B$ là một đồng cấu.
a) Chứng minh rằng $f(A)$ là nhóm xyclic sinh bởi $f(a)$ và cấp của $f(a)$ là một ước chung của m và n.
b) Hãy chỉ ra các tự đồng cấu của nhóm $\mathbb{Z}_6$.

5.16. Chứng minh rằng đối với phần tử g của nhóm G, tương ứng $n \mapsto g^n$ là một đồng cấu nhóm từ $\mathbb{Z}$ tới G và là đồng cấu duy nhất $\mathbb{Z} \to G$ với $1 \mapsto g$.

5.17. Hãy tìm tất cả các đồng cấu từ:
a) Một nhóm xyclic cấp n đến chính nó;
b) Một nhóm xyclic cấp 6 đến một nhóm xyclic cấp 18;
c) Một nhóm xyclic cấp 18 đến một nhóm xyclic cấp 6.

5.18. Tìm tất cả các đồng cấu nhóm từ:

a) C_3 vào C_4.

b) $\mathbb{Z}$ vào $\mathbb{Z}_4$.

c) $\mathbb{Z}$ vào D_4.

5.19. Ký hiệu $\mathrm{Aut}(G)$ là nhóm tất cả các tự đẳng cấu của nhóm G. Chứng minh rằng:

a) $\mathrm{Aut}(\mathbb{Z}_6) \cong \mathbb{Z}_2$,

b) $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$,

c) $(\mathbb{Z}_7^*, \times) \cong (\mathbb{Z}_6, +)$.

5.20. Chứng minh rằng mọi nhóm xyclic vô hạn đều có đúng hai tự đẳng cấu.

5.21. Chứng minh nếu hợp thành của hai đồng cấu $g : G \to H$, $h : H \to K$ là một đẳng cấu thì

a) g là một đơn cấu,

b) h là một toàn cấu,

c) $H = (\mathrm{Im}g)(\mathrm{Ker}h) = (\mathrm{Ker}h)(\mathrm{Im}g)$ và $\mathrm{Im}g \cap \mathrm{Ker}h = e$.

5.22. Đối với toàn cấu $f : G \to H$ và nhóm con B của H, hãy chứng tỏ B chuẩn tắc trong H khi và chỉ khi $f^{-1}(B)$ là chuẩn tắc trong G và khi đó hãy chứng minh

$$G/f^{-1}(B) \cong H/B.$$

5.23. Chứng minh rằng nếu A là một nhóm con chuẩn tắc của nhóm G thì tồn tại một song ánh từ tập hợp các nhóm con chuẩn tắc của G chứa A lên tập hợp các nhóm con chuẩn tắc của G/A.

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

5.25. Cho G là nhóm xyclic cấp nguyên tố p. Chứng minh rằng mọi phần tử của X, khác đơn vị, đều là phần tử sinh của G và mọi ánh xạ

$$\begin{aligned} \varphi_k : G &\to G \\ x &\mapsto x^k \end{aligned}$$

đều là tự đẳng cấu của G, với k là số nguyên dương thoả mãn $0 < k < p$.

5.26. Cho X và Y là hai nhóm xyclic có các phần tử sinh theo thứ tự là x và y, với các cấp tương ứng là s và t.
a) Chứng minh quy tắc φ cho tương ứng mỗi phần tử $x^n \in X$ với phần tử $(y^k)^n \in Y$, trong đó k là một số tự nhiên khác 0 cho trước, là một đồng cấu khi và chỉ khi sk là bội của t.
b) Chứng minh nếu $sk = mt$ và φ là đơn cấu thì $(s, m) = 1$.

5.27. Cho X, Y là hai nhóm aben hữu hạn, $f : X \to Y$ là một đồng cấu nhóm, A là một nhóm con của X. Gọi $B = f(A)$ và $K = \mathrm{Ker} f \cap A$. Chứng minh rằng:
a) Tương ứng

$$\begin{aligned} X/A &\to f(X)/B \\ xA &\mapsto f(x)B \end{aligned}$$

là một toàn cấu nhóm.
b) $[X : A] = [f(x) : B][\mathrm{Ker} f : K]$.

5.28. Giả sử A là một nhóm con chuẩn tắc của nhóm G sao cho $G/A \cong \mathbb{Z}_5$ và $A \cong \mathbb{Z}_2$. Chứng minh rằng $G \cong \mathbb{Z}_{10}$.

5.29. Tìm tất cả các lớp đẳng cấu của các nhóm cấp 10.

5.30. Trên tập hợp $G = \mathbb{Z}^3$ ta xác định một phép toán hai ngôi như sau:

$$(k_1, k_2, k_3)(l_1, l_2, l_3) = (k_1 + (-1)^{k_3} l_1, k_2 + l_2, k_3 + l_3)$$

Chứng minh rằng:
a) G cùng với phép toán hai ngôi trên là một nhóm.
b) Nhóm con $A = \langle (t, 0, 0) \rangle$ là chuẩn tắc trong G.
c) $G/A \cong \mathbb{Z}[i]$.

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

5.32. Tìm nhóm các tự đẳng cấu của 4-nhóm Klein.

5.33. Tìm nhóm các tự đẳng cấu của nhóm S_5.

5.34. Cho A là một nhóm cộng aben. Ký hiệu $\mathrm{End}(A)$ là tập tất cả các tự đồng cấu của nhóm A. Chứng minh:

a) $\mathrm{End}(A)$ 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 cộng các số nguyên.

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

5.35. Cho m, n là hai số nguyên dương và d là ước chung lớn nhất của chúng. Chứng minh rằng tập hợp $\mathrm{Hom}(\mathbb{Z}_m, \mathbb{Z}_n)$ các đồng cấu nhóm từ $\mathbb{Z}_m$ đến $\mathbb{Z}_n$ là một nhóm với phép cộng các hàm và đẳng cấu với $\mathbb{Z}_d$.

5.36. Cho nhóm G. Với mỗi phần tử $a \in G$ ta xét ánh xạ

$$\begin{aligned} f_a : G &\to G \\ x &\mapsto axa^{-1} \end{aligned}$$

Chứng minh rằng:

a) f_a là một tự đẳng cấu của G, gọi là *tự đẳng cấu trong* xác định bởi phần tử a.

b) Tập hợp các tự đẳng cấu trong của G lập thành một nhóm con của nhóm các tự đẳng cấu của G. Chứng minh rằng nhóm con H của G là chuẩn tắc nếu và chỉ nếu $f_a(H) = H$ với mọi tự đẳng cấu trong f_a của G.

c) Nhóm các tự đẳng cấu trong của G đẳng cấu với nhóm thương $G/Z(G)$ với $Z(G)$ là tâm của nhóm G.

5.37. Cho các đồng cấu nhóm $f : K \to H, g : G \to K$, trong đó f là một toàn cấu. Chứng minh rằng các điều kiện sau đây là tương đương:

a) Tồn tại một đồng cấu $h : H \to K$ sao cho $g = h \circ f$;

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

Nếu một trong các điều kiện đó được thoả mãn thì:

c) h là duy nhất;

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

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

5.38. Tìm bốn nhóm con khác nhau của S_4 đẳng cấu với S_3.

5.39. Cho G là một nhóm aben hữu hạn và p là một số nguyên tố sao cho $g^p = e$ với mọi $g \in G$, chứng minh rằng G đẳng cấu với $\mathbb{Z}_p^n$ với số nguyên n nào đó.

5.40. Cho

$$G_p = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_p) \mid ad - bc = 1 \right\}.$$

Nếu p là một số nguyên tố, chứng minh rằng G_p là một nhóm có cấp $p(p^2 - 1)$ và tìm một nhóm dẳng cấu với G_2.

5.41. Cho G là nhóm sinh bởi các ma trận $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ và $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ với phép nhân ma trận. Chứng tỏ rằng G là nhóm không aben cấp 8. Nó có đẳng cấu với nhóm D_4 hay với nhóm quatecnion Q hay không?

5.42. Cho nhóm G, hãy tìm cặp (A, α), trong đó A là nhóm aben, $\alpha : G \to A$ là đồng cấu nhóm sao cho cặp (A, α) có tính chất: đối với mỗi cặp (H, h) trong đó H là nhóm aben, $h : G \to H$ là đồng cấu nhóm thì tồn tại duy nhất $f : A \to H$ sao cho $h = f\alpha$.

Chương III

CẤU TRÚC NHÓM

1. Tích trực tiếp

Nếu A và B là hai nhóm thì tích Đề-các

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

lập thành một nhóm cùng với phép toán hai ngôi cho bởi

$$(a, b)(x, y) = (ax, by).$$

Nhóm $A \times B$ được gọi là *tích trực tiếp* của A và B.

Định nghĩa tích trực tiếp được mở rộng một cách tự nhiên cho một họ $(G_i \mid i \in I)$ các nhóm, với tập chỉ số I tuỳ ý. Tích Đề-các $\prod_I G_i$ gồm tất cả các họ (a_i), với $a_i \in G_i, i \in I$, là một nhóm với phép toán nhân theo từng thành phần, nghĩa là

$$(a_i)(b_i) = (a_i b_i).$$

Ta gọi nhóm này là *tích trực tiếp* của họ các nhóm (G_i). Nhóm con của $\prod_I G_i$ gồm tất cả các họ (a_i), sao cho chỉ có một số hữu hạn a_i khác đơn vị, được gọi là *tích trực tiếp yếu* của họ G_i. Hiển nhiên rằng, tích trực tiếp yếu của họ G_i trùng với tích trực tiếp của chúng khi và chỉ khi tập chỉ số I hữu hạn. Trong trường hợp các nhóm G_i là aben ta thường nói *tổng trực tiếp* thay cho tích trực tiếp yếu.

Giả sử A, B là hai nhóm con chuẩn tắc của nhóm G. Ta nói rằng G *phân tích được thành tích trực tiếp* của A và B nếu $G = AB$ và

$A \cap B = e$. Khi đó ta cũng nói rằng các nhóm A, B là các *hạng tử trực tiếp* của nhóm G. *Nếu G phân tích được thành tích trực tiếp của hai nhóm con chuẩn tắc A, B thì mỗi phần tử của A đều giao hoán được với mỗi phần tử của B và mỗi phần tử của G viết được một cách duy nhất dưới dạng $ab, a \in A, b \in B$.*

Liên hệ giữa sự phân tích một nhóm thành tích trực tiếp với tích trực tiếp của hai nhóm ta có: *Nhóm G phân tích được thành tích trực tiếp của các nhóm con chuẩn tắc A và B nếu và chỉ nếu ánh xạ*

$$\begin{aligned} \varphi : A \times B &\to G \\ (a, b) &\mapsto ab \end{aligned}$$

là một đẳng cấu. Bởi vậy, khi G phân tích được thành tích trực tiếp của A và B ta cũng nói rằng G là tích trực tiếp của A và B và ký hiệu $A \times B$ mà không sợ có sự hiểu lầm nào. Sự phân biệt hai khái niệm này sẽ được hiểu trong từng tình huống cụ thể. Nếu G là một nhóm aben và phép toán trong nhóm G ký hiệu bởi $+$ thì ta ký hiệu $G = A \oplus B$ thay cho $A \times B$ và gọi G là *tổng trực tiếp* của A và B.

Nếu $f : A \to X, g : B \to Y$ là hai đồng cấu nhóm thì ánh xạ

$$\begin{aligned} A \times B &\to X \times Y \\ (a, b) &\mapsto (f(a), g(b)) \end{aligned}$$

cũng là một đồng cấu và được ký hiệu bởi $f \times g$.

Nếu A, B lần lượt là nhóm con chuẩn tắc của các nhóm X, Y thì tích trực tiếp $A \times B$ là nhóm con chuẩn tắc của tích trực tiếp $X \times Y$ và

$$(X \times Y)/(A \times B) \cong (X/A) \times (Y/B).$$

2. Nhóm đối xứng

Trước hết ta nhắc lại khái niệm *vòng xích*. Nếu $a_1, a_2, \ldots, a_m$, $1 \leq m \leq n$, là các phần tử phân biệt của tập hợp $\{1, 2, \ldots, n\}$ thì phép thế f cho bởi $f(a_1) = a_2, f(a_2) = a_3, \ldots, f(a_{m-1}) = a_m, f(a_m) = a_1$, và $f(x) = x$ nếu $x \notin \{a_1, a_2, \ldots, a_m\}$, được gọi là một vòng xích độ dài m, hay một m-xích. Ta ký hiệu vòng xích này bởi $(a_1\ a_2\ \ldots\ a_m)$.

Mỗi m-vòng xích trong nhóm S_n có cấp m. Vòng xích có độ dài 2, $f = (i\ j)$, được gọi là một *chuyển trí*. Hai vòng xích được gọi là *độc lập* nếu chúng không có phần tử chung.

Mỗi phép thế khác phép đồng nhất là tích của những vòng xích độc lập. Và mỗi phép thế đều có thể phân tích được thành tích những phép chuyển trí.

Trong mọi dạng phân tích một phép thế đã cho thành tích các chuyển trí thì tính chẵn lẻ của số các chuyển trí là không thay đổi. Một phép thế được gọi là *chẵn* nếu nó được phân tích thành tích của một số chẵn các chuyển trí và được gọi là *lẻ* trong trường hợp ngược lại. Tập hợp A_n tất cả các phép thế chẵn bậc n lập thành một nhóm con của nhóm đối xứng S_n. Nhóm con này được gọi là *nhóm thay phiên. Nhóm thay phiên A_n là nhóm con chỉ số 2 trong S_n và do đó là nhóm con chuẩn tắc của S_n.*

Định lý Cayley: *Mỗi nhóm G đều đẳng cấu với một nhóm con của nhóm đối xứng $S(G)$ của nó.*

3. Nhúng một nửa nhóm vào nhóm

Để có thể nhúng nửa nhóm S vào nhóm G thì S phải thoả mãn luật giản ước:

$$\text{Từ } ac = bc \text{ cũng như từ } ca = cb \text{ suy ra } a = b.$$

Điều kiện cần này cũng là điều kiện đủ trong trường hợp nửa nhóm giao hoán.

Giả sử A là nửa nhóm aben và S là nửa nhóm con của A gồm các phần tử chính quy theo nghĩa

$$ax = bx \Rightarrow a = b, \text{ với } x \in S; a, b \in A.$$

Khi đó có thể nhúng A vào vị nhóm aben G sao cho mọi phần tử của S đều có phần tử nghịch đảo trong G.

Mỗi nửa nhóm aben A với luật giản ước đều có thể nhúng vào một nhóm aben G. Khi đó mỗi phần tử của G viết được dưới dạng ab^{-1}, với a, b thuộc A.

4. Tác động của nhóm trên một tập hợp

Cho G là một nhóm với đơn vị e và X là một tập hợp nào đó. Nhóm $(G, \cdot)$ được gọi là *tác động* lên tập X nếu có một ánh xạ

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

sao cho với mọi $g, h \in G$ và mọi $x \in X$ ta có

$$\begin{aligned} (gh)x &= g(hx) \\ ex &= x \end{aligned}$$

Khi đó X được gọi là một $G-$tập.

Mỗi tác động của nhóm G lên tập X hoàn toàn được xác định khi và chỉ khi đã cho một đồng cấu nhóm

$$\varphi : G \to S(X)$$

trong đó $S(X)$ ký hiệu cho nhóm đối xứng của tập X.

Nhóm G được gọi là tác động *trung thành* lên tập X nếu đồng cấu nhóm $\varphi : G \to S(X)$ là một đơn cấu. Khi đó phần tử của G, giữ cố định mọi phần tử của X, chỉ là đơn vị e của G. Do φ đơn cấu nên G đẳng cấu với ảnh $\mathrm{Im}\varphi$, và vì vậy ta có thể đồng nhất G với $\mathrm{Im}\varphi$ và xem G như một nhóm con của $S(X)$.

Nếu G tác động lên tập X và $x \in X$ thì tập

$$G_x = \{g \in G \mid gx = x\}$$

là một nhóm con của G. Nhóm con G_x được gọi là *cái ổn định* của x. Nó là tập các phần tử của G, giữ nguyên x.

Tập tất cả các ảnh của một phần tử $x \in X$ dưới tác động của nhóm G được gọi là *quỹ đạo* của x theo G và được ký hiệu bởi

$$Gx = \{gx \mid g \in G\}.$$

Nhóm con gHg^{-1} được gọi là *liên hợp* với H bởi g. Mỗi quỹ đạo của H gồm tất cả các nhóm con của G liên hợp với H. Nhóm con ổn định đối với H là

$$G_H = \{g \in G \mid gHg^{-1} = H\}.$$

Nhóm con này được gọi là *cái chuẩn hoá* của H, và H là nhóm con chuẩn tắc của nhóm này.

Nếu X là một $G-$tập thì X được phân hoạch bởi các quỹ đạo $Gx, x \in X$, và với mọi $x \in X$ có một song ánh

$$p : G/G_x \to Gx.$$

Đặc biệt, nếu G là nhóm hữu hạn thì với mỗi phần tử $x \in X$, ta có

$$| G | = | G_x | \, | Gx | .$$

Bài tập

1. Tích trực tiếp

Trong các bài tập từ 1.1 đến 1.4, cặp nhóm nào là đẳng cấu? Vì sao?

1.1. $\mathbb{Z}_6$ và $\mathbb{Z}_2 \times \mathbb{Z}_3$.

1.2. C_{60} và $C_{10} \times C_6$.

1.3. D_n và $C_n \times C_2$.

1.4. $\mathbb{Z}_4 \times \mathbb{Z}_2$ và $\left\{ \pm 1, \pm i, \pm \dfrac{1+i}{\sqrt{2}}, \pm \dfrac{1-i}{\sqrt{2}} \right\}$.

1.5. Cho hai nhóm G và H. Chứng minh rằng nếu $G \times H$ là nhóm xyclic thì G và H là cũng là những nhóm xyclic.

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

1.7. Chứng minh rằng mọi nhóm cấp 4 hoặc đẳng cấu với $\mathbb{Z}_4$ hoặc đẳng cấu với $\mathbb{Z}_2 \times \mathbb{Z}_2$.

1.8. Có thể phân tích $\mathbb{Z}$ thành tổng trực tiếp của hai nhóm aben không?

1.9. Chứng minh rằng nếu $f : G \to H$ là một toàn cấu nhóm và nếu A là một nhóm con chuẩn tắc của G sao cho *cái thu hẹp* $k = f \mid_A$ là một đẳng cấu thì G phân tích được thành tích trực tiếp của A và hạt nhân $B = \mathrm{Ker} f$.

1.10. Cho B, C là hai nhóm aben. Chứng minh rằng nếu $\beta : B \to C$ và $\gamma : C \to B$ là những đồng cấu thoả mãn điều kiện $\beta \circ \gamma = id_C$ thì $B = \mathrm{Ker}\beta \oplus \mathrm{Im}\gamma$.

1.11. Với các nhóm G và H bất kỳ, chứng minh rằng:

$$(G \times H)/G' \cong H \quad \text{và} \quad (G \times H)/H' \cong G,$$

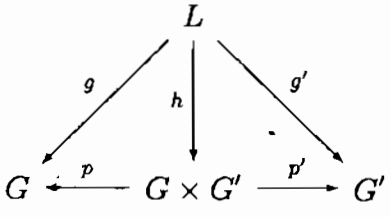
ở đó:

$$\begin{aligned} G' &= \{(g, e) \in G \times H \mid g \in G\} \\ H' &= \{(e, h) \in G \times H \mid h \in H\}. \end{aligned}$$

1.12. Cho X và Y là hai nhóm. Chứng minh rằng:
a) $X \times Y$ là một nhóm giao hoán khi và chỉ khi X và Y là những nhóm giao hoán.
b) Tâm của nhóm $X \times Y$ là $Z(X) \times Z(Y)$, với $Z(X), Z(Y)$ lần lượt là tâm của nhóm X và nhóm Y.

1.13. Cho ba nhóm X, Y, Z hai ánh xạ $f : X \to Y$, $g : X \to Z$. Ánh xạ $h : X \to Y \times Z$ được xác định bởi: $h(x) = (f(x), g(x))$. Chứng minh rằng:
a) h là một đồng cấu khi và chỉ khi f và g là những đồng cấu.
b) Nếu f hoặc g là một đơn cấu thì h cũng là một đơn cấu. Nếu h là một đơn cấu thì có suy ra được f, g là đơn cấu không?
c) Nếu h là một toàn cấu thì f và g là những toàn cấu. Nếu f và g là những toàn cấu thì h có là một toàn cấu không?

1.14. Chứng minh rằng đối với mỗi nhóm L và mỗi cặp đồng cấu nhóm $g : L \to G, g' : L \to G'$ đều tồn tại đồng cấu duy nhất $h : L \to G \times G'$ sao cho biểu đồ sau giao hoán



nghĩa là $g = p \circ h, g' = p' \circ h$, trong đó p, p' là các phép chiếu tự nhiên.

1.15. Giả sử G là nhóm nhân các ma trận vuông cấp 2 không kỳ dị trên trường số hữu tỷ. Chứng minh rằng $a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ có cấp 4 và $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ có cấp 3 nhưng ab có cấp vô hạn. Ngược lại, chứng tỏ rằng nhóm cộng $\mathbb{Z}_2 \oplus \mathbb{Z}$ chứa phần tử các phần tử khác không a, b có cấp vô hạn nhưng $a + b$ có cấp hữu hạn.

1.16. Cho một họ khác rỗng những nhóm $(X_i)_{i\in I}$ mà các phép toán ký hiệu bằng dấu nhân. Chứng minh rằng tập hợp tích Đề-các $X = \prod_{i\in I} X_i$ 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 trực tiếp* của các nhóm X_i).

1.17. Giả sử $(X_i)_{i\in I}$ là một họ khác rỗng các nhóm và $X = \prod_{i\in I} X_i$ là tích trực tiếp của họ $(X_i)_{i\in I}$. Các ánh xạ $p_i, i \in I$ cho bởi

$$\begin{aligned} p_i : X &\to X_i \\ x &\mapsto x_i. \end{aligned}$$

a) Chứng minh rằng p_i là toàn cấu với mọi $i \in I$.
b) Cho nhóm Y và cho họ đồng cấu $(f_i : Y \to X_i, i \in I)$. Chứng minh rằng tồn tại duy nhất đồng cấu $\overline{f} : Y \to X$ sao cho với mọi $i \in I$ ta có $f_i = p_i \circ \overline{f}$.

2. Nhóm đối xứng

2.1. Tìm cấp của mỗi phần tử của nhóm thay phiên A_4.

2.2. Nhóm con xyclic $\{(1), (123), (132)\}$ có là chuẩn tắc trong A_4 không?

2.3. Tìm nhóm con của nhóm A_4 đẳng cấu với 4-nhóm Klein.

2.4. Hai nhóm D_6 và A_4 có đẳng cấu không? Hãy giải thích.

2.5. Chứng minh rằng mọi nhóm cấp 6 hoặc đẳng cấu với nhóm $(\mathbb{Z}_6, +)$, hoặc đẳng cấu với nhóm S_3.

2.6. Chứng tỏ rằng $\mathbb{Z}_2 \times \mathbb{Z}_2$ có 6 tự đẳng cấu và $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$.

2.7. Chứng tỏ rằng tập hợp $\{f_1, f_2, \ldots, f_6\}$ các hàm từ $\mathbb{R} \setminus \{0, 1\}$ đến chính nó với phép toán hợp thành là đẳng cấu với S_3, trong đó

$$f_1(x) = x, \quad f_2(x) = 1 - x, \quad f_3(x) = \frac{1}{x},$$
$$f_4(x) = 1 - \frac{1}{x}, \quad f_5(x) = \frac{1}{1-x}, \quad f_6(x) = \frac{x}{x-1}.$$

2.8. Chứng minh rằng nhóm thay phiên A_4 không chứa nhóm con cấp 6 (*Bài tập này chứng tỏ rằng mệnh đề đảo của định lý Lagrange là không đúng*).

2.9. Cho π là r-vòng xích trong S_n, chứng minh rằng $\rho^{-1} \circ \pi \circ \rho$ cũng là một r-vòng xích đối với mỗi ρ thuộc S_n.

2.10. Tìm tất cả 10 nhóm con của A_4 và vẽ biểu đồ quan hệ theo quan hệ bao hàm.

2.11. Cho G là một nhóm con của S_n và G chứa một phép thế lẻ, chứng minh rằng G chứa một nhóm con chuẩn tắc có chỉ số 2.

2.12. Chứng minh rằng

$$K = \{(1), (12) \circ (34), (13) \circ (24), (14) \circ (23)\}$$

là một nhóm con của S_4 đẳng cấu với 4-nhóm Klein. Chứng minh rằng K là chuẩn tắc và $S_4/K \cong S_3$.

2.13. Cho K là nhóm được cho trong Bài tập 2.12, chứng minh rằng K là chuẩn tắc trong A_4 và $A_4/K \cong C_3$. Điều này chứng minh A_4 không phải là nhóm đơn.

2.14. Cho $f : S_n \to S_{n+1}$, ở đó $f(\pi)$ là phép thế trên $\{1, 2, ..., n+1\}$ xác định bởi $f(\pi)(i) = \pi(i)$ nếu $i \leq n$ và $f(\pi)(n+1) = n+1$. Hãy cho biết f có phải là một đồng cấu hay không? Tìm ảnh và hạt nhân của nó (nếu có).

2.15. Chứng tỏ rằng S_n sinh bởi các phần tử

$$(1\ 2), (2\ 3), \ldots, (n-1\ n).$$

2.16. Chứng tỏ rằng S_n sinh bởi các phần tử $(1\ 2\ 3 \ldots\ n)$ và $(1\ 2)$.

2.17. Chứng tỏ rằng nhóm S_n sinh bởi các phần tử $(1\ 2\ 3 \ldots\ n-1)$ và $(n-1\ \ n)$.

2.18. Chứng tỏ rằng A_n sinh bởi các các vòng xích độ dài 3.

2.19. Giả sử $\sigma = \sigma_1\sigma_2 \ldots \sigma_k$ là tích của những vòng xích độc lập trong nhóm đối xứng S_n. Chứng minh rằng cấp của σ là bội số chung nhỏ nhất của các cấp σ_i.

3. Nhúng nửa nhóm vào một nhóm

3.1. Mỗi một nửa nhóm aben A với luật giản ước đều có thể nhúng được vào một nhóm aben G, trong đó mỗi phần tử của G đều viết được dưới dạng ab^{-1}, với $a, b \in A$. Hãy xác định G trong các trường hợp sau đây:

a) $A = (\mathbb{N}, +)$;

b) $A = (\mathbb{N}, .)$;

c) $A = (\mathbb{Z}, .)$.

3.2. Cho M là vị nhóm giao hoán thoả mãn luật giản ước. Hãy chứng minh rằng tồn tại nhóm aben A và đồng cấu $k : M \to A$ của các vị nhóm với *tính chất phổ dụng* sau: *Với mỗi nhóm B và mỗi đồng cấu vị nhóm $f : M \to B$ tồn tại đồng cấu nhóm duy nhất $f' : A \to B$ sao cho $f = f' \circ k$.*

4. Tác động của một nhóm trên một tập

4.1. Cho nhóm G. Chứng minh rằng G là một $G-$tập với mỗi tác động sau:

a) $G \times G \to G, \quad (g, x) \mapsto gxg^{-1}$ (phép liên hợp).

b) $G \times G \to G, \quad (g, x) \mapsto gx$ (phép dời).

Hãy xác định các nhóm con ổn định G_x và các quỹ đạo Gx trong mỗi trường hợp trên.

4.2. Chứng minh rằng $(\mathbb{R}^*, \cdot)$ tác động lên $\mathbb{R}^{n+1}$ bởi phép nhân vô hướng. Quỹ đạo của các tác động này là gì?

4.3. Cho nhóm G và S là tập mọi nhóm con của G. Chứng minh rằng:

a) S là một $G-$tập với tác động

$$G \times S \to S, \quad (g, H) \mapsto gHg^{-1}.$$

b) Số các nhóm con liên hợp với nhóm con H bằng chỉ số của cái chuẩn hóa N_H trong G.

Với các Bài tập 4.4, 4.5, gọi

$$\mathbb{Z}_m^* = \{[x] \in \mathbb{Z}_m \mid \text{ƯCLN}(x, m) = 1\}.$$

Số các phần tử trong tập hợp này được ký hiệu là $\varphi(m)$ và được gọi là φ-hàm Euler. Ví dụ, $\varphi(4) = 2$ và $\varphi(8) = 4$.

4.4. Tìm các nhóm trong số C_7, C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_4, S_3 đẳng cấu với $(\mathbb{Z}_8^*, \cdot)$, $(\mathbb{Z}_9^*, \cdot)$, $(\mathbb{Z}_{10}^*, \cdot)$ và $(\mathbb{Z}_{15}^*, \cdot)$ và mô tả các đẳng cấu đó.

4.5. Chứng minh rằng nếu $\text{ƯCLN}(a, m) = 1$ thì $a^{\varphi(m)} \equiv 1 \bmod m$.
[Kết quả này được tìm ra bởi Leonhard Euler (1707 -1783).]

4.6. Chứng minh rằng nếu p là số nguyên tố thì với mọi số nguyên a ta có $a^p \equiv a \bmod p$.
[Kết quả này được tìm ra bởi Pierre Fermat (1601 - 1665).]

4.7. Cho S là một $G-$tập. Chứng minh rằng:

a) Nếu hai điểm $x, y \in S$ thuộc cùng một quỹ đạo thì các nhóm con ổn định của chúng liên hợp.

b) Nếu S là tập hữu hạn thì

$$S = \sum_{x \in I} [G : G_x]$$

trong đó I là tập các đại diện cho các quỹ đạo khác nhau, còn $[G : G_x]$ là chỉ số của nhóm con G_x trong G.

4.8. Cho G là nhóm hữu hạn cấp p^n, p là số nguyên tố, n là số nguyên dương. Hãy chứng minh tâm $Z(G) \neq e$. Từ đó suy ra rằng mọi nhóm hữu hạn cấp p^2 đều là nhóm aben.

4.9. Nếu G là một nhóm có cấp 35 tác động lên một tập hợp S có 13 phần tử, hãy chứng minh rằng G phải có một điểm cố định, nghĩa là một điểm $x \in S$ sao cho $gx = x$ với mọi $g \in G$.

4.10. Cho G là một nhóm có cấp p^r tác động lên một tập hợp có m phần tử, chứng minh rằng G có một điểm cố định nếu p không chia hết m.

4.11. Giả sử H và K là hai nhóm con của nhóm hữu hạn G. Đặt $HK = \{hk \mid h \in H, k \in K\}$. Chứng minh rằng

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Chương IV

VÀNH VÀ TRƯỜNG

1. Định nghĩa và ví dụ

Tập hợp R cùng với hai phép toán hai ngôi, được viết như phép cộng $(+)$ và phép nhân $(\times)$ thông thường, được gọi là một *vành* nếu các điều kiện sau được thoả mãn:

(i) $(R, +)$ là một nhóm aben,

(ii) $(R, \times)$ là một nửa nhóm,

(iii) Phép nhân phân phối về hai phía đối với phép cộng, nghĩa là:

$$\begin{aligned} a \times (b + c) &= a \times b + a \times c \\ (b + c) \times a &= b \times a + c \times a \end{aligned}$$

với mọi a, b, c thuộc R.

Vành R được gọi là *giao hoán* nếu phép nhân trong R có tính chất giao hoán: $a \times b = b \times a$, với mọi a, $b \in R$. Vành R được gọi là *có đơn vị* nếu phép nhân có đơn vị. Phần tử trung hoà của phép cộng được gọi là *phần tử không* của vành R và ký hiệu bởi 0. Nếu R là vành có đơn vị thì phần tử đơn vị được ký hiệu bởi e hoặc 1.

Mỗi vành R đều có tất cả các tính chất của một nhóm cộng giao hoán và thoả mãn một số tính chất cơ bản sau:

1) *Với mọi* $a \in R$, $0 \times a = a \times 0 = 0$.

2) *Nếu vành* R *có đơn vị* 1 *và có nhiều hơn một phần tử thì* $1 \neq 0$.

3) *Với mọi* a, b, c *thuộc* R *ta có:*

$$\begin{aligned} a(b - c) &= ab - ac \\ (b - c)a &= ba - ca. \end{aligned}$$

4) *Trong R có luật phân phối suy rộng, nghĩa là với mọi phần tử $a, b_1, b_2, ..., b_n$ $(n \geq 2)$ thuộc R ta có:*

$$a \sum_{i=1}^{n} b_i = \sum_{i=1}^{n} ab_i,$$

$$\left(\sum_{i=1}^{n} b_i \right) a = \sum_{i=1}^{n} b_i a.$$

5) *Quy tắc về dấu: Với mọi a, b thuộc R*

$$a(-b) = (-a)b = -ab; \quad (-a)(-b) = ab.$$

6) *Đối với mọi số nguyên n và mọi phần tử a, b thuộc vành R:*

$$n(ab) = (na)b = a(nb).$$

Phần tử $a \neq 0$ thuộc vành R được gọi là một *ước bên trái* (tương ứng *bên phải*) của *không* nếu tồn tại $b \in R, b \neq 0$, sao cho $ab = 0$ (tương ứng $ba = 0$). Nếu a vừa là ước bên trái, vừa là ước bên phải của không thì a được gọi là *ước của không.*

Hai tính chất sau là tương đương trong một vành giao hoán, có đơn vị $1 \neq 0$:

(i) *R không có ước của không.*

(ii) *Phép nhân trong R có luật giản ước cho những phần tử khác không.*

Vành R được gọi là một *miền nguyên* nếu nó là vành giao hoán, có đơn vị $1 \neq 0$ và không có ước của không. Vành F được gọi là một *trường* nếu F là một vành giao hoán, có đơn vị $1 \neq 0$ và mọi phần tử khác 0 của nó đều khả nghịch (theo nghĩa có nghịch đảo đối với phép nhân). *Một cách tương đương*, tập hợp F cùng với hai phép toán ký hiệu bởi $+, \times$ là một trường nếu:

(i) $(F, +)$ là một nhóm giao hoán với phần tử trung hoà 0,

(ii) $(F^*, \times)$ là một nhóm giao hoán, trong đó $F^* = F \setminus \{0\}$,

(iii) Phép nhân phân phối với phép cộng.

Mỗi trường đều là một miền nguyên, và ngược lại mỗi miền nguyên hữu hạn là một trường. Nói riêng, vành $\mathbb{Z}_n$ là trường khi và chỉ khi n là một số nguyên tố.

Cho A là một tập con ổn định đối với phép cộng và phép nhân của vành R. Nếu A cùng với các phép toán cảm sinh là một vành (tương ứng, là một trường) thì A được gọi là một *vành con* (tương ứng, là một *trường con*) của vành (trường) R. *Tập con A của vành R là một vành con của R khi và chỉ khi thoả mãn các điều kiện:*

(i) $0 \in A$,

(ii) $\forall a, b \in A \Rightarrow a - b \in A$ và $ab \in A$.

Tập con A của trường F là trường con của F khi và chỉ khi thoả mãn các điều kiện:

(i) $0 \in A, 1 \in A$,

(ii) $\forall a, b \in A \Rightarrow a - b \in A$,

(iii) $\forall a, b \in A, b \neq 0 \Rightarrow ab^{-1} \in A$.

Trong định nghĩa của chúng ta một vành không nhất thiết phải có đơn vị. Tuy nhiên, nếu A là một vành con của miền nguyên R, và có đơn vị thì đơn vị đó trùng với đơn vị của R.

2. Iđêan, vành thương

Vành con J của vành R được gọi là *iđêan trái* (tương ứng, *phải*) của R nếu $xa \in J$ (tương ứng, $ax \in J$) với mọi $a \in J, x \in R$. Nếu J vừa là iđêan trái vừa là iđêan phải của vành R thì J được gọi là *iđêan* của R. Đối với tập con J khác rỗng của vành R các điều sau là tương đương:

(i) *J là iđêan của R.*

(ii) *Nếu $a, b \in J$ và $x \in R$ thì $a - b \in J$ và $ax, xa \in J$.*

Nếu I là iđêan của vành R, chứa đơn vị, thì I trùng với vành R.

Cho M là một tập con của vành R. Giao của họ tất cả các iđêan của R chứa M là một iđêan bé nhất của R, chứa M. Iđêan này được gọi là iđêan *sinh bởi* M, ký hiệu (M).

Nếu M là một tập hữu hạn thì iđêan sinh bởi M được gọi là *iđêan hữu hạn sinh*. Nếu $M = \{a\}$ thì iđêan sinh bởi M được gọi là *iđêan chính* sinh bởi phần tử a và ký hiệu đơn giản là (a). Đặc biệt khi $M = \emptyset$ thì iđêan sinh bởi tập rỗng là 0.

Nếu R là một vành giao hoán có đơn vị và $a_1, a_2, ..., a_n$ là n phần tử thuộc R thì iđêan sinh bởi tập hợp $\{a_1, a_2, ..., a_n\}$ là

$$A = \{x_1a_1 + x_2a_2 + ... + x_na_n | x_i \in R\}$$

Một trường có thể được đặc trưng bởi các iđêan của nó: *Một vành giao hoán không tầm thường R là một trường nếu và chỉ nếu 0 và R là tất cả các iđêan của nó.*

Cho I và J là hai iđêan của vành R. Khi đó

$$I + J = \{a + b \mid a \in I, b \in J\},$$
$$IJ = \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_i \in J, n \geq 1 \right\}$$

là những iđêan của R, và được gọi tương ứng là *tổng, tích* của hai iđêan I, J.

Rõ ràng đối với hai iđêan I, J ta luôn có $IJ \subset I \cap J$. Trong vành các số nguyên $\mathbb{Z}$ tổng $m\mathbb{Z} + n\mathbb{Z}$ là iđêan chính $d\mathbb{Z}$, với d là ước chung lớn nhất của m và n. Giao $m\mathbb{Z} \cap n\mathbb{Z}$ là iđêan chính $b\mathbb{Z}$, với b là bội chung nhỏ nhất của m và n. Hơn nữa, ta còn có $(m\mathbb{Z})(n\mathbb{Z}) = mn\mathbb{Z}$, và do đó

$$m\mathbb{Z} \cap n\mathbb{Z} = (m\mathbb{Z})(n\mathbb{Z})$$

khi và chỉ khi m, n nguyên tố cùng nhau.

Nếu J là một iđêan của vành R thì tương ứng

$$\begin{aligned} (R/J) \times (R/J) &\to R/J \\ (x + J, y + J) &\mapsto xy + J \end{aligned}$$

là một ánh xạ. Hơn nữa, nhóm thương R/J trở thành một vành với phép nhân

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

Vành R/J được gọi là *vành thương* của vành R theo iđêan J.

Hai phép toán trong vành thương R/J thường được ký hiệu bởi

$$\overline{x} + \overline{y} = \overline{x + y}, \quad \overline{x}.\overline{y} = \overline{xy}.$$

Nếu R là vành giao hoán thì vành thương R/J cũng là vành giao hoán. Nếu vành R có đơn vị e thì R/J là vành có đơn vị $\overline{e} = e + J$.

Cho R là vành giao hoán, có đơn vị 1. Iđêan P của R được gọi là *iđêan nguyên tố* nếu $P \neq R$ và từ $ab \in P$ suy ra $a \in P$ hoặc $b \in P$ với mọi $a, b \in R$. Iđêan M được gọi là *iđêan tối đại* của R nếu $M \neq R$ và nếu với bất kỳ iđêan B của R sao cho $M \subset B \subset R$ thì $B = R$ hoặc $B = M$. Khi đó:

(i) *J là iđêan nguyên tố trong vành R khi và chỉ khi vành thương R/J là một miền nguyên;*

(ii) *J là một iđêan tối đại trong vành R khi và chỉ khi vành thương R/J là một trường.*

Mệnh đề trên cho thấy mọi iđêan tối đại đều là iđêan nguyên tố. Điều ngược lại nói chung không đúng. Tuy nhiên, *trong vành số nguyên $\mathbb{Z}$ mọi iđêan nguyên tố khác không đều là tối đại.*

3. Đồng cấu vành

Cho hai vành R và S. Ánh xạ $f : R \to S$ được gọi là một *đồng cấu* từ vành R đến vành S nếu:

$$\begin{aligned} f(a+b) &= f(a) + f(b) \\ f(ab) &= f(a)f(b) \end{aligned}$$

với mọi $a, b \in R$. Trong trường hợp $R = S$ đồng cấu f được gọi là một *tự đồng cấu* của R. Nếu f là một đơn ánh (tương ứng toàn ánh, song ánh) thì đồng cấu f được gọi là một *đơn cấu* (tương ứng *toàn cấu, đẳng cấu*). Nếu có một ánh xạ đẳng cấu từ vành R đến vành S thì ta nói rằng R và S *đẳng cấu* với nhau và ký hiệu $R \cong S$.

Cho $f : R \to S$ là một đồng cấu từ vành R đến vành S. Khi đó:

1) $f(0) = 0$, $f(-a) = -f(a)$, $\quad \forall a \in R$.

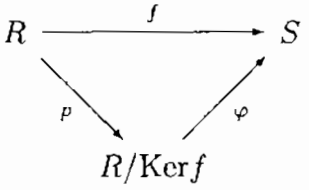
Tuy nhiên cần lưu ý rằng nếu R và S là những vành có đơn vị thì không nhất thiết xảy ra $f(1) = 1$.

2) Nếu A là một vành con của R thì $f(A)$ là một vành con của S. Đặc biệt, $\mathrm{Im}f$ là vành con của S.

3) Nếu I là một iđêan của S thì $f^{-1}(I)$ là một iđêan của R. Đặc biệt, $\mathrm{Ker}f$ là iđêan của R.

4) Vành con J là một iđêan của vành R khi và chỉ khi I là hạt nhân của đồng cấu vành $f : R \to S$ nào đó.

Định lý đồng cấu: *Cho f là một đồng cấu vành từ R đến vành S. Khi đó tồn tại duy nhất đồng cấu vành $\varphi : R/\mathrm{Ker}f \to S$ sao cho tam giác sau là giao hoán*



và $\mathrm{Im}\varphi = \mathrm{Im}f$, *trong đó* $p : R \to R/\mathrm{Ker}f$ *là phép chiếu tự nhiên. Hơn nữa* φ *là đơn cấu. Nói riêng, vành thương* $R/\mathrm{Ker}f$ *đẳng cấu với* $\mathrm{Im}f$.

Nếu I và J là hai iđêan của vành R thì

$$(I + J)/J \cong I/(I \cap J).$$

Đối với hai vành $(R, +, \times)$ và $(S, +, \times)$, tổng trực tiếp của hai nhóm aben $(R, +)$ và $(S, +)$ là một vành với phép nhân cho bởi

$$(a, x)(b, y) = (ab, xy).$$

Vành này được gọi là *tích trực tiếp* của hai vành R và S, và ký hiệu bởi $R \times S$.

Một cách tổng quát ta cũng có thể định nghĩa tích trực tiếp $\prod_I R_i$ của một họ những vành $(R_i | \ i \in I)$. Mỗi phần tử của tích trực tiếp là một họ (a_i), với $a_i \in R_i, i \in I$. Hai phép toán cộng và nhân được xác định bởi phép cộng và phép nhân theo từng thành phần, nghĩa là

$$\begin{aligned} (a_i) + (b_i) &= (a_i + b_i) \\ (a_i)(b_i) &= (a_i b_i) \end{aligned}$$

Vành con của tích trực tiếp $\prod_I R_i$ gồm tất cả các họ (a_i), sao cho chỉ có một số hữu hạn thành phần $a_i \neq 0$, được gọi là *tổng trực tiếp* của các vành R_i, và ký hiệu bởi $\bigoplus_I R_i$.

Tổng trực tiếp $\bigoplus_I R_i$ trùng với tích trực tiếp $\prod_I R_i$ khi và chỉ khi I là tập hữu hạn. Do vậy,

$$R_1 \times R_2 \times \ldots \times R_n = R_1 \oplus R_2 \oplus \ldots \oplus R_n$$

Trong trường hợp các vành R_i đều là vành có đơn vị thì tích trực tiếp $\prod_I R_i$ có đơn vị là (e_i), với e_i là đơn vị của vành R_i.

Các vành $\mathbb{Z}_{mn}$ và $\mathbb{Z}_m \times \mathbb{Z}_n$ đẳng cấu khi và chỉ khi m, n là hai số nguyên tố cùng nhau.

Bây giờ chúng ta nêu một ứng dụng của dạng biểu diễn của một vành nào đó thành tích trực tiếp của các vành. Cho $m = m_1 m_2 ... m_r$, với m_i là các số đôi một nguyên tố cùng nhau. Chúng ta biết rằng có một đẳng cấu vành

$$\mathbb{Z}_m \cong \prod_I \mathbb{Z}_{m_i}$$

Qua đẳng cấu này mỗi x trong $\mathbb{Z}_m$ được biểu diễn duy nhất dưới dạng một bộ r số $(a_1, a_2, ..., a_r)$, trong đó $x \equiv a_i \bmod m_i$. Khi đó ta nói rằng $(a_1, a_2, ..., a_r)$ là một *biểu diễn thặng dư* của x.

4. Trường các thương

Trong mục này vành R được giả thiết là một miền nguyên. Nếu miền nguyên R chứa trong một trường F nào đó thì giao Q của tất cả các trường con của F, chứa R, là trường con bé nhất của F chứa R. *Trường Q gồm tất cả các phần tử có dạng ab^{-1}, với $a, b \in R, b \neq 0$.*

Đối với mỗi miền nguyên R có thể xây dựng một trường tối tiểu Q chứa R như một vành con. Xét tập hợp

$$R \times R^* = \{(a, b) | a, b \in R, b \neq 0\}$$

gồm các cặp phần tử của R có thành phần thứ hai khác không, và xác định trên đó quan hệ hai ngôi cho bởi

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Để cho gọn ta sẽ ký hiệu lớp tương đương $\overline{(a, b)}$ chứa cặp (a, b) của $R \times R^*$ là $\frac{a}{b}$ và ký hiệu tập thương gồm các lớp tương đương đó là Q. Tập thương Q trở thành một trường với hai phép toán cho bởi

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

Hơn nữa Q chứa R như một vành con. Ta gọi Q là *trường các thương* của miền nguyên R. Mỗi phần tử của trường các thương Q viết được dưới dạng ab^{-1}, với $a, b \in R, b \neq 0$. Nói riêng, *trường số hữu tỷ* $\mathbb{Q}$ *là trường các thương của vành các số nguyên* $\mathbb{Z}$.

Rõ ràng, *trường các thương của miền nguyên* R *là trường tối tiểu chứa* R.

Vành R giao hoán, có đơn vị e, được gọi là vành *có đặc số* 0 (tương ứng, *đặc số* $n, 0 < n < \infty$) nếu trong nhóm cộng R, phần tử e có cấp vô hạn (tương ứng, có cấp n). Trong vành R có đặc số $n \neq 0$ thì $nx = 0$ với mọi $x \in R$, và nếu miền nguyên có đặc số $n \neq 0$ thì n là số nguyên tố.

Khái niệm đặc số cho ta một mô tả về cấu trúc của trường thông qua hai trường quen thuộc $\mathbb{Z}_p$ và $\mathbb{Q}$.

Nếu trường F *có đặc số* 0 *thì* F *chứa trường con đẳng cấu với trường số hữu tỷ* $\mathbb{Q}$, *còn nếu* F *có đặc số* $p \neq 0$ *thì nó chứa trường con đẳng cấu với trường* $\mathbb{Z}_p$ *các lớp thặng dư theo môđun* p.

5. Vành và trường sắp thứ tự

Trong mục này vành R đã cho được giả thiết là vành giao hoán và có đơn vị 1.

Cho R là một vành giao hoán có đơn vị 1. Nếu trong R có một quan hệ thứ tự toàn phần $\leq$ thoả mãn các điều kiện sau với mọi $a, b, c \in R$:

(i) $a \leq b$ kéo theo $a + b \leq b + c$,
(ii) $0 < a$ và $0 < b$ kéo theo $0 < ab$,

thì R được gọi là một *vành sắp thứ tự*. Một trường được gọi là *sắp thứ tự* nếu nó là một vành sắp thứ tự. Phần tử a thuộc vành sắp thứ tự R được gọi là *phần tử dương* nếu $0 < a$ và gọi là *phần tử âm* nếu $a < 0$.

Điều kiện đủ để một vành là sắp thứ tự: *Nếu trong vành* R *có một tập con* P *thoả mãn các điều kiện:*

(i) $a, b \in P$ *kéo theo* $a + b \in P$,
(ii) $a, b \in P$ *kéo theo* $ab \in P$,
(iii) $P \cap (-P) = \emptyset$, $P \cup \{0\} \cup (-P) = R$

thì trong R có một quan hệ thứ tự để R trở thành một vành sắp thứ tự.

Trong vành sắp thứ tự $(R, \leq)$ ta có:

(i) $x^2 \geq 0$ *với mọi* $x \in R$ *và* $1 > 0$.

(ii) R *là vành có đặc số* 0.

Từ diều (ii) suy ra rằng mọi trường sắp thứ tự đều chứa một trường con đẳng cấu với trường số hữu tỷ $\mathbb{Q}$. Từ diều (i) suy ra rằng không có một quan hệ thứ tự nào trong tập các số phức $\mathbb{C}$ để trường này trở thành một trường sắp thứ tự, vì $i^2 = -1 < 0$.

Nếu R là một miền nguyên sắp thứ tự thì trong trường các thương của Q có duy nhất một tập các phần tử dương P sao cho Q là một trường sắp thứ tự và $P \cap R$ là tập các phần tử dương của R.

Vành R được gọi là một *vành sắp thứ tự Acsimet* nếu $(R, \leq)$ là một vành sắp thứ tự và với mọi a, b thuộc R, $0 < a$, tồn tại số tự nhiên n sao cho $b < na$. Trường F được gọi là *trường sắp thứ tự Acsimet* nếu $(F, \leq)$ là một vành sắp thứ tự Acsimet.

Ta có nhận xét rằng, nếu R là một trường sắp thứ tự thì nó có đặc số 0 và vì vậy có thể nhúng trường số hữu tỷ $\mathbb{Q}$ vào R như một trường con. Với nhận xét này ta có thể phát biểu tính chất sau: *Mọi trường sắp thứ tự Acsimet F đều trù mật hữu tỷ theo nghĩa với mọi a, b thuộc F, $a < b$, đều tồn tại số hữu tỷ q sao cho $a < q < b$.*

Bài tập

1. Định nghĩa và ví dụ

1.1. Hãy lập các bảng cộng và bảng nhân của mỗi vành $\mathbb{Z}_4, \mathbb{Z}_3$.

Trong các bài tập từ 1.2 đến 1.6 hãy cho biết những tập hợp nào là vành với phép cộng và phép nhân. Nói rõ vì sao?

1.2. Mọi số hữu tỷ với mẫu số là số lẻ.

1.3. $\{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$.

1.4. $\{a + b\sqrt{2} + c\sqrt{3} \mid a, b, c \in \mathbb{Z}\}$.

1.5. $\{a + b\sqrt[3]{2} \mid a.b \in \mathbb{Q}\}$.

1.6. Mọi ma trận thực cỡ 2×2 với định thức bằng không.

1.7. Hệ đại số $(\mathbb{Z}, +, \times)$ có phải là vành không, trong đó phép cộng là thông thường, còn phép nhân được cho bởi $a \times b = 0$ với mọi $a, b \in \mathbb{Z}$.

1.8. Chứng minh rằng trong định nghĩa của vành có đơn vị, tiên đề về tính giao hoán của phép toán cộng có thể suy ra được từ các tiên đề còn lại.

1.9. Cho R là một vành. Đặt:

$$I = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a, b, c \in R \right\}$$

Chứng minh rằng I là vành con của vành $M_2(R)$.

1.10. Xác định các vành con của vành các số nguyên $\mathbb{Z}$.

Những vành nào trong các bài tập từ 1.11 đến 1.13 là miền nguyên? là trường?

1.11. $\mathbb{Z}_2 \times \mathbb{Z}_2$.

1.12. $\{a + bi \mid a, b \in \mathbb{Q}\}$.

1.13. $\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$.

1.14. Tìm các ước của không trong vành $\mathbb{Z}_{10}$.

1.15. Giả sử vành R có nhóm cộng $(R, +)$ là xyclic. Chứng minh rằng R là vành giao hoán.

1.16. Chứng minh rằng vành R là giao hoán nếu

$$x^2 - x \in Z(R), \ \forall x \in R,$$

trong đó $Z(R)$ là tập tất cả các phần tử giao hoán được với mọi phần tử của R.

1.17. Chứng minh rằng bộ phận

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

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

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

1.19. Cho hai phần tử $a, b \in R$. Chứng minh rằng $1 - ab$ là khả nghịch khi và chỉ khi $1 - ba$ là khả nghịch. Trong trường hợp đó hãy tìm $(1 - ba)^{-1}$.

1.20. Phần tử a của vành R được gọi là *luỹ linh* nếu tồn tại số nguyên dương n sao cho $a^n = 0$. Chứng minh rằng nếu a là một phần tử luỹ linh của vành R thì $1 \pm a$ là khả nghịch.

1.21. a) Cho R là một vành. Tập con

$$C(R) = \{a \in R \mid ax = xa,\ \forall x \in R\},$$

được gọi là *tâm* của R. Chứng minh rằng tâm của R là một vành con giao hoán của R.

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

1.22. Cho n là một số nguyên dương. Chứng minh rằng các khẳng định sau là tương đương:

a) n là một số nguyên tố.

b) $\mathbb{Z}_n$ là một trường.

c) $\mathbb{Z}_n$ là một miền nguyên.

1.23. Vành R được gọi là một vành *Boole* nếu $x^2 = x$ với mọi $x \in R$. Chứng minh rằng:

a) $x = -x$ với mọi $x \in R$;

b) R là vành giao hoán;

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

2. Iđêan

2.1. Tìm tất cả các iđêan trong vành số nguyên $\mathbb{Z}$.

2.2. Tìm tất cả các iđêan trong trường các số hữu tỷ $\mathbb{Q}$.

2.3. Giả sử $\{A_i\}_{i \in I}$ là một họ những iđêan của vành R sao cho với mọi $i, j \in I$, tồn tại $k \in I$ sao cho $A_i \subset A_k$, $A_j \subset A_k$. Chứng minh rằng $A = \bigcup\limits_{i \in I} A_i$ là một iđêan của R.

2.4. Cho vành R và $a \in R$. Chứng minh rằng các bộ phận

$$aR = \{ax \mid x \in R\}$$
$$Ra = \{xa \mid x \in R\}$$

lần lượt là idêan phải, idêan trái của R.

2.5. Cho R là một vành tuỳ ý, n là số nguyên cho trước. Chứng minh bộ phận sau là một idêan của R

$$A = \{x \in R \mid nx = 0\}.$$

2.6. 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.

2.7. Cho R là vành giao hoán có đơn vị là 1, I và J là hai idêan của R. Chứng minh nếu $I + J = R$ thì $IJ = I \cap J$.

2.8. Giả sử R là một miền nguyên với phần tử đơn vị e và n là cấp của e trong nhóm cộng R. Chứng minh:

a) n là một số nguyên tố.

b) Mọi phần tử khác không $x \in R$ có cấp n.

c) Bộ phận $mR = \{mx \mid x \in R\}$ với m là số nguyên cho trước là một idêan của R.

d) $R/mR \cong R$ nếu m là bội của n;
$R/mR \cong \{0\}$ nếu m không là bội của n.

2.10. Cho R là vành giao hoán có đơn vị $1 \neq 0$. Chứng minh rằng nếu mọi idêan thực sự của R đều là idêan nguyên tố thì R là một trường.

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

2.12. Cho R là một vành giao hoán có đơn vị là 1. Chứng minh rằng nếu $a \in R$ là phần tử không khả nghịch thì tồn tại idêan tối đại của R chứa a.

2.13. Giả sử I là một idêan thực sự của $\mathbb{Z}$. Chứng minh rằng I là một idêan tối đại của $\mathbb{Z}$ khi và chỉ khi $I = p\mathbb{Z}$ với p là một số nguyên tố.

2.14. Giả sử R là một vành giao hoán có đơn vị và mỗi phần tử $x \in R$ đều tồn tại số tự nhiên $n > 1$ (n phụ thuộc vào x) sao cho $x^n = x$. Chứng minh rằng mọi iđêan nguyên tố trong R đều là iđêan tối đại.

2.15. Cho R, S là hai vành. Trên tích $R \times S$ ta định nghĩa phép nhân và phép cộng như sau:

$$\begin{aligned}(x,y)(a,b) &= (xa, yb)\\ (x,y)+(a,b) &= (x+a, y+b).\end{aligned}$$

Chứng minh rằng $R \times S$ là một vành và X là một iđêan của $R \times S$ khi và chỉ khi $X = A \times B$ với A là một iđêan của R, B là một iđêan của S.

2.16. Cho R là một vành giao hoán, có đơn vị. Một phần tử $a \in R$ được gọi là *lũy linh* nếu $a^n = 0$ với $n \geq 0$ nào đó trong $\mathbb{Z}$. Tập $N(R)$ tất cả các phần tử lũy linh trong R được gọi là *căn* của R. Chứng minh rằng:

a) $N(R)$ là một iđêan của R.

b) $N[R/N(R)] = 0$.

c) $N(R)$ bằng giao của tất cả các iđêan nguyên tố của R.

2.17. Một vành giao hoán R được gọi là một vành *địa phương* nếu tồn tại một iđêan thực sự lớn nhất P (theo nghĩa với mọi iđêan thực sự $I \subset R$ ta có $I \subset P$). Chứng minh rằng các mệnh đề sau là tương đương:

a) R là một vành địa phương.

b) Tập các phần tử không khả nghịch của R là một iđêan.

c) Tồn tại một iđêan tối đại Q sao cho $1 + a$ khả nghịch với mọi $a \in Q$.

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

a) R chỉ có một iđêan tối đại duy nhất.

b) Tập các phần tử không khả nghịch của R lập thành một iđêan của R.

2.19. Cho vành địa phương R với $J(R)$ là iđêan gồm tất cả các phần tử không khả nghịch của R.

a) Chứng minh rằng mọi vành $\mathbb{Z}_{p^n}$ với mỗi số nguyên tố p và

$n \geq 1$, là địa phương, nhưng $\mathbb{Z}_6$ thì không là địa phương.

b) Chứng minh rằng $\mathbb{Z}_{(p)} = \left\{ \frac{r}{s} \in \mathbb{Q} \mid p \text{ không chia hết } s \right\}$ là một vành con địa phương của $\mathbb{Q}$ với mỗi số nguyên tố p.

c) Nếu R là địa phương, chứng minh rằng $R/J(R)$ là một trường.

d) Chứng minh rằng R là vành địa phương nếu $R/N(R)$ là một trường.

2.20. Nếu F là trường, chứng minh rằng $R = M_2(F)$ có đúng hai idêan là 0 và R (Bởi vì điều này, R được gọi là *vành đơn*).

3. Đồng cấu vành

3.1. Chứng minh rằng phương trình $x^3 - 5x^2 - x - 17 = 0$ không có nghiệm trong $\mathbb{Z}$.

3.2. Cho f là một đồng cấu từ vành R đến vành S (R và S là những vành giao hoán có đơn vị).

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

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

3.3. 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:

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

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

Chứng minh rằng B là một vành, hơn nữa B đẳng cấu với A.

3.4. Vành R được gọi là một vành *Bool* nếu $a^2 = a$ với mọi $a \in R$. Chứng minh rằng mỗi idêan nguyên tố P của vành Bool R là một idêan tối đại và $R/P \cong \mathbb{Z}_2$.

3.5. Chứng minh rằng

$$S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{R} \right\}$$

là vành con của vành $M_2(\mathbb{R})$, đẳng cấu với $\mathbb{C}$. Hãy tính

$$M = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}^{2008}.$$

3.6. Cho S là một vành. Đặt

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in S \right\},$$

$$A = \left\{ \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \mid a \in S \right\}$$

Chứng minh rằng A là một iđêan của R và $R/A \cong S \times S$.

3.7. Giả sử $f : R \to R$ là một tự đồng cấu của vành R. Chứng minh rằng tập hợp

$$A = \{x \in R \mid f(x) = x\}$$

là một vành con của R.

3.8. Cho m và n là hai số nguyên, m chia hết n. Tìm iđêan A của $\mathbb{Z}_n$ sao cho $\mathbb{Z}_n/A \cong \mathbb{Z}_m$.

3.9. Chứng minh rằng mọi iđêan tối đại trong vành $\mathbb{Z}_n$ đều có dạng $p\mathbb{Z}_n$, trong đó p là một ước nguyên tố của n.

3.10. Chứng minh rằng có duy nhất một đồng cấu vành từ vành các số hữu tỷ $\mathbb{Q}$ đến vành các số nguyên $\mathbb{Z}$.

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

3.12. Tìm tất cả các tự đồng cấu của vành $\mathbb{Z}[\sqrt{2}]$.

3.13. Tìm mọi tự đồng cấu của vành

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

3.14. Tìm mọi tự đồng cấu của vành

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

3.15. Tìm mọi đồng cấu từ vành từ $\mathbb{Z}$ đến $\mathbb{Z}_{10}$.

3.16. Tìm mọi đồng cấu từ $\mathbb{Z}_{15}$ đến $\mathbb{Z}_3$.

3.17. Tìm mọi tự đồng cấu của vành $\mathbb{Z} \times \mathbb{Z}$.

3.18. Tìm mọi đồng cấu từ $\mathbb{Z}_7$ đến $\mathbb{Z}_4$.

3.19. Hãy xác định vành các tự đồng cấu $End(\mathbb{Z}_2 \times \mathbb{Z}_2)$. Nó có là vành giao hoán không?

3.20. Trên vành $(R, +, .)$ xác định hai phép toán cho bởi

$$\begin{aligned} r \oplus s &= r + s + 1 \\ r \circ s &= r.s + r + s. \end{aligned}$$

Chứng tỏ rằng $(R, \oplus, \circ)$ là một vành đẳng cấu với vành $(R, +, .)$.

3.21. Cho R là một vành có đơn vị và không có ước của không. Giả sử $S = R \oplus \mathbb{Z}$ là tổng trực tiếp của hai nhóm cộng. Trên S cho phép nhân:

$$(r, k)(r', k') = (rr' + k'r + kr', kk').$$

Chứng minh rằng:
a) S là một vành.
b) Tập $A = \{(r, n) \in S \mid rx + nx = 0 \ \forall x \in R\}$ là một idêan trong S.
c) S/A có đơn vị và chứa vành con đẳng cấu với R.
d) S/A không có ước của không.

3.22. Giả sử R là một vành tuỳ ý, $\mathbb{Z}$ là vành các số nguyên. Trên $R \times \mathbb{Z}$ ta định nghĩa các phép toán như sau:

$$\begin{aligned} (x_1, n_1) + (x_2, n_2) &= (x_1 + x_2, n_1 + n_2), \\ (x_1, n_1)(x_2, n_2) &= (x_1x_2 + n_1x_2 + n_2x_1, n_1n_2). \end{aligned}$$

Chứng minh rằng $R \times \mathbb{Z}$ là một vành có đơn vị, chứa một vành con đẳng cấu với R.

3.23. Hãy tìm các tự đồng cấu của:
a) Trường các số hữu tỷ;
b) Trường các số thực;
c) Trường các số phức, giữ nguyên mọi số thực.

3.24. Tìm tập các tự đẳng cấu của trường

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

3.25. Cho m và n là hai số tự nhiên nguyên tố cùng nhau. Chứng minh đẳng cấu vành

$$\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$$

3.26. Cho $d = 7$ hoặc $d = 11$. Chứng minh

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

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

3.27. a) Chứng minh rằng mọi vành có đơn vị và có p phần tử (p là số nguyên tố) đều đẳng cấu với vành $\mathbb{Z}_p$.

b) Có đúng hay không mọi vành có đơn vị và có m phần tử đều đẳng cấu với $\mathbb{Z}_m$?

3.28. Cho $R = A \times B$ là tích Đề-các của hai vành A và B tuỳ ý. Chứng minh:

a) R là một vành;

b) Các bộ phận $\overline{A} = \{(a, 0) \mid a \in A\}$ và $\overline{B} = \{(0, b) \mid b \in B\}$ là những vành con của R theo thứ tự đẳng cấu với A và B;

c) $\overline{A}$ và $\overline{B}$ là hai iđêan của R thoả mãn các hệ thức:

$$\overline{A} \cap \overline{B} = \{(0, 0)\} \ , \ R = \overline{A} + \overline{B}.$$

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

3.29. Giả sử R là một vành và $a \in R$. Chứng minh rằng:

a) Ánh xạ

$$\begin{aligned} h_a : R &\to R \\ x &\mapsto ax \end{aligned}$$

là một tự đồng cấu (nhóm) của nhóm cộng R.

b) Ánh xạ

$$\begin{aligned} h : R &\to End(R) \\ a &\mapsto h(a) = h_a \end{aligned}$$

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

c) Tìm Ker$h$. Chứng minh rằng h là đơn cấu khi R có đơn vị.

3.30. Giả sử $f : X \to Y$ 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 $f(A) \subset B$;

$$p : X \to X/A \ , \ p' : Y \to Y/B$$

là các toàn cấu chính tắc. Chứng minh rằng tồn tại một đồng cấu duy nhất $\overline{f}$ từ X/A đến Y/B sao cho hình vuông

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle p'} \\ X/A & \xrightarrow{\overline{f}} & Y/B \end{array}$$

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

3.31. Cho I và J là hai iđêan của vành giao hoán, có đơn vị R, và cho ánh xạ

$$\begin{array}{rcl} p : R & \to & (R/I) \times (R/J) \\ a & \mapsto & (a + I, a + J) \end{array}$$

Hãy chứng minh:
a) p là một đồng cấu;
b) p là một toàn cấu khi và chỉ khi $I + J = R$;
c) Hãy mở rộng các kết quả trên cho tập $I_1, I_2, ..., I_n$, với $n > 2$, những iđêan của vành A.

3.32. Giả sử R là vành giao hoán, có đơn vị; A, B là hai iđêan của R sao cho $R = A + B$. Chứng minh rằng

$$R/AB \cong (R/A) \times (R/B).$$

3.33. Giả sử $f : V \to R$, $g : V \to Y$ là hai đồng cấu vành với f là toàn cấu. Chứng minh các điều kiện sau đây là tương đương:
a) Tồn tại đồng cấu $h : R \to Y$ sao cho $g = h \circ f$.
b) Ker$f \subseteq$ Ker$g$.
Khi một trong các điều kiện đó được thoả mãn thì:

c) h là duy nhất;
d) h là đơn cấu nếu và chỉ nếu $\mathrm{Ker}f = \mathrm{Ker}g$.
e) h là toán cấu nếu và chỉ nếu g là đơn ánh.

4. Trường các thương

4.1. Tìm trường các thương của các miền nguyên sau:

$$\mathbb{Z}(\sqrt{2}),\ \ \mathbb{Z}(i),\ \ \mathbb{Z}(\sqrt[3]{2}).$$

4.2. Giả sử R là một trường với phần tử đơn vị e. Xét bộ phận

$$A = \{ne \mid n \in \mathbb{Z}\}.$$

a) Chứng minh A là một vành con của vành R, A có phải là một miền nguyên không?
b) Chứng minh A đẳng cấu với vành các số nguyên $\mathbb{Z}$ khi R có đặc số 0, và đẳng cấu với trường các số nguyên $mod p$, khi R có đặc số p.

4.3. Giả sử p là một số nguyên tố. Chứng minh rằng tập hợp các số hữu tỷ có dạng m/n, trong đó n nguyên tố với p, là một miền nguyên. Tìm trường các thương của miền nguyên này.

4.4. Giả sử A là một vành con của một trường F.
a) Chứng minh rằng nếu A có nhiều hơn một phần tử và A có đơn vị thì phần tử đơn vị của A trùng với phần tử đơn vị của F, và khi đó A là một miền nguyên.
b) Giả sử A là một miền nguyên. Chứng minh rằng bộ phận

$$P = \left\{ab^{-1} \mid a, b \in A, b \neq 0\right\}$$

là một trường con của F và P là trường các thương của A.
c) Chứng minh rằng P là trường con bé nhất trong các trường con của F chứa A.

4.5. Cho I là một iđêan của vành giao hoán R. Chứng minh rằng I là iđêan nguyên tố khi và chỉ khi I là hạt nhân của một đồng cấu vành từ R vào một trường.

4.6. Cho R là một vành. Nếu tồn tại số nguyên dương n nhỏ nhất sao cho $na = 0$ với mọi $a \in R$ thì R được gọi là có đặc số n. Nếu số nguyên dương n như vậy không tồn tại thì R được gọi là có đặc số 0. Chứng minh rằng mỗi vành R nhúng được vào một vành S có đơn vị. Vành S có thể được chọn sao cho có cùng đặc số với R.

5. Vành và trường sắp thứ tự

5.1. Chứng minh các tính chất sau đây trong một vành sắp thứ tự R:

a) $a + x < a + y \Rightarrow x < y$;

b) $a - x < a - y \Rightarrow x > y$;

c) Với $c > 0$, từ $a \leq b$ suy ra $ac \leq bc$;

d) Với $c < 0$, từ $a \leq b$ suy ra $bc \leq ac$;

e) Với $a > 0$, từ $ax < ay$ suy ra $x < y$;

f) Với $a < 0$, từ $ax < ay$ suy ra $y < x$;

g) Nếu $a \neq 0$ thì $a^2 > 0$.

5.2. Cho R là một vành sắp thứ tự với P là tập các phần tử dương của R, và A là một vành con chứa đơn vị của R. Chứng minh rằng A là một vành sắp thứ tự với tập con dương là $A \cap P$.

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

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

Chứng minh các quy tắc sau:

$$\begin{aligned} |ab| &= |a| \cdot |b|; \\ |a + b| &\leq |a| + |b|; \\ -|a| &\leq a \leq |a|; \\ |a| - |b| &\leq |a - b|. \end{aligned}$$

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

$$x < z < y.$$

5.5. Có thể trang bị một quan hệ thứ tự trên vành $\mathbb{Z}_n, n \in \mathbb{N},\ n > 1$ để nó trở thành một vành sắp thứ tự không, vì sao?

Chương V

VÀNH ĐA THỨC VÀ VÀNH ƠCLIT

1. Vành đa thức

Cho R là một vành giao hoán có đơn vị $1 \neq 0$. Một *đa thức của x trên vành R* là một biểu thức dạng

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

trong đó $a_0, \ldots, a_n \in R$ và $a_n \neq 0$ nếu $n > 0$. Phần tử a_i được gọi là *hệ tử* của x^i trong $f(x)$. Phần tử a_n được gọi là *hệ tử cao nhất* của $f(x)$.

Hai đa thức $f(x)$ và $g(x)$ được gọi là *bằng nhau* nếu các hệ tử tương ứng của x^i trong cả hai đa thức bằng nhau. Đặc biệt

$$a_0 + a_1 x + \cdots + a_n x^n = 0$$

nếu và chỉ nếu $a_0 = a_1 = \cdots = a_n = 0$. Nếu n là số tự nhiên lớn nhất sao cho $a_n \neq 0$ thì ta sẽ nói n là bậc của $f(x)$, và ký hiệu $n = \deg f(x)$. Nếu mọi hệ tử của $f(x)$ đều bằng không thì $f(x)$ được gọi là *đa thức không*, và bậc của nó không được định nghĩa. Các đa thức bậc 0 là mọi phần tử khác không a thuộc R, chúng còn được gọi là các *đa thức hằng*.

Tập hợp tất cả các đa thức của x trên vành giao hoán R ký hiệu bởi $R[x]$. Đối với hai đa thức trên R

$$a(x) = \sum_{i=0}^{n} a_i x^i, \; b(x) = \sum_{i=0}^{m} b_i x^i$$

phép cộng và phép nhân được xác định bởi

$$a(x) + b(x) = \sum_{i=0}^{s}(a_i + b_i)x^i, \text{ với } s = \max(m, n);$$

$$a(x).b(x) = \sum_{i=0}^{m+n} c_i x^i, \text{ ở đó } c_k = \sum_{i+j=k} a_i b_j$$

Tập hợp $R[x]$ cùng với hai phép toán vừa nêu là một vành giao hoán có đơn vị. Đóng vai trò phần tử không là đa thức không 0 và phần tử đơn vị là đa thức hằng 1.

Phép dựng vành đa thức của ẩn x có thể mở rộng cho đa thức n biến $x_1, x_2, ..., x_n$ với hệ tử trên vành R. Chúng ta có thể định nghĩa bằng quy nạp

$$R[x_1, x_2, ..., x_n] = R[x_1, x_2, ..., x_{n-1}][x_n]$$

Nếu R là một miền nguyên và $f(x), g(x)$ là hai đa thức khác không của vành $R[x]$ thì

$$\deg(f(x).g(x)) = \deg f(x) + \deg g(x).$$

Do đó nếu R là một miền nguyên thì vành đa thức $R[x]$ cũng là miền nguyên.

Vành đa thức $F(x)$ trên trường F có một tính chất quan trọng, tương tự như trong vành các số nguyên $\mathbb{Z}$, là thuật toán *chia với dư*.

Nếu R là một miền nguyên và $a(x), b(x)$ là hai đa thức trong $R[x]$, ngoài ra hệ tử cao nhất của $b(x)$ khả nghịch trong R thì tồn tại duy nhất cặp đa thức $q(x), r(x) \in R[x]$ sao cho

$$a(x) = b(x).q(x) + r(x),$$

với $\deg r(x) < \deg b(x)$ *nếu* $r(x) \neq 0$.

Từ sự kiện cơ bản này ta có một kết quả quan trọng là: *Mọi iđêan trong vành đa thức $F[x]$ trên trường F đều là iđêan chính.*

Nếu trên vành R các đa thức $p(x), a(x) \neq 0$ thoả mãn đẳng thức $p(x) = a(x)b(x)$, với $b(x) \in R[x]$ thì $a(x)$ được gọi là *ước* của $p(x)$, còn $p(x)$ là *bội* của $a(x)$. Ta cũng nói $a(x)$ *chia hết* $p(x)$, còn $p(x)$ *chia hết cho* $a(x)$.

Đa thức $p(x)$ trong vành $R[x]$ gọi là *khả quy* (trên R) nếu $p(x) = a(x)b(x)$ đối với các đa thức không khả nghịch $a(x), b(x)$ nào đó thuộc $R[x]$. Đa thức $p(x)$ được gọi là *bất khả quy* nếu $p(x)$ không khả nghịch và không khả quy. Nói riêng, khi vành R là một trường F thì đa thức $f(x) \in F[x]$ là khả quy nếu $f(x) = a(x)b(x)$ với các đa thức $a(x), b(x)$ không là hằng.

Giả sử R là vành con của vành V, và $f(x) \in R[x]$ có dạng

$$f(x) = a_0 + a_1x + \cdots + a_nx^n.$$

Phần tử $c \in V$ được gọi là *nghiệm* của $f(x)$ nếu

$$f(c) = a_0 + a_1c + \cdots + a_nc^n = 0.$$

Phần tử $u \in V$ gọi là *đại số trên* R nếu u là nghiệm của một đa thức $g(x) \neq 0$ nào đó của $R[x]$. Trong trường hợp trái lại u được gọi là phần tử *siêu việt* trên R.

Phần tử c thuộc miền nguyên R là nghiệm của đa thức $p(x) \in R[x]$ khi và chỉ khi $x - c$ là ước của đa thức $p(x)$. Do đó, một đa thức bậc n trên một miền nguyên R có nhiều nhất n nghiệm trong R.

Đa thức bất khả quy tính có chất cơ bản sau: *Nếu E là một trường mở rộng của trường F, u là một phần tử thuộc E, và $f(x)$ là đa thức bất khả quy trong $F[x]$ nhận u là nghiệm thì:*

(i) *$f(x)$ là đa thức có bậc thấp nhất nhận u là nghiệm.*

(ii) *$f(x)$ chia hết $g(x)$, với mọi $g(x) \in F[x]$ cũng nhận u là nghiệm.*

Giả sử F là một trường, và $P = (p(x))$ là idêan trong $F[x]$ sinh bởi đa thức $p(x)$ có bậc $n > 0$. Khi đó mỗi phần tử của vành thương $F[x]/(p(x))$ *biểu diễn được một cách duy nhất dưới dạng*

$$a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + P,$$

trong đó $a_0, a_1, \ldots, a_{n-1} \in F$.

2. Thuật toán chia trong miền nguyên

Cho a và b là hai phần tử của miền nguyên R. Phần tử a được gọi là *chia hết* b nếu tồn tại $c \in R$ sao cho $b = ac$. Khi đó ta cũng nói rằng

a là *ước* của b, ký hiệu $a|b$. Thay cho ký hiệu $a|b$ ta còn viết $b \vdots a$, và nói rằng b *chia hết cho* a hay b là *bội* của a.

Tập các ước của 1 trong miền nguyên R là một nhóm aben với phép nhân trong R. Nó được gọi là *nhóm nhân các ước của đơn vị* của miền nguyên R. Các ước của đơn vị còn được gọi là các *phần tử khả nghịch*.

Phần tử a được gọi là *liên kết* với phần tử b nếu tồn tại phần tử khả nghịch u sao cho $a = bu$. *Quan hệ liên kết trên miền nguyên R là một quan hệ tương đương.* Hơn nữa, với $a, b, c \in R$ thì các điều sau tương đương:

(i) a *liên kết với* c,
(ii) $a|c$ *và* $c|a$,
(iii) $aR = cR$.

Cho a là phần tử thuộc miền nguyên R. Các phần tử liên kết với a và các phần tử khả nghịch được gọi là các *ước không thực sự* của a. Các ước còn lại của a được gọi là *ước thực sự*.

Phần tử $p \neq 0$, không khả nghịch của miền nguyên R được gọi là phần tử *bất khả quy* nếu nó không có ước thực sự. Phần tử $p \neq 0$, không khả nghịch, được gọi là phần tử *nguyên tố* nếu với mọi $a, b \in R$, p là ước của tích ab kéo theo p hoặc là ước của a, hoặc là ước của b. *Trong miền nguyên R mọi phần tử nguyên tố đều là phần tử bất khả quy.*

Cho a, b là những phần tử của vành R. Khi đó phần tử $d \in R$ được gọi là *ước chung lớn nhất* của a và b nếu d là ước chung của a và b, và d chia hết cho mọi ước chung của a và b. Ước chung lớn nhất của a và b được ký hiệu bởi

$$d = (a, b) \text{ hoặc } \text{UCLN}(a, b).$$

Ước chung lớn nhất của hai phần tử a và b nói chung không duy nhất. Nếu d là một ước chung lớn nhất của a và b thì d' là ước chung lớn nhất của a và b khi và chỉ nó liên kết với d, nghĩa là chúng sai khác nhau một nhân tử khả nghịch. Các phần tử a và b được gọi là *nguyên tố cùng nhau* nếu ước chung lớn nhất của chúng là ước của đơn vị. Trong trường hợp này ta thường viết $(a, b) = 1$.

3. Vành chính

Miền nguyên D được gọi là một *vành chính* nếu mọi iđêan của D đều là iđêan chính.

Một dây chuyền (hay một dãy) tăng những iđêan của miền nguyên R:

$$J_1 \subset J_2 \subset J_3 \subset \cdots \subset J_n \cdots \qquad (1)$$

được gọi là *dừng* nếu tồn tại số nguyên dương n_0 sao cho

$$J_n = J_{n_0} \text{ với mọi } n > n_0.$$

Dễ thấy dãy (1) dừng khi và chỉ khi nó chỉ có một số hữu hạn các J_i khác nhau. *Trong vành chính R mọi dãy tăng những iđêan đều dừng.*

Trong vành chính R xảy ra những điều sau:

1) *Mọi cặp phần tử khác không a, b đều có ước chung lớn nhất d, và d là một tổ hợp tuyến tính của a, b :*

$$d = as + bt,$$

với $s, t \in R$. Nói riêng, ước chung lớn nhất của hai đa thức khác không trên trường F luôn tồn tại.

2) *Nếu a, b, c là những phần tử thuộc R sao cho $(a, b) = 1$ và $a|bc$ thì $a|c$.*

3) *Nếu p là phần tử bất khả quy trong vành chính R và c là một phần tử bất kỳ thuộc R thì hoặc $p|c$, hoặc $(p, c) = 1$.* Nói riêng, nếu $p(x)$ là một đa thức bất khả quy và $f(x)$ là một đa thức bất kỳ trên trường F thì hoặc $p(x)$ chia hết $f(x)$ hoặc chúng là nguyên tố cùng nhau.

4) *Nếu p là phần tử bất khả quy trong vành chính R và nếu $p|ab$ thì $p|a$ hoặc $p|b$.*

5) *Mỗi phần tử khác không và không khả nghịch đều chứa trong một iđêan tối đại.*

6) *Phần tử a là bất khả quy khi và chỉ khi iđêan aR tối đại.*

Định lý nhân tử hoá: *Mỗi phần tử khác 0 và không khả nghịch trong vành chính R đều phân tích được một cách duy nhất thành tích các nhân tử bất khả quy, sai khác một thứ tự các nhân tử và một nhân*

tử khả nghịch. Nói riêng, mọi đa thức $f(x)$ trên trường F, bậc $n \geq 1$, đều phân tích được một cách duy nhất thành tích những đa thức bất khả quy.

4. Vành Ơclit

Miền nguyên R được gọi là *vành Ơclit* nếu có một ánh xạ

$$\begin{array}{rccc} \delta: & R^* & \to & \mathbb{N} \\ & x & \mapsto & \delta(x) \end{array}$$

từ tập các phần tử khác 0 của R đến tập các số tự nhiên $\mathbb{N}$ thỏa mãn các điều kiện:

(i) $\forall a, b \in R^*$, $a|b$ kéo theo $\delta(a) \leq \delta(b)$.

(ii) $\forall a, b \in R$, $b \neq 0$ tồn tại $q, r \in R$ sao cho $a = bq + r$ với $r = 0$, hoặc nếu $r \neq 0$ thì $\delta(r) < \delta(b)$.

Ánh xạ δ được gọi là *ánh xạ Ơclit.*

Trong vành Ơclit E đối với $x, y \in E^*$, $\delta(xu) = \delta(x)$ nếu u khả nghịch và $\delta(xu) > \delta(x)$ trong trường hợp ngược lại. Từ đó ta thấy rằng phần tử u khả nghịch khi và chỉ khi $\delta(u) = \delta(1)$, và nếu hai phần tử a, b liên kết thì $\delta(a) = \delta(b)$.

Lớp vành Ơclit chứa trong lớp vành chính. Do đó trong vành Ơclit ước chung lớn nhất của hai phần tử khác không a, b luôn tồn tại. Hơn nữa, ước chung lớn nhất đó có thể tìm được nhờ một thuật toán tương tự như thuật toán đã trình bày cho vành các số nguyên $\mathbb{Z}$.

Nếu $a = bq$ thì hiển nhiên $(a, b) = b$.

Nếu $a = bq_0 + r_0$, với $\delta(r_0) < \delta(b)$ thì ta có

$$(a, b) = (b, r_0).$$

Tiếp tục quá trình này sau hữu hạn bước ta được

$$\begin{aligned} b &= r_0 q_1 + r_1, \text{ với } \delta(r_1) < \delta(r_0) \\ \cdots &= \cdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n, \text{ với } \delta(r_n) < \delta(r_{n-1}) \\ r_{n-1} &= r_n q_n, \end{aligned}$$

và khi đó

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

nghĩa là ước chung lớn nhất của a, b bằng số dư cuối cùng r_n trong thuật toán nói trên.

Bây giờ chúng ta xác định khi nào thì thương của một vành Ơclit là một trường. Kết quả này cho phép chúng ta xác định nhiều trường mới. *Cho a là một phần tử của vành Ơclit E. Vành thương $E/(a)$ là một trường nếu và chỉ nếu a bất khả quy trong E.* Nói riêng, vành $F[x]/(p(x))$ là một trường nếu và chỉ nếu đa thức $p(x)$ bất khả quy trên trường F. Hơn nữa, vành $F[x]/(p(x))$ luôn chứa một vành con đẳng cấu với trường F.

Giả sử $p(x) = a_0 + a_1x + \cdots + a_nx^n$ $(n > 1)$ là một đa thức bất khả quy trên trường F. Khi đó tồn tại một trường E là mở rộng của F và chứa một nghiệm c của p(x).

Bài tập

1. Vành đa thức

1.1. Trong vành $\mathbb{Z}_6[x]$ hãy thực hiện phép nhân

$$(2x^3 + 4x^2 + x)(3x^2 + 3x + 2).$$

Vành này có ước của 0 hay không?

1.2. Trong vành $\mathbb{Z}_7[x]$ hãy xác định p để $x^3 + px + 5$ chia hết cho $x^2 + 5x + 6$.

1.3. Tìm đa thức trong vành $\mathbb{Z}[x]$ có bậc bé nhất sao cho:
a) Chia cho $(x - 1)^2$ còn dư $2x$ và chia cho $(x - 2)^2$ 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 $2x^2 - 3$.

Với các bài tập từ 1.4 đến 1.9, tìm thương và phần dư.

1.4. Chia $3x^4 + 4x^3 - x^2 + 5x - 1$ cho $2x^2 + x + 1$ trong $\mathbb{Q}[x]$.

1.5. Chia $x^6 + x^4 - 4x^3 + 5x$ cho $x^3 + 2x^2 + 1$ trong $\mathbb{R}[x]$.

1.6. Chia $x^7 + x^6 + x^4 + x + 1$ cho $x^3 + x + 1$ trong $\mathbb{Z}_2[x]$.

1.7. Chia $2x^5 + x^4 + 2x^3 + x^2 + 2$ cho $x^3 + 2x + 2$ trong $\mathbb{Z}_3[x]$.

1.8. Trong vành $\mathbb{Z}[x]$ xét xem các đa thức sau có phải là bất khả quy hay không?
a) $f(x) = 2x + 3$;
b) $g(x) = x^2 + 1$;
c) $h(x) = x^2 + 2x - 2$.

1.9. Giả sử $a \in A$ và $f(x) \in A[x]$. Chứng minh rằng $f(x)$ là bất khả quy khi và chỉ khi $f(x + a)$ bất khả quy.

1.10. Chứng minh rằng nếu đa thức $a_0 + a_1x + \cdots + a_nx^n$ bất khả quy trên trường A và có bậc $n > 1$ thì đa thức $a_n + a_{n-1}x + \cdots + a_0x^n$ cũng là bất khả quy.

1.11. Chứng minh rằng nếu p là số nguyên tố thì đa thức $x^p - x$ và đa thức 0 cùng xác định một hàm không trên $\mathbb{Z}_p$. Hãy áp dụng kết quả đó để tìm trong $\mathbb{Z}_5[x]$ hai đa thức cùng xác định một hàm $x^2 - x + 1$.

1.12. Cho K là một trường con của trường F và u là một phần tử của F. Xét đồng cấu vành

$$\begin{array}{rccc} \varphi: & K[x] & \to & F \\ & f(x) & \mapsto & f(u) \end{array}$$

Chứng minh rằng $\mathrm{Ker}\varphi$ là một iđêan nguyên tố của $K[x]$. Kết luận còn đúng không nếu K là vành con chứa đơn vị của một miền nguyên F?

1.13. Cho I là một iđêan của vành số nguyên $\mathbb{Z}$. Chứng minh rằng:
a) Tập $I[x]$ mọi đa thức $f(x)$ với hệ số thuộc I là một iđêan của $\mathbb{Z}[x]$. Hơn nữa: $\mathbb{Z}[x]/I[x] \cong (\mathbb{Z}/I)[x]$.
b) Nếu I là iđêan nguyên tố trong $\mathbb{Z}$ thì $I[x]$ có là iđêan nguyên tố trong $\mathbb{Z}[x]$ hay không? Có là iđêan tối đại không?

1.14. Trong vành đa thức $\mathbb{Z}[x]$ xét iđêan I sinh bởi $n \in \mathbb{N}$ và x. Chứng minh rằng I là một iđêan nguyên tố nếu và chỉ nếu n là một số nguyên tố.

1.15. Chứng minh rằng đa thức $x^2 + 14 \in \mathbb{Z}_{15}[x]$ có 4 nghiệm trong $\mathbb{Z}_{15}$.

1.16. Chứng minh rằng đa thức $x^3 + 5x \in \mathbb{Z}_6[x]$ có 6 nghiệm trong $\mathbb{Z}_6$.

1.17. Trong vành $\mathbb{Q}[x]$ chứng minh rằng đa thức

$$(x+1)^{2n} - x^{2n} - 2x - 1$$

chia hết cho các đa thức:
a) $2x + 1$;
b) $x + 1$;
c) x.

1.18. Giả sử đa thức

$$f(x) = (x - a_1)(x - a_2)...(x - a_n) - 1,$$

có các hệ số a_i là những số nguyên phân biệt. Chứng minh rằng $f(x)$ là bất khả quy trong $\mathbb{Q}[x]$.

1.19. Cho p là một số nguyên tố và $f(x)$ là một đa thức thuộc $\mathbb{Z}[x]$ có hệ tử cao nhất bằng 1. Chứng minh rằng nếu $\overline{f}(x)$ bất khả quy trên $\mathbb{Z}_p$ thì $f(x)$ bất khả quy trên $\mathbb{Q}$.

1.20. Cho đa thức với các hệ số nguyên

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Chứng minh rằng nếu phân số tối giản $\frac{p}{q}$, với $p, q \in \mathbb{Z}$, là nghiệm của $f(x)$ thì
a) $p|a_0$ và $q|a_n$.
b) $p - mq$ là ước của $f(m)$ với m nguyên; đặc biệt $p - q$ là ước của $f(1)$, $p + q$ là ước của $f(-1)$.
Áp dụng: Tìm nghiệm hữu tỷ của đa thức

$$10x^5 - 81x^4 + 90x^3 - 102x^2 + 80x - 21.$$

1.21. Giả sử F là trường các thương của vành chính R, $\alpha \in F$ là một nghiệm của đa thức

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,\ a_i \in R.$$

Khi đó $\alpha \in R$.

1.22. Chứng minh trực tiếp rằng nếu u là đại số trên F thì đa thức có bậc nhỏ nhất với hệ tử cao nhất bằng 1 nhận nghiệm u là bất khả quy trên F.

1.23. Chứng minh trực tiếp rằng nếu u là một phần tử bất kỳ của trường F và K là một trường con của F thì tập hợp tất cả các đa thức $g(x)$ với các hệ tử trong K nhận u làm nghiệm là một iđêan của $K[x]$.

1.24. Tìm hạt nhân và ảnh của đồng cấu vành $\psi : \mathbb{R}[x] \to \mathbb{C}$ được định nghĩa bởi $\psi(p(x)) = p(i)$, trong đó $i = \sqrt{-1}$.

1.25. Tìm hạt nhân và ảnh của đồng cấu vành $\psi : \mathbb{R}[x] \to \mathbb{C}$ được định nghĩa bởi $\psi(p(x)) = p(1 + i\sqrt{3})$.

1.26. Tìm một đa thức trong $\mathbb{Q}[x]$ nhận $\sqrt{2} + \sqrt{3}$ là nghiệm. Từ đó chứng minh rằng $\sqrt{2} + \sqrt{3}$ là số vô tỷ.

Với các bài tập từ 1.27 đến 1.30, tính tổng và tích của các phần tử trong vành thương đã cho.

1.27. $3x + 4$ và $5x - 2$ trong $\mathbb{Q}[x]/(x^2 - 7)$.

1.28. $x^2 + 3x + 1$ và $-2x^2 + 4$ trong $\mathbb{Q}[x]/(x^3 + 2)$.

1.29. $x^2 + 1$ và $x + 1$ trong $\mathbb{Z}_2[x]/(x^3 + x + 1)$.

1.30. $ax + b$ và $cx + d$ trong $\mathbb{R}[x]/(x^2 + 1)$, trong đó $a, b, c, d \in \mathbb{R}$.

Với các bài tập từ 1.31 đến 1.38, chứng minh các đẳng cấu.

1.31. $\mathbb{R}[x]/(x^2 + 5) \cong \mathbb{C}$.

1.32. $\mathbb{Z}[x]/(x^2 + 1) \cong \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.

1.33. $\mathbb{Q}[x]/(x^2 - 7) \cong \mathbb{Q}(\sqrt{7}) = \{a + b\sqrt{7} \mid a, b \in \mathbb{Q}\}$.

1.34. $\mathbb{Z}[x]/(2x - 1) \cong \{\frac{a}{b} \in \mathbb{Q} \mid a \in \mathbb{Z}, b = 2^r, r \geq 0\}$, (một vành con của $\mathbb{Q}$.)

1.35. $\mathbb{Z}_{14}/([7]_{14}) \cong \mathbb{Z}_7$.

1.36. $\mathbb{Z}_{14}/([2]_{14}) \cong \mathbb{Z}_2$.

1.37. $\mathbb{R}[x, y]/(x + y) \cong \mathbb{R}[y]$.

1.38. $(R \times S)/((1, 0)) \cong S$.

1.39. Cho I là tập tất cả các đa thức với hệ số tự do bằng không trong $\mathbb{R}[x, y]$. Tìm một đồng cấu vành từ $\mathbb{R}[x, y]$ đến $\mathbb{R}$ có hạt nhân là iđêan I. Chứng minh rằng I không phải là một iđêan chính.

1.40. $\{p(x) \in \mathbb{Q}[x] \mid p(0) = 3\}$ có phải là một iđêan của $\mathbb{Q}[x]$ không?

1.41. Cho I là một iđêan của vành giao hoán A. Chứng minh rằng:

a) Bộ phận $I[x] = \left\{\sum_{i=0}^{n} a_i x^i \in A[x],\ a_i \in I,\ i = 0, 1, ..., n\right\}$ là một iđêan của vành đa thức $A[x]$.

b) $A[x]/I[x] \cong (A/I)[x]$.

c) I là một iđêan nguyên tố của A khi và chỉ khi $I[x]$ là một iđêan nguyên tố của $A[x]$.

d) Nếu I là một iđêan tối đại thì $I[x]$ có là một iđêan tối đại hay không?

2. Thuật toán chia trong miền nguyên

Các đa thức bất khả quy nói trong các bài tập dưới đây được hiểu là những phần tử bất khả quy của vành đang xét.

2.1. Trong vành đa thức $\mathbb{R}[x]$, với $\mathbb{R}$ là trường số thực, chứng minh các đa thức $ax^2 + bx + c$ với $b^2 - 4ac < 0$ là những đa thức bất khả quy. Điều đó có còn đúng nữa không nếu thay trường số thực $\mathbb{R}$ bởi trường số phức $\mathbb{C}$.

2.2. Xét vành $F[x]$ với F là một trường.

a) Chứng minh rằng mọi đa thức bậc nhất của $F[x]$ đều là bất khả quy. Nếu F là một miền nguyên thì điều đó còn đúng nữa không?

b) Chứng minh rằng các đa thức bậc hai và bậc ba của $F[x]$ là bất khả quy khi và chỉ khi chúng không có nghiệm trong F.

2.3. Trong vành $\mathbb{Z}[x]$, xét xem các đa thức sau đây có phải là bất khả quy hay không:

$$f(x) = 2x + 8;\ g(x) = 2x^2 + 1;\ h(x) = x^2 + 4x - 2$$

2.4. Cho $f(x) = x^5 - x^4 - 3x^3 + 2x + 4$. Phân tích $f(x)$ thành tích những đa thức bất khả quy trên các vành: $\mathbb{Z}$; $\mathbb{Z}(\sqrt{2})$; $\mathbb{Q}$ và $\mathbb{R}$.

Trong các bài tập từ 2.5 đến 2.8, những đa thức đã cho có bất khả quy trong vành đã cho hay không? Tại sao?

2.5. $x^3 + x^2 + x + 1$ trong $\mathbb{Q}[x]$.

2.6. $x^4 + x^2 - 6$ trong $\mathbb{Q}[x]$.

2.7. $4x^3 + 3x^2 + x + 1$ trong $\mathbb{Z}_5[x]$.

2.8. $x^4 - 2x^3 + x^2 + 1$ trong $\mathbb{R}[x]$.

2.9. 5 có bất khả quy trong $\mathbb{Z}[i]$ hay không?

2.10. Giả sử A là một vành giao hoán, a là phần tử luỹ linh. Chứng minh rằng đa thức $1 + ax \in A[x]$ khả nghịch. Tổng quát hơn, nếu a_0 khả nghịch và $a_1, ..., a_n$ luỹ linh thì $\sum_{i=0}^{n} a_i x^i$ khả nghịch.

3. Vành chính

3.1. Cho F là trường. Chứng minh trực tiếp rằng:
a) $F[x]$ là vành chính.
b) Nếu $p(x)$ là đa thức bất khả quy trên F thì idêan chính sinh bởi $p(x)$ là tối đại trong $F[x]$, từ đó suy ra vành thương $\overline{F} = F[x]/(p(x))$ là một trường.

3.2. a) Chứng minh rằng hai đa thức bất khả quy trên cùng một trường không thể có nghiệm chung.
b) Nếu $f(x)$ và $g(x)$ có nghiệm chung và $f(x)$ là bất khả quy trên trường F thì $f(x) \mid g(x)$.

3.3. Nếu $f(x)$ là đa thức bất khả quy trên trường F, có bậc $n \geq 1$ thì không tồn tại trong F hai đa thức khác không có bậc nhỏ hơn n mà tích của chúng chia hết cho $f(x)$.

3.4. Giả sử a và b là hai phần tử nguyên tố cùng nhau của vành chính A. Chứng minh idêan sinh ra bởi a và b là vành A.

3.5. Cho p là một phần tử khác 0 của một vành chính A. Chứng minh p là bất khả quy khi và chỉ khi Ap là một idêan tối đại của A.

3.6. Chứng minh rằng trong một vành chính, các idêan nguyên tố khác 0 đều là các idêan tối đại.

3.7. Chứng minh một trường là một vành chính.

3.8. Vành thương của một vành chính có phải là một vành chính không?

3.9. Giả sử R là vành chính và A là idêan của R. Chứng minh rằng:
a) Mọi idêan của vành R/A đều là idêan chính.
b) Vành thương R/A là vành chính khi và chỉ khi A là idêan nguyên tố.

3.10. Vành con của một vành chính có phải là một vành chính không?

3.11. Giả sử $A = \{a + b\sqrt{3}i | a, b \in \mathbb{Z}\}$.
a) Chứng minh rằng A cùng với phép cộng và phép nhân các số phức là một miền nguyên.
b) Chứng minh rằng $2, 1 + \sqrt{3}i, 1 - \sqrt{3}i$ là những phần tử bất khả quy của A nhưng không phải là những phần tử nguyên tố. Từ đó suy ra A không phải là một vành chính.

3.12. Chứng minh rằng vành

$$A = \{a + b\sqrt{2}i \mid a, b \in \mathbb{Z}\}$$

là một vành chính.

3.13. Chứng minh rằng vành $A = \{\frac{m}{n} \in \mathbb{Q} \mid (m, n) = 1,\ n \text{ lẻ}\}$ là một vành chính.

3.14. Chứng minh rằng vành $\mathbb{Z}[x]$ không là vành chính, nhưng vành thương $\mathbb{Z}(x)/(x^2 + 2)$ là một vành chính.

3.15. Cho K là một vành giao hoán có đơn vị $1 \neq 0$.
a) Chứng minh rằng $K[x]$ là vành chính khi và chỉ khi K là một trường.
b) Mệnh đề a) còn đúng không khi thay $K[x]$ bởi vành $K[c]$, với c là phần tử đại số trên K.

3.16. Cho K là vành giao hoán có đơn vị $1 \neq 0$. Chứng minh:
a) Nếu K là vành chính thì mọi idêan của vành $K \times \mathbb{Z}$ đều là chính. $K \times \mathbb{Z}$ có là vành chính không?
b) Vành đa thức $K[x]$ là vành chính khi và chỉ khi K là vành đơn (theo nghĩa là vành chỉ có 2 idêan là 0 và K).

3.17. Cho K là một trường. Vành đa thức hai ẩn $K[x, y]$ có phải là một vành chính không, tại sao?

3.18. Tìm các số nguyên dương n sao cho vành đa thức $\mathbb{Z}_n[x]$ là một vành chính.

3.19. Cho đa thức $f(x) = x^2 + 1 \in \mathbb{Z}_3[x]$, I là idêan của $\mathbb{Z}_3[x]$ sinh bởi $f(x)$.

a) Chứng minh rằng vành thương $K = \mathbb{Z}_3[x]/I$ là một trường. Xác định mọi phần tử của K và tìm nghiệm của $f(x)$ trong K.

b) Xác định đặc số của K.

Phân tích các đa thức trong các bài tập từ 3.18 đến 3.29 thành các nhân tử bất khả quy trong vành đã cho.

3.20. $x^5 - 1$ trong $\mathbb{Q}[x]$.

3.21. $x^5 + 1$ trong $\mathbb{Z}_2[x]$.

3.22. $x^4 + 1$ trong $\mathbb{Z}_5[x]$.

3.23. $2x^3 + x^2 + 4x + 2$ trong $\mathbb{Q}[x]$.

3.24. $2x^3 + x^2 + 4x + 2$ trong $\mathbb{C}[x]$.

3.25. $x^8 - 16$ trong $\mathbb{C}[x]$.

3.26. $x^8 - 16$ trong $\mathbb{R}[x]$.

3.27. $x^8 - 16$ trong $\mathbb{Q}[x]$.

3.28. $x^8 - 16$ trong $\mathbb{Z}_{17}[x]$.

3.29. Chứng minh rằng $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ không có tính chất nhân tử hoá duy nhất.

Miền nguyên R được gọi là thỏa mãn điều kiện có ước chung lớn nhất (viết tắt là UCLN) nếu trong R mọi cặp phần tử a, b không đồng thời bằng không đều có ước chung lớn nhất. Chứng minh các mệnh đề từ bài 3.30 đến bài 3.33 sau.

3.30. Cho a, b, c thuộc miền nguyên R thỏa mãn điều kiện có UCLN. Khi đó ta có:

1) $c(a, b) = (ca, cb)$,

2) Nếu $(a, b) = 1$ và $(a, c) = 1$ thì $(a, bc) = 1$.

3.31. Cho R là một miền nguyên thỏa mãn điều kiện có UCLN, p là phần tử bất khả quy thuộc R. Khi đó với mọi a thuộc R, hoặc a chia hết cho p hoặc a và p nguyên tố cùng nhau.

3.32. Trong vành R thỏa mãn điều kiện có UCLN, một phần tử là bất khả quy khi và chỉ khi nó là nguyên tố.

3.33. Cho R là miền nguyên thoả mãn điều kiện có UCLN, $p \in R$ là phần tử bất khả quy. Nếu $a_1, a_2, ..., a_n$ $(n \geq 2)$ là những phần tử của R sao cho $p | a_1 a_2 ... a_n$ thì tồn tại a_k sao cho $p | a_k$.

Dãy các phần tử khác không của miền nguyên R

$$a_1, a_2, ..., a_n, ...$$

được gọi là một dây chuyền giảm những ước nếu $a_{n+1} \mid a_n$ với $n = 1, 2, ...$ Dây chuyền được gọi là dừng nếu tồn tại số nguyên dương s sao cho a_n liên kết với a_s với mọi $n > s$.

3.34. Cho R là một miền nguyên thoả mãn điều kiện dừng những ước thực sự. Chứng minh rằng nếu $a \in R, a \neq 0$ và không khả nghịch thì a có một ước bất khả quy.

Miền nguyên R được gọi là vành nhân tử hoá (hay vành Gauss) nếu mọi phần tử khác 0 và không khả nghịch của nó đều phân tích được một cách duy nhất thành một tích những nhân tử bất khả quy, sai khác thứ tự các nhân tử và sai khác các nhân tử khả nghịch. Chứng minh các mệnh đề từ 3.35 đến 3.40 sau.

3.35. Cho R là một miền nguyên thoả mãn điều kiện dừng những ước thực sự và điều kiện có ƯCLN. Khi đó R là một vành nhân tử hoá (hay vành Gauss). Từ đó suy ra mọi vành chính đều là vành Gauss.

3.36. Vành nhân tử hoá thoả mãn điều kiện dừng những ước thực sự và điều kiện có ƯCLN.

3.37. Cho ví dụ chứng tỏ:

a) Vành con chứa đơn vị của vành nhân tử hoá có thể không là vành nhân tử hoá.

b) Vành thương R/A của vành nhân tử hoá R theo iđêan A có thể không là vành nhân tử hoá, kể cả khi R/A là miền nguyên.

3.38. Cho A là một vành Gauss, $\overline{A}$ là trường các thương của A.

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

được gọi là một đa thức *nguyên bản* nếu ước chung lớn nhất của các hệ tử $a_0, a_1, ..., a_n$ bằng 1. Chứng minh rằng:

a) Tích của hai đa thức nguyên bản là một đa thức nguyên bản.

b) Nếu đa thức $f(x) \in A[x]$ khả quy trong $\overline{A}[x]$ thì nó cũng khả quy trong $A[x]$.

3.39. Giả sử $p(x)$ là một đa thức với hệ số nguyên và bất khả quy trong $\mathbb{Z}[x]$. Chứng minh rằng trong $\mathbb{Z}[x]$ nếu $p(x)$ chia hết tích $f(x).g(x)$ thì hoặc $p(x)$ chia hết $f(x)$ hoặc $p(x)$ chia hết $g(x)$.

3.40. Chứng minh rằng nếu A là một vành Gauss thì vành $A[x]$ cũng là vành Gauss. Tính chất này còn đúng không nếu thay giả thiết "vành Gauss" bằng giả thiết "vành chính".

4. Vành Ơclit (Euclide)

4.1. Chứng minh rằng các vành sau là vành Ơclit:
a) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$;
b) $\mathbb{Z}[i\sqrt{2}] = \{a + b\sqrt{2}i \mid a, b \in \mathbb{Z}\}$;
c) $\mathbb{Z}[x]/(x^2 + 2)$;
d) $A = \mathbb{Z}\left[\dfrac{1+\sqrt{-11}}{2}\right] = \left\{a + b\dfrac{1+\sqrt{-11}}{2} \middle| a, b \in \mathbb{Z}\right\}$.

4.2. Chứng minh rằng vành $A = \{\dfrac{m}{n} \in \mathbb{Q} \mid (m, n) = 1, \quad n \text{ lẻ } \}$ là một vành Ơclit.

4.3. Chứng minh rằng mỗi trường là một vành Ơclit.

4.4. Cho một ví dụ chứng tỏ rằng vành con chứa đơn vị của một vành Ơclit có thể không phải là vành Ơclit.

4.5. Giả sử R là một vành Ơclit và A là iđêan của R. Chứng minh vành thương R/A là vành Ơclit khi và chỉ khi A là iđêan nguyên tố của R.

4.6. Giả sử A là một vành Ơclit. Chứng minh rằng A là một trường khi và chỉ khi $\delta(x)$ là hằng với mọi $x \in A^*$.

4.7. Giả sử

$$f(x) = x^5 + x^3 + x^2 + x + 1,$$
$$g(x) = x^3 + 2x^2 + x + 1.$$

Tìm ước chung lớn nhất của $f(x)$ và $g(x)$ trong $\mathbb{Z}[x]$.

Với các bài tập từ 4.8 đến 4.14, tìm ƯCLN của các phần tử a, b trong vành Ơclit đã cho, và tìm các phần tử s, t trong vành đó thoả mãn $as + bt = ƯCLN(a, b)$.

4.8. $a = 33, b = 42$ trong $\mathbb{Z}$.

4.9. $a = 2891, b = 1589$ trong $\mathbb{Z}$.

4.10. $a = 2x^3 - 4x^2 - 8x + 1, b = 2x^3 - 5x^2 - 5x + 2$ trong $\mathbb{Q}[x]$.

4.11. $a = x^6 - x^3 - 16x^2 + 12x - 2, b = x^5 - 2x^2 - 16x + 8$ trong $\mathbb{Q}[x]$.

4.12. $a = x^4 + x + 1, b = x^3 + x^2 + x$ trong $\mathbb{Z}_3[x]$.

4.13. $a = x^4 + 2, b = x^3 + 3$ trong $\mathbb{Z}_5[x]$.

4.14. $a = 4 - i, b = 1 + i$ trong $\mathbb{Z}[i]$.

4.15. $\mathbb{Z}[x]$ có phải là một vành Oclit cùng với ánh xạ cho bởi $\delta(f(x)) = \deg f(x)$ với mỗi đa thức khác 0 hay không? $\mathbb{Z}[x]$ có phải là một vành Oclit với một định nghĩa nào khác của $\delta(f(x))$ hay không?

4.16. Xét vành Oclit $\mathbb{Z}[i]$ với chuẩn:

$$N : \mathbb{Z}[i] \setminus \{0\} \longrightarrow \mathbb{N},\ m + ni \mapsto m^2 + n^2.$$

Chứng minh rằng với mọi $\alpha \in \mathbb{Z}[i] \setminus \{0\}$ mà $N(\alpha)$ nguyên tố trong $\mathbb{Z}$ thì α là phần tử nguyên tố trong $\mathbb{Z}[i]$. Điều ngược lại có đúng không?

4.17. Nếu R là một miền nguyên. Chứng minh rằng các khẳng định sau là tương đương:

a) R là một trường.

b) $R[x]$ là một vành Oclit.

c) $R[x]$ là một vành chính.

4.18. Chứng minh rằng không tồn tại miền nguyên R sao cho vành đa thức hai ẩn $R[x, y]$ là một vành Oclit.

Với các bài tập 4.19, 4.20, xác định bảng cộng và nhân cho các vành đã cho. Tìm tất cả các ước của 0 trong mỗi vành. Vành nào trong các vành này là trường?

4.19. $\mathbb{Z}_2[x]/(x^3 + 1)$.

4.20. $\mathbb{Z}_3[x]/(x^2 + 2x + 2)$.

Các phần tử nào trong các bài tập từ 4.21 đến 4.26 là bất khả quy trong các vành đã cho? Nếu có phần tử bất khả quy, tìm trường các thương tương ứng theo môđun iđêan sinh bởi phần tử đó.

4.21. $x^2 - 2$ trong $\mathbb{R}[x]$.

4.22. $x^3 + x^2 + 2$ trong $\mathbb{Z}_3[x]$.

4.23. $x^4 - 2$ trong $\mathbb{Q}[x]$.

4.24. $x^7 + 4x^3 - 3ix + 1$ trong $\mathbb{C}[x]$.

4.25. $x^2 - 3$ trong $\mathbb{Q}(\sqrt{2})[x]$.

4.26. $3x^5 - 4x^3 + 2$ trong $\mathbb{Q}[x]$.

4.27. Giả sử vành E với ánh xạ $\delta : E^* \to \mathbb{N}$ là một vành Ơclit. Chứng minh tồn tại ánh xạ Ơclit:

$$\delta' : E^* \to \mathbb{N}$$

sao cho $\delta'(E^*) = \{0, 1, ..., n\}$ với $n \geq 0$ hoặc $\delta'(E^*) = \mathbb{N}$.

4.28. Giả sử E là một vành Ơclit với ánh xạ Ơclit δ. Chứng minh $\delta(u)$ là phần tử bé nhất của $\delta(E^*)$ khi và chỉ khi u khả nghịch trong E.

4.29. Giả sử E là một miền nguyên nhưng không là trường. Chứng minh rằng điều kiện cần để E là vành Ơclit là tồn tại một phần tử không khả nghịch $x \in E$ sao cho mọi lớp của $E/(x)$ có một đại diện hoặc khả nghịch, hoặc bằng 0.

4.30. Chứng minh vành:

$$A = \left\{ a + b\frac{1 + i\sqrt{19}}{2} \mid a, b \in \mathbb{Z} \right\}$$

không phải là một vành Ơclit. (Người ta có thể chứng minh A là vành chính).

Chương VI

PHÂN TÍCH ĐA THỨC TRÊN CÁC TRƯỜNG SỐ

1. Phân tích các đa thức thực và phức

Ta nhắc lại rằng, một đa thức $f(x)$ có bậc dương được gọi là *khả quy trên* trường F nếu nó có thể phân tích được thành tích của hai đa thức có bậc dương trong $F[x]$. Nếu nó không thể phân tích như vậy, $f(x)$ được gọi là *bất khả quy trên* F, và $f(x)$ là một phần tử bất khả quy của vành $F[x]$.

Định lý cơ bản của Đại số: *Nếu $f(x)$ là một đa thức trong $\mathbb{C}[x]$ có bậc dương, thì $f(x)$ có nghiệm trong $\mathbb{C}$.*

Các nghiệm phức của các đa thức *thực* tồn tại theo từng cặp liên hợp:

(i) *Nếu $z = a+bi$ là một nghiệm phức của đa thức thực $f(x) \in \mathbb{R}[x]$, thì liên hợp của nó $\overline{z} = a-bi$ cũng là một nghiệm. Do đó đa thức thực*

$$(x - z)(x - \overline{z}) = x^2 - 2ax + (a^2 + b^2)$$

là một nhân tử của $f(x)$.

(ii) *Nếu $a, b, c \in \mathbb{Q}$ và $a + b\sqrt{c}$ là một nghiệm vô tỷ của đa thức hữu tỷ $f(x) \in \mathbb{Q}[x]$, thì $a - b\sqrt{c}$ cũng là một nghiệm, và đa thức hữu tỷ*

$$x^2 - 2ax + (a^2 - b^2c)$$

là một nhân tử của $f(x)$.

Các đa thức bất khả quy trong vành $\mathbb{C}[x]$ là các đa thức bậc 1. Các đa thức bất khả quy trong vành $\mathbb{R}[x]$ là các đa thức bậc 1 cùng với các đa thức bậc 2 có dạng $ax^2 + bx + c$, trong đó $b^2 < 4ac$.

2. Phân tích các đa thức nguyên và hữu tỷ

Một đa thức hữu tỷ luôn luôn có thể đưa được về một đa thức nguyên bằng cách nhân nó với bội chung nhỏ nhất (BCNN) của các mẫu số của các hệ số của nó. Bây giờ chúng ta đưa ra các phương pháp khác nhau để xác định xem một đa thức nguyên có nghiệm hữu tỷ hoặc bất khả quy trên $\mathbb{Q}$.

Định lý nghiệm hữu tỷ: *Cho đa thức với hệ số nguyên*

$$p(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x].$$

Nếu r/s là nghiệm hữu tỷ của $p(x)$ và $UCLN(r, s) = 1$, thì:

(i) $r|a_0$.
(ii) $s|a_n$.

Nói riêng, *nếu đa thức $p(x) \in \mathbb{Z}[x]$ với hệ tử cao nhất bằng 1 thì nghiệm hữu tỷ (nếu có) của $f(x)$ là nghiệm nguyên, và số nguyên này là ước của số hạng tự do.*

Nghiệm hữu tỷ của đa thức $p(x) \in \mathbb{Z}[x]$ cũng có thể được tính theo phương pháp sau: Nhân hai vế của phương trình $p(x) = 0$ với a_n^{n-1} và đặt $y = a_nx$ ta được phương trình

$$q(y) = b_0 + b_1y + \ldots + b_{n-1}y^{n-1} + y^n = 0,$$

ở đó hệ số của y^n bằng 1. Khi đó theo Hệ quả 2.2 nghiệm hữu tỷ của phương trình $q(y) = 0$ nếu có phải là số nguyên và là ước của b_0. Trong trường hợp đơn giản ta có thể kiểm tra trực tiếp những ước này có là nghiệm của phương trình hay không. Đối với trường hợp chung ta có thể làm giảm số phép thử nhờ một kỹ thuật đơn giản được trình bày dưới dây.

Giả sử $q(1) \neq 0$ và $q(-1) \neq 0$. Nếu c là một nghiệm nguyên của $q(y)$ thì $q(y)$ chia hết cho $y - c$:

$$q(y) = (y - c)h(y).$$

Theo định lý về phép chia với dư ta có $h(y) \in \mathbb{Z}[y]$, nghĩa là các hệ số của $h(y)$ đều là số nguyên. Từ đó

$$h(1) = \frac{q(1)}{1-c}, -h(-1) = \frac{q(-1)}{1+c}$$

là những số nguyên. Điều này cho phép chúng ta chỉ cần kiểm tra đối với những ước c của b_0 mà

$$\frac{q(1)}{1-c}, \frac{q(-1)}{1+c}$$

đều là những số nguyên.

Nếu $q(1) = 0$ hoặc $q(-1) = 0$ thì ta chia $q(y)$ cho $y-1$ (tương ứng cho $y+1$) và tiếp tục làm như trên với đa thức thương.

Bổ đề Gauss: *Cho đa thức với hệ số nguyên*

$$f(x) = a_0 + a_1 + \cdots + a_n x^n \in \mathbb{Z}[x].$$

Nếu $f(x)$ có thể phân tích được trong $\mathbb{Q}[x]$ thành $f(x) = g(x)h(x)$ với $g(x), h(x) \in \mathbb{Q}[x]$, thì $f(x)$ cũng phân tích được trong $\mathbb{Z}[x]$.

Một cách tương đương, *nếu đa thức $f(x) \in \mathbb{Z}[x]$, bậc $n > 1$, bất khả quy trên $\mathbb{Z}$ thì cũng bất khả quy trên $\mathbb{Q}$.*

Tiêu chuẩn Eisenstein: *Cho đa thức với các hệ số nguyên*

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n, \quad (n > 1)$$

và giả sử tồn tại số nguyên tố p sao cho p không chia hết a_n nhưng chia hết các hệ số còn lại và p^2 không chia hết a_0. Khi đó $f(x)$ là bất khả quy trong $\mathbb{Q}[x]$.

Tiêu chuẩn bất khả quy thu gọn: *Cho p là một số nguyên tố và đa thức*

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x],$$

có đa thức $\overline{f}(x)$ tương ứng

$$\overline{f}(x) = \overline{a}_0 + \overline{a}_1 x + \ldots + \overline{a}_n x^n \in \mathbb{Z}_p[x]$$

sao cho $\overline{f}(x) \neq 0$ và bậc của $\overline{f}(x)$ bằng bậc của $f(x)$. Khi đó, nếu $\overline{f}(x)$ là đa thức bất khả quy trong $\mathbb{Z}_p[x]$ thì $f(x)$ bất khả quy trong $\mathbb{Q}[x]$.

Tiêu chuẩn Eisenstein vẫn đúng nếu thay $\mathbb{Z}$ bởi vành A và $\mathbb{Q}$ bởi trường các thương của A.

3. Phân tích các đa thức trên trường hữu hạn

Một đa thức trong $\mathbb{Z}_2[x]$ có nhân tử $x+1$ nếu và chỉ nếu nó có một số chẵn các hệ số khác 0.

Bài tập

1. Phân tích các đa thức thực và phức

1.1. 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 k của $g(x)$ cũng là nghiệm bội lớn hơn hoặc bằng k của $f(x)$.

1.2. Trong vành $\mathbb{Q}[x]$, chứng minh rằng đa thức:

$$f(x) = x^{3k} + x^{3l+1} + x^{3n+2} \quad (k, l, n \in \mathbb{N})$$

chia hết cho đa thức $g(x) = x^2 + x + 1$.

1.3. Có thể định nghĩa được một thuật toán chia trong $\mathbb{R}[x, y]$ hay không? Có thể chia $x^3 + 3xy + y + 4$ cho $xy + y^3 + 2$ hay không?

1.4. Giả sử K là một trường, $f(x)$ và $g(x)$ là hai đa thức nguyên tố cùng nhau trong $K[x]$. Chứng minh rằng $yf(x) + g(x)$ là một đa thức bất khả quy trong $K[x, y]$.

1.5. Một ánh xạ $\varphi : \mathbb{C} \to \mathbb{C}$ được gọi là ánh xạ đa thức trên $\mathbb{C}$ nếu tồn tại một đa thức $f(x) \in \mathbb{C}[x]$ sao cho $\varphi(a) = f(a)\ \forall a \in \mathbb{C}$.
a) Chứng minh rằng có một song ánh giữa tập $\mathbb{C}[x]$ và tập các ánh xạ đa thức trên $\mathbb{C}$.
b) Mệnh đề a) còn đúng không nếu thay trường $\mathbb{C}$ bởi trường K tuỳ ý.

2. Phân tích các đa nguyên và hữu tỷ

2.1. Nếu r/s là một nghiệm hữu tỷ, ở dạng tối giản, của một đa thức $p(x)$ với hệ số nguyên, chứng minh rằng $p(x) = (sx - r)g(x)$ với một đa thức $g(x)$ nào đó với hệ số nguyên.

2.2. Chứng minh rằng r/s, ở dạng tối giản, không thể là một nghiệm của đa thức nguyên $p(x)$ trừ khi $(s - r) \mid p(1)$. Điều này có thể được sử dụng để rút ngắn danh sách các nghiệm hữu tỷ có thể có của một đa thức nguyên.

2.3. Chứng minh rằng $\sqrt{2}/\sqrt[3]{5}$ là số vô tỷ.

2.4. 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 không, là một đa thức bất khả quy.

2.5. Tìm nghiệm hữu tỷ 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) $x^5 + 2x^4 + 6x^3 + 3x^2 - 12x - 48$.

2.6. 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.

2.7. Chứng minh rằng nếu đa thức

$$f(x) = ax^2 + bx + c \in \mathbb{Z}[x] \ (a \neq 0)$$

có nghiệm hữu tỷ thì ít nhất một trong ba số a, b, c chẵn.

2.8. Dùng tiêu chuẩn Eisenstein chứng minh rằng các đa thức sau là bất khả quy trong $\mathbb{Q}[x]$:
a) $x^5 + 15$,
b) $3x^8 - 4x^6 + 8x^5 - 10x + 6$,
c) $x^3 - 3x - 1$,
d) $x^4 - x^3 + 2x + 1$,
e) $x^4 - 8x^3 + 12x^2 - 6x + 3$.

Trong các Bài tập từ 2.9 đến 2.11, hãy phân tích các đa thức thành các nhân tử bất khả quy trong $\mathbb{Q}[x]$:

2.9. $x^4 - 9x + 3$.

2.10. $x^3 - 4x + 1$.

2.11. $x^4 + 3x^3 + 9x - 9$.

2.12. Cho $a_1, a_2, ..., a_n$ là các số nguyên phân biệt. Chứng minh rằng đa thức

$$(x - a_1)^2(x - a_2)^2 \cdots (x - a_n)^2 + 1$$

là bất khả quy trong $\mathbb{Q}[x]$.

2.13. Tìm điều kiện cần và đủ để đa thức $f(x) = x^4 + px^2 + q$ là bất khả quy trong $\mathbb{Q}[x]$.

2.14. Phân tích mỗi đa thức sau thành tích những đa thức bất khả quy trong $\mathbb{Q}[x, y]$.

a) $x^3 - y^3$,

b) $x^4 - y^2$,

c) $x^6 - y^6$,

d) $x^7 + 2x^3y + 3x^2 + 9y$.

2.15. Chứng minh rằng đa thức $x^3 + 3x^2y^2 + 2x^2y + xy^4 + 7y + y^2$ là bất khả quy trong $\mathbb{Q}[x, y]$.

2.16. *(Tiêu chuẩn bất khả quy thu gọn).* Cho p là số nguyên tố và đa thức

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$$

có đa thức $\overline{f}(x)$ tương ứng

$$\overline{f}(x) = \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_n}x^n \in \mathbb{Z}_p[x]$$

sao cho $\overline{f}(x) \neq 0$ và bậc của $\overline{f}(x)$ bằng bậc của $f(x)$. Khi đó nếu $\overline{f}(x)$ là đa thức bất khả quy trong $\mathbb{Z}_p[x]$ thì $f(x)$ bất khả quy trong $\mathbb{Q}[x]$.

2.17. Xét tính khả quy của đa thức $x^4 - 15x^3 + 7$ trong vành $\mathbb{Q}[x]$.

2.18. Cho đa thức $p(x) = x^3 - 3x + 1$. Chứng minh rằng:

a) $p(x)$ bất khả quy trên $\mathbb{Q}$ và cả ba nghiệm của nó trong $\mathbb{C}$ đều là thực.

b) Nếu c là một nghiệm của $p(x)$ thì c và $c + 2$ là hai phần tử khả nghịch trong vành $A = \mathbb{Z}[c]$.

c) $2A$ là một iđêan nguyên tố của A.

3. Phân tích các đa thức trên trường hữu hạn

3.1. Tìm tất cả các đa thức bất khả quy bậc 2 trên $\mathbb{Z}_2$.

3.2. Tìm một đa thức bất khả quy bậc 2 trên $\mathbb{Z}_5$.

3.3. Tìm một đa thức bất khả quy bậc 2 trên $\mathbb{Z}_7$.

3.4. Cho L_p là tập tất cả các hàm tuyến tính $f : \mathbb{Z}_p \to \mathbb{Z}_p$ có dạng $f(x) = ax + b$, trong đó $a \neq 0$ trong $\mathbb{Z}_p$. Chứng minh rằng L_p cùng với phép toán hợp thành các ánh xạ là một nhóm có cấp $p(p-1)$.

3.5. Nếu p là một số nguyên tố, chứng minh rằng $(x-a)|(x^{p-1}-1)$ trong $\mathbb{Z}_p[x]$ với mọi số $a \neq 0$ trong $\mathbb{Z}_p$. Từ đó chứng minh rằng

$$x^{p-1} - 1 = (x-1)(x-2)...(x-p+1) \text{ trong } \mathbb{Z}_p[x].$$

3.6. *(Định lý Wilson).* Chứng minh rằng: $(n-1)! \equiv -1 \pmod{n}$ nếu và chỉ nếu n là số nguyên tố.

Phần thứ hai

LỜI GIẢI VÀ HƯỚNG DẪN

Chương I

CƠ SỞ

1. Tập hợp

1.1. Giả sử $S \subset T$. Khi đó:

Với mọi $x \in S$ ta có $x \in T$ nên $x \in S \cap T$. Suy ra $S \subset S \cap T$. Bao hàm ngược lại: $S \cap T \subset S$ là hiển nhiên. Vậy $S \cap T = S$.

Với mọi $x \in S \cup T$ ta có $x \in S$ hoặc $x \in T$. Do $S \subset T$ nên ta có $x \in T$ hay $S \cup T \subset T$. Bao hàm ngược lại $T \subset S \cup T$ là hiển nhiên. Vậy $S \cup T = T$.

Các chứng minh còn lại hoàn toàn tương tự.

1.3. Dựa vào định nghĩa.

1.6. Giả sử $A \in P(X)$. Khi đó ta có $A \subset X \subset Y$ hay $A \in P(Y)$.

1.7. Nếu $A \setminus (A \setminus B) = B$ thì hiển nhiên $B \subset A$.

Ngược lại, giả sử $B \subset A$.

Nếu $x \in B$ thì do $B \subset A$ nên $x \in A$ và $x \notin A \setminus B$ hay $x \in A \setminus (A \setminus B)$.

Nếu $x \in A \setminus (A \setminus B)$ thì $x \in A$ và $x \notin A \setminus B$ hay $x \in A$ và $x \in B$ (vì không thể xảy ra trường hợp $x \notin A$).

1.8. a) và b) là hiển nhiên.

c) Giả sử $x \in B \cap (\bigcup\limits_{i \in I} A_i)$. Khi đó $x \in B$ và $x \in \bigcup\limits_{i \in I} A_i$. Suy ra tồn tại $i_0 \in I$ để $x \in B$ và $x \in A_{i_0}$ hay $x \in B \cap A_{i_0}$. Vậy $x \in \bigcup\limits_{i \in I} (B \cap A_i)$.

Đảo lại, giả sử $x \in \bigcup\limits_{i \in I} (B \cap A_i)$ thì tồn tại $i_0 \in I$ để $x \in B \cap A_{i_0}$ hay $x \in B$ và $x \in A_{i_0}$ do đó $x \in B$ và $x \in \bigcup\limits_{i \in I} A_i$.

Vậy $x \in B \cap (\bigcup_{i \in I} A_i)$.

1.9. a) Hiển nhiên $\bigcup_{i=1}^{n} B_i \subset E$. Giả sử x là phần tử bất kỳ thuộc E. Khi đó tồn tại k với $1 \leq k \leq n$ sao cho $x \in A_k$ nhưng $x \notin A_{k-1}$. Suy ra $x \in B_{k-1}$. Vậy $E \subset \bigcup_{i=1}^{n} B_i$, và do đó $E = \bigcup_{i=1}^{n} B_i$.

b) Ta có $B_k \cap A_l = \emptyset \ \forall \ l < k$. Không mất tính tổng quát ta giả sử $i > j$. Khi đó $B_i \cap A_j = \emptyset$. Mà $B_j \subset A_j$ nên $B_i \cap B_j = \emptyset$.

1.10. Lấy một phần tử tùy ý $A_{i_0} \in \{A_1, A_2, ..., A_n\}$. Nếu A_{i_0} không chứa tập nào còn lại thì A_{i_0} là tập cần tìm. Nếu nó chứa tập A_{i_1} thì ta lại lập luận với A_{i_1} như đối với A_{i_0}. Cứ như vậy ta sẽ được một dãy giảm thực sự:

$$A_{i_0} \supset A_{i_1} \supset ... \supset A_{i_k} \supset ...$$

Dãy này phải dừng vì chỉ có một số hữu hạn tập A_i. Nghĩa là có ít nhất một tập A_i không chứa một tập nào trong số các tập còn lại.

1.11. a) Ta có $A \cup B = (A \setminus B) \cup (A \cap B) \cup (B \setminus A)$ nên

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

b) Hiển nhiên do tính giao hoán của phép hợp và phép giao.

c) $A \cap (B \triangle C) = A \cap [(B \setminus C) \cup (C \setminus B)] = [A \cap (B \setminus C)] \cup [A \cap (C \setminus B)]$
$= [(A \cap B) \setminus (A \cap C)] \cup [(A \cap C) \setminus (A \cap B)] = (A \cap B) \triangle (A \cap C)$.

2. Ánh xạ

2.1. Ánh xạ là ngược trái đồng thời của f, g và h là ánh xạ $k : \mathbb{Z} \to \mathbb{Z}$, $k(n) = \left[\frac{n}{3}\right]$ (trong đó $[x]$ là phần nguyên của x).

2.2. a) Giả sử g có ngược trái là $g' : Y \to X$, f có ngược trái là $f' : Z \to Y$. Khi đó, ngược trái của $f \circ g$ là $g' \circ f' : Z \to X$.

b) Xét các ánh xạ:

$$f(n) = \left[\frac{n}{2}\right], \ g(n) = 2n$$

từ $\mathbb{Z}$ vào $\mathbb{Z}$. Khi đó $f \circ g(n) = n$ có ngược trái, song f không có ngược trái vì f không phải là đơn ánh.

2.3. a) $2.C_3^2$. b) 0.

2.4. Ký hiệu $f(x) = x^2$ thì ta có $f(\mathbb{N}) = f(\mathbb{Z})$ bằng tập các số chính phương,

$$f(\mathbb{Q}) = \left\{ \frac{p^2}{q^2} \mid (p,q) = 1; p, q \in \mathbb{Z} \right\}$$

và $f(\mathbb{C}) = \mathbb{C}$. Trong số đó chỉ có ánh xạ từ tập $\mathbb{N}$ lên chính nó là đơn ánh.

2.5. Ánh xạ ngược của ánh xạ f là:

$$f^{-1} : \mathbb{R} \to \mathbb{R}$$
$$x \mapsto \frac{2-x}{6}$$

2.6. Nếu $n = 0$ thì f là một song ánh. Nếu $n \geq 1$ thì f là một đơn ánh nhưng không là toàn ánh và do đó cũng không phải là song ánh.

2.7. Ta chỉ cần chứng minh f đơn ánh $\Leftrightarrow$ f toàn ánh. Thật vậy, giả sử $X = \{x_1, x_2, ..., x_n\}$, nếu f là đơn ánh thì ta có: $f(x_i) \neq f(x_j)$ với mọi $x_i \neq x_j$. Do đó:

$$\mathrm{Im}f = \{f(x_i) \mid x_i \in X\} \subset X,$$

đồng thời $|\mathrm{Im}f| = |X| = n$. Vậy f là toàn ánh.

Ngược lại, nếu f là toàn ánh và $x_i \neq x_j$ thì ta có $f(x_i) \neq f(x_j)$ (vì nếu không thì sẽ mâu thuẫn với giả thiết $f(X) = X$). Hay f là đơn ánh.

Ánh xạ $f : \mathbb{N} \to \mathbb{N}, x \mapsto 2x$ là đơn ánh mà không là toàn ánh. Còn ánh xạ: $f : \mathbb{N} \to \mathbb{N}, x \mapsto \left[\frac{x}{2}\right]$ là toán ánh mà không là đơn ánh.

2.8. a) Giả sử $y \in f(A) \setminus f(B)$. Do $y \in f(A)$ nên tồn tại $x \in A$ sao cho $y = f(x)$. Mặt khác do $f(x) = y \notin f(B)$ nên $x \notin B$. Vậy tồn tại $x \in A \setminus B$ sao cho $y = f(x) \in f(A \setminus B)$. Từ đó suy ra

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

Với ánh xạ $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ và $A = \{0; -1\}$, $B = \{1\}$ thì ta có: $A \setminus B = \{0; -1\}$ nên

$$f(A) \setminus f(B) = \{0, 1\} \setminus \{1\} = \{0\} \neq f(A \setminus B) = \{0; 1\}.$$

b) Ta còn phải chứng minh: $f(A \setminus B) \subset f(A) \setminus f(B)$. Thật vậy, lấy $y \in f(A \setminus B)$ khi đó tồn tại $x \in A \setminus B$ để $y = f(x)$ hay tồn tại $x \in A$ mà $x \notin B$ để $y = f(x)$.

Ta có $y = f(x) \in f(A)$ và $y = f(x) \notin f(B)$ (vì nếu $y = f(x) \in f(B)$ thì tồn tại $x' \in B$ để $f(x') = y$ và dĩ nhiên $x' \neq x$, điều này trái với giả thiết f là đơn ánh).

2.9. a) Giả sử $y \in f(A \cup B)$. Khi đó tồn tại $x \in A \cup B$ để $y = f(x)$. Vì $x \in A$ hoặc $x \in B$ nên $y = f(x) \in f(A)$ hoặc $y = f(x) \in f(B)$. Hay $y \in f(A) \cup f(B)$.

Ngược lại, giả sử $y \in f(A) \cup f(B)$ suy ra $y \in f(A)$ hoặc $y \in f(B)$. Do đó tồn tại $x \in A$ hoặc $x \in B$ để $y = f(x)$. Hay $y \in f(A \cup B)$.

c) Giả sử $x \in f^{-1}(C \cup D)$. Ta có: $f(x) \in C \cup D$, nghĩa là: $f(x) \in C$ hoặc $f(x) \in D$. Do đó $x \in f^{-1}(C)$ hoặc $x \in f^{-1}(D)$. Vậy $x \in f^{-1}(C) \cup f^{-1}(D)$.

Ngược lại, giả sử $x \in f^{-1}(C) \cup f^{-1}(D)$. Khi đó $x \in f^{-1}(C)$ hoặc $x \in f^{-1}(D)$ nên $f(x) \in C$ hoặc $f(x) \in D$. Do đó $f(x) \in C \cup D$ và suy ra $x \in f^{-1}(C \cup D)$.

Các đẳng thức và bao hàm thức còn lại được chứng minh tương tự.

2.11. a) Giả sử f là đơn ánh. Theo Bài tập 2.10 ta có:

$$f^{-1}(f(A)) \supset A.$$

Bây giờ ta chứng minh bao hàm thức ngược lại. Với $x \in f^{-1}(f(A))$ ta có $f(x) \in f(A)$. Suy ra tồn tại $a \in A$ sao cho $f(a) = f(x)$. Do giả thiết f là đơn ánh nên $x = a \in A$. Vậy $f^{-1}(f(A)) \subset A$.

Dảo lại, giả sử $A = f^{-1}(f(A))$ với mọi $A \subset X$ và f không là đơn ánh. Khi đó tồn tại hai phần tử phân biệt $x_1, x_2 \in X$ sao cho $f(x_1) = f(x_2)$. Xét $A = \{x_1\}$. Khi đó ta có:

$$f^{-1}(f(A)) = f^{-1}\{f(x_1)\} = \{x_1, x_2\} \neq A,$$

trái giả thiết. Vậy f là một đơn ánh.

b) Giả sử f là đơn ánh. Theo Bài tập 2.9 ta có

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

Bây giờ, với mọi $y \in f(A) \cap f(B)$ ta có $y \in f(A)$ và $y \in f(B)$ suy ra tồn tại $x_1 \in A$ để $f(x_1) = y$ và tồn tại $x_2 \in B$ để $f(x_2) = y$. Do f là

đơn ánh nên $x_1 = x_2 = x$. Vậy $x \in A \cap B$ và do đó $y = f(x) \in f(A \cap B)$.

Ngược lại, giả sử $f(A \cap B) = f(A) \cap f(B)$ với mọi $A, B \subset X$. Giả sử phản chứng rằng f không phải là đơn ánh. Khi đó tồn tại $x_1, x_2 \in X, x_1 \neq x_2$ sao cho

$$f(x_1) = f(x_2) = y.$$

Lấy $A = \{x_1\}, B = \{x_2\}$ thì ta có $f(A) = f(B) = \{y\}$. Suy ra

$$f(A) \cap f(B) = \{y\}.$$

Nhưng $A \cap B = \emptyset$ nên $f(A \cap B) = \emptyset$. Vậy $f(A \cap B) \neq f(A) \cap f(B)$, trái với giả thiết.

2.12. a) Giả sử $h = gf$ là một đơn ánh và $x_1, x_2 \in X$ sao cho $f(x_1) = f(x_2)$. Từ đó suy ra

$$h(x_1) = gf(x_1) = gf(x_2) = h(x_2).$$

Do h là đơn ánh nên $x_1 = x_2$. Vậy f là một đơn ánh.

Giả sử thêm f là toàn ánh và với $y_1, y_2 \in Y$ sao cho

$$g(y_1) = g(y_2) = z \in Z.$$

Do f là toàn ánh nên tồn tại $x_1, x_2 \in X$ sao cho $f(x_1) = y_1$ và $f(x_2) = y_2$. Suy ra:

$$h(x_1) = g(f(x_1)) = g(y_1) = g(y_2) = g(f(x_2)) = h(x_2).$$

Do h là đơn ánh nên $x_1 = x_2$. Vậy $y_1 = f(x_1) = f(x_2) = y_2$, nghĩa là g là đơn ánh.

b) Giả sử $h = gf$ là toàn ánh và z là một phần tử bất kỳ thuộc Z. Khi đó tồn tại $x \in X$ để $h(x) = z$. Đặt $y = f(x) \in Y$, khi đó

$$g(y) = g(f(x)) = gf(x) = h(x) = z.$$

Vậy g là toàn ánh.

Nếu giả thiết thêm g là một đơn ánh và y là một phần tử tùy ý thuộc Y thì ta có $g(y) = z \in Z$. Do h là toàn ánh nên tồn tại $x \in X$ để

$$h(x) = gf(x) = g(f(x)) = z.$$

Hay $g(y) = g(f(x))$. Lại do g là đơn ánh nên $y = f(x)$. Vậy f là một toàn ánh.

2.13. Theo Bài tập 2.12, do fgf là đơn ánh nên f là đơn ánh. Lại do fgf là toàn ánh nên f là toàn ánh. Vậy f là song ánh. Còn

$$g = f^{-1}(fgf)f^{-1}$$

là tích của ba song ánh nên g là song ánh.

2.14. Với mỗi $A \subset X$ ta xét ánh xạ:

$$\begin{array}{rccc} \delta_A : & X & \to & Y \\ & x & \mapsto & \begin{cases} 1 \text{ nếu } x \in A \\ 0 \text{ nếu } x \notin A \end{cases} \end{array}$$

Như vậy, $\mathrm{Hom}(X, Y) = \{\delta_A \mid A \in P(X)\}$. Khi đó, ánh xạ:

$$\begin{array}{rccc} f : & P(X) & \to & \mathrm{Hom}(X, Y) \\ & A & \mapsto & \delta_A \end{array}$$

là một song ánh.

2.15. a) $\Rightarrow$ b). Giả sử f là đơn ánh và $fg = fg'$. Khi đó với mọi $v \in V$ ta có $fg(v) = fg'(v)$ hay $f(g(v)) = f(g'(v))$. Do f là đơn ánh nên $g(v) = g'(v)$. Vậy $g = g'$.

b) $\Rightarrow$ a). Giả sử ngược lại rằng f không phải là một đơn ánh. Khi đó tồn tại hai phần tử $x_1, x_2 \in X$, $x_1 \neq x_2$ sao cho $f(x_1) = f(x_2)$. Xét tập hợp $V = \{1, 2\}$ và hai ánh xạ:

$$\begin{array}{rccc} g : & V & \to & X \\ & 1 & \mapsto & x_1 \\ & 2 & \mapsto & x_2 \end{array} \qquad \begin{array}{rccc} g' : & V & \to & X \\ & 1 & \mapsto & x_1 \\ & 2 & \mapsto & x_1 \end{array}$$

Rõ ràng ta có $fg = fg'$ nhưng $g \neq g'$. Điều này trái với giả thiết. Vậy f là đơn ánh.

2.16. a) $\Rightarrow$ b). Giả sử f là một toàn ánh và $hf = h'f$. Khi đó với $y \in Y$ tùy ý, tồn tại $x \in X$ sao cho $f(x) = y$. Do đó:

$$h(y) = h[f(x)] = h'[f(x)] = h'(y).$$

Vậy $h = h'$.

b) $\Rightarrow$ a). Giả sử ngược lại rằng f không phải là một toàn ánh. Khi đó tồn tại $y_0 \in Y$ sao cho $f^{-1}(y_0) = \emptyset$. Xét tập $Z = \{0, 1\}$ và hai ánh xạ:

$$\begin{array}{rccc} h : & Y & \to & Z \\ & y & \mapsto & 0 \end{array}$$

$$h' : Y \to Z$$
$$y \mapsto \begin{cases} 0 \text{ nếu } y \neq y_1 \\ 1 \text{ nếu } y = y_0 \end{cases}$$

Rõ ràng ta có $hf = h'f$ nhưng $h \neq h'$. Điều này mâu thuẫn với giả thiết. Vậy f là toàn ánh.

2.17. Ta sẽ chứng minh khẳng định b).

Giả sử $y \in f(\bigcap_{i\in I} A_i)$. Khi đó tồn tại $x \in \bigcap_{i\in I} A_i$ sao cho $y = f(x)$ hay tồn tại $x \in A_i \ \forall\, i \in I$ để $y = f(x)$. Do đó $y = f(x) \in A_i \ \forall\, i \in I$ hay

$$f(x) \in \bigcap_{i\in I} f(A_i).$$

Các khẳng định a), c) và d) được chứng minh tương tự.

3. Quan hệ hai ngôi

3.1. a) Phản xạ, đối xứng, bắc cầu nhưng không phản đối xứng.
b) Đối xứng nhưng không phản xạ, không phản đối xứng và không bắc cầu.
c) Phản xạ, phản đối xứng, bắc cầu nhưng không đối xứng.
d) Phản đối xứng và bắc cầu nhưng không phản xạ và không đối xứng.
e) Đối xứng và bắc cầu nhưng không phản xạ và không phản đối xứng.

3.2. a) Quan hệ $\boldsymbol{\rho}$ là đối xứng nhưng không bắc cầu.
b) Quan hệ $\boldsymbol{\delta}$ vừa là đối xứng vừa là bắc cầu.

3.3. a) Ta dễ thử lại được S là một quan hệ tương đương trên $\mathbb{R}^2$. Khi đó, mỗi lớp tương đương theo quan hệ S là:

$$\overline{(a,b)} = \{(x,y) \mid x = a\} = \{(a,y) \mid y \in \mathbb{R}\}.$$

Đấy chính là tập hợp các điểm trong mặt phẳng có hoành độ $x = a$ hay đó là đường thẳng có phương trình $x = a$.

b) Ánh xạ $f : \mathbb{R}^2/S \to \mathbb{R}$, $\overline{(a,b)} \mapsto a$ là một song ánh.

3.4. a) Với mọi $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$ ta có: $ab = ba$ nên $(a,b)\mathfrak{R}(a,b)$.
Giả sử $(a,b)\mathfrak{R}(c,d)$, nghĩa là $ad = bc$, suy ra $cb = da$. Vậy $(c,d)\mathfrak{R}(a,b)$.

Cuối cùng, giả sử $(a,b)\mathfrak{R}(c,d)$ và $(c,d)\mathfrak{R}(e,f)$, nghĩa là $ad = bc$ và $cf = de$ suy ra $adf = bcf$ và $cfb = deb$. Do đó: $adf = deb$. Vậy $af = eb$ hay $(a,b)\mathfrak{R}(e,f)$.

b) Ánh xạ $f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{N}^*/\mathfrak{R}$
$\frac{p}{q} \mapsto \overline{(p,q)}$
là một song ánh.

3.5. Dựa vào định nghĩa ta có điều phải chứng minh.

3.6. Xét quy tắc $g : X/E \to S$ như sau: $g(\overline{x}) = f(x)$. Khi đó quy tắc này không phụ thuộc vào đại diện x của lớp $\overline{x}$. Thật vậy, nếu $\overline{x} = \overline{x'}$ thì xEx' hay $f(x) = f(x')$ nên

$$g(\overline{x}) = f(x) = f(x') = g(\overline{x'}).$$

Vậy g được xác định như trên là một ánh xạ.

Hơn nữa, với mọi $x \in X$: $g(p(x)) = g(\overline{x}) = f(x)$ hay $f = g \circ p$.

Giả sử còn có ánh xạ $g' : X/E \to S$ thoả mãn điều kiện $f = g' \circ p$ thì suy ra $g \circ p = g' \circ p$. Do p là toàn ánh nên $g = g'$. Hay ánh xạ g xác định như trên là duy nhất.

Tiếp theo, ta sẽ chỉ ra g là một đơn ánh. Thật vậy, nếu $g(\overline{x}) = g(\overline{x'})$ thì $f(x) = f(x')$, suy ra $\overline{x} = \overline{x'}$.

Hơn nữa, do f là toàn ánh nên với mọi $y \in S$ đều tồn tại $x \in X$ sao cho $f(x) = y$. Suy ra tồn tại $\overline{x} \in X/E$ sao cho $g(\overline{x}) = f(x) = y$. Vậy g là một toàn ánh và do đó g là một song ánh.

3.7. a) Dễ thấy $\mathfrak{R}$ có tính chất bắc cầu.

Giả sử ta có $x\mathfrak{R}y$, nghĩa là tồn tại $x_1 = x, x_2, ..., x_n = y$ sao cho

$$x_1 T x_2, x_2 T x_3, ..., x_{n-1} T x_n.$$

Do T có tính chất đối xứng nên ta có:

$$x_n T x_{n-1}, ..., x_3 T x_2, x_2 T x_1$$

hay $y\mathfrak{R}x$. Vậy $\mathfrak{R}$ có tính chất đối xứng.

Cuối cùng, giả sử $x\mathfrak{R}y$ và $y\mathfrak{R}z$. Khi đó tồn tại $x_1 = x, x_2, ..., x_n = y$ và $y_1 = y, y_2, ..., y_m = z$ sao cho

$$x_1 T x_2, x_2 T x_3, ..., x_{n-1} T x_n$$

và

$$y_1 T y_2, y_2 T y_3, ..., y_{m-1} T y_m.$$

Vậy ta có $x_1 = x, x_2, ..., x_n, y_2, ..., y_m = z$ thỏa mãn

$$x_1 T x_2, x_2 T x_3, ..., x_{n-1} T x_n, x_n T y_2, ..., y_{m-1} T y_m.$$

Suy ra $x \mathfrak{R} z$ hay $\mathfrak{R}$ có tính chất bắc cầu.

Vậy $\mathfrak{R}$ là quan hệ tương đương. Hơn nữa, theo cách xây dựng của $\mathfrak{R}$ thì ta có: $T \subset \mathfrak{R}$.

b) Giả sử $H \subset S^2$ là một quan hệ tương đương sao cho $T \subset H$ và giả sử $(x, y) \in \mathfrak{R}$, nghĩa là tồn tại $x_1 = x, x_2, ..., x_n = y$ sao cho

$$x_1 T x_2, x_2 T x_3, ..., x_{n-1} T x_n.$$

Do $T \subset H$ nên ta cũng có

$$x_1 H x_2, x_2 H x_3, ..., x_{n-1} H x_n.$$

Lại từ tính chất bắc cầu của H suy ra xHy hay $(x, y) \in H$. Vậy $\mathfrak{R} \subset H$.

3.8. *Sự tồn tại.* Trên X, xét quan hệ S như sau: xSy khi và chỉ khi $x = y$. Dễ thấy S vừa là quan hệ tương đương vừa là quan hệ thứ tự.

Tính duy nhất. Giả sử trên X còn quan hệ $T \neq S$ mà vừa là quan hệ tương đương vừa là quan hệ thứ tự. Khi đó tồn tại $x, y \in X$, $x \neq y$ sao cho xTy. Do tính chất đối xứng của T nên yTx. Kết hợp với tính phản xứng của T suy ra $x = y$, điều này là mâu thuẫn. Vậy quan hệ S xác định như trên vừa là quan hệ tương đương vừa là quan hệ thứ tự duy nhất.

3.9. Giải tương tự Bài tập 3.8.

3.10. Dễ chứng minh $\mathfrak{R}$ là một quan hệ thứ tự dựa vào tính đơn ánh của f.

Mặt khác, với mọi $x, y \in X$ ta có $f(x), f(y) \in \mathbb{N}$. Do $(\mathbb{N}, \leq)$ là tập sắp thứ tự toàn phần nên $f(x) \leq f(y)$ hoặc $f(y) \leq f(x)$. Nghĩa là $x \mathfrak{R} y$ hoặc $y \mathfrak{R} x$. Vậy $\mathfrak{R}$ là một quan hệ thứ tự toàn phần.

3.11. a) Dễ thấy $\mathfrak{R}$ có tính chất phản xạ.

Giả sử $f \mathfrak{R} g$ và $g \mathfrak{R} f$, nghĩa là g là kéo dài của f và f là kéo dài của g nên $f = g$.

Cuối cùng, giả sử $f \mathfrak{R} g$ và $g \mathfrak{R} h$. Chẳng hạn: $f : A \to Y$, $g : B \to Y$

với $A \subset B$ và $g\big|_A = f$; $h : C \to Y$ với $B \subset C$ và $h\big|_B = g$. Khi đó $h\big|_A = g\big|_A = f$ nên h là kéo dài của f hay $f \mathfrak{R} h$.

Vậy $\mathfrak{R}$ là một quan hệ thứ tự.

b) Giả sử $S \neq \emptyset$.

Nếu $Y = \{y\}$ là tập chỉ có một phần tử thì $\Phi(S, Y)$ có phần tử bé nhất là ánh xạ $\emptyset$, phần tử lớn nhất là ánh xạ:

$$\begin{array}{rccc} f: & S & \to & Y \\ & x & \mapsto & y \end{array}$$

Nếu Y có nhiều hơn một phần tử thì mỗi ánh xạ $f : S \to Y$ đều là phần tử tối đại. Mỗi ánh xạ đi từ tập $\{x\}$ đến Y đều là phần tử tối tiểu, với x là phần tử tùy ý của X và không kể đến ánh xạ rỗng trong $\Phi(S, Y)$.

3.12. Giả sử $a \in S$ là phần tử bé nhất của tập sắp thứ tự S, nghĩa là $a \leq x$ với mọi $x \in S$. Giả sử rằng có phần tử $a' \in S$ để $a' \leq a$ thì kết hợp với $a \leq a'$ suy ra $a = a'$. Vậy a là phần tử tối tiểu. Hơn nữa, nếu a_1 và a_2 là hai phần tử bé nhất của S thì ta có các quan hệ: $a_1 \leq a_2$ và $a_2 \leq a_1$ suy ra $a_1 = a_2$.

Đối với phần tử tối đại, ta chứng minh tương tự.

3.13. Giả sử S sắp thứ tự tốt. Với hai phần tử bất kỳ $x, y \in S$, tập $\{x, y\}$ có phần tử bé nhất. Như vậy nếu x là phần tử bé nhất thì $x \leq y$ hoặc nếu y là phần tử bé nhất thì $y \leq x$. Nghĩa là cặp x, y luôn so sánh được.

Vậy S là tập sắp thứ tự toàn phần.

4. Số nguyên

4.1. Ta có

$$(mq + np) - (mp + nq) = (m - n).(q - p) \vdots (m - n)$$

Kết hợp với giả thiết ta suy ra: $(mq + np) \vdots (m - n)$.

4.2. Ta có: $(ac - bd) - (a - b)c = b(c - d)$ nên n là ước của $b(c - d)$.

Mặt khác, $(a - b, b) = (a, b) = 1$. Do n là ước của $a - b$ nên ta có $(n, b) = 1$. Vậy $b(c - d) \vdots n$ suy ra $(c - d) \vdots n$.

4.3. Giả sử ngược lại rằng cả ba số a, b, c đều không chia hết cho 3. Khi đó:

Nếu cả ba số có dạng $3k+1$ thì $a^3+b^3+c^3 = 9A+3$ không chia hết cho 9.

Nếu hai số có dạng $3k+1$ và một số có dạng $3k-1$ thì $a^3+b^3+c^3 = 9A+1$ không chia hết cho 9.

Nếu hai số có dạng $3k-1$ và một số có dạng $3k+1$ thì $a^3+b^3+c^3 = 9A-1$ không chia hết cho 9.

Nếu cả ba số có dạng $3k-1$ thì $a^3+b^3+c^3 = 9A-3$ không chia hết cho 9.

Vậy không thể xảy ra các trường hợp trên hay ít nhất một trong ba số a, b, c phải chia hết cho 3.

4.4. a) Nếu $x = 3k,\ k \in \mathbb{Z}$ thì $x^2+1 = 9k+1$ không chia hết cho 3.

Nếu $x = 3k \pm 1$ thì $x^2+1 = 3A+2$ không chia hết cho 3.

Vậy không có cặp số nguyên x, y nào thỏa mãn $x^2+1 = 3y$.

b) Xét các trường hợp $x = 5k, x = 5k \pm 1$ và $x = 5k \pm 2$ tương tự như câu a).

4.5. Ta chứng minh mệnh đề bằng phép quy nạp theo n.

Với $n = 1$ ta có 2 chia hết cho 2^1 nên mệnh đề đúng.

Giả sử mệnh đề đúng với $n = k \geq 1$. Khi đó, với $n = k+1$ ta có:

$$\begin{aligned}&(n+1)(n+2)...(n+n)\\ &= (k+2)(k+3)...(k+k+1).2(k+1)\\ &= 2[(k+1)(k+2)...(k+k)](2k+1)\end{aligned}$$

chia hết cho 2^{k+1}.

4.6. Xét các số n có dạng $n = 3^k$ $(k = 0, 1, ...)$. Ta sẽ chứng minh 2^n+1 chia hết cho n bằng quy nạp.

Thật vậy, với $k = 0$ thì khẳng định đúng vì $2^{3^0}+1$ chia hết cho 3^0. Giả sử khẳng định trên đúng với k, nghĩa là: $2^{3^k}+1 = 3^k.A$ với $A \in \mathbb{Z}$. Khi đó

$$\begin{aligned}2^{3^{k+1}}+1 &= (2^{3^k})^3+1 = (3^k.A-1)^3+1\\ &= 3^{k+1}(A^3.3^{2k-1} - A^2 3^k + A)\end{aligned}$$

chia hết cho $n = 3^{k+1}$. Ta có điều phải chứng minh.

4.7. Giả sử ngược lại rằng tồn tại số nguyên b sao cho $P(b) = 0$. Khi đó ta có:

$$P(x) = (x-b)Q(x)$$

với $Q(x)$ là đa thức có hệ số nguyên. Đặt $b = aq + r,\ 1 \leq r < a$, ta có:

$$P(r) = (r - b)Q(r) = -aqQ(r)$$

nên $P(r)$ chia hết cho a, trái với giả thiết. Vậy ta có điều phải chứng minh.

4.8. Do $(a, c) = 1$ nên tồn tại hai số $x, y \in \mathbb{Z}$ sao cho $ax + cy = 1$. Suy ra

$$axm + cym = m.$$

Mặt khác, $m = aa_1 = cc_1$ nên ta có:

$$axcc_1 + cyaa_1 = m$$

hay $ac(xc_1 + ya_1) = m$. Vậy $ac|m$.

4.9. Giả sử $(b, c) = d$. Khi đó tồn tại $x, y \in \mathbb{Z}$ sao cho $bx + cy = d$, suy ra

$$(ab)x + (ac)y = ad.$$

Vậy mọi ước chung của ab và ac đều là ước của ad.

Mặt khác, do $d|b$ và $d|c$ nên $ad|ab$ và $ad|ac$ hay ad là ước chung của ab và ac.

Vậy $ad = (ac, ab)$.

4.11. Ta có:

$$8a + 13b = 2(3a + 5b) + (2a + 3b).$$
$$3a + 5b = 1(2a + 3b) + (a + 2b).$$
$$2a + 3b = 2(a + 2b) - b.$$

Vậy $(8a + 13b, 3a + 5b) = (3a + 5b, 2a + 3b) = (2a + 3b, a + 2b)$
$= (a + 2b, b) = (a, b)$.

4.12. Ta có: $a + b = (a - b) + 2b$ và $a - b = -(a + b) + 2a$ nên

$$m = (a + b, a - b) = (a - b, 2b) = (a + b, 2a)$$

suy ra m là ước chung của $2a$ và $2b$ hay m là ước của $2d$.

Mặt khác, d là ước chung của $a + b$ và $a - b$ nên d là ước của m. Vậy $m = d$ hoặc $m = 2d$.

4.13. a) Ta có: $a = 21m + 4 = (14m + 3) + (7m + 1)$.

$$b = 14m + 3 = 2(7m + 1) + 1.$$

Do đó: $(a, b) = (14m + 3, 7m + 1) = (7m + 1, 1) = 1$.

b) Ta có: $b = m.a + (m^2 + 1)$.

$a = m(m^2 + 1) + m.$

$m^2 + 1 = m.m + 1.$

Do đó: $(a, b) = (m^3 + 2m, m^2 + 1) = (m^2 + 1, m) = (m, 1) = 1.$

c) Ta có: $a = m(mn + 1) + m$ nên $(a, b) = (mn + 1, m) = (m, 1) = 1.$

4.14. *Điều kiện cần:* Giả sử $(2^p - 1, 2^q - 1) = 1$ và $k = (p, q)$. Đặt $p = ku$, $q = kv$. Khi đó:

$$2^p - 1 = (2^k)^u - 1 \vdots 2^k - 1.$$

Tương tự, ta cũng có: $(2^p - 1) \vdots (2^k - 1)$.

Như vậy, $2^k - 1$ là một ước chung của $2^p - 1$ và $2^q - 1$. Kết hợp với giả thiết ta suy ra $2^k - 1 = 1$, nghĩa là $k = 1$. Vậy p và q nguyên tố cùng nhau.

Điều kiện đủ: Giả sử $(p, q) = 1$. Khi đó tồn tại các số nguyên s, t sao cho $ps + qt = 1$. Gọi $d = (2^p - 1, 2^q - 1)$.

Xét trường hợp $s > 0$. Khi đó $t < 0$. Đặt $v = -t > 0$. Suy ra $ps - qv = 1$. Ta có:

$$2^{ps} - 1 \vdots 2^p - 1 \Rightarrow 2^{ps} - 1 \vdots d.$$

Tương tự ta có: $2^{qv} - 1 \vdots d$. Từ đó suy ra:

$$(2^{ps} - 1) - (2^{qv} - 1) \vdots d$$

nghĩa là:

$$2^{qv}(2^{ps-qv} - 1) \vdots d.$$

Kết hợp với đẳng thức $ps - qv = 1$ ta suy ra: $2^{qv} \vdots d$.

Mặt khác do $2^p - 1$ là một số lẻ nên d lẻ. Từ đó suy ra $d = 1$.

Trường hợp $s < 0, t > 0$ được xét tương tự. Tóm lại ta có:

$$(2^p - 1, 2^q - 1) = 1.$$

4.15. Trước hết, ta chứng minh bằng quy nạp theo n khẳng định sau:

$$(a^m - 1, a^n - 1) = a^{(m,n)} - 1 \qquad (*)$$

với mọi $m, n \in \mathbb{N},\ m \neq 0$.
Thật vậy, với $n = 0$ thì $a^n - 1 = 0$ và $(m, n) = m$ nên:

$$(a^m - 1, a^n - 1) = a^m - 1 = a^{(m,n)} - 1.$$

Vậy đẳng thức (*) đúng với $n = 0$.

Giả sử đẳng thức (*) đúng với mọi $0 \leq k < n,\ n \neq 0$. Theo định lý về phép chia với dư ta có:

$$m = nq + r,\ q \in \mathbb{N} \text{ và } 0 \leq r < n.$$

Nếu $q = 0$ thì $a^{nq} - 1 = 0$, còn nếu $q \geq 1$ thì:

$$a^{nq} - 1 = (a^n - 1)(a^{n(q-1)} + ... + a^n + 1).$$

Do đó $a^{nq} - 1$ luôn chia hết cho $a^n - 1$.
Ta có: $a^m - 1 = a^{nq+r} - 1 = a^r.a^{nq} - 1 = a^r(a^{nq} - 1) + (a^r - 1)$.
Do $r < n$ nên theo giả thiết quy nạp ta có:

$$(a^r - 1, a^n - 1) = a^{(r,n)} - 1.$$

Mặt khác, từ $m = nq + r$ suy ra $(m, n) = (r, n)$.
Vậy $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$, nghĩa là khẳng định (*) đúng với mọi cặp số tự nhiên m, n.

Bây giờ áp dụng đẳng thức (*) và giả thiết $(m, n) = 1$ ta có:

$$(a^m - 1, a^n - 1) = a - 1.$$

Từ đó: $a^m - 1 = (a - 1).A$ và $a^n - 1 = (a - 1).B$ với $(A, B) = 1$.
Ta cũng có: $a^{mn} - 1 = (a - 1).C$ và $(a^{mn} - 1) \vdots (a^n - 1)$ nên

$$(a - 1).C \vdots (a - 1).A \Rightarrow C \vdots A$$

Tương tự, ta có: $C \vdots B$. Do $(A, B) = 1$ nên $C \vdots AB$.
Suy ra: $(a-1)^2.C \vdots (a-1)^2AB \Rightarrow (a-1)(a^{mn}-1) \vdots (a^m-1)(a^n-1)$.

4.16. Không mất tính tổng quát, ta giả sử $a > b$. Đặt $s_a = 5^a + 7^a$.

Nếu $a \geq 2b$ ta có: $s_a = s_b s_{a-b} - 5^b 7^b s_{a-2b}$. Do đó:

$$(s_a, s_b) = (s_b, s_{a-2b}).$$

Tương tự, nếu $b < a < 2b$ thì ta có: $(s_a, s_b) = (s_b, s_{2b-a})$.

Vậy từ thuật toán Ơclit ta suy ra nếu $a+b$ là số chẵn thì $(s_a, s_b) = (s_1, s_1) = 12$, còn nếu $a + b$ là số lẻ thì $(s_a, s_b) = (s_0, s_1) = 2$.

4.17. a) Nếu $n = 0$ thì $2^n - 1 = 0$. Nếu $n > 0$ thì:

$$2^n + 1 = (2^n - 1) + 2.$$

Do đó $(2^n + 1, 2^n - 1) = (2^n - 1, 2) = 1$.
Suy ra: $[2^n + 1, 2^n - 1] = (2^n + 1)(2^n - 1) = 4^n - 1$.

b) Trước hết, ta có: $(a, a + 2) = \begin{cases} 1 \text{ nếu } a \text{ là số lẻ} \\ 2 \text{ nếu } a \text{ là số chẵn} \end{cases}$

và $A = [a, a + 2] = [|a|, |a + 2|] = \dfrac{|a(a + 2)|}{(a, a + 2)}$

Do đó $A = |a(a + 2)|$ nếu a là số lẻ và $A = \dfrac{1}{2}|a(a + 2)|$ nếu a là số chẵn.

4.18. Giả sử $a, a + 1, a + 2$ là ba số nguyên liên tiếp. Trước hết, ta nhận xét rằng:

$$(a(a + 2), a + 1) = 1.$$

Thật vậy từ đẳng thức: $a(a + 2) = a(a + 1) + a$ ta suy ra:

$$(a(a + 2), a + 1) = (a + 1, a) = (a, 1) = 1.$$

Bây giờ tuỳ theo tính chẵn lẻ của a, áp dụng Bài tập 4.17b) ta có:

Nếu a là số lẻ thì:

$$[a, a + 1, a + 2] = [[a, a + 2], a + 1] =$$

$$= [|a(a + 2)|, a + 1] = |a(a + 1)(a + 2)|.$$

Nếu a là số chẵn thì

$$[a, a + 1, a + 2] = [[a, a + 2], a + 1]$$

$$\left[\frac{1}{2}|a(a + 2)|, a + 1\right] = \frac{1}{2}|a(a + 1)(a + 2)|$$

4.19. Gọi $d = (a, b)$ ta có $a = da_1$, $b = db_1$ với $(a_1, b_1) = 1$. Khi đó:

$$(a + b, m) = (da_1 + db_1, da_1b_1) = d(a_1 + b_1, a_1b_1).$$

Ta có: $(a_1 + b_1, a_1) = (a_1, b_1) = 1$ và $(a_1 + b_1, b_1) = (a_1, b_1) = 1$ nên $(a_1 + b_1, a_1 b_1) = 1$. Từ đó suy ra:

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

4.20. Ta có D chia hết M_i và M_i chia hết M với $i = 1, 2, ..., n$ do đó D chia hết M. Đặt $q = \dfrac{M}{D}$ ta có:

$$M_i = Dq_i \Rightarrow a_i D q_i = a_i M_i = M \Rightarrow a_i q_i = \frac{M}{D} = q.$$

Suy ra q chia hết cho a_i với mọi $i = 1, 2, ..., n$.

Giả sử m là một bội chung của các a_i $(i = 1, 2, ..., n)$. Đặt $m = a_i r_i$ ta có: $mM_i = r_i a_i M_i = r_i M$. Do đó M chia hết mM_i. Suy ra:

$$M \mid (mM_1, ..., mM_n) \Rightarrow M \mid m(M_1, ..., M_n) \Rightarrow M \mid mD.$$

Từ đó $q = \dfrac{M}{D}$ chia hết m. Như vậy $q = \dfrac{M}{D}$ là một bội chung của các a_i và mọi bội chung khác của các a_i đều là bội của q. Điều đó chứng tỏ

$$q = \frac{M}{D} = [a_1, a_2, ..., a_n].$$

4.21. a) Ta chứng minh $(n!)^k$ là ước của $(nk)!$ bằng quy nạp theo k.

Với $k = 1$ mệnh đề đúng.

Giả sử $(n!)^k$ là ước của $(nk)!$. Khi đó ta có:

$$C^n_{n(k+1)} = \frac{(n(k+1))!}{n!(nk)!} \in \mathbb{Z} \Rightarrow (n(k+1))! \vdots n!(nk)!$$

Theo giả thiết quy nạp, ta có: $(nk)! \vdots (n!)^k$ nên:

$$(n(k+1))! \vdots n!(n!)^k = (n!)^{k+1}$$

Hoàn toàn tương tự, ta chứng minh được $(k!)^n$ là ước của $(nk)!$.

b) Theo câu a) ta có $(nk)!$ là một bội chung của $(n!)^k$ và $(k!)^n$. Do đó $(nk)!$ là một bội của $[(n!)^k, (k!)^n]$.

4.22. Do p là một số nguyên tố lớn hơn 3 nên p có dạng $p = 3k \pm 1$.

Nếu $p = 3k + 1$ thì $2p + 1 = 6k + 3 = 3(2k + 1)$ không phải là một

số nguyên tố nên trường hợp này không thể xảy ra.

Nếu $p = 3k - 1$, $k \geq 2$ thì $4p + 1 = 12k - 3 = 3(4k - 1)$. Do $4k - 1 \geq 7$ nên $4p + 1$ là hợp số.

4.23. Nếu $p = 3$ thì $p + 4 = 7$, $p + 8 = 11$ đều là những số nguyên tố.

Nếu $p = 3k + 1$ thì $p + 8 = 3k + 9 = 3(k + 3)$ là hợp số.

Nếu $p = 3k - 1$ thì $p + 4 = 3k + 1 = 3(k + 1)$ là hợp số.

Vậy $p = 3$ là số nguyên tố duy nhất phải tìm.

4.24. Ta sẽ chứng minh rằng nếu $a = 4k^4$ với k là một số nguyên dương lớn hơn 1 thì với mọi số nguyên dương n, $n^4 + a$ luôn là một hợp số. Thật vậy,

$$n^4 + a = n^4 + 4k^4 = n^4 + 4n^2k^2 + 4k^4 - 4n^2k^2$$
$$= (n^2 + 2k^2)^2 - (2nk)^2 = (n^2 + 2nk + 2k^2)(n^2 - 2nk + 2k^2).$$

Trong đó: $n^2 + 2nk + 2k^2 = (n + k)^2 + k^2 > k^2 > 1$

$$n^2 - 2nk + 2k^2 = (n - k)^2 + k^2 \geq k^2 > 1$$

Suy ra: $n^4 + a$ là hợp số.

4.25. Giả sử $a = 4p + 1$ và $b = 4q + 1$. Khi đó:

$$ab = (4p + 1)(4q + 1) = 4(4pq + p + q) + 1.$$

Để chứng minh có vô số nguyên tố dạng $4m + 3$ ta giả sử ngược lại rằng chỉ có một số hữu hạn số nguyên tố dạng $4m + 3$ là:

$$p_1 = 3, p_2 = 7, ..., p_n.$$

Khi đó xét số: $a = 4p_1p_2...p_n - 1$. Nếu tất cả các ước nguyên tố của a đều có dạng $4k + 1$ thì theo trên a cũng có dạng đó, trái với giả thiết về a ($a = 4u - 1$). Bởi vậy a phải có một ước nguyên tố q có dạng $4k + 3$. Dĩ nhiên q không trùng với các p_i ($i = 1, 2, ..., n$) vì nếu q trùng với một trong các p_i thì q sẽ là ước của $1 = 4p_1p_2...p_n - a$, điều này là vô lý.

Lập luận trên đây chứng tỏ có vô số số nguyên tố dạng $4m + 3$.

Để giải bài toán đối với các số nguyên tố có dạng $6m + 5$, trước hết ta cũng chứng minh rằng tích của hai số có dạng $6m + 1$ lại là một số có dạng $6m + 1$. Sau đó lại lập luận như trường hợp các số nguyên tố dạng $4m + 3$.

4.26. Do $m > 2$ nên $m! - 1 > 4$. Gọi p là một ước nguyên tố của $a = m! - 1$ ta có: $p \leq a \Rightarrow p < m!$.

Bây giờ ta chứng tỏ $p > m$. Giả sử ngược lại rằng $p \leq m$. Khi đó

p là ước của $m!$ và do đó p là ước của $m! - (m! - 1) = 1$, điều này là vô lý. Vậy p là số nguyên tố thoả mãn $m < p < m!$.

4.27. Trước hết ta nhận xét rằng nếu n là một số chính phương thì trong sự phân tích tiêu chuẩn của n

$$n = p_1^{\alpha_1}.p_2^{\alpha_2}...p_k^{\alpha_k}$$

các số mũ α_i đều chẵn.

Giả sử $x^2 + y^2 + z^2 = u^2$.

Nếu trong ba số x, y, z chỉ có một số chẵn, giả sử là z thì ta có thể đặt:

$$x = 2m + 1,\ y = 2n + 1,\ z = 2k.$$

Khi đó:

$$u^2 = (2m + 1)^2 + (2n + 1)^2 + (2k)^2 = 2[2(m^2 + n^2 + k^2 + m + n) + 1]$$

Vậy trong sự phân tích tiêu chuẩn của u^2, 2 có luỹ thừa lẻ, mâu thuẫn với nhận xét trên.

Nếu cả ba số x, y, z đều là lẻ thì $x^2 + y^2 + z^2 = u^2$ sẽ có dạng $4q + 3$. Trong khi nếu u lẻ thì u có dạng $4k \pm 1$ nên u^2 có dạng $4q + 1$. Do đó trường hợp này cũng không thể xảy ra.

Vậy trong ba số x, y, z phải có ít nhất hai số chẵn.

Chương II

NHÓM-ĐỒNG CẤU NHÓM

1. Đại số hai ngôi

1.1. Phép toán đã cho có tính chất kết hợp, giao hoán và có đơn vị là ma trận không.

1.2. Phép toán đã cho có tính chất kết hợp, giao hoán và có đơn vị là 12.

1.3. Phép toán đã cho có tính chất kết hợp, giao hoán và có đơn vị là $0 + 0\sqrt{2}$.

1.4. Phép toán đã cho có tính chất kết hợp, giao hoán và có đơn vị là 0.

1.5. Phép toán không đóng trên tập hợp đã cho.

1.6. Phép toán đã cho có tính chất kết hợp, giao hoán và có đơn vị là 1.

1.7. Phép toán đã cho có tính chất kết hợp, giao hoán và có đơn vị là: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

1.8. A có hai phần tử nên $A \times A$ có 4 phần tử. Do đó có $2^4 = 16$ ánh xạ từ $A \times A$ vào A. Nghĩa là có 16 phép toán hai ngôi trên A.

1.9. Gọi e là phần tử đơn vị của đại số hai ngôi $(X, *)$. Khi đó trong đẳng thức

$$x * (y * z) = (x * z) * y \qquad (1)$$

thay x bởi e ta được

$$e * (y * z) = (e * z) * y \Rightarrow y * z = z * y$$

Điều đó chứng tỏ phép toán $*$ là giao hoán. Áp dụng luật này với (1) ta được

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

Luật kết hợp đã được chứng minh.

1.10. Phép toán $m*n = m-n$ không kết hợp cũng không giao hoán. Phép toán $m*n = m^2+n^2$ không kết hợp nhưng giao hoán. Phép toán $m*n = 2(m+n)$ không kết hợp nhưng giao hoán.

1.11. Các phép toán hai ngôi lần lượt được cho bởi các bảng sau đây:

a)

$\cdot$	a	b	c
a	a	b	c
b	b	b	b
c	c	c	c

b)

$\cdot$	a	b	c
a	a	b	c
b	a	b	c
c	c	c	c

c)

$\cdot$	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

Trong đó, để xây dựng phép toán hai ngôi có một đơn vị trái (giả sử là a) ta phải có:

$$aa = a,\ ab = b,\ ac = c.$$

Các hợp thành còn lại: ba, bb, bc, ca, cb, cc có thể được đặt tương ứng với a, b hoặc c sao cho chỉ có đúng một đơn vị trái a (chẳng hạn như bảng a)).

Tương tự, ta xây dựng được phép toán có đúng hai đơn vị trái. Trong trường hợp phép toán có ba đơn vị trái ta có duy nhất một cách xác định như bảng c).

1.12. a) Dễ chứng minh phép toán hai ngôi đã cho có tính kết hợp. Do đó X là nửa nhóm.

b) Giả sử a là phần tử bất kỳ của X. Ta có $ab = b$ với mọi $b \in X$ nên a là đơn vị trái của X. Vậy mọi phần tử của X đều là đơn vị trái.

c) Giả sử X có đơn vị là e. Khi đó, với mọi $x \in X$ ta có $ex = x$ và $xe = e$ nên $x = e$, nghĩa là X có một phần tử.

Phép toán hai ngôi trên X giao hoán khi và chỉ khi với mọi $a, b \in X$ ta có $ab = ba$ hay $b = a$, nghĩa là X chỉ có một phần tử.

Vậy nếu X chỉ có một phần tử thì X có đơn vị. Khi đó phép toán hai ngôi trên X cũng giao hoán.

1.14. a) Giả sử $y, y' \in f(A)$, suy ra tồn tại $x, x' \in A$ sao cho $y = f(x)$ và $y' = f(x')$. Do A là nửa nhóm con của X nên $xx' \in A$, suy ra

$$f(xx') = f(x)f(x') = yy' \in f(A).$$

b) Tương tự a).

1.15. a) Giả sử hợp thành $\beta \circ \alpha$ là một toàn cấu

$$\beta \circ \alpha : A \to C.$$

Lấy $c \in C$ tuỳ ý. Khi đó tồn tại $a \in A$ sao cho

$$(\beta \circ \alpha)a = c \text{ hay } \beta(\alpha a) = c$$

Điều này chứng tỏ β là toàn cấu.

b) Giả sử hợp thành $\beta \circ \alpha$ là một đơn cấu và giả sử $\alpha(a) = \alpha(a')$. Khi đó $(\beta \circ \alpha)a = (\beta \circ \alpha)a'$. Nhưng do $\beta \circ \alpha$ là một đơn cấu nên $a = a'$. Điều này chứng tỏ α là một đơn cấu.

1.16. a)⇒b). Trước hết $f(A) = \text{Im}f$ là nửa nhóm con của B. Do a) nên

$$e_B = f(e_A) \in f(A)$$

và do đó $f(A)$ là vị nhóm con của B.

b)⇒c). Giả sử $f(A)$ là vị nhóm con của B. Thế thì $e_B \in f(A)$. Đặt $U = f^{-1}(e_B)$ ta sẽ chứng minh U là tập con đóng. Thật vậy, với $x, y \in U$ ta có $f(x) = f(y) = e_B$. Từ đó

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

và do đó $xy \in U$.

Sau cùng ta chứng tỏ $e_A \in U$. Thật vậy $f(e_A)$ là đơn vị của nửa nhóm $f(A)$. Nhưng do đơn vị là duy nhất nên $e_B = f(e_A)$, hay $e_A \in U$, và do đó U là vị nhóm con của A.

c)⇒a). Do $U = f^{-1}(e_B)$ là vị nhóm con của A nên $e_A \in U$, và do đó

$$e_B = f(e_A).$$

Nếu $f^{-1}(e_B) = \{e_A\}$ thì không suy ra được f là đơn cấu. Chẳng hạn,

$$\begin{aligned} f : (\mathbb{N}, \cdot) &\to (\mathbb{N}, \cdot) \\ 1 &\mapsto 1 \\ n &\mapsto 0 \end{aligned}$$

là một đồng cấu vị nhóm thỏa mãn điều kiện $f^{-1}(e_N) = \{e_N\}$ song f không phải là một đơn cấu.

1.17. Giả sử trong nửa nhóm X ta có $ab = ba$. Trước hết ta chứng minh bằng quy nạp theo n rằng, $ab^n = b^n a$ với mọi số tự nhiên $n \geq 1$. Thật vậy, với $n = 1$ theo giả thiết ta có $ab = ba$. Giả sử với $m = n - 1$ ta có

$$ab^m = b^m a \text{ hay } ab^{n-1} = b^{n-1}a.$$

Khi đó

$$\begin{aligned} ab^n &= a(b^{n-1}b) = (ab^{n-1})b = (b^{n-1}a)b \\ &= b^{n-1}(ab) = b^{n-1}(ba) = (b^{n-1}b)a = b^n a. \end{aligned}$$

Bây giờ ta chứng minh $(ab)^n = a^n b^n$ bằng quy nạp theo n. Thật vậy, với $n = 1$ ta có $ab = ba$.
Giả sử với $m = n - 1$ ta có

$$(ab)^m = a^m b^m, \text{ hay } (ab)^{n-1} = a^{n-1}b^{n-1}.$$

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 $(ab)^2 = a^2b^2$ thì chưa thể suy ra $ab = ba$.
Ta sẽ chỉ ra một nửa nhóm có tính chất như vậy. Cho X là một tập tuỳ ý có nhiều hơn một phần tử, trên đó có xác định phép toán cho bởi $xy = x$ với mọi $x, y \in X$. Khi đó với $a, b \in X$ $a \neq b$ ta có

$$a^2 = a, b^2 = b, ab = a, a^2b^2 = a$$

nên $(ab)^2 = a^2b^2$ nhưng $ab = a \neq b = ba$.

2. Nhóm

2.1. $(M_n(\mathbb{R}) \setminus \{0\}, \cdot)$ không là nhóm vì ma trận với định thức bằng 0 không có nghịch đảo.

2.2. $(\{e, a\}, *)$ không là nhóm vì phần tử a không có nghịch đảo.

2.3. Phép toán $\circ$ trên $\mathbb{R}^*$ có đơn vị là 1, nghịch đảo của x là $\dfrac{1}{x}$ nếu $x > 0$ và là chính nó nếu $x < 0$. Do đó $(\mathbb{R}^*, \circ)$ là một nhóm.

Với mọi $x > 1, y < 0$ ta có $x \circ y \neq y \circ x$ nên phép toán $\circ$ không có tính chất giao hoán. Vậy $(\mathbb{R}^*, \circ)$ là nhóm không giao hoán.

2.4. Phép toán $*$ trên $\mathbb{Z}$ có đơn vị là 0, nghịch đảo của m là $-m$ nếu m chẵn và là chính nó nếu m lẻ. Do đó $(\mathbb{Z}, *)$ là một nhóm.

Với m là một số chẵn khác 0 và n là một số lẻ ta có $m * n \neq n * m$ nên phép toán $\circ$ không có tính chất giao hoán. Vậy $(\mathbb{Z}, *)$ là nhóm không giao hoán.

2.5. $\mathbb{Z}_6^* = \mathbb{Z}_6 \setminus \{\overline{0}\}$ không là nhóm vì phép toán đã cho không đóng trên $\mathbb{Z}_6^*$. Thật vậy, $\overline{2}.\overline{3} = \overline{2.3} = \overline{0} \notin \mathbb{Z}_6^*$.

2.6. Ta sẽ trang bị phép toán hai ngôi cho A để A trở thành một nhóm trong trường hợp A có 4 phần tử.

Chọn một phần tử làm phần tử đơn vị (chẳng hạn a). Khi đó:

$$aa = a,\ ab = ba = b,\ ac = ca = c,\ ad = da = d.$$

Để xác định được các hợp thành còn lại ta lưu ý rằng trên mỗi hàng hoặc mỗi cột của bảng phép toán đều có mặt đủ 4 phần tử a, c, b và d. Chẳng hạn ta có bảng phép toán:

$\cdot$	a	b	c	d
a	a	b	c	d
b	b	d	a	c
c	c	a	d	b
d	d	c	b	a

Tương tự ta lập được bảng phép toán trong trường hợp A có hai hoặc ba phần tử.

2.7. a) Dễ chứng minh phép toán hai ngôi đã cho có tính chất kết hợp. Do đó A là nửa nhóm. Mặt khác 1 là phần tử đơn vị của nửa nhóm A nên A là một vị nhóm.

b) A là nhóm khi và chỉ khi với mọi $a \in A$ đều tồn tại $b \in A$ sao cho $a * b = 1$, nghĩa là tồn tại k sao cho $ab = kn + 1$ hay $ab - kn = 1$, nghĩa là $(a, n) = 1$ với mọi $a < n$. Vậy A là nhóm khi và chỉ khi n là số nguyên tố.

2.8. Trước hết hãy thử lại rằng phép toán đã cho là kết hợp. Bây giờ ta sẽ chỉ ra rằng phép toán có đơn vị trái. Thật vậy, phần tử (x, y) là đơn vị trái khi và chỉ khi

$$(x, y)(a, b) = (a, b) \Leftrightarrow (xa, ya + b) = (a, b)$$

Từ đó suy ra $x = 1, y = 0$. Phần tử (x, y) là nghịch đảo trái của (a, b) khi và chỉ khi

$$(x, y)(a, b) = (1, 0) \Leftrightarrow (xa, ya + b) = (0, 1)$$

Từ đó suy ra $x = a^{-1}, y = -ba^{-1}$. Vậy G cùng với phép toán đã cho là một nhóm.

2.9. Giả sử rằng phần tử đơn vị của nhóm G là e. Ta có:

$(a_1a_2 \dots a_n)(a_n^{-1} \dots a_2^{-1}a_1^{-1}) = (a_1a_2 \dots a_{n-1})(a_na_n^{-1})(a_{n-1}^{-1} \dots a_2^{-1}a_1^{-1})$
$= \dots = e.$

Tương tự, $(a_n^{-1} \dots a_2^{-1}a_1^{-1})(a_1a_2 \dots a_n) = e$. Vậy

$$(a_1a_2 \dots a_n)^{-1} = a_n^{-1} \dots a_2^{-1}a_1^{-1}.$$

2.10. Từ tính kết hợp của phép nhân và định nghĩa tích bội k của $a^{-1}ba$ ta suy ra điều cần chứng minh.

2.11. Ta chứng minh bài toán bằng quy nạp theo i.

Với $i = 1$ thì khẳng định đúng. Giả sử khẳng định đúng với $i = k \geq 1$. Ta sẽ chứng minh khẳng định đúng với $i = k + 1$.

Thật vậy, theo giải thiết quy nạp ta có

$$b^kab^{-k} = a^{r^k}$$

Suy ra $(b^kab^{-k})^r = a^{r^{k+1}}$, hay $b^ka^rb^{-k} = a^{r^{k+1}}$. Theo giả thiết ta có $a^r = bab^{-1}$ nên

$$b^kbab^{-1}b^{-k} = a^{r^{k+1}} \Rightarrow b^{k+1}ab^{-k-1} = a^{r^{k+1}}$$

Vậy khẳng định đúng với $i = k + 1$.

2.12. Với $a, b \in G$ ta có:

$$(ab)^2 = e = e.e \Rightarrow abab = a^2b^2$$

Thực hiện phép giản ước bên trái cho a và bên phải cho b ta được $ab = ba$.

Ta cũng có thể biến đổi như sau. Với mọi $a \in X$ ta có $a^2 = e$. Từ đó $a = a^{-1}$. Bây giờ với a và b tuỳ ý thuộc G, ta có

$$(ab)^2 = ab.ab = e$$

Từ đó: $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$.

2.13. Giả sử ngược lại rằng $ab = ba$. Khi đó

$$a^4b = ba^5 \Rightarrow a^3ab = baa^4 \Rightarrow a^3ba = aba^4.$$

Lần lượt giản ước bên trái và bên phải cho a ta được $a^2b = ba^3$. Từ đó suy ra

$$aab = baa^2 \Rightarrow aba = aba^2 \Rightarrow b = ba \Rightarrow a = e.$$

Điều này mâu thuẫn với giả thiết. Vậy $ab \neq ba$.

2.14. Do $G \neq \emptyset$ nên tồn tại $a \in G$.

Theo giả thiết ta có: $aG = Ga = G$ nên $a \in Ga$, nghĩa là có phần tử $e \in G$ sao cho $a = ea$. Ta sẽ chứng minh $ex = x$ với mọi $x \in G$. Thật vậy, do $aG = G$ nên tồn tại $x_0 \in G$ sao cho $x = ax_0$, suy ra

$$ex = e(ax_0) = (ea)x_0 = ax_0 = x.$$

Giả sử $x \in G$ là một phần tử tuỳ ý, do $e \in Gx$ nên tồn tại phần tử $x' \in G$ sao cho $e = x'x$. Vậy ta có X là một nhóm.

Đảo lại, nếu G là một nhóm thì hiển nhiên ta có $aG = Ga = G$ với mọi $a \in G$.

2.16. Nếu G là một nhóm aben thì hiển nhiên ta có các điều kiện i), ii) và iii).

Ngược lại, nếu G thoả mãn các điều kiện i), ii) và iii) thì theo Bài tập 1.9, từ điều kiện i) suy ra phép toán đã cho có tính chất kết hợp và giao hoán. Kết hợp với điều kiện ii) và iii) suy ra G là một nhóm aben.

2.17. (i)⇒ (ii). Do G là nhóm aben nên $\forall a, b \in G$ ta có $ab = ba$. Từ đó

$$(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = a^2b^2$$

(ii)⇒(iii). Do G là nhóm nên nó thoả mãn luật giản ước:

$$\begin{aligned}&(ab)^2 = a^2b^2 \Leftrightarrow abab = aabb \Leftrightarrow ba = ab\\ &\Leftrightarrow baa^{-1}b^{-1} = aba^{-1}b^{-1} \Leftrightarrow e = (ab)a^{-1}b^{-1}\\ &\Leftrightarrow (ab)^{-1} = a^{-1}b^{-1}\end{aligned}$$

(iii)⇒(iv). Trước hết ta chứng minh được

$$ab^n = b^n a \ \forall n \in \mathbb{N}$$

bằng quy nạp theo n. Từ đó, cũng bằng phương pháp quy nạp ta chứng minh được

$$(ab)^n = a^n b^n$$

(iv)⇒(v). Hiển nhiên.

(v)⇒(i). Với mọi $a, b \in G$ ta có:

$$(ab)^n = a^n b^n, \ \ (ab)^{n+1} = a^{n+1}b^{n+1}, \ \ (ab)^{n+2} = a^{n+2}b^{n+2}.$$

Do G là nhóm nên G thỏa mãn luật giản ước. Suy ra

$$(ab)^{n+1} = (ab)^n(ab) = a^n b^n(ab) = a^{n+1}b^{n+1} \Leftrightarrow b^n a = ab^n$$

Hoàn toàn tương tự từ $(ab)^{n+2} = a^{n+2}b^{n+2}$ ta có

$$b^{n+1}a = ab^{n+1}$$

Từ đó,

$$ab^{n+1} = b^{n+1}a = b(b^n a) = b(ab^n) = (ba)b^n$$

Do đó, $ba = ab$.

Nếu thay giả thiết ba số n liên tiếp bởi hai số n liên tiếp thì khẳng định (v)⇒(i) không còn đúng nữa. Thật vậy, xét nhóm S_n các phép thế bậc n.

Ta có S_n là nhóm hữu hạn và các phần tử có cấp hữu hạn. Do đó tồn tại $m \in \mathbb{N}$ sao cho :

$$a^m = e \ \ \forall a \in S_n.$$

(có thể lấy m là bội số chung nhỏ nhất của tất cả các cấp của các phần tử của S_n).

Suy ra $(ab)^m = e = a^m b^m$ với $\forall a, b \in S_n$.
Mà $(ab)^{m+1} = (ab)(ab)^m = abe = ab$ và $a^{m+1}b^{m+1} = aebe = ab$ nên

$$(ab)^{m+1} = a^{m+1}b^{m+1} \quad \forall a, b \in S_n.$$

Rõ ràng S_n không là nhóm aben.

2.18. Áp dụng Bài tập 2.14 ta chỉ cần chứng minh $aG = G$ và $Ga = G$ với mọi $a \in G$.

Giả sử $G = \{x_1, x_2, ..., x_n\}$ gồm n phần tử. Với mỗi $x_i \in G$, tập hợp $x_iG = \{x_ix_1, x_ix_2, ..., x_ix_n\}$ là một bộ phận của G gồm n phần tử phân biệt vì nếu $k \neq l$ thì $x_k \neq x_l$ và do đó $x_ix_k \neq x_ix_l$ (do G thoả mãn luật giản ước). Vậy $x_iG = G$. Tương tự ta có $Gx_i = G$ với mọi $x_i \in G$.

3. Nhóm con

3.1. a) Trường hợp 1: Một trong hai phần tử có cấp vô hạn, chẳng hạn g. Giả sử ngược lại rằng g^{-1} có cấp hữu hạn. Khi đó tồn tại số tự nhiên n sao cho $(g^{-1})^n = e$. Từ đó suy ra $(g^n)^{-1} = e$ hay $g^n = e$, trái với giả thiết g có cấp vô hạn. Vậy g^{-1} cũng có cấp vô hạn.

Trường hợp 2: Giả sử g và g^{-1} có cấp hữu hạn tương ứng là n và m. Từ $g^n = e$ suy ra

$$(g^{-1})^n = (g^n)^{-1} = e^{-1} = e.$$

Vậy n chia hết cho m.

Tương tự, ta có m chia hết cho n. Từ đó suy ra $m = n$.
b) Trường hợp 1: Một trong hai phần tử có cấp vô hạn, chẳng hạn ab. Giả sử ngược lại rằng ba có cấp hữu hạn. Khi đó tồn tại số tự nhiên n sao cho $(ba)^n = e$. Từ đó suy ra

$$b(ab)^{n-1}a = e \Leftrightarrow (ab)^{n-1} = b^{-1}a^{-1} = (ab)^{-1} \Leftrightarrow (ab)^n = e,$$

trái với giả thiết ab có cấp vô hạn. Vậy ba cũng có cấp vô hạn.

Trường hợp 2: Giả sử ab và ba cùng có cấp hữu hạn tương ứng là n và m. Khi đó từ $(ba)^m = e$ lập luận tương tự trường hợp 1 ta được $(ab)^m = e$, hay m chia hết cho n.

Tương tự, ta được n chia hết cho m. Vậy $n = m$.

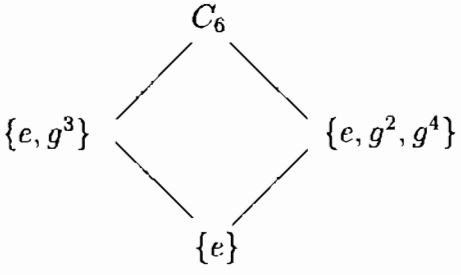
3.2. Ta có:

$$A_a^n = \begin{bmatrix} a^n & 0 & \cdots & 0 \\ 0 & a^n & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & a^n \end{bmatrix}.$$

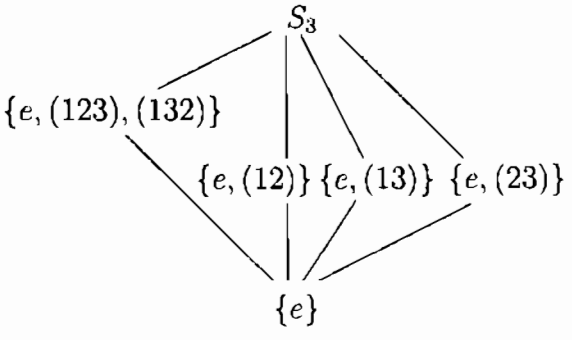
Nếu $a = 1$ thì $A_a = E$ nên A_a có cấp bằng 1.
Nếu $a = -1$ thì $A_a^2 = E$ nên A_a có cấp bằng 2.
Nếu $a \neq \pm 1$ thì $A_a^n \neq E$ nên A_a có cấp vô hạn.

3.3. Phần tử e có cấp 1, các phần tử a, b, c có cấp 2.

3.4. Giả sử C_6 sinh bởi phần tử g. Khi đó ta có sơ đồ các nhóm con như sau:



3.5. Các nhóm con của S_3 được biểu diễn trong sơ đồ sau:



3.6. Bảng nhân của tập

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

được thể hiện như sau:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Nhìn vào bảng toán trên ta có $aA = A$ và $Aa = A$ nên theo Bài tập 2.14 ta có A là một nhóm. Mặt khác, bảng nhân này có tính chất đối xứng nên A là một nhóm aben.

3.7. Giả sử $H = \{a \in A \mid \exists n \in \mathbb{N} : a^n = e\}$. Hiển nhiên $e \in H$ nên $H \neq \emptyset$. Với mọi $a, b \in H$, giả sử a có cấp n, b có cấp m. Mặt khác, do A aben nên $(ab)^{mn} = a^{mn}b^{mn} = e$, nghĩa là ab có cấp hữu hạn, hay $ab \in H$. Cuối cùng, với mọi $a \in H$, giả sử a có cấp n. Khi đó $(a^{-1})^n = (a^n)^{-1} = e$ nên $a^{-1} \in H$. Vậy H là nhóm con của A.

3.8. Theo Bài tập 3.5, S_3 có một nhóm con cấp 3 là:

$$\{e, (123), (132)\}.$$

3.9.

$\cdot$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	$-k$
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Việc tìm cấp của mỗi phần tử dành cho bạn đọc.

3.10. Từ $gh = hg^2$ suy ra $hg = g^2h$. Do đó nhóm sinh bởi g và h là: $\{e, g, g^2, h, gh, g^2h\}$. Và ta có bảng nhân như sau:

$\cdot$	e	g	g^2	h	gh	g^2h
e	e	g	g^2	h	gh	g^2h
g	g	g^2	e	gh	g^2h	h
g^2	g^2	e	g	g^2h	h	gh
h	h	g^2h	gh	e	g^2	g
gh	gh	h	g^2h	g	e	g^2
g^2h	g^2h	gh	h	g^2	g	e

3.11. Do H là nhóm con của G nên $gHg^{-1} \neq \emptyset$. Dễ thấy gHg^{-1} là bộ phận ổn định của G. Mặt khác với phần tử $ghg^{-1} \in gHg^{-1}$ bất kỳ thì nghịch đảo của nó là $gh^{-1}g^{-1} \in gHg^{-1}$. Vậy gHg^{-1} là nhóm con của G.

3.12. a) $\Rightarrow$ b). Giả sử $a \in G$ và $a \neq e$. Gọi H là nhóm con sinh bởi a. Do G không có nhóm con thực sự nên $H = G$.

Bây giờ ta giả sử n là cấp của a. Nếu $n = pq$ với $0 < p, q < n$ thì nhóm con K sinh bởi a^p có cấp là q, trái với giả thiết. Vậy G là nhóm con xyclic cấp n nguyên tố.

b) $\Rightarrow$ a). Hiển nhiên.

3.13. Giả sử G là một nhóm cấp 4. Nếu trong G có một phần tử cấp 4 thì G là một nhóm xyclic sinh bởi phần tử cấp 4 đó. Nếu G không có phần tử nào cấp 4 thì G có ba phần tử cấp 2, ngoài phần tử đơn vị.

3.14. Theo Hệ quả của định lý Lagrange, các nhóm có cấp $1, 2, 3, 5$ là những nhóm xyclic nên chúng là nhóm giao hoán.

Giả sử G là nhóm có cấp 4. Nếu G là xyclic thì G giao hoán. Nếu không thì mọi phần tử của G có cấp 1 hoặc 2 (theo Bài tập 3.13). Do đó với mọi $a \in G$ ta có $a^2 = e$. Vậy theo bài tập 2.12, G là nhóm giao hoán.

3.15. Hiển nhiên nếu H là nhóm con của G thì H đóng đối với phép toán trong G. Ngược lại, nếu H đóng đối với phép toán trong G thì H là một nửa nhóm hữu hạn và luật giản ước được thực hiện với mọi phần tử của H. Do đó H là một nhóm con của nhóm G.

3.16. Giả sử $A = \langle a \rangle$ có cấp n và $d \mid n$. Đặt $n = dq$, $q \in \mathbb{N}^*$. Ta sẽ chứng minh rằng nhóm con xyclic $H = \langle a^q \rangle$ của G có cấp bằng d. Thật vậy ta có:

$$(a^q)^d = a^{dq} = a^n = e.$$

Mặt khác giả sử $(a^q)^k = e$, nghĩa là $a^{qk} = e$. Do phần tử a có cấp bằng n nên ta có:

$$qk \vdots n \Rightarrow qk \vdots qd \Rightarrow k \vdots d.$$

Vậy phần tử a^q có cấp bằng d, và do đó H có cấp bằng d.

Bây giờ ta giả sử K cũng là một nhóm con của G có cấp bằng d. Do G là nhóm xyclic sinh bởi a nên K cũng là một nhóm xyclic sinh bởi một phần tử có dạng a^r, với $r \in \mathbb{N}$. Do nhóm K có cấp bằng d

nên ta có:

$$(a^r)^d = e \Rightarrow a^{rd} = e \Rightarrow rd \vdots n \Rightarrow rd \vdots dq \Rightarrow r \vdots q.$$

Do đó: $a^r \in \langle a^q \rangle = H$. Từ đó suy ra: $K \subset H$. Mặt khác ta có $|K| = |H| = d$ nên ta suy ra $K = H$. Vậy G chỉ có duy nhất một nhóm con cấp d.

3.17. Nếu X là nhóm xyclic vô hạn được sinh bởi phần tử a thì dễ thấy X cũng được sinh bởi phần tử a^{-1}. Bây giờ giả sử $X = \langle b \rangle$. Ta có $b = a^m, b^n = a^{-1}$ với $m, n \in \mathbb{Z}$. Suy ra $a^{-1} = a^{mn}$ nên $mn = -1$ do đó $m, n = \pm 1$. Vậy $b = a$ hoặc $b = a^{-1}$ và X có đúng hai phần tử sinh.

3.18. Nhóm $(\mathbb{Z}[i], +)$ không là nhóm xyclic.

3.19. Ta có $\mathbb{Z}_6^* = \langle 5 \rangle$ và $\mathbb{Z}_{17}^* = \langle 3 \rangle$.

3.20. a) Hiển nhiên $e \in A_n$. Giả sử $a, b \in A_n$. Ta có: $a^n = b^n = e$. Do A là nhóm aben nên

$$(ab)^n = a^n b^n = e \Rightarrow ab \in A_n.$$

Mặt khác với mọi $a \in A_n$, vì $a^n = e$ nên $(a^{-1})^n = (a^n)^{-1} = e$ hay $a^{-1} \in A_n$. Vậy A_n là một nhóm con của A.

b) Theo giả thiết m và n nguyên tố cùng nhau nên tồn tại hai số nguyên s, t sao cho $ms + nt = 1$. Lấy $x \in A_m \cap A_n$. Ta có: $x^m = e$, $x^n = e$. Từ đó suy ra:

$$x = x^{ms+nt} = (x^m)^s.(x^n)^t = e^s.e^t = e.$$

Vậy $A_m \cap A_n = \{e\}$.

c) Do $(m, n) = 1$ nên tồn tại $u, v \in \mathbb{Z}$ sao cho $nu + mv = 1$. Từ đó với $a \in A$

$$a = a^{nu+mv} = a^{nu} a^{mv}$$

Đặt $x = a^{nu}, y = a^{mv}$ ta có

$$x^m = a^{mnu} = e, y^n = a^{mnv} = e,$$

do $A = A_{mn}$. Nghĩa là, $x \in A_m, y \in A_n$ và $a = xy$.

3.21. Giả sử A là nhóm con khác không của $(\mathbb{Q}, +)$. Khi đó A có chứa một phân số tối giản $\frac{a}{n} \neq 0$. Từ đó suy ra

$$a = n\frac{a}{n} \in A \Rightarrow a\mathbb{Z} \subset A.$$

Bởi vậy nếu A, B là hai nhóm con khác không của $(\mathbb{Q}, +)$ thì A, B lần lượt chứa các nhóm con $a\mathbb{Z}, b\mathbb{Z}$, trong đó $a \neq 0$ và $b \neq 0$. Hai nhóm này giao nhau khác không vì chúng cùng chứa số nguyên ab.

3.22. Ta có $[0] = \left[\frac{0}{p}\right] \in \mathbb{Z}(p^\infty)$. Mặt khác với mọi $\left[\frac{a}{p^i}\right], \left[\frac{b}{p^j}\right] \in \mathbb{Z}(p^\infty)$ ta có

$$\left[\frac{a}{p^i}\right] - \left[\frac{b}{p^j}\right] = \left[\frac{ap^j - bp^i}{p^{i+j}}\right] \in \mathbb{Z}(p^\infty)$$

Vậy $\mathbb{Z}(p^\infty)$ là nhóm con của $\mathbb{Q}/\mathbb{Z}$.

Để chứng minh $\mathbb{Z}(p^\infty)$ có vô hạn phần tử ta xét tập:

$$A = \left\{ \left[\frac{1}{p^i}\right] \,\middle|\, i \geq 0 \right\} \subset \mathbb{Z}(p^\infty)$$

Xét ánh xạ :

$$\begin{array}{rccc} f : & \mathbb{N} & \longrightarrow & A \\ & k & \longmapsto & \left[\frac{1}{p^k}\right] \end{array}$$

Dễ chứng minh f là song ánh. Vậy card A = card $\mathbb{N}$. Suy ra $\mathbb{Z}(p^\infty)$ vô hạn phần tử.

3.23. Ta chứng minh khẳng định tương đương: Mọi nhóm G vô hạn đều có vô hạn nhóm con.

Trước hết, xét trường hợp $G = \langle a \rangle$ là một nhóm xyclic vô hạn. Khi đó, với mỗi số tự nhiên n thì $\langle a^n \rangle$ là một nhóm con xyclic của G và nếu $n \neq m$ thì $\langle a^n \rangle \neq \langle a^m \rangle$. Nghĩa là G có vô hạn nhóm con.

Bây giờ, xét trường hợp G là nhóm vô hạn bất kỳ. Nếu trong G có một phần tử a cấp vô hạn thì $A = \langle a \rangle$ là một nhóm con xyclic cấp vô hạn của G. Nhóm này có vô hạn nhóm con, các nhóm con này cũng là nhóm con của G. Vậy G có vô hạn nhóm con.

Nếu mọi phần tử của G đều có cấp hữu hạn thì tập các nhóm con xyclic sinh bởi các phần tử của G là vô hạn vì

$$\bigcup_{x \in G} \langle x \rangle = G$$

3.25. Giả sử HK là nhóm con của G, ta sẽ chứng minh $HK = KH$.

Thật vậy với mọi $k \in K$ và $h \in H$ ta có

$$h^{-1}k^{-1} \in HK \Rightarrow (h^{-1}k^{-1})^{-1} \in HK \Rightarrow kh \in HK$$

Do đó $KH \subset HK$. Mặt khác, theo trên ta có

$$k^{-1}h^{-1} \in HK, k \in HK$$

Suy ra $k^{-1}h^{-1}k \in HK$, nghĩa là tồn tại $h' \in H, k' \in K$ để

$$k^{-1}h^{-1}k = h'k'$$

Vậy nên $hkh'k' = k \Rightarrow hk = kk'^{-1}h'^{-1} \in KH$. Suy ra $HK \subset KH$, và do đó $KH = HK$.

Bây giờ giả sử $HK = KH$, ta sẽ chứng minh HK là nhóm con của G. Thật vậy, rõ ràng $e \in HK$. Với mọi $h \in H; k \in K$ do $HK = KH$ nên ta có $hk = k'h'$ với $h' \in H; k' \in K$. Bây giờ nếu có $ax, by \in HK$ thì từ đẳng thức vừa nêu và do H, K là những nhóm con ta suy ra được

$$(ax)(by)^{-1} = axy^{-1}b^{-1} \in HK$$

Vậy HK là nhóm con của G.

3.26. Giả sử aA là một nhóm con của G và e là đơn vị của G. Khi đó $e = aa' \in aA$ với $a' \in A$. Vậy $a' = a^{-1} \in A$ nên $a \in A$.

Dảo lại, nếu $a \in A$ thì ta có $aA = A$ và do đó aA là một nhóm con của nhóm G.

3.27. Giả sử $G = \langle a \rangle$ có cấp n và $b = a^k \in G$. 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 d_1 nguyên tố cùng nhau. Ta có

$$b^{n_1} = (a^k)^{n_1} = a^{kn_1} = a^{k_1 dn_1} = e^{k_1} = e$$

Hơn nữa, nếu $b^t = e$ hay $a^{kt} = e$ thì kt chia hết cho n. Như vậy $kt = k_1 dt = n_1 ds$ 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 $n_1 = \dfrac{n}{d}$ là cấp của $b = a^k$.

b) Phần tử $b = a^k$ là phần tử sinh của nhóm G khi và chỉ khi cấp của b bằng cấp của X và bằng n. Theo câu a) ta có b là phần tử sinh khi và chỉ khi $d = 1$, nghĩa là khi n và k nguyên tố cùng nhau. Vậy số các

phần tử sinh của G bằng số các số tự nhiên bé hơn n và nguyên tố cùng nhau với n.

3.28. Số phần tử sinh của nhóm xyclic C_n, $(n > 1)$ bằng $\varphi(n)$, số các số nguyên dương bé hơn n và nguyên tố cùng nhau với n.

3.30. Giả sử A là một nhóm có cấp là số chẵn. Ta phân các phần tử của A ra làm 3 loại: e, các phần tử có cấp 2 và các phần tử có cấp lớn hơn 2. Nếu $a \in A$ là phần tử có cấp lớn hơn 2 thì $a^{-1} \in A$ cũng là phần tử có cấp lớn hơn 2 và $a \neq a^{-1}$. Bởi vậy số các phần tử có cấp lớn hơn 2 của A là số chẵn. Suy ra số các phần tử của A có cấp 2 là một số lẻ. Nghĩa là có ít nhất một phần tử của A có cấp 2.

4. Nhóm con chuẩn tắc - nhóm thương

4.1. Dễ thấy quan hệ C có tính chất phản xạ và đối xứng. Ta sẽ chỉ ra rằng C có tính chất bắc cầu khi và chỉ khi nếu nhóm G giao hoán. Thật vậy, giả sử C có tính chất bắc cầu. Rõ ràng với $a \in G$ thì $ae = ea$ nên aCe. Tương tự, eCb với $b \in G$. Suy ra aCb, nghĩa là hai phần tử bất kỳ của G giao hoán.

Ngược lại, nếu nhóm G giao hoán thì mọi cặp phần tử của nó đều có quan hệ C với nhau, và do đó hiển nhiên có tính bắc cầu. Trong trường hợp này chỉ có một lớp tương đương là toàn thể nhóm G.

4.2. Giả sử G là nhóm có cấp n, H là nhóm con duy nhất của G có cấp k. Khi đó với mọi $g \in G$, gHg^{-1} cũng là một nhóm con của G. Hơn nữa, gHg^{-1} và H có cùng lực lượng. Mà theo giả thiết, H là nhóm con duy nhất có cấp k nên $gHg^{-1} = H$ với mọi $g \in G$. Do đó H là nhóm con chuẩn tắc.

4.3. Tương ứng $gH \leftrightarrow Hg^{-1}$ là một tương ứng 1-1 giữa tập các lớp ghép trái của H trong G và tập các lớp ghép phải của H trong G.

4.4. Các lớp ghép trái của H trong S_4 bao gồm:

$$
\begin{aligned}
H &= \{(1), (12), (34), (12) \circ (34)\} \\
(13)H &= \{(13), (123), (134), (1234)\} \\
(14)H &= \{(14), (124), (143), (1243)\} \\
(23)H &= \{(23), (132), (234), (1342)\} \\
(24)H &= \{(24), (142), (243), 1432)\} \\
(1324)H &= \{(1324), (14) \circ (23), (13) \circ (24), (1423)\}.
\end{aligned}
$$

Các lớp ghép phải của H trong S_4 bao gồm:

$$\begin{aligned} H &= \{(1), (12), (34), (12) \circ (34)\} \\ H(13) &= \{(13), (132), (143), (1432)\} \\ H(14) &= \{(14), (142), (134), (1342)\} \\ H(23) &= \{(23), (123), (243), (1243)\} \\ H(24) &= \{(24), (124), (234), 1234)\} \\ H(1324) &= \{(1324), (13) \circ (24), (14) \circ (23), (1423)\}. \end{aligned}$$

4.5. Nhóm con xyclic $A = \{(1), (123), (132)\}$ không là nhóm con chuẩn tắc trong S_4 vì:

$$(14)A = \{(14), (1234), (1324)\}, A(14) = \{(14), (1423), (1432)\}.$$

Do đó $(14)A \neq A(14)$.

4.6. Nhóm con $H = \{(1), (1234), (13) \circ (24), (1432), (13), (24), (14) \circ (23), (12) \circ (34)\}$ không là chuẩn tắc trong S_4 vì $H(12) \neq (12)H$.

4.7. S_3 có các nhóm con là

$\{e\}$, $\{e, (1\ 2)\} = \langle(1\ 2)\rangle$, $\{e, (1\ 3)\} = \langle(1\ 3)\rangle$, $\{e, (2\ 3)\} = \langle(2\ 3)\rangle$, $\{e, (1\ 2\ 3), (1\ 3\ 2)\} = \langle(1\ 2\ 3)\rangle = \langle(1\ 3\ 2)\rangle$ và S_3.

Trong số đó có $\{e\}, S_3$ và $\langle(1\ 2\ 3)\rangle$ là ba nhóm con chuẩn tắc của S_3.

4.8. Ta có $es = se = e$ với mọi $s \in S$ nên $e \in C(S)$ hay $C(S) \neq \emptyset$. Mặt khác, giả sử $g, g' \in C(S)$, nghĩa là $gs = sg$ và $g's = sg'$ với mọi $s \in S$. Suy ra

$$(gg')s = g(g's) = g(sg') = (gs)g' = (sg)g' = s(gg')$$

hay $gg' \in C(S)$.

Cuối cùng giả sử $g \in C(S)$, từ $gs = sg$ ta nhân vào bên trái và bên phải lần lượt với g^{-1} sẽ được $sg^{-1} = g^{-1}s$ hay $g^{-1} \in C(S)$. Vậy $C(S)$ là một nhóm con của G.

Bây giờ ta sẽ chứng minh

$$C(G) = \{g \in G | gx = xg \ \forall\, x \in G\}$$

là nhóm con chuẩn tắc của G.

Theo trên ta có $C(G)$ là một nhóm con của G. Mặt khác, với mọi $x \in X$ và $g \in C(G)$ ta có: $gx = xg$. Do đó

$$x^{-1}gx = x^{-1}xg = eg = g \in C(G).$$

Vậy $C(G)$ là nhóm con chuẩn tắc của G.

4.9. A là nhóm con của G có chỉ số 2, nghĩa là số các lớp ghép trái của G theo nhóm con A bằng số các lớp ghép phải của G theo nhóm con A và bằng 2. Trong hai lớp ghép đó có một lớp là A và một lớp là phần bù của A trong G. Do đó mỗi lớp ghép trái của G theo A là một lớp ghép phải của G theo A và ngược lại. Vậy A là nhóm con chuẩn tắc của G.

4.10. Ký hiệu $\{B_i\}_{i\in I}$ là tập hợp các nhóm con liên hợp với nhóm con A. Theo định nghĩa, với mỗi i, tồn tại $a_i \in G$ sao cho

$$B_i = a_i^{-1} A a_i.$$

Đặt $B = \bigcap\limits_{i\in I} B_i$ thì B là một nhóm con của G.

Mặt khác, với mỗi $x \in G$ và $i \in I$ ta có $x^{-1}B_i x = (a_i x)^{-1} A (a_i x)$ là một nhóm con liên hợp với A nên $\{x^{-1}B_i x\}_{i\in I}$ cũng chính là tập hợp các nhóm con liên hợp với nhóm A. Do đó:

$$x^{-1}Bx = x^{-1}(\bigcap_i B_i)x = \bigcap_i x^{-1}B_i x = B,$$

suy ra $Bx = xB$. Vậy B là nhóm con chuẩn tắc.

4.11. Với mọi $a \in A$ và $b \in B$, xét $x = (ab)(ba)^{-1}$. Ta có:

$$x = (ab)(a^{-1}b^{-1}) = (aba^{-1}).b^{-1} = b'b^{-1} \in B.$$

Tương tự:

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

Do đó: $x \in A \cap B = \{e\}$. Vậy $x = e$, nghĩa là $ab = ba$.

4.12. Xét tập hợp $G = \{(m, n, \varepsilon) \mid m, n \in \mathbb{Z}, \varepsilon = \pm 1\}$. Ta định nghĩa phép nhân trên G như sau:

$$(k_1, k_2, 1)(l_1, l_2, \varepsilon) = (k_1 + l_1, k_2 + l_2, \varepsilon)$$

$$(k_1, k_2, -1)(l_1, l_2, \varepsilon) = (k_1 + l_2, k_2 + l_1, -\varepsilon)$$

Khi đó G là một nhóm với phần tử đơn vị là $(0, 0, 1)$ và

$$(m, n, 1)^{-1} = (-m, -n, 1); \quad (m, n, -1)^{-1} = (-m, -n, -1).$$

Xét nhóm con A của G sinh bởi hai phần tử $(1,0,1)$ và $(0,1,1)$. Vì hai phần tử có toạ độ thứ ba bằng 1 giao hoán được với nhau nên mỗi phần tử của A có dạng:

$$a = (1,0,1)^m(0,1,1)^n = (m,0,1)(0,n,1) = (m,n,1)$$

với $m, n \in \mathbb{Z}$. Giả sử $x = (k,l,\varepsilon) \in G$, ta có:

$$\varepsilon = 1,\ xax^{-1} = (k,l,1)(m,n,1)(-k,-l,1) = a \in A.$$

$$\varepsilon = -1,\ xax^{-1} = (k,l,-1)(m,n,1)(-k,-l,-1) = (m,n,1) \in A.$$

Do đó A là một nhóm con chuẩn tắc của G.

Nhóm con $B = \langle(1,0,1)\rangle$ chuẩn tắc trong A vì mọi phần tử của B giao hoán với mọi phần tử của A.

Tuy nhiên B không phải là một nhóm con chuẩn tắc trong G. Thật vậy ta có:

$$B = \{(m,0,1) \mid m \in \mathbb{Z}\}$$

Với mọi $m \neq 0$, ta có:

$$(1,1,-1)(m,0,1)(1,1,-1)^{-1} = (0,m,1) \notin B.$$

4.13. Ta có thể chứng minh một kết quả tổng quát hơn, đó là: nếu $\{A_i\}_{i\in I}$ là một họ các nhóm con chuẩn tắc của G thì $A = \bigcap\limits_{i\in I} A_i$ là một nhóm con chuẩn tắc của G.

Thật vậy, giả sử $x \in G, a \in A$ suy ra $a \in A_i$ với mọi i. Do A_i là chuẩn tắc nên $xax^{-1} \in A_i$ với mọi i. Suy ra $xax^{-1} \in A$. Vậy A chuẩn tắc trong G.

Bây giờ ta chứng minh rằng nếu A, B là hai nhóm con chuẩn tắc của X thì $AB = BA$. Thật vậy, với mọi $a \in A, b \in B$ ta có $b_1 = aba^{-1} \in B$ (do B chuẩn tắc). Do đó $ab = b_1a \in BA$. Vậy $AB \subset BA$. Tương tự, ta có: $BA \subset AB$. Vậy $AB = BA$.

Ta có $e = ee \in AB$. Nếu a_1b_1 và $a_2b_2 \in AB$ thì ta có:

$$(a_1b_1)(a_2b_2)^{-1} = a_1(b_1b_2^{-1}a_2^{-1})$$

Phần tử $(b_1b_2^{-1})a_2^{-1} \in BA = AB$ nên $(a_1b_1)(a_2b_2)^{-1} \in AB$. Do đó AB là một nhóm con của G.

Mặt khác, với mọi $ab \in AB, x \in G$, ta có:

$$xabx^{-1} = (xax^{-1})(xbx^{-1}) \in AB$$

Vậy AB chuẩn tắc trong G.

4.14. Giả sử ngược lại rằng HK là một nhóm. Ta chứng minh

$$|HK/H| = |K/H \cap K|.$$

Thật vậy, xét tương ứng

$$\begin{aligned} f : HK/H &\to K/H \cap K \\ \overline{ax} &\mapsto \overline{x} \end{aligned}$$

thì tương ứng này không phụ thuộc vào đại diện. Hơn nữa, f còn là một song ánh. Do đó ta có

$$|HK/H| = |K/H \cap K|.$$

Do HK là nhóm con của G nên $|G| \vdots |HK|$. Suy ra

$$p^k m \vdots |HK|$$

Mà H là nhóm con của HK nên $|HK| \vdots |H|$. Suy ra

$$|HK| = p^k t,\ t \in \mathbb{Z}$$

Từ đó suy ra $p^k m \vdots p^k t \Rightarrow m \vdots t.$ (1)

Ta có $|HK/H| = p^k t : p^k = t$ nên $t = |K/H \cap K|$. Do K không thuộc H nên

$$|H \cap K| < |K| = p^d$$

mà $|K|$ chia hết cho $|H \cap K|$ nên $|H \cap K| = p^i$, với $0 \leq i < d$.
Suy ra

$$|K/H \cap K| = p^d/p^i \geq p \quad (\text{do } d - i \geq 1).$$

Vậy $t = p^{d-i} \vdots p$ (2)

Từ (1) và (2) ta có $m \vdots p$, trái với giả thiết $(p, m) = 1$.

Vậy HK không là nhóm con của G.

4.15. Tâm của nhóm $D_3 = \{e, g, g^2, h, gh, g^2h\}$ là $\{e\}$. Tâm của nhóm $D_4 = \{e, g, g^2, g^3, h, gh, g^2h, g^3h\}$ là $\{e, g^2\}$.

4.16. a) Giả sử G' là nhóm con của nhóm G sinh bởi tất cả các giao hoán tử. Khi đó phần tử $b = a^{-1}x^{-1}ax \in G'$ với mọi $a \in G'$ và với

mọi $x \in G$. Do đó $x^{-1}ax = ab \in G'$. Vậy G' là một nhóm con chuẩn tắc của G.

b) Đối với hai phần tử u, v bất kỳ thuộc nhóm thương G/G' ta có $u = \overline{a}$ và $v = \overline{b}$, với $a, b \in G$. Do

$$(ab)(ba)^{-1} = aba^{-1}b^{-1} \in G'$$

nên $\overline{ab} = \overline{ba}$. Từ đó $\overline{a}\overline{b} = \overline{b}\overline{a}$, nghĩa là nhóm thương G/G' là nhóm aben.

c) Giả sử G/A là một nhóm aben, như vậy với mọi phần tử aA và bA thuộc G/A ta có

$$(aA)(bA) = (bA)(aA), \text{ hay } abA = baA.$$

Do đó $ab(ba)^{-1} = aba^{-1}b^{-1} \in A$. Từ đó suy ra nhóm con G' sinh bởi các giao hoán tử của G là chứa trong A.

Đảo lại, nếu nhóm con G' sinh bởi các giao hoán tử của G chứa trong A thì $aba^{-1}b^{-1} \in A$ với mọi $a, b \in G$. Từ đó suy ra $abA = baA$ hay $(aA)(bA) = (bA)(aA)$, tức là G/A là một nhóm aben.

4.17. 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) $\langle a\rangle/\langle a^5\rangle = \{\langle a^5\rangle, a\langle a^5\rangle, a^2\langle a^5\rangle, a^3\langle a^5\rangle, a^4\langle a^5\rangle\}$.

d) Gọi $\mathbb{R}^*$ là nhóm nhân các số thực khác không, $\mathbb{R}_+^*$ là nhóm nhân các số thực dương. Khi đó ta có: $\mathbb{R}^*/\mathbb{R}_+^* = \{\mathbb{R}_+^*, \mathbb{R}_-^*\}$, trong đó $\mathbb{R}_-^*$ là tập hợp các số thực âm.

4.18. Nhóm các giao hoán tử của nhóm các phép thế S_3 là

$$H = \langle(1\ 2\ 3)\rangle.$$

4.19. Giả sử $|G| = p^m, p$ nguyên tố. Lấy $g \in G$. Khi đó:

Nếu g có cấp bằng p thì nhóm con sinh bởi g có cấp p. Khẳng định được chứng minh.

Nếu g không có cấp p thì do cấp của g là ước của cấp của G nên cấp của g có dạng p^k $(2 \le k \le m)$. Khi đó $g^{p^k} = (g^{p^{k-1}})^p = e$. Do p^k là cấp của g nên $g^{p^{k-1}} \neq e$ và p là số nguyên tố nên phần tử $g^{p^{k-1}}$ có cấp p. Và như vậy nhóm con sinh bởi $g^{p^{k-1}}$ có cấp p.

4.20. Do $(n, m) = 1$ nên tồn tại $x, y \in \mathbb{Z}$ sao cho $mx + ny = 1$. Suy ra $h = h^{mx+ny} = h^{mx}h^{ny} = (h^x)^m e = g^m$ với $g = h^x$.

4.21. a) Trước hết, ta chứng minh tập MN đóng với phép nhân. Giả sử $xy, x'y' \in MN$. Do N là nhóm con chuẩn tắc trong G nên $x'N = Nx'$. Từ đó tồn tại $z \in N$ sao cho $x'z = yx'$. Khi đó

$$(xy)(x'y') = x(yx')y' = x(x'z)y' = (xx')(zy') \in MN.$$

Bây giờ nếu $xy \in MN$ thì

$$(xy)^{-1} = y^{-1}x^{-1} \in Nx^{-1} = x^{-1}N \subset MN.$$

Điều này chứng tỏ MN là một nhóm con của G.
b) Bây giờ giả sử M, N là hai nhóm con chuẩn tắc của G. Với $xy \in MN$ và $g \in G$ ta có

$$gxg^{-1} = x' \in M,\ gyg^{-1} = y' \in N.$$

Từ đó: $g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = x'y' \in MN$.
Nghĩa là MN là nhóm con chuẩn tắc trong G.

4.22. a) Giả sử $a, b \in N_S$. Thế thì

$$(ab)S(ab)^{-1} = a(bSb^{-1})a^{-1} = aSa^{-1} = S.$$

Mặt khác, từ $aSa^{-1} = S$ suy ra $a^{-1}Sa = S$. Vậy $ab \in N_S$ và $a^{-1} \in N_S$. Hay N_S là một nhóm con của G.
b) Giả sử K là nhóm con của G và H là một nhóm con chuẩn tắc trong K. Lấy $a \in K$, thế thì $aHa^{-1} = H$. Suy ra $a \in N_H$ hay $A \subset N_H$.
c) Bây giờ giả sử H là một nhóm con của G và K là một nhóm con của N_H. Dễ thấy H là chuẩn tắc trong N_H, và khi đó ta có $KH = HK$ là một nhóm con của N_H.

Bởi vì $H \subset KH \subset N_H$ và H là chuẩn tắc trong N_H nên H chuẩn tắc trong KH.
d) Giả sử A là một nhóm con của G nhận H làm nhóm con chuẩn tắc, nghĩa là $aHa^{-1} = H$ với mọi $a \in A$. Đẳng thức này chứng tỏ $a \in N_H$. Vậy $A \subset N_H$.

4.23. Dễ thấy phép toán $\circ$ trên A có tính chất kết hợp. A có phần tử đơn vị là $(1, 0)$ và nghịch đảo của phần tử (x, y) là phần tử $(x^{-1}, -yx^{-1})$. Do đó A là một nhóm.

Mặt khác, với mọi $(u, v) \in A$ và với mọi $(1, y) \in H$ ta có:

$$(u, v)(1, y)(u, v)^{-1} = (u, v)(1, y)(u^{-1}, -vu^{-1})$$

$$= (uu^{-1}, vu^{-1} + yu^{-1} - vu^{-1}) = (1, yu^{-1}) \in H.$$

Vậy H là nhóm con chuẩn tắc trong A.

4.24. Xét ánh xạ:

$$\begin{aligned} f : \mathbb{C}^* &\to (\mathbb{R}^+, \cdot) \\ \alpha &\mapsto |\alpha| \end{aligned}$$

trong đó $(\mathbb{R}^+, \cdot)$ là nhóm nhân các số thực dương. Ta có

$$f(\alpha.\beta) = |\alpha.\beta| = |\alpha|.|\beta| = f(\alpha).f(\beta)$$

nên f là một đồng cấu nhóm.

Hơn nữa, với mọi $x \in \mathbb{R}^+$ ta có $f(x + 0i) = x$ nên f là một toàn cấu nhóm.

Mặt khác, $\mathrm{Ker} f = \{\alpha \in \mathbb{C}^* \mid |\alpha| = 1\} = W$ nên theo Định lý đồng cấu nhóm ta có:

$$\mathbb{C}^*/W \cong (\mathbb{R}^+, \cdot).$$

4.25. Giả sử G là một nhóm mêta aben, nghĩa là nó có một nhóm con chuẩn tắc K sao cho cả K và G/K đều giao hoán.

a) Giả sử H là một nhóm con tuỳ ý của G. Khi đó $K \cap H$ là một nhóm con chuẩn tắc của H và

$$H/K \cap H \cong KH/K$$

Mặt khác $K \cap H$ cũng là nhóm con của nhóm aben K nên $K \cap H$ cũng là nhóm aben. Còn KH/K là nhóm con của nhóm aben G/K nên KH/K là nhóm aben. Do đó $H/K \cap H$ là nhóm aben. Như vậy H là nhóm mêta aben.

Giả sử N là một nhóm con chuẩn tắc nào đó của G, ta chứng minh nhóm thương G/N cũng là một nhóm mêta aben. Thật vậy, ta có K/N là một nhóm con chuẩn tắc của G/N. Do K là nhóm aben nên K/N cũng là nhóm aben. Mặt khác

$$(G/N)/(K/N) \cong G/K$$

mà G/K là nhóm aben nên $(G/N)/(K/N)$ cũng là nhóm aben. Vậy G/N là nhóm mêta aben.

b) Giả sử G là mêta aben. Khi đó G/K là aben, nên theo Bài tập 4.16 ta có nhóm giao hoán tử $G' \subset K$, nghĩa là G' giao hoán.

Ngược lại, nếu G' giao hoán thì cũng theo Bài tập 4.16, G' là nhóm con chuẩn tắc aben của G và nhóm thương G/G' cũng là nhóm aben.

4.26. a) Với mọi $g \in G$ và $k \in K$, ta có: $gk = kg$ nên $k = g^{-1}kg \in K$, nghĩa là K là nhóm con chuẩn tắc của G.

b) Nếu G/K là xyclic thì tồn tại $g \in G$ sao cho $G/K = \langle gK \rangle$. Với mọi $a, b \in G$ thì $aK, bK \in G/K$ nên tồn tại các số tự nhiên n, m sao cho $aK = g^nK, bK = g^mK$ hay $a = g^nk, b = g^mk'$ với $k, k' \in K$. Khi đó:

$$ab = (g^nk)(g^mk') = g^n(kg^m)k' = g^ng^mkk' = g^{m+n}kk'.$$

$$ba = (g^mk')(g^nk) = g^m(k'g^n)k = g^mg^nk'k = g^{m+n}k'k.$$

Do $k, k' \in K$ nên $kk' = k'k$, do đó $ab = ba$ hay G là nhóm giao hoán.

5. Đồng cấu nhóm

5.1. f không phải là đồng cấu nhóm.

5.2. f là đồng cấu nhóm và với mọi $g^k \in C_{12}$ ta có $f(g^k) = g^{3k}$. Do đó $\mathrm{Ker}f = \{e, g^4, g^8\}$ và $\mathrm{Im}f = \{e, g^3, g^6, g^9\}$

5.3. f là đồng cấu nhóm. $\mathrm{Ker}f = 4\mathbb{Z}$ và $\mathrm{Im}f = \{([0]_2, [0]_4), ([1]_2, [1]_4), ([0]_2, [2]_4), ([1]_2, [3]_4)\}$.

5.4. f là đồng cấu nhóm. $\mathrm{Ker}f = \{[0]_8, [2]_8, [4]_8, [6]_8\}$ và $\mathrm{Im}f = \mathbb{Z}_2$.

5.5. Giả sử G là một nhóm xyclic sinh bởi phần tử a và $f : G \to H$ là một đồng cấu từ G đến H. Khi đó ta có $f(a) \in \mathrm{Im}f$ và do đó $\mathrm{Im}f = \{f(a)^n = f(a^n) \mid n \in \mathbb{Z}\}$ là nhóm xyclic sinh bởi phần tử a.

5.6. Để cho tiện ta cũng xem A là nhóm với phép toán cộng. Khi đó tương ứng:

$$\begin{array}{rccc} f' : & \mathbb{Z} & \to & A \\ & n & \mapsto & \begin{cases} f(n), n \in \mathbb{N} \\ -f(-n), n \notin \mathbb{N} \end{cases} \end{array}$$

trong đó $-f(-n)$ là phần tử nghịch đảo của $f(-n)$ trong nhóm A, là một đồng cấu nhóm.

Khi đó với mọi $n \in \mathbb{N}$ ta có: $f' \circ i(n) = f'(i(n)) = f'(n)$ hay $f' \circ i = f$.

Giả sử còn có đồng cấu nhóm $\varphi : \mathbb{Z} \to A$ sao cho $\varphi \circ i = f$. Khi đó

với mọi $n \in \mathbb{Z}$ ta có:

Nếu $n \in \mathbb{N}$ thì $f'(n) = f'(i(n)) = f(n) = \varphi(i(n)) = \varphi(n)$.

Nếu $n \notin \mathbb{N}$ thì $f'(n) = -f(-n) = -\varphi(i(-n)) = -\varphi(-n) = \varphi(n)$.

Tóm lại $f' = \varphi$. Vậy f' xác định như trên là duy nhất.

5.7. Giả sử $G/A = \{x_1A, x_2A, \cdots, x_nA\}$ là tập các lớp ghép của A trong G, S_n là nhóm các phép thế của tập G/A. Vì trong nhóm có luật giản ước nên với mỗi $a \in G$, ánh xạ:

$$\begin{array}{rccc} t_a: & G/A & \to & G/A \\ & xA & \mapsto & axA \end{array}$$

là một đơn ánh, và do đó là song ánh, tức là $t_a \in S_n$.

Bây giờ xét ánh xạ:

$$\begin{array}{rccc} t: & G & \to & S_n \\ & a & \mapsto & t_a \end{array}$$

Vì $t_at_b = t_{ab}$ nên t là đồng cấu nhóm. Hơn nữa nếu $a \in \mathrm{Ker}t$ thì $t_a = 1_{S_n}$ nên $xA = axA$ với mọi x, đặc biệt $A = aA$ nên $a \in A$. Vậy ta được $\mathrm{Ker}t \subset A$. Đặt $B = \mathrm{Ker}t$ ta được B là nhóm con chuẩn tắc. Hơn nữa G/B đẳng cấu với $\mathrm{Im}t$ là nhóm con của S_n nên G/B là nhóm hữu hạn.

5.8. Ta có $\mathrm{Ker}\varphi = \{0\}$ và $\varphi^{-1}(12\mathbb{Z}) = 2\mathbb{Z}$.

5.9. a) Với mọi số nguyên k ta có: $k \in m\mathbb{Z} \cap n\mathbb{Z}$ khi và chỉ khi $k \in m\mathbb{Z}$ và $k \in n\mathbb{Z} \Leftrightarrow k \vdots m$ và $k \vdots n$, nghĩa là $k \vdots b$. Do đó $m\mathbb{Z} \cap n\mathbb{Z} = b\mathbb{Z}$.

b) Do $(m, n) = d$ nên tồn tại hai số r và s sao cho $mr + ns = d$. Suy ra: $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$. (Điều này được suy ra ngay từ phép chứng minh sự tồn tại ước chung lớn nhất của hai số nguyên).

c) Xét ánh xạ: $f: \mathbb{Z} \to m\mathbb{Z}/mn\mathbb{Z}$, $k \mapsto nk + mn\mathbb{Z}$. Dễ chứng minh f là một toàn cấu nhóm. Hơn nữa, $\mathrm{Ker}f = n\mathbb{Z}$. Suy ra:

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

5.10. Giả sử $f: (\mathbb{Z}, +) \to (\mathbb{Q}, +)$ là một đồng cấu từ $(\mathbb{Z}, +)$ đến $(\mathbb{Q}, +)$. Khi đó với mọi $n \in \mathbb{Z}$ ta có $f(n) = f(n.1) = nf(1)$ với $f(1) = a \in \mathbb{Q}$. Vậy mọi đồng cấu $f: \mathbb{Z} \to \mathbb{Q}$ đều được xác định bởi $f(n) = na$ với mọi $n \in \mathbb{Z}$, trong đó a là một phần tử nào đó của $\mathbb{Q}$.

5.11. $(\mathbb{Z}, +)$ không đẳng cấu với $(\mathbb{Q}^*, \cdot)$ vì $(\mathbb{Q}^*, \cdot)$ có một phần tử cấp 2 (là -1) trong khi $(\mathbb{Z}, +)$ không có phần tử cấp 2.

5.12. $(\mathbb{R}, +)$ đẳng cấu với $(\mathbb{R}^+, \times)$. Thật vậy, xét ánh xạ

$$\begin{array}{rccc} \lg: & \mathbb{R}^+ & \to & \mathbb{R} \\ & x & \mapsto & \lg x. \end{array}$$

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. Hơn nữa, với mỗi $a \in \mathbb{R}$ ta có $10^a \in \mathbb{R}^+$ thoả mãn $\lg 10^a = a$ nên lg là một toàn cấu. Vậy lg là một đẳng cấu.

5.13. Mỗi số phức thuộc H có dạng lượng giác là: $r\left(\cos\frac{k\pi}{2} + i\sin\frac{k\pi}{2}\right)$ với $k \in \mathbb{Z}$ và $r > 0$.

Vậy $H = \left\{r(\cos\frac{k\pi}{2} + i\sin\frac{k\pi}{2}) \mid r > 0,\ k \in \mathbb{Z}\right\}$.

Xét ánh xạ $f : \mathbb{C}^* \to U,\ r(\cos\varphi + i\sin\varphi) \mapsto \cos 4\varphi + i\sin 4\varphi$. Dễ kiểm tra f là một đồng cấu nhóm. Hơn nữa, với mọi $\cos\varphi + i\sin\varphi \in U$ ta có:

$$f\left(\cos\frac{\varphi}{4} + i\sin\frac{\varphi}{4}\right) = \cos\varphi + i\sin\varphi.$$

Vậy f là toàn cấu. Mặt khác,

$$\begin{aligned} \mathrm{Ker} f &= \{\alpha = r(\cos\varphi + i\sin\varphi) \mid f(\alpha) = 1\} \\ &= \{\alpha = r(\cos\varphi + i\sin\varphi) \mid \cos 4\varphi + i\sin 4\varphi = 1\} \\ &= \{\alpha = r(\cos\varphi + i\sin\varphi) \mid 4\varphi = 2k\pi,\ k \in \mathbb{Z}\} \\ &= \{\alpha = r(\cos\varphi + i\sin\varphi) \mid \varphi = \frac{k\pi}{2},\ k \in \mathbb{Z}\} \\ &= \left\{\alpha = r\left(\cos\frac{k\pi}{2} + i\sin\frac{k\pi}{2}\right) \mid k \in \mathbb{Z}\right\} = H. \end{aligned}$$

Do đó H là nhóm con của $\mathbb{C}^*$ và

$$C^*/H = C^*/\mathrm{Ker} f \cong U$$

5.14. Xét ánh xạ $g : \mathbb{R} \to U,\ r \mapsto \cos 2\pi r + i\sin 2\pi r$. Dễ chứng minh g là một toàn cấu nhóm và $\mathrm{Ker} g = \mathbb{Z}$ nên $\mathbb{R}/\mathbb{Z} \cong U$.

5.15. a) Theo Bài tập 5.5, ta có $f(A)$ là một nhóm xyclic sinh bởi $f(a)$. Do $f(a)$ là một phần tử của B nên cấp của $f(a)$ là ước của cấp

của B, nghĩa là ước của n.

Mặt khác, do a có cấp m nên $a^m = e_A$, suy ra

$$[f(a)]^m = f(a)^m = f(e_A) = e_B$$

nên cấp của $f(a)$ là ước của m. Vậy cấp của $f(a)$ là một ước chung của m và n.

b) Mỗi tự đồng cấu của nhóm $\mathbb{Z}_6 = \langle \overline{1} \rangle$ hoàn toàn được xác định bởi $f(\overline{1}) \in \mathbb{Z}_6$ nên $\mathbb{Z}_6$ có đúng 6 tự đồng cấu.

5.16. Dễ chứng minh f là đồng cấu nhóm. Giả sử $\varphi : \mathbb{Z} \to G$ là một đồng cấu nhóm thoả mãn $\varphi(1) = g$. Khi đó với mọi $n \in \mathbb{Z}$ ta có:

$$\varphi(n) = \varphi(1 + 1 + \cdots + 1) = [\varphi(1)]^n = g^n = f(n) \Rightarrow \varphi = f$$

Vậy f là duy nhất.

5.17. a) Giả sử $G = \langle a \rangle$ là một nhóm xyclic cấp n. Mỗi tự đồng cấu của G cho ta một giá trị xác định của $f(a) \in G$. Đảo lại với mỗi $b = a^k \in G$, ánh xạ

$$\begin{array}{rccc} f: & X & \to & X \\ & a & \mapsto & a^k, \end{array}$$

với $k = 1, 2, ..., n$ là một tự đồng cấu của G. Như vậy mỗi tự đồng cấu f của G hoàn toàn xác định bởi $f(a) \in G$. Do đó có đúng n tự đồng cấu của G.

b) Mỗi đồng cấu $f : \mathbb{Z}_m \to \mathbb{Z}_n$ cho một giá trị xác định $f(\overline{1}) \in \mathbb{Z}_n$. Cấp của $f(\overline{1})$ là ước của n. Vì $\overline{1}$ có cấp m nên cấp của $f(\overline{1})$ là ước của m. Do đó cấp của $f(\overline{1})$ là ước chung của m và n.

Đảo lại, với phần tử $\overline{b} \in \mathbb{Z}_n$ có cấp là ước chung của m và n thì ánh xạ $\overline{k} \to \overline{kb}$ 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 $f : \mathbb{Z}_m \to \mathbb{Z}_n$ sao cho

$$f(\overline{1}) = \overline{0},\ f(\overline{1}) = \overline{3},\ f(\overline{1}) = \overline{6},$$

$$f(\overline{1}) = \overline{9},\ f(\overline{1}) = \overline{12},\ f(\overline{1}) = \overline{15}.$$

c) Theo câu b) ta có sáu đồng cấu từ $\mathbb{Z}_{18}$ đến $\mathbb{Z}_6$, đó là các đồng cấu

$$f(\overline{1}) = \overline{0},\ f(\overline{2}) = \overline{2},\ f(\overline{1}) = \overline{3},$$

$$f(\overline{1}) = \overline{4},\ f(\overline{1}) = \overline{5},\ f(\overline{1}) = \overline{1}.$$

5.18. a) $f : C_3 \to C_4$ được xác định bởi $f(g^r) = e$.

b) $f : \mathbb{Z} \to \mathbb{Z}_4$ được xác định bởi $f(1) = [0]_4$ hoặc $f(1) = [1]_4$ hoặc $f(1) = [2]_4$ hoặc $f(1) = [3]_4$. Khi đó với mọi $x \in \mathbb{Z}$: $f(x) = xf(1)$.

c) Ta có $D_4 = \{e, g, g^2, g^3, h, gh, g^2h, g^3h\}$. Do đó $f : \mathbb{Z} \to D_4$ được xác định bởi $f(1) = a$ với $a \in D_4$. Khi đó với mọi $x \in \mathbb{Z}$: $f(x) = xf(1)$.

5.19. a) Theo Bài tập 5.15 có 6 tự đồng cấu của nhóm $\mathbb{Z}_6$ được xác định bởi $f(1) = \overline{a}$ với $a = 0, 1, ..., 5$. Dễ chứng minh rằng trong số đó chỉ có hai tự đồng cấu xác định bởi $f(1) = 1$ và $f(1) = 5$ là những đẳng cấu. Do đó $\mathrm{Aut}(\mathbb{Z}_6)$ gồm có hai phần tử. Vậy $\mathrm{Aut}(\mathbb{Z}_6) \cong \mathbb{Z}_2$.

b) Mỗi tự đồng cấu của $\mathbb{Z}$ hoàn toàn được xác định bởi $f(1)$ vì $f(n) = nf(1)$ với mọi $n \in \mathbb{Z}$. Nếu $f \in \mathrm{Aut}(\mathbb{Z})$ thì $f(1) = \pm 1$, vì nếu $f(1) \neq \pm 1$ thì $f(\mathbb{Z}) = f(1)\mathbb{Z} \neq \mathbb{Z}$ do đó trái với giả thiết f là toàn ánh. Bởi vậy nếu $f \in \mathrm{Aut}(\mathbb{Z})$ thì $f(n) = n$ với mọi $n \in \mathbb{Z}$ hoặc $f(n) = -n$ với mọi $n \in \mathbb{Z}$. Hay nói cách khác, $\mathrm{Aut}(\mathbb{Z})$ gồm có hai phần tử là $1_{\mathbb{Z}}$ và $-1_{\mathbb{Z}}$, nghĩa là $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

c) Dễ thấy $(\mathbb{Z}_7^*, \times)$ là một nhóm xyclic cấp 6 sinh bởi phần tử 5 nên

$$(\mathbb{Z}_7^*, \times) \cong (\mathbb{Z}_6, +).$$

5.20. Giả sử X là nhóm xyclic vô hạn. Theo Bài tập 3.17, X có đúng hai phần tử sinh là a và a^{-1}. Khi đó mỗi tự đẳng cấu của X là một ánh xạ biến a thành một phần tử sinh là a hoặc a^{-1}. Tương ứng ta có hai tự đẳng cấu của X, đó là phép đồng nhất và $a \mapsto a^{-1}$.

5.21. Giả sử $f = hg : G \to K$ là đẳng cấu.

a) Do $f = hg$ là đơn cấu nên g là đơn cấu.

b) Do $f = hg$ là toàn cấu nên h là toàn cấu.

c) Lấy $x \in H$ suy ra $h(x) \in K$. Do $f = hg$ là đẳng cấu nên tồn tại $a \in G$ sao cho $f(a) = h(x)$ hay

$$hg(a) = h(x) \Rightarrow h(g(a)x^{-1}) = e \Rightarrow g(a)x^{-1} = b \in \mathrm{Ker}h.$$

Do đó $x = b^{-1}g(a) \in (\mathrm{Ker}h)(\mathrm{Im}g)$. Vậy $H \subset (\mathrm{Ker}h)(\mathrm{Im}g)$.

Ngược lại, lấy $x \in (\mathrm{Ker}h)(\mathrm{Im}g)$. Suy ra $x = bg(a)$, trong đó $h(b) = e$ và $a \in G$. Từ đó

$$h(x) = h(b)hg(a) = f(a) \in K = h(H)$$

(do h là toàn cấu). Suy ra $x \in H$. Vậy $(\mathrm{Ker}h)(\mathrm{Im}g) \subset H$. Tóm lại ta có $H = (\mathrm{Ker}h)(\mathrm{Im}g)$.

Bây giờ giả sử $x \in \mathrm{Ker}h \cap \mathrm{Im}g$. Khi đó tồn tại $a \in G$ sao cho $x = g(a)$ và $h(x) = e$. Suy ra $h(x) = hg(a) = f(a) = e$. Do f là đẳng cấu nên $a = e$. Từ đó $x = g(a) = g(e) = e$. Vậy $\mathrm{Ker}h \cap \mathrm{Im}g = \{e\}$.

5.22. Theo tính chất của đồng cấu nhóm, nếu B là nhóm con chuẩn tắc trong H thì $f^{-1}(B)$ chuẩn tắc trong G.

Ngược lại, giả sử $f^{-1}(B)$ là chuẩn tắc trong G. Khi đó với mọi $b \in B$ và với mọi $x \in H$, do f là toàn cấu nên tồn tại $a \in f^{-1}(B)$ để $f(a) = b$ và $g \in G$ để $f(g) = x$. Do $f^{-1}(B)$ chuẩn tắc trong G nên $g^{-1}ag \in f^{-1}(B)$. Suy ra $f(g^{-1}ag) \in f(f^{-1}(B)) = B$ (do f là toàn cấu). Hay $f(g^{-1}ag) = [f(g)]^{-1}f(a)f(g) = x^{-1}bx \in B$. Vậy B là nhóm con chuẩn tắc trong H.

Tiếp đến, xét ánh xạ $\varphi : G \to H/B$ được xác định bởi $\varphi(x) = f(x)B$. Khi đó φ là một toàn cấu và $\mathrm{Ker}\varphi = f^{-1}(B)$. Theo Định lý đồng cấu nhóm ta có: $G/f^{-1}(B) \cong H/B$.

5.23. Theo Bài tập 5.22 ta có: nếu $f : X \to Y$ là một toàn cấu nhóm và A là một nhóm con chuẩn tắc của X thì $f(A)$ là một nhóm con chuẩn tắc của Y.

Bây giờ, do phép chiếu chính tắc $p : X \to X/A$ là một toàn cấu nhóm nên 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.

5.24. Giả sử H là nhóm con chuẩn tắc tối đại của G. Giả sử N là một nhóm con chuẩn tắc của G/H. Xét phép chiếu chính tắc

$$p : G \to G/H.$$

Tạo ảnh toàn phần $K = p^{-1}(N)$ là một nhóm con chuẩn tắc của G và chứa H. Do tính tối đại của H trong G nên ta phải có $K = H$ hoặc $K = G$. Khi đó $N = \{e\}$ hoặc $N = G/H$. Vậy G/H là một nhóm đơn.

Đảo lại, nếu G/H là một nhóm đơn và B là một nhóm con chuẩn tắc của G chứa H. Khi đó B/H là nhóm con của G/H. Do G/H là nhóm đơn nên $B/H = 0$ hoặc $B/H = G/H$. Suy ra $B = H$ hoặc $B = G$.

5.25. Giả sử a là phần tử tuỳ ý khác đơn vị của X và có cấp $n > 1$. Khi đó nhóm con xyclic A sinh bởi a có cấp n và n là ước của cấp p của G. Do p nguyên tố nên $n = p$. Nghĩa là $A = G$.

Dễ chứng minh φ_k là một tự đồng cấu nhóm. Ta có với mọi $x^i \in X$ thì $\varphi_(x^i) = x^{ik}$.

Giả sử $\varphi_k(x_i) = \varphi_k(x_j)$, nghĩa là

$$x^{ik} = x^{jk} \Rightarrow x^{(i-j)k} = e,$$

do đó $(i-j)k \vdots p \Rightarrow i = j + np$. Vậy $x^i = x^j$ hay φ_k là đơn cấu.

Giả sử $x^n \in X$ là phần tử tuỳ ý. Do $(k,p) = 1$ nên tồn tại $a, b \in \mathbb{Z}$ sao cho $ka + pb = 1 \Rightarrow kna + pnb = n$ nên $x^n = x^{k(qp+i)} = x^{ki}$. Vậy $\varphi_k(x^i) = x^{ki} = x^n$, do đó φ_k là toàn cấu.

5.26. a) Ta xét xem khi nào φ là ánh xạ. Do $x^r = x^{r+ls}, \forall l \in \mathbb{Z}$, nên φ là ánh xạ khi và chỉ khi

$$y^{kr} = y^{k(r+ls)} \Leftrightarrow y^{klr} = e, \forall l \in \mathbb{Z}$$

$$\Leftrightarrow kls \vdots t, \forall l \in \mathbb{Z} \Leftrightarrow ks \vdots t.$$

b) Bây giờ giả sử φ là một đơn cấu. Thế thì $X \cong \varphi(X)$, nghĩa là $\varphi(x) = y^k$ có cấp s (bằng cấp của x). Giả sử $sk = mt$. Nếu $(s,m) = d$ thì $\frac{s}{d}k = \frac{m}{d}t$, từ đó

$$(y^k)^{s/d} = (y^t)^{m/d} = e.$$

Bởi vậy, $\frac{s}{d} \vdots s$, nghĩa là $d = 1$.

5.27. a) Trước hết ta có thể chứng minh tương ứng

$$\begin{aligned} \varphi : X/A &\to f(X)/B \\ xA &\mapsto f(x)B \end{aligned}$$

là một ánh xạ, nghĩa là φ không phụ thuộc vào phần tử đại diện x. Dễ thấy φ là toàn cấu.

b) Theo Định lý đồng cấu ta có

$$\begin{aligned} f(X)/B &\cong (X/A)/\mathrm{Ker}\varphi \\ &\Rightarrow [X : A] = [f(X) : B]|\mathrm{Ker}\varphi|. \end{aligned}$$

Bây giờ nếu $xA \in \mathrm{Ker}\varphi$ thì $\varphi(xA) = f(x) \in f(A)$. Khi đó tồn tại $a \in A$ sao cho $f(x) = f(a)$. Từ đó

$$x = ac \quad \text{với} \quad c \in \mathrm{Ker}f.$$

Ta có đẳng cấu

$$A.\mathrm{Ker}f/A \cong \mathrm{Ker}f/(A \cap \mathrm{Ker}f) = \mathrm{Ker}f/K.$$

Vậy $|\mathrm{Ker}\varphi| = [\mathrm{Ker}f : K]$. Từ đó suy ra điều phải chứng minh.

5.28. Giả sử $A = \{e, a\}$ và $X/A = \{A, bA, b^2A, b^3A, b^4A\}$. Ta có X sinh bởi hai phần tử a và b. Mặt khác, vì A là một nhóm con chuẩn tắc nên $bA = Ab$. Như vậy $\{b, ba\} = \{b, ab\} \Rightarrow ab = ba$. Do đó $X = \langle a, b\rangle$ là một nhóm aben. Theo Định lý Lagrange, cấp của X bằng $2.5 = 10$. Do đó cấp của b bằng 5 hoặc 10. Nếu cấp của b bằng 10 thì $X = \langle b\rangle$ là nhóm xyclic sinh bởi b. Nếu cấp của b bằng 5 thì cấp của ab bằng 10. Do đó $X = \langle ab\rangle$. Như vậy X là một nhóm xyclic cấp 10 và $X \cong \mathbb{Z}_{10}$.

5.29. Giả sử X là một nhóm cấp 10. Nếu trong X có một phần tử cấp 10 thì X là một nhóm xyclic cấp 10 và do đó X đẳng cấu với nhóm $\mathbb{Z}_{10}$.

Bây giờ ta xét trường hợp nhóm X không có phần tử nào cấp 10. Từ Định lý Lagrange ta suy ra, mọi phần tử (khác đơn vị) của nhóm X có cấp bằng 2 hoặc 5. Ta sẽ chứng tỏ trong X tồn tại những phần tử cấp 2, những phần tử cấp 5. Thật vậy, giả sử mọi phần tử (khác đơn vị) của X đều có cấp bằng 2. Khi đó X là một nhóm giao hoán. Lấy $a, b \in X$. Đặt $c = ab = ba$. Ta có:

$$c^2 = abab = aabb = ee = e, \; ac = ca = b, bc = cb = a.$$

Từ đó suy ra $A = \{e, a, b, c\}$ là một nhóm con của X, điều này trái với Định lý Lagrange vì X là nhóm cấp 10, A là nhóm cấp 4.

Bây giờ ta giả sử mọi phần tử (khác đơn vị) của X đều có cấp bằng 5. Lấy $a \in X$, $a \neq e$. Vì $a^5 = e$ nên tồn tại $b \notin \langle a\rangle$. Từ đó kết hợp với giả thiết $b^5 = e$, suy ra chín phần tử sau là phân biệt:

$$\{e, a, a^2, a^3, a^4, b, b^2, b^3, b^4\}.$$

Xét tích $ab \in X$. Ta thấy ab không có dạng a^k vì nếu ngược lại thì $b = a^{k-1} \in \langle a\rangle$, trái giả thiết. Tương tự ab không có dạng b^k. Vậy

$$X = \{e, a, a^2, a^3, a^4, b, b^2, b^3, b^4, ab\}.$$

Xét $a^2b \in X$. Từ điều kiện $b \notin \langle a \rangle$, suy ra a^2b không có dạng a^i, b^j. Từ đó suy ra $a^2b = ab$, do vậy $a = e$. Điều này là vô lý.

Vậy trong nhóm X tồn tại những phần tử cấp 2, chẳng hạn là a, và những phần tử cấp 5, chẳng hạn là b.
Nếu $ab = ba$ thì ab có cấp bằng 10, trái giả thiết. Do đó $ab \neq ba$. Vậy nhóm X sinh bởi hai phần tử a, b thoả mãn các điều kiện

$$a^2 = b^5 = e, \ ab \neq ba.$$

Trong trường hợp này X đẳng cấu với nhóm D_5. Vậy mọi nhóm cấp 10 hoặc đẳng cấu với nhóm $\mathbb{Z}_{10}$, hoặc đẳng cấu với nhóm D_5.

5.30. a) Dễ thấy rằng G là một nhóm với phần tử đơn vị là $(0,0,0)$, nghịch đảo của phần tử (k_1, k_2, k_3) là $((-1)^{k_3+1}k_1, -k_2, -k_3)$.
b, c) Bằng quy nạp ta có thể chứng minh rằng

$$(1,0,0)^n = (n,0,0), \text{ với mọi } n \in \mathbb{N}.$$

Mặt khác, $(1,0,0)^{-n} = [(1,0,0)^{-1}]n = (-1,0,0)^n = (-n,0,0)$ với mọi $n \in \mathbb{N}$. Như vậy: $A = \{(n,0,0) | n \in \mathbb{Z}\}$.

Ánh xạ: $f : G \to \mathbb{Z}[i]$, $(k_1, k_2, k_3) \mapsto k_2 + ik_3$ là một toàn cấu nhóm. Ta có:

$$(k_1, k_2, k_3) \in \mathrm{Ker} f \Leftrightarrow k_2 + ik_3 = 0 \Leftrightarrow k_2 = k_3 = 0$$

$$\Leftrightarrow (k_1, k_2, k_3) = (k_1, 0, 0) \in A$$

Vậy $A = \mathrm{Ker} f$ là một nhóm con chuẩn tắc của G và ta có $G/A \cong \mathbb{Z}[i]$.

5.31. Giả sử $f : \mathbb{Q} \to \mathbb{Z}$ là một đồng cấu từ nhóm cộng $\mathbb{Q}$ đến nhóm cộng $\mathbb{Z}$. Nếu f không là đồng cấu không thì tồn tại một số hữu tỷ $q \neq 0$ sao cho $f(q) \neq 0$. Giả sử $q = \dfrac{r}{s} \in \mathbb{Q}$, với $r, s \in \mathbb{Z}$, $s > 0$. Khi đó $r = qs$ và $f(r) = f(qs) = s.f(q) \neq 0$.

Mặt khác, $f(r) = f(r.1) = rf(1)$ nên $f(1) = a \neq 0$. Bây giờ với $n \neq 0$ là một số nguyên bất kỳ ta có

$$f(1) = f(n.\frac{1}{n}) = n.f(\frac{1}{n}).$$

Như vậy, n là ước của $f(1) = a$. Điều này là vô lý.

Vậy chỉ có một đồng cấu duy nhất là đồng cấu không từ $\mathbb{Q}$ vào

$\mathbb{Z}$. Từ đó suy ra $\mathbb{Q}$ không đẳng cấu với $\mathbb{Z}$ nên $\mathbb{Q}$ không là một nhóm xyclic.

5.32. Nhóm các tự đẳng cấu của 4-nhóm Klein chính là S_3.

5.34. b) Ta có ánh xạ

$$\begin{array}{rccc} F: & \mathrm{End}(\mathbb{Z}) & \to & \mathbb{Z} \\ & f & \mapsto & F(f) = f(1) \end{array}$$

là một đẳng cấu. Thật vậy, với mọi f và g thuộc $\mathrm{End}(\mathbb{Z})$ ta có

$$F(f+g) = (f+g)(1) = f(1) + g(1) = F(f) + F(g).$$

Nếu $F(f) = F(g)$ thì $f(1) = g(1)$. Từ đó với mọi $n \in \mathbb{Z}$ ta có

$$f(n) = nf(1) = ng(1) = g(n)$$

nghĩa là $f = g$, và do đó F đơn cấu.

Với mọi $n \in \mathbb{Z}$, ánh xạ

$$\begin{array}{rccc} f: & \mathbb{Z} & \to & \mathbb{Z} \\ & a & \mapsto & na \end{array}$$

là một tự đồng cấu của $\mathbb{Z}$, và do $F(f) = f(1) = n$ nên F là một toàn cấu. Vậy

$$\mathrm{End}(\mathbb{Z}) \cong \mathbb{Z}.$$

c) Tương tự câu b) ánh xạ

$$\begin{array}{rccc} F: & \mathrm{End}(\mathbb{Q}) & \to & \mathbb{Q} \\ & f & \mapsto & f(1) \end{array}$$

là một đẳng cấu.

5.35. Xét đồng cấu $f: \mathbb{Z}_m \to \mathbb{Z}_n$, $[1]_m \mapsto [h]_n$, ta có:

$$[0]_n = f([0]_m) = f(m[1]_m) = mf([1]_m) = m[h]_n = mh[1]_n$$

từ đó, $mh \vdots n \Rightarrow \dfrac{m}{d}h \vdots \dfrac{n}{d} \Rightarrow h \vdots k$, với $k = \dfrac{m}{d}$. Suy ra

$$f([1]_m) = [h]_n = [tk]_n = k[t]_n \in k\mathbb{Z}_n \ (\cong Z_d).$$

Bây giờ xét tương ứng:

$$\begin{aligned}\Phi : \mathrm{Hom}(\mathbb{Z}_m, \mathbb{Z}_n) &\to k\mathbb{Z}_n \\ f &\mapsto f([1]_m)\end{aligned}$$

Nếu $f \in \mathrm{Ker}\Phi$ thì $f([1]_m) = 0$, nghĩa là f là đồng cấu không và do đó Φ đơn cấu.

Lấy $u \in k\mathbb{Z}_n, u = k[h]_n = [kh]_n$. Thế thì với $f([1]_m) = [kh]_n$ ta có $\Phi(f) = u$, nghĩa là Φ là toàn cấu và do đó Φ là đẳng cấu.

Cách 2. Ta chứng minh $\mathrm{Hom}(\mathbb{Z}_m, \mathbb{Z}_n)$ sinh bởi f, với $f([1]_m) = [k]_n$, $k = \dfrac{n}{d}$. Lấy $g : \mathbb{Z}_m \to \mathbb{Z}_n$ là một đồng cấu. Thế thì $g([1]_m) = [h]_n$. Phần tử $[h]_n$ có cấp s là ước của d. Từ đó, do $s[h]_n = [sh]_n = 0$ nên $sh \vdots kd$, suy ra $h \vdots k\dfrac{d}{s}$, và do đó $h = kt$. Bởi vậy $[h]_n = t[k]_n = tf([1]_m) = (tf)([1]_m)$. Điều này chứng tỏ $g = tf$.

Sau cùng ta chứng tỏ f có cấp bằng d. Thật vậy, dễ thấy $df = 0$. Nếu $sf = 0$ với $s \in \mathbb{Z}$ thì

$$0 = (sf)([1]_m) = sk[1]_n \Rightarrow sk \vdots n \Rightarrow s \vdots \frac{n}{k} = d.$$

Vậy d là cấp của f và do đó $\mathrm{Hom}\,(\mathbb{Z}_m, \mathbb{Z}_n) = \langle f \rangle \cong \mathbb{Z}_d$.

5.36. a) Trước hết, f là một đồng cấu, bởi vì với x và y thuộc G ta có

$$f_a(xy) = axya^{-1} = (axa^{-1})(aya^{-1}) = f_a(x)f_a(y).$$

Nếu $f_a(x) = f_a(y)$ tức là $axa^{-1} = aya^{-1}$ thì sau khi giản ước ta được $x = y$. Với mỗi $y \in G$ ta có $x = a^{-1}ya \in G$ 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 $a, b \in G$ thì $f_a f_b = f_{ab}$. Thật vậy, với mọi $x \in G$,

$$f_a.f_b(x) = f_a[f_b(x)] = f_a(bxb^{-1}) = abx(ab)^{-1} = f_{ab}(x).$$

Như vậy, tập hợp các tự đẳng cấu trong của nhóm G là một tập con ổn định của $Aut(G)$. Hơn nữa với mọi $a \in G$ ta có

$$f_{a^{-1}}.f_a = f_{a^{-1}a} = f_e = 1_X.$$

Do đó, tập hợp các tự đẳng cấu trong của G là nhóm con của $Aut(G)$. Bây giờ, giả sử H là một nhóm con chuẩn tắc của G 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 $a \in G$. Khi đó H là chuẩn tắc.

c) Xét ánh xạ

$$\begin{array}{rccc} f: & G & \to & A \\ & a & \mapsto & f(a) = f_a \end{array}$$

với A là nhóm các tự đẳng cấu trong của G. Khi đó 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 $a \in \mathrm{Ker}f$ khi và chỉ khi $f_a = 1_G$, nghĩa là với mọi $x \in G$ ta có

$$axa^{-1} = x \ \forall x \in G \Leftrightarrow ax = xa \ \forall x \in G \ \Leftrightarrow \ a \in Z(G).$$

Vậy $\mathrm{Ker}f = Z(G)$. Theo định lý đồng cấu ta có $G/Z(G) \cong A$.

5.37. Ta hãy chứng minh a) $\Rightarrow$ b). Giả sử tồn tại một đồng cấu $h : H \to K$ sao cho $g = h \circ k$. Nếu $x \in G$ sao cho $f(x) = e_H$ thì

$$g(x) = hf(x) = h(f(x)) = h(e_H) = e_K,$$

nghĩa là $\mathrm{Ker}f \subset \mathrm{Ker}g$.

b) $\Rightarrow$ a). Giả sử $\mathrm{Ker}f \subset \mathrm{Ker}g$. 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 $f(x_1) = f(x_2)$ thì

$$f(x_1x_2^{-1}) = e_H \text{ hay } x_1x_2^{-1} \in \mathrm{Ker}f \subset \mathrm{Ker}g.$$

Khi đó: $g(x_1x_2^{-1}) = e_K$ hay $g(x_1) = g(x_2)$. Dễ thấy, h là một đồng cấu. Hơn nữa, theo cách xây dựng h ta có $g = h \circ f$.

c) Tính duy nhất của h được suy ra từ tính chất f là toàn cấu.

d) Ta hãy tìm $\mathrm{Ker}h$. Ta có

$$\begin{aligned} \mathrm{Ker}h &= \{y \in H \mid h(y) = e_K\} \\ &= \{f(x) \mid h(f(x)) = g(x) = e_K\} = f(\mathrm{Ker}g). \end{aligned}$$

Vậy nếu h là một đơn cấu thì $\mathrm{Ker}h = f(\mathrm{Ker}g) = \{e_H\}$, suy ra $\mathrm{Ker}g \subseteq \mathrm{Ker}f$ và do đó $\mathrm{Ker}g = \mathrm{Ker}f$.

Đảo lại, nếu $\mathrm{Ker}g = \mathrm{Ker}f$ thì $\mathrm{Ker}h = \{e_H\}$ do đó h là đơn cấu.

e) Ta có $\mathrm{Im}h = h \circ f(G) = f(G)$. Vậy

$$h(H) = \mathrm{Im}h = K \Leftrightarrow g(G) = K$$

hay h là toàn ánh khi và chỉ khi g là toàn ánh.

5.39. Do $g^p = e$ với mọi $g \in G$ và p là số nguyên tố nên mọi phần tử của G đều có cấp 1 hoặc p. Trong đó e là phần tử duy nhất có cấp 1, còn lại mọi phần tử khác của G đều có cấp p.

Chọn các phần tử $g_1, g_2, ..., g_n \in G$ sao cho $g_i \neq e$ và g_i không thể viết được dưới dạng tích của các luỹ thừa của $g_1, ..., g_{i-1}$. Hơn nữa, chọn n là số lớn nhất thoả mãn điều kiện đó. Vì vậy mọi phần tử của G đều biểu diễn được qua các luỹ thừa của các phần tử g_i.

Có thể thấy ánh xạ

$$\begin{array}{ccc} f : \mathbb{Z}_p^n & \to & G \\ (\bar{z}_1, ..., \bar{z}_n) & \mapsto & g_1^{z_1} ... g_n^{z_n} \end{array}$$

là một đẳng cấu. Thật vậy,

$$\begin{aligned} f((z_1, ..., z_n)(y_1, ..., y_n)) &= f(z_1 + y_1, ..., z_n + y_n) \\ &= g_1^{z_1+y_1} ... g_n^{z_n+y_n} = g_1^{z_1} ... g_n^{z_n} . g_1^{y_1} ... g_n^{y_n} \text{ (do } G \text{ abel)} \\ &= f(z_1, ..., z_n) f(y_1, ..., y_n) \end{aligned}$$

Vậy f là một đồng cấu nhóm.

Giả sử $(z_1, ..., z_n) \in \mathrm{Ker}f$ và z_i là số cuối cùng bé hơn p (nghĩa là $z_{i+1}, ..., z_n$ đều bằng p). Khi đó

$$g_1^{z_1} ... g_i^{z_i} = e$$

Nhân hai vế của đẳng thức này với $g_i^{p-z_i}$ ta được: $g_i^{p-z_i} = g_1^{z_1} ... g_{i-1}^{z_{i-1}}$. Điều này mâu thuẫn với cách chọn g_i. Vậy $z_i = p$ với mọi $i = 1, ..., n$ hay f là đơn ánh.

Tính toàn ánh của f được suy ra từ cách chọn các phần tử g_i. Vậy f là đẳng cấu và ta có $G \cong Z_p^n$.

5.40. Dễ thấy tích của hai ma trận có định thức bằng 1 lại là một ma trận có định thức bằng 1. Ma trận $A \in G_p$ có $\det A = 1 \neq 0$ nên nó có

ma trận nghịch đảo và ma trận nghịch dảo cũng có định thức bằng 1. Ngoài ra, ma trận

$$\begin{bmatrix} \overline{1} & 0 \\ 0 & \overline{1} \end{bmatrix}$$

là phần tử đơn vị của G_p. Vậy G_p là một nhóm.

$\mathbb{Z}_p$ có p phần tử. Từ dẳng thức $ad - bc = 1$ suy ra a có thể lấy một trong p giá trị của $\mathbb{Z}_p$. Tương tự, b và c có thể nhận một trong p giá trị của $\mathbb{Z}_p$. Do dó nếu đã chọn được a, b, c thì do đẳng thức $ad - bc = 1$, d chỉ có thể nhận một giá trị duy nhất. Vậy theo quy tắc nhân ta có $p.p.p.1$ bộ 4 giá trị của a, b, c, d thoả mãn $ad - bc = 1$. Nhưng trong đó có p cặp giá trị của b và c trùng nhau nên thực ra ta có $p^3 - p = p(p^2 - 1)$ bộ giá trị của a, b, c, d. Vậy G_p có cấp $p(p^2 - 1)$.

Ta có $G_2 \cong S_3$.

5.41. Giả sử nhóm G được sinh bởi hai ma trận:

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \qquad B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Đặt $E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ là ma trận đơn vị cấp 2, ta có:

$$A^2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$A^3 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

$$A^4 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = E$$

$$B^2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = E$$

$$AB = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = BA^3$$

$$BA = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = A^3B$$

$$A^2B = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} = BA^2$$

Vậy $G = \{E, A, A^2, A^3, B, AB, A^2B, A^3B\}$ nên G có cấp 8. Do

$AB \neq BA$ nên G không aben.

Ta có $G \cong D_4$.

5.42. Lấy A là nhóm thương G/G', trong đó G' là nhóm con của G sinh bởi các phần tử có dạng $xyx^{-1}y^{-1}$, $x, y \in G$. Đồng cấu $\alpha : G \to A$ được chọn là phép chiếu tự nhiên.

Giả sử H là nhóm aben và $h : G \to H$ là một đồng cấu nhóm. Gọi $K = \text{Ker}h$, thế thì có một đơn cấu: $G/K \to H$ và do đó G/K là giao hoán,

$$(xK)(yK) = (yK)(xK) \Rightarrow xyx^{-1}y^{-1} \in K.$$

Từ đó $G' \subset K$. Khi đó thiết lập đồng cấu:

$$\begin{aligned} f : A = G/G' &\to H \\ xG' &\mapsto i(xK) \end{aligned}$$

Dễ kiểm tra lại được rằng f là đồng cấu duy nhất thoả mãn $h = f\alpha$.

Chương III

CẤU TRÚC NHÓM

1. Tích trực tiếp

1.1. Do $(2,3) = 1$ nên $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$.

1.2. Với mọi $x \in C_{10}$, $y \in C_6$ ta có:

$$x^{10} = e,\ y^6 = e.$$

Do đó

$$(x,y)^{30} = ((x^{10})^3, (y^6)^5) = (e,e).$$

Vậy mọi phần tử của nhóm $C_{10} \times C_6$ đều có cấp nhỏ hơn hoặc bằng 30. Mặt khác, nhóm C_{60} là nhóm xyclic cấp 60 nên phần tử sinh có cấp 60. Do đó, hai nhóm C_{60} và $C_{10} \times C_6$ không đẳng cấu với nhau.

1.3. D_n và $C_n \times C_2$ không đẳng cấu với nhau vì $C_n \times C_2$ là nhóm giao hoán, còn D_n không giao hoán.

1.4. Không, mọi phần tử của nhóm $\mathbb{Z}_4 \times \mathbb{Z}_2$ đều có cấp nhỏ hơn hoặc bằng 4, trong khi đó phần tử $(1+i)/\sqrt{2}$ có cấp bằng 8.

1.5. Giả sử (g,h) là một phần tử sinh của nhóm $G \times H$. Ta sẽ chứng tỏ G, H là những nhóm xyclic tương ứng sinh bởi g và h.

Thật vậy, lấy $x \in G$ bất kỳ. Khi đó ta có: $(x, e_H) \in G \times H$. Do vậy, tồn tại số nguyên n sao cho

$$(x, e_H) = (g,h)^n.$$

Từ đó suy ra $x = g^n$. Vậy G là nhóm xyclic sinh bởi g. Chứng minh tương tự, H là nhóm xyclic sinh bởi h.

1.6. Giả sử $X \times Y$ là một nhóm xyclic và $(m, n) = d > 1$. Khi đó với mọi $(x, y) \in X \times Y$ ta có:

$$(x, y)^{\frac{mn}{d}} = ((x^m)^{\frac{n}{d}}, (y^n)^{\frac{m}{d}}) = (e_X, e_Y).$$

Từ đó suy ra trong nhóm $X \times Y$, mọi phần tử đều có cấp nhỏ hơn hoặc bằng $\frac{mn}{d}$, và do đó nó không có một phần tử nào có cấp bằng mn. Điều này trái với giả thiết $X \times Y$ là một nhóm xyclic có cấp bằng mn. Vậy m, n nguyên tố cùng nhau.

Dảo lại, giả sử m, n nguyên tố cùng nhau. Gọi g, h tương ứng là phần tử sinh của X, Y. Ta sẽ chứng minh (g, h) là phần tử sinh của $X \times Y$. Thật vậy ta có:

$$(g, h)^{mn} = ((g^m)^n, (h^n)^m) = (e_X, e_Y).$$

Bây giờ giả sử $(g, h)^k = (e_X, e_Y)$, nghĩa là $(g^k, h^k) = (e_X, e_Y)$. Dọ g, h có cấp tương ứng bằng m, n nên ta suy ra $k \vdots m$, $k \vdots n$. Vì m, n nguyên tố cùng nhau nên ta suy ra $k \vdots mn$. Vậy (g, h) có cấp bằng mn, nghĩa là (g, h) là phần tử sinh của nhóm $X \times Y$. Vậy $X \times Y$ là một nhóm xyclic.

1.7. Giả sử X là một nhóm cấp 4. Nếu trong X tồn tại một phần tử cấp 4 thì X là một nhóm xyclic cấp 4, và do đó nó dẳng cấu với nhóm $\mathbb{Z}_4$. Nếu trong X không tồn tại một phần tử cấp 4 thì từ định lý Lagrange ta suy ra mọi phần tử khác đơn vị của X đều có cấp bằng 2. Giả sử $X = \{e, a, b, c\}$, trong đó $a^2 = b^2 = c^2 = e$. Xét tích ab. Nếu $ab = e$ thì $ab = e = aa$, suy ra $a = b$, điều này không xảy ra. Vậy $ab \neq e$. Chứng minh tương tự ta suy ra $ab \neq a, b$. Vậy $ab = c$. Lập luận tương tự, trong nhóm X ta có:

$$ab = ba = c,\ bc = cb = a,\ ac = ca = b.$$

Xét ánh xạ

$$\begin{aligned} f : X &\to \mathbb{Z}_2 \times \mathbb{Z}_2 \\ e &\mapsto 0 \\ a &\mapsto (\overline{1}, \overline{0}) \\ b &\mapsto (\overline{0}, \overline{1}) \\ c &\mapsto (\overline{1}, \overline{1}). \end{aligned}$$

Chúng ta có thể thử lại được rằng f là một đẳng cấu. Vậy $X \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

1.8. Không thể phân tích $\mathbb{Z}$ thành tích của hai nhóm aben vì hai nhóm con thực sự của $\mathbb{Z}$ đều có giao khác rỗng.

1.9. Trước hết ta chứng tỏ rằng $A \cap B = e$. Thật vậy, giả sử $x \in A \cap B$. Do $x \in B = \mathrm{Ker} f$ nên ta có $f(x) = e$, suy ra $k(x) = e$. Do k là một đẳng cấu nên ta có $x = e$.

Với $x \in G$ bất kỳ, do $k = f|_A$ là một đẳng cấu nên tồn tại $a \in A$ sao cho $k(a) = g(x)$. Khi đó ta có:

$$g(x.a^{-1}) = g(x)g(a^{-1}) = g(x)(g(a))^{-1} = g(x)(k(a))^{-1} = e.$$

Suy ra $x.a^{-1} = b \in \mathrm{Ker} f = B$. Vậy $x = a.b \in AB$. Giả sử ta còn có thể phân tích $x = cd$ với $c \in A, d \in B$. Khi đó: $a.c^{-1} = d.b^{-1} \in A \cap B$. Theo nhận xét ở trên ta suy ra $a.c^{-1} = d.b^{-1} = e$. Từ đó suy ra $a = c$. $b = d$. Vậy $G = AB$.

1.10. Giả sử $x \in \mathrm{Ker}\beta \cap \mathrm{Im}\gamma$. Khi đó tồn tại $c \in C$ sao cho $x = \gamma(c)$. Từ đó:

$$c = (\beta \circ \gamma)(c) = \beta(x) = 0.$$

Suy ra $x = \gamma(c) = 0$. Vậy $\mathrm{Ker}\beta \cap \mathrm{Im}\gamma = 0$.

Lấy $b \in B$ bất kỳ. Đặt $u = \gamma(\beta(b)) \in \mathrm{Im}\gamma$. Ta có

$$\beta(u) = \beta(\gamma(\beta(b))) = (\beta\gamma)[\beta(b)] = \beta(b).$$

Suy ra $\beta(b - u) = 0$, nghĩa là: $b - u = v \in \mathrm{Ker}\beta$. Vậy:
$b = u + v \in \mathrm{Ker}\beta \oplus \mathrm{Im}\gamma$, và do đó $B = \mathrm{Ker}\beta \oplus \mathrm{Im}\gamma$.

1.11. Ta có ánh xạ

$$\begin{aligned} p_1 : G \times H &\to G \\ (g, h) &\mapsto g \end{aligned}$$

là một toàn cấu có: $\mathrm{Ker} p_1 = H'$. Từ đó suy ra $(G \times H)/H' \cong G$. Chứng minh tương tự ta được $(G \times H)/G' \cong H$.

1.12. a) $X \times Y$ là nhóm giao hoán khi và chỉ khi

$$(a, b).(x, y) = (x, y).(a, b)$$

với mọi (a, b). $(x, y) \in X \times Y$. Điều này tương dương với

$$ax = xa, \quad by = yb$$

với mọi $a, x \in X$; $b, y \in Y$, nghĩa là X, Y là những nhóm giao hoán.

b) Phần tử (a, b) thuộc tâm của nhóm $X \times Y$ khi và chỉ khi

$$(a, b).(x, y) = (x, y).(a, b)$$

với mọi $(x, y) \in X \times Y$. Điều này xảy ra khi và chỉ khi

$$ax = xa, \quad by = yb$$

với mọi $x \in X$, $y \in Y$. Điều này có nghĩa là $a \in Z(X)$, $b \in Z(Y)$. Vậy tâm của nhóm $X \times Y$ là $Z(X) \times Z(Y)$.

1.13. a) h là một đồng cấu khi và chỉ khi $h(x_1x_2) = h(x_1)h(x_2)$, nghĩa là:

$$(f(x_1x_2), g(x_1x_2)) = (f(x_1), g(x_1)).(f(x_2), g(x_2))$$

với mọi $x_1, x_2 \in X$. Điều này xảy ra khi và chỉ khi

$$f(x_1x_2) = f(x_1)f(x_2), \quad g(x_1x_2) = g(x_1)g(x_2).$$

Vậy h là một đồng cấu khi và chỉ khi f và g là những đồng cấu.

b) Giả sử f là đơn ánh. Nếu $h(x) = 0$ thì ta suy ra $f(x) = 0$. Từ đó suy ra $x = 0$. Vậy h là một đơn cấu.
Tương tự nếu g là một đơn cấu thì h là một đơn cấu.

Nếu h là một đơn cấu thì ta không suy ra được f, g là đơn cấu. Ví dụ:

Chọn $X = Y = Z$ là nhóm xyclic cấp 6 sinh bởi x, còn f, g là những ánh xạ xác định bởi:

$$f(x) = x^2, \quad g(x) = x^3.$$

Khi đó ta dễ thấy f và g không phải là đơn ánh, tuy nhiên h là đơn ánh.

c) Giả sử h là một toàn cấu. Khi đó với mọi $y \in Y, z \in Z$, tồn tại $x \in X$ sao cho $h(x) = (y, z)$. Từ đó suy ra $f(x) = y$, $g(x) = z$. Vậy f và g là những toàn cấu.

Nếu f và g là những toàn cấu thì không suy ra được h là toàn cấu. Chẳng hạn lấy $f = g = id : \mathbb{Z} \to \mathbb{Z}$. Khi đó không tồn tại $x \in \mathbb{Z}$ để $h(x) = (0, 1)$.

1.14. Dễ thấy ánh xạ

$$\begin{aligned} h : L &\to G \times G' \\ x &\mapsto (g(x), g'(x)) \end{aligned}$$

là một đồng cấu nhóm thoả mãn các điều kiện $g = p \circ h,\ g' = p' \circ h$.

Bây giờ giả sử $k : L \to G \times G'$ cũng là một đồng cấu thỏa mãn $g = p \circ k,\ g' = p' \circ k$. Đặt $k(x) = (u(x), v(x)),\ x \in L$. Ta có

$$g(x) = p \circ k(x) = p((u(x), v(x))) = u(x).$$

Từ đó suy ra $u(x) = g(x)$. Chứng minh tương tự ta có $v(x) = g'(x)$. Vậy $k = h$.

1.15. Ta có $a^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ -0 & -1 \end{pmatrix} = -I$

Suy ra $a^4 = (-I)^2 = I$. Vậy a có cấp 4.

$$b^2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$$

$$b^3 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Vậy b có cấp 3. Ta có

$$ab = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Bằng quy nạp ta chứng minh được

$$(ab)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

Vậy ab có cấp vô hạn.

Ngược lại $a = (\overline{1}, 1), b = (\overline{1}, -1) \in \mathbb{Z}_2 \oplus \mathbb{Z}$ là hai phần tử khác không có cấp vô hạn nhưng $a + b = (\overline{0}, 0) = e$ có cấp hữu hạn bằng 1.

2. Nhóm đối xứng

2.1. Đơn vị có cấp 1, các phần tử $(12)(34), (13)(24), (14)(23)$ có cấp bằng 2; tất cả các phần tử còn lại đều có cấp bằng 3.

2.2. Nhóm con $X = \{(1), (123), (132)\}$ không chuẩn tắc trong A_4 vì với $f = (12)(34)$ ta có:

$$f \circ (123) \circ f^{-1} = (142) \notin X.$$

2.3. $K = \{id, (12)(34), (13)(24), (14)(23)\}$.

2.4. Không, D_6 có chứa những phần tử cấp 6, A_4 không có phần tử nào cấp 6 (xem Bài tập 2.1).

2.5. Giả sử X là một nhóm cấp 6.

Nếu trong nhóm X tồn tại một phần tử cấp 6 thì X là một nhóm xyclic cấp 6, và do đó X đẳng cấu với nhóm $\mathbb{Z}_6$.

Bây giờ ta xét trường hợp trong nhóm X không có phần tử nào cấp 6. Chúng ta sẽ chỉ ra rằng trong X tồn tại những phần tử có cấp 2, những phần tử có cấp 3.

Thật vậy, giả sử trong nhóm X, những phần tử khác đơn vị đều có cấp bằng 3. Lấy $a \in X$, $a \neq e$.

Lấy $b \notin \langle a \rangle$. Khi đó $b^2 \notin \langle a \rangle$, vì nếu $b^2 \in \langle a \rangle$ thì $b = b^4 \in \langle a \rangle$ (mâu thuẫn). Vậy $b\langle a \rangle \neq \langle a \rangle$, $b^2\langle a \rangle \neq \langle a \rangle$. Mặt khác do số lớp ghép trái của X theo nhóm con $\langle a \rangle$ bằng 2 nên ta có $b^2\langle a \rangle = b\langle a \rangle$. Do đó $b^2.b^{-1} \in \langle a \rangle$, hay là $b \in \langle a \rangle$, trái với cách chọn b. Điều này chứng tỏ trong nhóm X có những phần tử cấp 2.

Tiếp theo ta giả sử trong nhóm X, những phần tử khác đơn vị đều có cấp bằng 2. Lấy $a \in X$, $a \neq e$. Đặt

$$X \setminus \langle a \rangle = \{m, n, p, q\}.$$

Khi đó $m\langle a \rangle, n\langle a \rangle, p\langle a \rangle, q\langle a \rangle$ đều khác $\langle a \rangle$. Mặt khác do số lớp ghép trái của nhóm X theo nhóm con $\langle a \rangle$ bằng 3 nên tồn tại ít nhất hai lớp ghép trái nói trên là trùng nhau, chẳng hạn $m\langle a \rangle = n\langle a \rangle$. Do a, m, n có cấp bằng 2 nên ta suy ra $m = an, n = am$. Khi đó $\{e, a, m, n\}$ là một nhóm con cấp 4 của nhóm X có cấp bằng 6. Điều này mâu thuẫn với định lý Lagrange.

Vậy trong nhóm X tồn tại một phần tử a có cấp 3, một phần tử b có cấp 2.

Nếu $ab = ba$ thì phần tử ab có cấp bằng 6, trái với giả thiết trong X không có phần tử cấp 6.

Vậy $ab \neq ba$. Khi đó

$$X = \left\{e, a, a^2, b, ab, ba\right\}.$$

Lập bảng toán trên X và so sánh với bảng toán trên S_3 ta suy ra:

$$X \cong S_3.$$

2.6. Ta có: $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{0, a, b, c\}$, trong đó:

$$0 = (\bar{0}, \bar{0}), a = (\bar{1}, \bar{0}), b = (\bar{0}, \bar{1}), c = (\bar{1}, \bar{1}).$$

Lấy $f \in \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ và $f \neq id$. Hiển nhiên $f(0) = 0$. Do f là một đơn cấu nên ta có $f(a) \neq f(0) = 0$. Do đó: $f(a) \in \{a, b, c\}$.

Trường hợp 1: $f(a) = a$. Khi đó do f là một đơn cấu nên ta có

$$f(b) \neq f(a) = a, \ f(b) \neq f(0) = 0.$$

Do vậy $f(b) = b$ hoặc $f(b) = c$. Mặt khác do $f \neq id$ nên $f(b) = c$. Từ đó suy ra $f(c) = b$. Ta thấy ánh xạ xác định như trên là một đồng cấu. Vậy f là một đẳng cấu.

· Trường hợp 2: $f(a) = b$. Do f là một đơn cấu nên ta suy ra $f(b) = a$ hoặc $f(b) = c$.

Nếu $f(b) = a$ thì ta suy ra $f(c) = c$.

Nếu $f(b) = c$ thì ta suy ra $f(c) = a$.

Trong trường hợp này ta thu được hai tự đẳng cấu của $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Trường hợp 3: $f(a) = c$. Lập luận tương tự trường hợp 2, ta thu được 2 tự đẳng cấu của $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Tóm lại $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ là một nhóm cấp 6. Hơn nữa đây là nhóm không giao hoán. Do đó, theo Bài tập 2.5, $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ đẳng cấu với nhóm S_3.

2.7. Đặt $X = \{f_1, f_2, f_3, f_4, f_5, f_6\}$. Chúng ta có thể thử lại được rằng X là một nhóm cấp 6. Mặt khác ta có:

$$f_2 f_3(x) = f_2(\frac{1}{x}) = 1 - \frac{1}{x}$$

$$f_3 f_2(x) = f_3(1 - x) = \frac{1}{1 - x}$$

Từ đó suy ra $f_2 f_3 \neq f_3 f_2$. Vậy X là một nhóm cấp 6 không giao hoán. Theo Bài tập 2.5, X đẳng cấu với nhóm S_3.

2.8. Giả sử tồn tại nhóm con G của A_4 có cấp bằng 6. Khi đó theo Bài tập 2.5, hoặc G đẳng cấu với nhóm $\mathbb{Z}_6$, hoặc G đẳng cấu với nhóm S_3.

Mặt khác, do mọi phần tử của A_4 đều không có cấp 6 nên $G \cong S_3$. Điều này không thể xảy ra bởi vì trong nhóm S_3 tồn tại ba phép chuyển trí có cấp bằng 2, còn trong A_4 có đúng ba phần tử cấp 2 và không phải là các phép chuyển trí:

$$(12)(34),\ (13)(24),\ (14)(23).$$

Vậy nhóm A_4 không có nhóm con nào có cấp 6.

2.9. Để thuận lợi khi trình bày, ta có thể giả sử $\pi = (1\ 2\ \ldots\ r)$. Do mỗi $\rho \in S_n$ đều là tích của các phép chuyển trí nên ta chỉ cần chứng minh cho trường hợp ρ là một phép chuyển trí. Giả sử $\rho = (i\ j)$ với $i < j$.

Nếu $i, j > r$ thì $\rho^{-1} \circ \pi \circ \rho = \pi$ là một $r-$vòng xích.

Nếu $i, j < r$ thì

$$\rho^{-1} \circ \pi \circ \rho = (1\ 2\ \ldots\ (i-1)\ j\ (i+1)\ (i+2)\ \ldots (j-1)\ i\ (j+1)\ \ldots\ r)$$

là một $r-$vòng xích.

Các trường hợp $j = r$ hoặc $i = r$ hoặc $i < r < j$ được xét tương tự.

2.10. A_4 là một nhóm cấp 12 với các các phần tử là: e, $a_1 = (12)(34)$, $a_2 = (13)(24)$, $a_3 = (14)(23)$, $b_1 = (123)$, $b_1^2 = (132)$, $b_2 = (124)$, $b_2^2 = (142)$, $b_3 = (134)$, $b_3^2 = (143)$, $b_4 = (234)$, $b_4^2 = (243)$, trong đó các phần tử a_1, a_2, a_3 có cấp bằng 2, các phần tử b_1, b_2, b_3, b_4 có cấp bằng 3.

Giả sử H là một nhóm con bất kỳ của A_4. Vì A_4 là một nhóm có cấp bằng 12 nên theo Định lý Lagrange, cấp của H chỉ có thể là 1, 2, 3, 4, 6, 12. Theo Bài tập 2.8, cấp của H không thể bằng 6.

Nếu H có cấp 1 thì $H = \{e\}$.

Nếu H có cấp bằng 12 thì $H = A_4$.

Nếu H có cấp bằng 2 thì H là một nhóm xyclic. Khi đó H chỉ có thể là một trong ba nhóm: $\langle a_1 \rangle$, $\langle a_2 \rangle$, $\langle a_3 \rangle$.

Nếu H có cấp bằng 3 thì H là một nhóm xyclic cấp 3. Khi đó H chỉ có thể là một trong các nhóm: $\langle b_1 \rangle$, $\langle b_2 \rangle$, $\langle b_3 \rangle$, $\langle b_4 \rangle$.

Nếu H là một nhóm cấp 4 thì $H = \{e, a_1, a_2, a_3\}$.

2.11. Gọi A là tập các phép thế chẵn trong G thì $A \neq \emptyset$ vì $Id \in A$.

Với a, b là các phép thế lẻ bất kỳ trong G ta có ab^{-1} là phép thế chẵn nên $ab^{-1} \in A_n$.

Với c, d là các phép thế chẵn bất kỳ trong G thì cd^{-1} là phép thế chẵn và $cd^{-1} \in A$.

Vậy tập các phép thế lẻ trong G lập thành một lớp ghép theo A và tập các phép thế chẵn trong G lập thành một lớp ghép theo A. Do đó A là nhóm con có chỉ số 2 của G.

Khi đó trong G có sự phân lớp theo lớp ghép trái $\{A, gA\}$ và sự phân lớp theo lớp ghép phải $\{A, Ag\}$. Từ đó $Ag = gA$ hay A là nhóm con chuẩn tắc của G.

2.12. Lập bảng nhân của K, suy ra K là nhóm con giao hoán của S_4. Hơn nữa, mọi phần tử khác đơn vị của K đều có cấp bằng 2. Từ đó suy ra K đẳng cấu với 4−nhóm Klein.

Mặt khác, với mọi phần tử f của S_4 ta có:

$$f \circ (i\ j) \circ f^{-1} = (f(i)\ f(j)).$$

Do đó:

$$\begin{aligned} f \circ (1\ 2) \circ (3\ 4) \circ f^{-1} &= f \circ (1\ 2) \circ f^{-1} \circ f \circ (3\ 4) \circ f^{-1} \\ &= (f(1)\ f(2)) \circ (f(3)\ f(4)) \in K. \end{aligned}$$

Tương tự

$$f \circ (1\ 3) \circ (2\ 4) \circ f^{-1},\ f \circ (1\ 4) \circ (2\ 3) \circ f^{-1} \in K.$$

Từ đó suy ra K là nhóm con chuẩn tắc của S_4.

S_4/K là nhóm cấp 6 không giao hoán, kết hợp với Bài tập 2.5. ta suy ra nó đẳng cấu với nhóm S_3.

2.13. Theo Bài tập 2.12, K là nhóm con chuẩn tắc của S_4. Mặt khác vì A_4 là nhóm con của S_4 chứa K nên K là nhóm con chuẩn tắc của A_4.

Bởi vì A_4 là nhóm cấp 12, K là nhóm con cấp 4 nên A_4/K là một nhóm có cấp bằng 3. Từ Định lý Lagrange ta suy ra A_4/K là một nhóm xyclic, và do đó nó đẳng cấu với nhóm C_3.

2.14. Ta dễ dàng kiểm tra được rằng f là một đồng cấu với

$$\mathrm{Ker} f = e,\ \mathrm{Im} f = \{\sigma \in S_{n+1} |\ \sigma(n+1) = n+1\}.$$

2.15. Do mỗi phép thế đều là tích của những phép chuyển trí nên ta chỉ cần chứng minh mỗi phép chuyển trí đều thuộc nhóm con X sinh bởi tập $\{(12),\ (23),\ ...,(n-1\ \ n)\}$. Để đạt được điều này, ta sẽ chứng tỏ rằng với mỗi i cố định, $k = 1, 2, ...$ ta có $(i\ i+k) \in X$.
Hiển nhiên với $k = 1$ ta có $(i\ i+k) = (i\ i+1) \in X$.
Giả sử ta đã có $(i\ i+k) \in X$. Khi đó từ đẳng thức:

$$(i\ \ i+k+1) = (i\ \ k)(k\ \ k+1)(i\ \ k)$$

ta suy ra $(i\ i+k+1) \in X$.

2.16. Đặt $\sigma = (1\ 2\ 3\ ...\ n)$, $\tau = (1\ 2)$. Ta sẽ chứng minh bằng phương pháp quy nạp hệ thức sau:

$$(i\ \ i+1) = \sigma^{i-1} \circ \tau \circ \sigma^{1-i}.$$

Hiển nhiên hệ thức trên đúng với $i = 1$. Giả sử hệ thức trên đã đúng với $i > 1$. Ta có:

$$\begin{aligned}(i+1\ i+2)\sigma &= (1\ 2\ ...\ i\ i+2\ i+3\ ...\ n);\\ \sigma(i\ i+1) &= (1\ 2\ ...\ i\ i+2\ i+3\ ...\ n).\end{aligned}$$

Suy ra $(i+1\ i+2)\sigma = \sigma(i\ i+1)$. Do đó:

$$(i+1\ i+2) = \sigma(i\ i+1)\sigma^{-1} = \sigma\sigma^{i-1} \circ \tau \circ \sigma^{1-i}\sigma^{-1} = \sigma^i \circ \tau \circ \sigma^{-i}.$$

Vậy với mọi i ta có $(i\ i+1) \in \langle\{\sigma, \tau\}\rangle$. Từ đó theo Bài tập 2.15 ta suy ra $S_n = \langle\{\sigma, \tau\}\rangle$.

2.17. Đặt $f = (1\ 2\ ...\ n-1), \tau = (n-1\ n)$. Với mỗi $i = 1, 2, ..., n-1$ ta có:

$$(i\ n) = f\tau f^{-1}.$$

Mặt khác với mọi phép chuyển trí $(i\ j)$ ta có:

$$(i\ j) = (i\ n)(j\ n)(i\ n).$$

Do đó mọi phép chuyển trí $(i\ j)$ là tích của những luỹ thừa của f và τ. Vì S_n được sinh ra từ các phép chuyển trí nên S_n được sinh ra bởi f và τ.

2.18. Mỗi phần tử của A_n là tích của một số chẵn các phép chuyển trí. Với hai phép chuyển trí khác nhau, ta có:

Nếu $\tau = (ij)$ và $\tau' = (kl)$ độc lập với nhau thì

$$\tau'\tau = (ikj)(ilj)(ijk)(ijl).$$

Nếu τ và τ' không độc lập với nhau, $\tau = (ij), \tau' = (jk)$, thì

$$\tau\tau' = (ij)(jk) = (jki).$$

Như vậy $\tau\tau'$ là tích của một số hữu hạn những vòng xích độ dài 3 và do đó mỗi phần tử $f \in A_n$ cũng vậy. Vậy A_n sinh bởi các vòng xích độ dài 3.

2.19. Chúng ta lưu ý rằng hai vòng xích độc lập thì giao hoán với nhau. Trước hết ta chứng minh bài toán cho trường hợp $\sigma = \sigma_1\sigma_2$, với σ_1, σ_2 độc lập.

Gọi n_1, n_2 lần lượt là cấp của σ_1, σ_2. Gọi $d = (n_1, n_2)$. Khi đó $n_1 = dx_1$, $n_2 = dx_2$ với $(x_1, x_2) = 1$. Ta có $[n_1, n_2] = dx_1x_2$. Do $\sigma_1\sigma_2 = \sigma_2\sigma_1$ nên ta có

$$\sigma^{dx_1x_2} = \sigma_1^{n_1x_2}\sigma_2^{n_2x_1} = id.$$

Bây giờ giả sử $\sigma^k = id$. Suy ra $\sigma_1^k = \sigma_2^{-k}$. Do σ_1, σ_2 độc lập nên ta suy ra $\sigma_1^k = \sigma_2^{-k} = id$. Do đó $k \vdots n_1$, $k \vdots n_2$. Suy ra $k \vdots [n_1, n_2]$. Vậy cấp của σ bằng $[n_1, n_2]$.

Bây giờ ta giả sử rằng với $\sigma_1, \sigma_2, ..., \sigma_r$ độc lập, cấp của phần tử $\sigma_1\sigma_2...\sigma_r$ bằng $n = [n_1, n_2, ..., n_r]$, trong đó n_i là cấp của phần tử σ_i, $i = 1, 2, ..., r$. Với $n = r + 1$ ta đặt $f = \sigma_1\sigma_2...\sigma_r$. Do $\sigma_1, ..., \sigma_r, \sigma_{r+1}$ độc lập nên f, σ_{r+1} độc lập. Theo chứng minh trên, cấp của phần tử $f\sigma_{r+1}$ bằng $[n, n_{r+1}]$, trong đó $n = [n_1, n_2, ..., n_r]$. Vậy cấp của phần tử $\sigma_1\sigma_2...\sigma_r\sigma_{r+1}$ bằng $[n, n_{r+1}] = [n_1, n_2, ..., n_{r+1}]$.

3. Nhúng một nửa nhóm vào một nhóm

3.1. a) $(\mathbb{Z}, +)$.
b) $(\mathbb{Q}_+, .)$, trong đó $\mathbb{Q}_+$ là tập hợp các số hữu tỷ dương.
c) $(\mathbb{Q}, .)$.

3.2. Do M là một vị nhóm thoả mãn luật giản ước nên M có thể nhúng vào một nhóm giao hoán A bởi đơn cấu $k : M \to A$ của các vị nhóm, và các phần tử của A được viết dưới dạng

$$k(m).k(n)^{-1}.$$

Bây giờ giả sử $f : M \to B$ là một đồng cấu giữa các vị nhóm, trong đó B là một nhóm. Ta xây dựng tương ứng $f' : A \to B$ như sau:

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

Do k là một đơn cấu nên ta có thể suy ra f' là một ánh xạ. Hơn nữa do k và f là những đồng cấu nên ta suy ra f' là một đồng cấu thoả mãn $f = f' \circ k$.

Bây giờ ta giả sử $g : A \to B$ cũng là một đồng cấu nhóm thoả mãn điều kiện $f = g \circ k$. Do mỗi phần tử của A đều có dạng $k(m).k(n)^{-1}$ nên ta có

$$g(k(m)k(n)^{-1}) = g(k(m)).g(k(n))^{-1} = f(m).f(n)^{-1}.$$

Từ đó suy ra

$$g(k(m)k(n)^{-1}) = f'(k(m)k(n)^{-1})$$

với mọi $m, n \in M$. Vậy $g = f'$.

4. Tác động của một nhóm trên một tập hợp

4.1. a) Với $g, h, x \in G$ ta có

$$(g,(h,x)) = (g,(hxh^{-1})) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = (gh,x).$$

Hơn nữa: $(e,x) = exe^{-1} = x$, $\forall x \in G$. Vậy G là một $G-$tập với tác động bởi phép liên hợp. Với $x \in G$, quỹ đạo Gx được xác định bởi:

$$Gx = \{(g,x) \mid g \in G\} = \{gxg^{-1} \mid g \in G\}$$

hay quỹ đạo Gx là tập hợp các phần tử liên hợp với x. Nhóm con ổn định G_x là:

$$\begin{aligned} G_x &= \{g \in G \mid (g,x) = x\} = \{g \in G \mid gxg^{-1} = x\} \\ &= \{g \in G \mid gx = xg\} \end{aligned}$$

Vậy nhóm con ổn định G_x bao gồm các phần tử của G giao hoán với x.

b) Với $g, h, x \in G$ ta có

$$(g,(h,x)) = (g,hx) = g(hx) = (gh)x = (gh,x).$$

Mặt khác, với mọi x thuộc G ta có $(e,x) = ex = x$. Vậy G là một $G-$tập với tác động là phép dời trong G. Với $x \in G$, quỹ đạo Gx là:

$$Gx = \{(g,x) \mid g \in G\} = \{gx \mid g \in G\}.$$

Nhóm con ổn định G_x là

$$G_x = \{g \in G \mid (g,x) = x\} = \{g \in G \mid gx = x\}.$$

4.2. Xét ánh xạ:

$$\begin{aligned} \mathbb{R}^* \times \mathbb{R}^{n+1} &\to \mathbb{R}^{n+1} \\ (k,(x_1,x_2,...,x_{n+1})) &\mapsto (kx_1,kx_2,...,kx_{n+1}) \end{aligned}$$

Hiển nhiên ta có

$$\begin{aligned} (k_1k_2)x &= k_1(k_2x) \\ 1.x &= x \end{aligned}$$

với mọi $k_1, k_2 \in \mathbb{R}^*, x \in \mathbb{R}^{n+1}$. Vậy nhóm $(\mathbb{R}^*,.)$tác động lên $\mathbb{R}^{n+1}$ bởi phép nhân vô hướng. Với mỗi phần tử $x = (x_1,x_2,....,x_{n+1}) \in \mathbb{R}^{n+1}$, quỹ đạo của x theo $\mathbb{R}^*$ là:

$$\mathbb{R}^*x = \{kx = (kx_1,kx_2,...,kx_{n+1}) \mid k \neq 0\}.$$

Vậy quỹ đạo của tác động này là một phương của $\mathbb{R}^{n+1}$.

4.3. a) Với $g, h \in G,\ H \in S$ ta có

$$(g,(h,H)) = (g,(hHh^{-1})) = g(hHh^{-1})g^{-1} = (gh)H(gh)^{-1} = (gh,H).$$

Hơn nữa: $(e,H) = eHe^{-1} = H,\ \forall H \in S$. Vậy S là một $G-$tập với tác động đã cho.

b) Với $H \in S$, quĩ đạo GH của H là

$$GH = \{(g,H) \mid g \in G\} = \{gHg^{-1} \mid g \in G\}$$

Từ đó suy ra số nhóm con liên hợp của nhóm con H bằng $|GH|$. Ta có:

$$|GH| = [G : G_H]$$

trong đó

$$\begin{aligned} G_H &= \{g \in G \mid (g, H) = H\} = \{g \in G \mid gHg^{-1} = H\} \\ &= \{g \in C \mid gH = Hg\} = N_H. \end{aligned}$$

Vậy $|GH| = [G : G_H] = [G : N_H]$, nghĩa là số nhóm con liên hợp với nhóm con H bằng chỉ số của cái chuẩn hóa N_H trong G.

4.7. a) Giả sử $y \in Gx$, $y = sx$ với phần tử s nào đó thuộc G. Ta chứng tỏ rằng khi đó

$$G_y = sG_xs^{-1}.$$

Thật vậy, nếu $g \in G_y$ thì $gy = y$, hay $gsx = sx$, do đó $(s^{-1}gs)x = x$. Điều này chứng tỏ $s^{-1}gs$ thuộc G_x, và bởi vậy

$$s^{-1}G_ys \subset G_x \Rightarrow G_y \subset sG_xs^{-1}.$$

Tương tự ta có

$$sG_xs^{-1} \subset G_y$$

Từ đó suy ra $G_y = sG_xs^{-1}$.

b) Ánh xạ $f : G/G_x \to Gx$ cho bởi $f(gG_x) = gx$ là một song ánh nên $|Gx| = [G : G_x]$. Trong trường hợp S hữu hạn thì S có sự phân hoạch bởi hữu hạn quỹ đạo $Gx, x \in I$, với I là tập các đại diện cho các qũi đạo. Và bởi vậy ta có

$$|S| = \sum_{i \in I} |Gx| = \sum_{i \in I} [G : G_x].$$

4.8. Giả sử G tác động lên chính nó bởi phép liên hợp. Khi đó phần tử x thuộc tâm $Z(G)$ khi và chỉ khi

$$xg = gx \quad \forall g \in G \Leftrightarrow x = gxg^{-1} \quad \forall g \in G.$$

Điều này chứng tỏ quỹ dạo $Gx = \{x\}$. Bởi vậy, theo Bài tập 4.7 thì

$$|G| = |Z(G)| + \sum_{y \in J} [G : G_y]$$

trong đó J là tập các đại diện cho các quỹ đạo khác nhau có nhiều hơn một phần tử. Bởi vì $|G|$ và $[G : G_y]$, $y \in I$, đều chia hết cho p nên $|Z(G)|$ chia hết cho p, nghĩa là $Z(G) \neq \{e\}$.

Bây giờ ta giả sử G là một nhóm cấp p^2. Theo Định lý Lagrange, mọi phần tử khác đơn vị của G đều có cấp bằng p hoặc p^2.

Nếu trong G tồn tại một phần tử có cấp bằng p^2 thì G là nhóm xyclic và do đó G là nhóm aben.

Bây giờ ta xét trường hợp trong G không có phần tử nào có cấp bằng p^2. Theo chứng minh trên, do $|Z(G)| > 1$ nên tồn tại $a \in Z(G), a \neq e$. Lấy $b \notin \langle a \rangle$. Ta có $ab = ba$. Vì b có cấp bằng p và $b \notin \langle a \rangle$ nên p^2 phần tử

$$a^i b^j \text{ với } i, j = 0, 1, ..., p-1.$$

là phân biệt. Và do đó

$$G = \{a^i b^j \text{ với } i, j = 0, 1, ..., p-1\}.$$

Vì $ab = ba$ nên G là nhóm aben.
Vậy mọi nhóm cấp p^2 đều là nhóm aben.

4.9. Giả sử G là nhóm cấp 35 tác động lên tập X có 13 phần tử. Khi đó ta có:

$$13 = \sum_{x \in I} |G : G_x| \quad (*)$$

trong đó I là tập các đại diện cho các quỹ đạo.

Vì nhóm G có cấp bằng 35 nên với mỗi $x \in I$, $|G : G_x|$ chỉ có thể bằng 1, 5, 7 hoặc 35. Từ đó kết hợp với đẳng thức $(*)$, suy ra tồn tại $x_o \in X$ sao cho $|G : G_{x_o}| = 1$, nghĩa là x_o là một điểm cố định.

4.10. Giả sử G là nhóm cấp p^r tác động lên tập X có m phần tử, với m không chia hết cho p. Khi đó ta có:

$$m = \sum_{x \in I} | G : G_x | \qquad (*)$$

trong đó I là tập các đại diện cho các quỹ đạo.

Vì nhóm G có cấp bằng p^r nên với mỗi $x \in I$, $|G : G_x|$ chỉ có thể bằng 1, hoặc chia hết cho p.

Nếu không tồn tại $x \in I$ sao cho $|G : G_x| = 1$ thì ta có $|G : G_x| \vdots p$ với mọi $x \in I$. Kết hợp với dẳng thức $(*)$ ta suy ra: $m \vdots p$, trái giả thiết. Vậy tồn tại $x_o \in X$ sao cho $|G : G_{x_o}| = 1$, nghĩa là x_o là một diểm cố dịnh.

4.11. Đặt $X = \{aK \mid a \in G\}$. Xét tương ứng:

$$\begin{aligned} H \times X &\to X \\ (h, aK) &\mapsto haK \end{aligned}$$

Ta chứng tỏ rằng tương ứng trên không phụ thuộc vào phần tử đại diện. Thật vậy, giả sử $aK = bK$. Khi đó $a^{-1}b = k \in K$. Suy ra

$$hbK = hakK = haK.$$

Vậy tương ứng trên là một ánh xạ. Hơn nữa, ánh xạ này xác dịnh một tác động của nhóm H lên tập hợp X. Quỹ dạo của lớp ghép $eK = K$ dưới tác động này là:

$$H(eK) = \{h(eK) \mid h \in H\}.$$

Chú ý rằng hợp của các lớp ghép phân biệt của $H(eK)$ chính là HK. Bởi vì với mỗi $h \in H$ ta có $|hK| = |K|$ nên ta có

$$|HK| = |K|.|H(eK)|.$$

Ta có

$$|H| = |H_{eK}|.|H(eK)|$$

trong đó

$$H_{eK} = \{h \in H \mid heK = eK = K\} = \{h \in H \mid h \in K\} = H \cap K.$$

Từ đó $|H_{eK}| = |H|/|H \cap K|$. Vậy

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Chương IV

VÀNH VÀ TRƯỜNG

1. Định nghĩa và ví dụ

1.4. $\{a+b\sqrt{2}+c\sqrt{3} \mid a,b,c \in \mathbb{Q}\}$ không lập thành một vành với phép cộng và phép nhân thông thường vì tập hợp này không đóng kín với phép nhân.

1.5. $\{a+b\sqrt[3]{2} \mid a,b \in \mathbb{Q}\}$ không lập thành một vành với phép cộng và phép nhân thông thường vì nó không đóng kín với phép nhân.

1.6. Từ các tính chất của ma trận ta suy ra tập các ma trận thực vuông cấp 2 với định thức bằng 0 là một vành với phép cộng và phép nhân các ma trận theo nghĩa thông thường.

1.7. Ta thấy $(\mathbb{Z},+)$ là một nhóm giao hoán. Hơn nữa, $\mathbb{Z}$ cùng với phép nhân:

$$a \times b = 0, \quad \forall a,b \in \mathbb{Z}$$

là một nửa nhóm, đồng thời phép nhân phân phối với phép cộng. Vậy hệ đại số $(\mathbb{Z},+,\times)$ là một vành, với phép cộng là thông thường, phép nhân được cho bởi $a \times b = 0$.

1.8. Giả sử R là một vành có đơn vị. Ta sẽ chứng minh với mọi $a,b \in R$, đẳng thức $a+b=b+a$ được suy ra từ các tiên đề khác của vành.

Cách 1: Ta khai triển $(1+a)(1+b)$ theo hai cách như sau:

$$\begin{aligned}(1+a).(1+b) &= (1+a).1+(1+a).b \\ &= 1+a+b+ab \\ (1+a).(1+b) &= 1.(1+b)+a.(1+b) \\ &= 1+b+a+ab\end{aligned}$$

Do đó

$$1 + a + b + ab = 1 + b + a + ab.$$

Vì R là một nhóm với phép cộng nên ta có thể giản ước cả hai vế, suy ra $a + b = b + a$.

Cách 2 : Xét tích: $(1 + 1).(a + b)$. Ta có:

$$\begin{aligned}(1 + 1).(a + b) &= (1 + 1).a + (1 + 1).b \\ &= a + a + b + b \\ (1 + 1).(a + b) &= 1.(a + b) + 1.(a + b) \\ &= a + b + a + b\end{aligned}$$

Vậy: $a + a + b + b = a + b + a + b$, và do đó: $a + b = b + a$.

1.9. Với $M_1 = \begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}, M_2 = \begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \in I$ ta có:

$$M_1 - M_2 = \begin{pmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & c_1 - c_2 \end{pmatrix} \in I;$$

$$M_1.M_2 = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{pmatrix} \in I.$$

Vậy I là một vành con của $\mathbb{M}_2(R)$.

1.10. Giả sử I là một vành con của $\mathbb{Z}$. Khi đó $(I, +)$ là một nhóm con của $(\mathbb{Z}, +)$. Do đó tồn tại số tự nhiên m sao cho $I = m\mathbb{Z}$. Đảo lại, nếu $I = m\mathbb{Z}$ thì ta dễ thử lại được rằng I là vành con của $\mathbb{Z}$. Vậy các vành con của $\mathbb{Z}$ có dạng $m\mathbb{Z}$, trong đó m là một số tự nhiên.

1.11. $\mathbb{Z}_2 \otimes \mathbb{Z}_2$ không là một miền nguyên vì trong $\mathbb{Z}_2 \otimes \mathbb{Z}_2$ tồn tại hai phần tử khác có tích bằng 0:

$$(\overline{0}, \overline{1}).(\overline{1}, \overline{0}) = (\overline{0}, \overline{0}) = 0.$$

1.12. Ta có thể thử lại được rằng $R = \{a + bi \mid a, b \in \mathbb{Q}\}$ là một trường con của trường các số phức $\mathbb{C}$, do đó R là một trường.

1.13. $\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ là một miền nguyên, không là một trường vì trong tập hợp đó có những phần tử không có nghịch đảo, chẳng hạn 2.

1.14. Giả sử a là một ước của 0 trong vành $\mathbb{Z}_{10}$. Khi đó tồn tại $b \in \mathbb{Z}_{10}$, $b \neq 0$ sao cho $ab = 0$. Đặt $a = \overline{x}, b = \overline{y}$. Ta có:

$$0 = ab = \overline{xy}.$$

Do đó $xy \vdots 10$. Vì $a, b \neq 0$ nên x và y đều không chia hết cho 10. Do đó chỉ có thể xảy ra hai khả năng sau:

Nếu $x \vdots 2$ thì $y \vdots 5$. Khi đó $\overline{x} \in \{\overline{2}, \overline{4}, \overline{6}, \overline{8}\}$, $\overline{y} = \overline{5}$.

Nếu $x \vdots 5$ thì $y \vdots 2$. Khi đó $\overline{x} = \overline{5}$; $\overline{y} \in \{\overline{2}, \overline{4}, \overline{6}, \overline{8}\}$.

Vậy các ước của $\overline{0}$ trong vành $\mathbb{Z}_{10}$ là: $\overline{2}, \overline{4}, \overline{5}, \overline{6}, \overline{8}$.

1.16. Xét hai phần tử bất kỳ $a, b \in R$, ta chứng minh $ab = ba$. Đặt $x = a + b$. Ta có

$$\begin{aligned} x^2 - x &= (a+b)^2 - (a+b) \\ &= a^2 - a + b^2 - b + ab + ba \end{aligned}$$

Theo giả thiết ta có $a^2 - a$, $b^2 - b$, $x^2 - x \in Z(R)$ nên

$$ab + ba \in Z(R).$$

Do đó

$$\begin{aligned} a^2b + aba &= a(ab + ba) \\ = (ab + ba)a &= aba + ba^2. \end{aligned}$$

Từ đó $a^2b = ba^2$ với mọi $b \in R$. Do đó $a^2 \in Z(R)$. Suy ra

$$a = a^2 - (a^2 - a) \in Z(R).$$

Vậy $ab = ba$ với mọi $a, b \in R$, hay R là một vành giao hoán.

1.17. Rõ ràng $A \neq \emptyset$. Chúng ta dễ thử lại rằng với mọi $x, y \in A$ ta có $x - y$, $x.y \in A$. Cuối cùng chúng ta cần phải chỉ ra rằng với mọi

$$x = a + b\sqrt[3]{2} + c\sqrt[3]{4} \in A, \ x \neq 0$$

thì $x^{-1} \in A$. Điều này dễ dàng nhận được từ đẳng thức:

$$\frac{1}{x+y+z} = \frac{x^2 + y^2 + z^2 - xy - yz - zx}{x^3 + y^3 + z^3 - 3xyz}.$$

1.18. Giả sử A là một trường con của trường số hữu tỷ $\mathbb{Q}$, ta cần chứng minh $A = \mathbb{Q}$. Do A là trường con của $\mathbb{Q}$ nên $1 \in A$. Với mọi số nguyên dương n ta có

$$n = \underbrace{1 + 1 + \ldots + 1}_{n \text{ lần}} \in A.$$

Từ $n \in A$ suy ra $-n$, $\dfrac{1}{n} \in A$. Với mỗi số hữu tỷ $\dfrac{p}{q}$ $(q \neq 0)$ có thể coi $q > 0$, và khi đó

$$\frac{p}{q} = p.\frac{1}{q} \in A.$$

Vậy $\mathbb{Q} \subset A$, do đó $\mathbb{Q} = A$.

1.19. Giả sử $1 - ab$ khả nghịch. Đặt $x = (1 - ab)^{-1}$. Ta có

$$x(1 - ab) = 1 \Rightarrow bx(1 - ab)a = ba$$

$$\Rightarrow (1 - ba) + bx(1 - ab)a = 1.$$

Dẫn đến

$$\begin{aligned}(1 - ba) + bxa(1 - ba) &= 1\\ \Rightarrow (1 - ba)(1 + bxa) &= 1.\\ \Rightarrow (1 - ba)^{-1} &= 1 + bxa.\end{aligned}$$

Vậy $(1 - ba)$ khả nghịch và

$$(1 - ba)^{-1} = 1 + bxa, \text{ với } x = (1 - ab)^{-1}.$$

1.20. Từ giả thiết $a \in R$ là phần tử luỹ linh nên tồn tại số nguyên dương n sao cho $a^n = 0$. Đặt $u = 1 + a + a^2 + ... + a^{n-1}$. Khi đó ta có

$$(1 - a)u = u(1 - a) = 1.$$

Vậy $1 - a$ khả nghịch.

Nếu a luỹ linh thì $-a$ cũng luỹ linh. Do đó $1 - (-a)$ khả nghịch, nghĩa là $1 + a$ khả nghịch.

1.21. a) Giả sử $a, b \in C(R)$. Khi đó với mọi $x \in R$ ta có

$$\begin{aligned}(a - b)x = ax - bx &= xa - xb = x(a - b);\\ (ab)x = a(bx) = a(xb) &= (ax)b = (xa)b = x(ab)\end{aligned}$$

Vậy $a - b$, $ab \in C(R)$, do đó $C(R)$ là một vành con của R.

b) $C(M(n, \mathbb{R})) = \{aI_n |\ a \in \mathbb{R}\}$, trong đó I_n là ma trận đơn vị cấp n.

1.22. a)$\Rightarrow$ b). Chúng ta có thể chứng tỏ ngay được rằng $\mathbb{Z}_n$ luôn là một vành giao hoán, có đơn vị khác không.

Giả sử n là một số nguyên tố. Để chứng minh $\mathbb{Z}_n$ là một trường chúng ta chỉ cần chứng tỏ rằng mọi phần tử khác không của $\mathbb{Z}_n$ đều có nghịch đảo. Thật vậy, giả sử $\overline{a} \in \mathbb{Z}_n$, $\overline{a} \neq \overline{0}$, điều này có nghĩa là a không chia hết cho p. Do p là một số nguyên tố nên a và p nguyên tố cùng nhau. Do đó, tồn tại các số nguyên u và v sao cho

$$au + pv = 1.$$

Chuyển qua lớp ta được:

$$\overline{a}.\overline{u} = \overline{1}, \quad \text{do } \overline{p} = 0.$$

Vậy $\overline{a}$ khả nghịch.

b)⇒ c). Hiển nhiên.

c)⇒ a). Vì $\mathbb{Z}_n$ là một miền nguyên nên $\mathbb{Z}_n$ có nhiều hơn một phần tử, do đó $n > 1$. Giả sử n là một hợp số, $n = a.b$, $1 < a, b < n$. Khi đó $\overline{a}$, $\overline{b} \neq 0$, đồng thời

$$\overline{a}.\overline{b} = \overline{a.b} = \overline{0},$$

nghĩa là $\mathbb{Z}_n$ có ước của không, trái với giả thiết $\mathbb{Z}_n$ là một miền nguyên. Vậy n là một số nguyên tố.

1.23. a) Với mọi $x \in R$ ta có:

$$-x = (-x)^2 = x^2 = x.$$

b) Với mọi $x, y \in R$ ta có:

$$\begin{aligned} x + y = (x + y)^2 &= x^2 + xy + yx + y^2 \\ &= x + xy + yx + y \end{aligned}$$

Do vậy $xy + yx = 0$, suy ra:

$$xy = -yx = yx.$$

Vậy R là một vành giao hoán.

c) Với mọi $x \in R, x \neq 0$ và với mọi $y \in R$ ta có

$$xy = x^2y = x(xy).$$

Vì R không có ước của không nên trong đẳng thức trên giản ước x ở hai vế ta được

$$xy = y.$$

Vậy x là phần tử đơn vị của R. Trong trường hợp này vành R chỉ có hai phần tử là 0 và đơn vị e.

2. Iđêan, vành thương

2.1. Giả sử I là iđêan của $\mathbb{Z}$. Khi đó $(I,+)$ là một nhóm con của $(\mathbb{Z},+)$. Do đó tồn tại số tự nhiên m sao cho $I = m\mathbb{Z}$. Đảo lại, nếu $I = m\mathbb{Z}$ thì ta dễ thử lại được rằng I là iđêan của $\mathbb{Z}$. Vậy các iđêan của $\mathbb{Z}$ có dạng $m\mathbb{Z}$, trong đó m là một số tự nhiên.

2.2. Giả sử I là iđêan của $\mathbb{Q}$. Nếu $I \neq 0$ thì tồn tại $x \in I$, $x \neq 0$. Ta có $x^{-1} \in \mathbb{Q}$, $x \in I$. do đó $1 = x.x^{-1} \in I$. Suy ra $I = \mathbb{Q}$. Vậy các iđêan của $\mathbb{Q}$ là 0 và $\mathbb{Q}$.

2.5. Rõ ràng $0 \in A$. Với $a, b \in A$ ta có $na = nb = 0$, do đó

$$n(a-b) = na - nb = 0 - 0 = 0.$$

Vậy $a - b \in A$.

Bây giờ giả sử $a \in A$ và $x \in R$ bất kỳ. Khi đó ta có

$$n(ax) = (na)x = 0, \quad n(xa) = x(na) = 0.$$

Vậy $ax, xa \in A$, từ đó suy ra A là một iđêan của R.

2.6. Ta có $\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}$ khi và chỉ khi $1 \in m\mathbb{Z} + n\mathbb{Z}$. Điều này xảy ra khi và chỉ khi tồn tại những số nguyên u, v sao cho

$$1 = mu + nv,$$

nghĩa là m và n nguyên tố cùng nhau.

2.7. Hiển nhiên ta có $IJ \subset I \cap J$. Lấy x bất kỳ thuộc $I \cap J$. Do

$$1 \in R = I + J$$

nên tồn tại $u \in I$, $v \in J$ sao cho $1 = u + v$. Khi đó ta có:

$$x = 1x = (u+v)x = ux + vx = ux + xv \in IJ.$$

Từ đó suy ra $I \cap J \subset IJ$, và do đó: $IJ = I \cap J$.

2.8. a) Do $e \neq 0$ nên ta có $n > 1$. Giả sử $n = p.q$, với $p, q > 1$. Khi đó ta có

$$(pe)(qe) = \underbrace{(e+e+...+e)}_{p \text{ lần}}.\underbrace{(e+e+...+e)}_{q \text{ lần}} = \underbrace{e+e+...+e}_{n \text{ lần}} = ne = 0$$

Do R là một miền nguyên nên $pe = 0$ hoặc $qe = 0$. Điều này trái với giả thiết n là cấp của phần tử e trong nhóm cộng R. Vậy n là một số nguyên tố.

b) Giả sử $x \in R$, $x \neq 0$. Khi đó ta có

$$\begin{aligned} nx &= \underbrace{x+x+...+x}_{n \text{ lần}} = \underbrace{ex+ex+...+ex}_{n \text{ lần}} = \underbrace{(e+e+...+e)}_{n \text{ lần}}x \\ &= (ne)x = 0 \end{aligned}$$

Giả sử k là số nguyên sao cho $kx = 0$. Khi đó

$$\begin{aligned} 0 &= kx = \underbrace{x+x+...+x}_{k \text{ lần}} = \underbrace{ex+ex+...+ex}_{k \text{ lần}} = \underbrace{(e+e+...+e)}_{k \text{ lần}}x \\ &= (ke)x \end{aligned}$$

Do R là một miền nguyên và $x \neq 0$ nên ta có $ke = 0$, từ đó suy ra k chia hết cho n. Vậy cấp của phần tử x bằng n.

c) Ta dễ thử lại được rằng $mR = \{mx \mid x \in R\}$ là iđêan của R.

d) Nếu m là bội của n thì $m = nq$. Khi đó với mọi $x \in R$ ta có

$$\begin{aligned} (qe)(ne) &= \underbrace{(e+e+...+e)}_{q \text{ lần}}.\underbrace{(e+e+...+e)}_{n \text{ lần}} = \underbrace{e+e+...+e}_{m \text{ lần}} \\ &= me = 0. \end{aligned}$$

Do đó $mR = 0$, từ đó suy ra $R/mR \cong R$.

Khi m không chia hết cho n, do n là một số nguyên tố thì m và n nguyên tố cùng nhau, do đó tồn tại các số nguyên u, v sao cho $mu + nv = 1$. Do đó với mọi $x \in R$ ta có

$$x = x(mu + nv) = m(xu) + n(xv) = m(xu) \in mR.$$

Do đó $R = mR$, từ đó suy ra $R/mR \cong \{0\}$.

2.10. Do idêan 0 là idêan nguyên tố nên R là một miền nguyên. Xét một phần tử $a \in R,\ a \neq 0$.

Theo giả thiết a^2R là một idêan nguyên tố và do $a.a \in a^2R$ nên ta có $a \in a^2R$. Từ đó suy ra tồn tại $r \in R$ sao cho $a = a^2r$. Do R là một miền nguyên nên ta có $ar = 1$. Điều này chứng tỏ a khả nghịch, và do đó R là một trường.

2.11. Gọi Γ là tập hợp tất cả các idêan thực sự của R chứa I. Khi đó Γ là một tập khác $\emptyset$ vì $I \in \Gamma$. Gọi L là một dây chuyền tăng của Γ (Γ được sắp xếp theo quan hệ bao hàm) và đặt

$$J = \cup A,\ A \in L.$$

Có thể chứng minh được rằng hợp của những dãy tăng những idêan thực sự của R lại là một idêan thực sự của R nên $J \in \Gamma$. Khi đó theo Bổ đề Zorn, Γ có phần tử tối đại M. Đó chính là idêan tối đại của R chứa I.

2.12. Do $a \in R$ là phần tử không khả nghịch nên (a) là idêan thực sự của R. Theo Bài tập 2.11, tồn tại idêan tối đại M của R chứa (a), do đó M chứa a.

2.13. Giả sử I là idêan tối đại của $\mathbb{Z}$. Theo Bài tập 2.1, tồn tại số tự nhiên n sao cho $I = n\mathbb{Z}$. Do I là idêan thực sự của $\mathbb{Z}$ nên $n \neq 0, 1$. Gọi q là một ước bất kỳ của n. Ta có $q\mathbb{Z}$ là idêan của $\mathbb{Z}$ chứa I. Do I là idêan tối đại của $\mathbb{Z}$ nên $q\mathbb{Z} = \mathbb{Z}$ hoặc $q\mathbb{Z} = I$. Từ đó suy ra $q = 1$ hoặc $q = n$. Vậy n là số nguyên tố.

Đảo lại, giả sử $I = p\mathbb{Z}$ là một số nguyên tố. Khi đó ta có I là idêan thực sự của $\mathbb{Z}$. Giả sử M là idêan của $\mathbb{Z}$ chứa I. Theo Bài tập 2.1, tồn tại số tự nhiên m sao cho $M = m\mathbb{Z}$. Từ bao hàm

$$I = p\mathbb{Z} \subset M = m\mathbb{Z}$$

suy ra $p \in m\mathbb{Z}$, và do đó $p \vdots m$. Do p là số nguyên tố nên $m = 1$ hoặc $m = p$, nghĩa là $M = \mathbb{Z}$ hoặc $M = I$. Vậy I là idêan tối đại của $\mathbb{Z}$.

2.14. Giả sử P là idêan nguyên tố và A là idêan của R sao cho $P \subsetneq A$. Khi đó tồn tại $x \in A,\ x \notin P,\ n \in \mathbb{N}^*$ sao cho $x^n = x$. Từ đó

$$x(x^{n-1} - 1) = x^n - x = 0 \in P.$$

Do $x \notin P$ nên $x^{n-1} - 1 \in P$, suy ra $x^{n-1} - 1 \in A$. Do $x \in A$ nên

$$1 = x^{n-1} - (x^{n-1} - 1) \in A.$$

Từ đó suy ra: $A = R$ và do đó P là idêan tối đại.

2.15. Dễ thử lại rằng $R \times S$ là một vành. Hơn nữa, nếu A và B tương ứng là những idêan của R và S thì $X = A \times B$ cũng là một idêan của vành $R \times S$.

Ngược lại, giả sử X là một idêan của $R \times S$. Ta chứng minh: $X = A \times B$, với A và B lần lượt là những idêan của R và S.

Thật vậy, đặt:

$$A = \{a \in R \mid (a, 0) \in X\}$$
$$B = \{b \in S \mid (0, b) \in X\}.$$

Ta chứng minh A là idêan của R. Thật vậy, với mọi $a, a' \in A$ ta có: $(a, 0),\ (a', 0) \in X$. Do đó

$$(a - a', 0) = (a, 0) - (a', 0) \in X,$$

suy ra $a - a' \in A$. Hơn nữa, với mọi $r \in R$ ta có:

$$(ra, 0) = (r, 0).(a, 0) \in X,$$

do đó $ra \in A$.

Tương tự: $ar \in A$. Vậy A là một idêan của R.

Chứng minh tương tự ta dược B là idêan của S. Để kết thúc chứng minh ta sẽ chỉ ra $X = A \times B$. Thật vậy, nếu $(r, s) \in X$ thì

$$(r, 0) = (r, s).(1, 0) \in X \text{ và } (0, s) = (r, s).(0, 1) \in X.$$

Suy ra $r \in A,\ s \in B$, và do đó $(r, s) \in A \times B$, hay $X \subset A \times B$.
Nếu $(a, b) \in A \times B$ thì

$$(a, b) = (a, 0) + (0, b) \in X.$$

Vậy $A \times B \subset X$ và do đó $X = A \times B$.

2.16. Rõ ràng $0 \in N(R)$. Giả sử $a, b \in N(R)$. Khi đó tồn tại các số nguyên dương m, n sao cho

$$a^m = 0,\ b^n = 0.$$

Khi đó theo công thức khai triển Niutơn ta có $(a - b)^{m+n} = 0$, tức là $a - b \in N(R)$.

Giả sử $x \in R, a \in N(R)$. Khi đó tồn tại $m \in \mathbb{N}^*$ sao cho $a^m = 0$. Từ đó

$$(ax)^m = a^m.x^m = 0.x^m = 0,$$

và do đó $ax \in N(R)$. Những điều này chứng tỏ $N(R)$ là một iđêan của R.

b) Giả sử $\overline{r} \in N[R/N(R)]$, khi đó tồn tại số nguyên dương m sao cho $\overline{r}^m = \overline{0}$, nghĩa là $r^m \in N(R)$. Do đó, tồn tại số nguyên dương n sao cho $(r^m)^n = 0$, hay $r^{mn} = 0$. Vậy $r \in N(R)$, hay $\overline{r} = \overline{0}$.

c) Giả sử $a \in N(R)$. Khi đó tồn tại $m \in \mathbb{N}^*$ sao cho $a^m = 0$. Nếu P là iđêan nguyên tố thì từ $a^m \in P$ suy ra $a \in P$. Điều này chứng tỏ $N(R)$ là tập con của giao các iđêan nguyên tố của R.

Bây giờ giả sử ngược lại $a \notin N(R)$. Ta sẽ chứng tỏ rằng tồn tại một iđêan nguyên tố Q không chứa a. Đặt

$$S = \{a^n \mid n \in \mathbb{N}\},$$

và gọi Γ là tập các iđêan của R mà không giao với S. Vì $a \notin N(R)$ nên $a^n \neq 0$, $\forall n > 0$ nên $0 \in \Gamma$.

Gọi L là một dây chuyền tăng của Γ (Γ được sắp xếp theo quan hệ bao hàm) và đặt

$$J = \cup A,\ A \in L.$$

Có thể chứng minh được rằng hợp của những dãy tăng những iđêan của R lại là một iđêan của R nên J là iđêan của R. Mặt khác với mỗi $A \in L$, A không giao với S. Do đó J cũng không giao với S. Vậy $J \in \Gamma$, nghĩa là J là một chặn trên của dây chuyền L. Theo Bổ đề Zorn, Γ có phần tử tối đại Q. Ta có thể chứng minh được Q là một iđêan nguyên tố của R và hiển nhiên $a \notin Q$. Vậy $N(R)$ là giao của tất cả các iđêan nguyên tố của R.

2.17. a)$\Rightarrow$ c). Nếu $a \in P$ thì $1 + a \notin P$. Do đó $1 + a$ không sinh ra một iđêan thực sự của P, hay $1 + a$ khả nghịch.

c)$\Rightarrow$ b). Xét phần tử $a \in R$. Nếu $a \in P$ thì a không khả nghịch. Nếu $a \notin P$ thì do R/P là một trường nên tồn tại $b \notin P$ sao cho

$$(a + P)(b + P) = 1 + P.$$

Từ đó $ab = 1 + x$ với $x \in P$. Do $1 + x$ khả nghịch nên a cũng khả nghịch. Vậy P là tập hợp các phần tử không khả nghịch của R.

b)⇒ a). Giả sử P là idêan gồm tất cả các phần tử không khả nghịch của R. Khi đó do không có idêan thực sự nào chứa phần tử khả nghịch nên mọi idêan thực sự của R đều nằm trong P, hay R là một vành địa phương.

2.18. a)⇒ b). Giả sử R chỉ có một idêan tối đại duy nhất M. Khi đó tập hợp M các phần tử không khả nghịch của R là một idêan của R (theo Bài tập 2. 17.)

b)⇒ a). Giả sử tập M các phần tử không khả nghịch của R là một idêan của R. Rõ ràng M là idêan tối đại của R.

Giả sử M' là một idêan tối đại bất kỳ của R. Khi đó theo Bài tập 2. 17, ta có $M' \subset M$. Từ đó suy ra $M' = M$, nghĩa là R chỉ có một idêan tối đại duy nhất.

2.19. a) Ta dễ thấy $\overline{x} = x + p^n\mathbb{Z}$ không khả nghịch trong $\mathbb{Z}_{p^n}$ khi và chỉ khi $p \mid x$. Do đó tập các phần tử không khả nghịch P của $\mathbb{Z}_{p^n}$ là

$$P = \{pt + p^n\mathbb{Z} \mid t \in \mathbb{Z}\}.$$

Từ đó suy ra P là một idêan của vành $\mathbb{Z}_{p^n}$, do đó theo Bài tập 2. 17, $\mathbb{Z}_{p^n}$ là một vành địa phương.

Chúng ta thấy tập hợp các phần tử không khả nghịch của vành $\mathbb{Z}_6$ là

$$\overline{0}, \overline{2}, \overline{3}, \overline{4}.$$

Tập hợp này không là một idêan của $\mathbb{Z}_6$. Do đó $\mathbb{Z}_6$ không là một vành địa phương.

b) Trước hết ta dễ chỉ ra được rằng $\mathbb{Z}_{(p)}$ là một vành con của $\mathbb{Q}$. Sau đó ta có thể chỉ ra được rằng phần tử $\dfrac{r}{s}$ không khả nghịch trong $\mathbb{Z}_{(p)}$ khi và chỉ khi $p \mid r$.

Từ đó ta suy ra tập các phần tử không khả nghịch của $\mathbb{Z}_{(p)}$ là một idêan của nó, do đó $\mathbb{Z}_{(p)}$ là một vành địa phương.

c) Do R là một vành địa phương nên $J(R)$ là một idêan của R. Do vậy $R/J(R)$ là một vành giao hoán, có đơn vị. Ta còn phải chỉ ra rằng mọi phần tử $\overline{x} \in R/J(R)$, $\overline{x} \neq \overline{0}$ đều khả nghịch.

Thật vậy ta có $x \notin J(R)$, do đó x khả nghịch. Do vậy tồn tại $y \in R$ sao cho $xy = 1$. Từ đó suy ra $\overline{x}^{-1} = \overline{y}$.

d) Theo giả thiết $R/N(R)$ là một trường nên $N(R)$ là một idêan tối đại của R.

Với mỗi phần tử $a \in N(R)$, theo Bài tập 1. 20 ta có $1 + a$ khả nghịch. Kết hợp với Bài 2. 17 ta suy ra R là một vành địa phương.

2.20. Giả sử I là một iđêan khác không của vành $M_2(F)$ và

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \ A \in I.$$

Không mất tính chất tổng quát ta có thể giả sử $a \neq 0$. Khi đó, với mọi $x, y, z, t \in F$ ta có

$$\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \frac{x}{a} & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in I;$$

$$\begin{pmatrix} 0 & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \frac{y}{a} & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in I;$$

$$\begin{pmatrix} 0 & 0 \\ z & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ \frac{z}{a} & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in I;$$

$$\begin{pmatrix} 0 & 0 \\ 0 & t \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ \frac{t}{a} & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in I.$$

Vì mỗi phần tử của R đều là tổng của bốn phần tử có dạng trên nên mọi phần tử của R đều thuộc I, và do đó $I = R$.

3. Đồng cấu vành

3.1. Xét phép chiếu tự nhiên

$$\begin{aligned} p : \mathbb{Z} &\to \mathbb{Z}_5 \\ k &\mapsto \overline{k} \end{aligned}$$

Giả sử n là một nghiệm của phương trình đã cho trong $\mathbb{Z}$. Khi đó trong $\mathbb{Z}_5$ ta có đẳng thức:

$$\overline{n}^3 - 5\overline{n}^2 - \overline{n} - \overline{2} = \overline{n}^2 - \overline{n} - \overline{2} = \overline{0} \in \mathbb{Z}_5$$

Như vậy $\overline{n}$ là một nghiệm của phương trình

$$x^3 - x - 2 = 0.$$

Lần lượt thay $\overline{n} = \overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4} \in \mathbb{Z}_5$ vào phương trình này ta đều có $\overline{n}^3 - \overline{n} - \overline{2} \neq \overline{0}$. Vậy phương trình trên không có nghiệm trong $\mathbb{Z}$.

3.2. a) Trước hết ta có $0 = f(0) \in f(I)$. Giả sử $a', b' \in f(I)$. Khi đó tồn tại $a, b \in R$ sao cho

$$a' = f(a),\ b' = f(b).$$

Như vậy

$$a' - b' = f(a) - f(b) = f(a - b) \in I.$$

Giả sử $a' = f(a) \in f(I),\ a \in I$ và $y \in S$. Vì f là toàn cấu nên tồn tại $x \in R$ sao cho $f(x) = y$. Khi đó

$$a'y = f(a)f(x) = f(ax) \in f(I).$$

Tương tự $ya' \in f(I)$. Vậy $f(I)$ là một idêan của S.

Nếu f không là toàn cấu thì khẳng định trên không còn đúng. Chẳng hạn xét phép nhúng tự nhiên từ vành số nguyên $\mathbb{Z}$ vào trường số hữu tỷ $\mathbb{Q}$,

$$\begin{array}{rccc} i: & \mathbb{Z} & \to & \mathbb{Q} \\ & n & \mapsto & n \end{array}$$

$\mathbb{Z}$ là một idêan của $\mathbb{Z}$ nhưng $i(\mathbb{Z}) = \mathbb{Z}$ không là một idêan của $\mathbb{Q}$.

b) Ta đã biết nếu P là idêan của S thì $f^{-1}(P)$ là idêan của R. Bây giờ giả sử P là idêan nguyên tố của S, ta chứng minh $Q = f^{-1}(P)$ là idêan nguyên tố của R. Thật vậy với $x, y \in R$ sao cho $xy \in Q$. Khi đó

$$f(x)f(y) = f(xy) \in P.$$

Do P là idêan nguyên tố nên hoặc $f(x) \in P$ hoặc $f(y) \in P$. Từ đó $x \in Q$ hoặc $y \in Q$. Điều này chứng tỏ $Q = f^{-1}(P)$ là idêan nguyên tố của S.

Nếu P là idêan tối đại của S thì không thể kết luận $f^{-1}(P)$ là idêan tối đại của R. Chẳng hạn chúng ta vẫn xét phép nhúng tự nhiên

$$i: \mathbb{Z} \to \mathbb{Q}.$$

Ta có 0 là iđêan tối đại của $\mathbb{Q}$ nhưng $i^{-1}(0) = 0$ không là iđêan tối đại của $\mathbb{Z}$.

3.4. Do R là một vành Boole nên ta có $\overline{a}^2 = \overline{a}$ $(*)$ với mọi $\overline{a} \in R/P$.

Mặt khác do P là iđêan nguyên tố của R nên R/P là một miền nguyên. Do đó với mọi $\overline{a} \in R/P$, từ đẳng thức $(*)$ ta suy ra $\overline{a} = \overline{0}$ hoặc $\overline{a} = \overline{1}$. Do đó R/P là một trường. Vậy P là iđêan tối đại và $R/P \cong \mathbb{Z}_2$.

3.5. Ta dễ dàng kiểm tra được rằng S là vành con của $M_2(\mathbb{R})$. Hơn nữa ánh xạ

$$\begin{array}{rcl} \varphi : S & \to & \mathbb{C} \\ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} & \mapsto & a + bi \end{array}$$

là một đẳng cấu vành.

Dựa vào đẳng cấu φ, chúng ta tính được: $M = \begin{pmatrix} 2^{1004} & 0 \\ 0 & 2^{1004} \end{pmatrix}$.

3.6. Ta dễ kiểm tra được rằng A là một iđêan của R. Hơn nữa ánh xạ

$$\begin{array}{rcl} \varphi : R & \to & S \times S \\ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} & \mapsto & (a, c) \end{array}$$

là một toàn cấu có

$$\mathrm{Ker}\varphi = A.$$

Từ đó suy ra: $R/A \cong S \times S$.

3.8. Xét tương ứng

$$\begin{array}{rcl} \varphi : \mathbb{Z}_n & \to & \mathbb{Z}_m \\ k + n\mathbb{Z} & \mapsto & k + m\mathbb{Z} \end{array}$$

Do m là một ước của n nên φ là một ánh xạ. Hơn nữa φ còn là một toàn cấu vành. Ta có:

$$\begin{array}{rcl} \mathrm{Ker}\varphi & = & \{k + n\mathbb{Z} \mid k + m\mathbb{Z} = m\mathbb{Z}\} \\ & = & \{k + n\mathbb{Z} \mid m|k\} = m\mathbb{Z}_n. \end{array}$$

Vậy $A = m\mathbb{Z}_n$.

3.9. Giả sử I là một idêan bất kỳ của $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Khi đó $I = J/n\mathbb{Z}$, trong đó J là một idêan của $\mathbb{Z}$ chứa $n\mathbb{Z}$. Theo Bài tập 2.1, J có dạng $m\mathbb{Z}$, $m \in \mathbb{N}$. Vì $n\mathbb{Z} \subset J = m\mathbb{Z}$ nên n chia hết cho m. Vậy mọi idêan của $\mathbb{Z}_n$ đều có dạng $m\mathbb{Z}_n$ với $m| n$. Ta có idêan $m\mathbb{Z}_n$ là idêan tối đại khi và chỉ khi $\mathbb{Z}_n/m\mathbb{Z}_m$ là một trường. Xét đồng cấu vành

$$\begin{aligned} \varphi : \mathbb{Z}_n &\to \mathbb{Z}_m \\ x + n\mathbb{Z} &\mapsto x + m\mathbb{Z} \end{aligned}$$

Dễ thấy φ là một toàn cấu, hơn nữa

$$\mathrm{Ker}\varphi = m\mathbb{Z}_n.$$

Theo định lý đồng cấu ta có

$$\mathbb{Z}_n/\mathrm{Ker}\varphi = \mathbb{Z}_n/m\mathbb{Z}_n \cong \mathbb{Z}_m.$$

Do đó $m\mathbb{Z}_n$ là một idêan tối đại trong $\mathbb{Z}_n$ khi và chỉ khi $\mathbb{Z}_m$ là một trường, hay m là một ước nguyên tố của n.

3.10. Giả sử $\varphi : \mathbb{Q} \to \mathbb{Z}$ là một đồng cấu vành. Giả sử $\varphi(1) = m \in \mathbb{Z}$. Khi đó với mọi số nguyên dương n ta có

$$m = \varphi(1) = \varphi(\underbrace{\frac{1}{n} + \frac{1}{n} + ... + \frac{1}{n}}_{n \text{ lần}}) = \underbrace{\varphi(\frac{1}{n}) + \varphi(\frac{1}{n}) + ... + \varphi(\frac{1}{n})}_{n \text{ lần}}$$

Do đó $\varphi(\frac{1}{n}) = \frac{m}{n}$. Với mọi số nguyên dương n ta có $\varphi(\frac{1}{n}) \in \mathbb{Z}$, do vậy $\frac{m}{n} \in \mathbb{Z}$ với mọi $n \in \mathbb{Z}$. Từ đó suy ra $m = 0$, và do vậy $\varphi = 0$.

3.11. Giả sử $f : \mathbb{Z} \to \mathbb{Z}$ là một tự đồng cấu. Khi đó ta có

$$f(1) = f(1).f(1).$$

Suy ra $f(1) = a$ với $a = 0$ hoặc $a = 1$. Với mọi số nguyên dương n ta có

$$f(n) = f(\underbrace{1 + 1 + ... + 1}_{n \text{ lần}}) = \underbrace{f(1) + f(1) + ... + f(1)}_{n \text{ lần}} = na$$

Với mọi số nguyên âm n ta có

$$f(n) = -f(-n) = -(-n.a) = na$$

Tóm lại $f(n) = na$ với mọi $n \in \mathbb{Z}$.
Vậy với $a = 0$ ta có $f = 0$, với $a = 1$ ta có $f = id_{\mathbb{Z}}$.

3.12. Giả sử $\varphi : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ là một tự đồng cấu vành. Ta có

$$\varphi(1) = \varphi(1).\varphi(1),$$

do đó $\varphi(1) = 0$ hoặc $\varphi(1) = 1$. Nếu $\varphi(1) = 0$ thì ta dễ dàng suy ra được $\varphi = 0$.

Nếu $\varphi(1) = 1$ thì với mọi $a \in \mathbb{Z}$ ta có $\varphi(a) = a$. Từ đó, với mọi $x = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ ta có

$$\varphi(x) = \varphi(a) + \varphi(b).\varphi(\sqrt{2}) = a + b\varphi(\sqrt{2})$$

Mặt khác

$$2 = \varphi(2) = \varphi(\sqrt{2}).\varphi(\sqrt{2})$$

nên $\varphi(\sqrt{2}) = \sqrt{2}$ hoặc $\varphi(\sqrt{2}) = -\sqrt{2}$.

Nếu $\varphi(\sqrt{2}) = \sqrt{2}$ thì với mọi $x \in \mathbb{Z}[\sqrt{2}]$ ta có $\varphi(x) = x$. Vậy φ là tự đẳng cấu đồng nhất.

Nếu $\varphi(\sqrt{2}) = -\sqrt{2}$ thì với mọi $x = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ ta có

$$\varphi(x) = a - b\sqrt{2}$$

Do đó φ là ánh xạ liên hợp của $\mathbb{Z}[\sqrt{2}]$.

3.13. $\mathbb{Z}[i]$ có ba tự đồng cấu vành là các tự đồng cấu không, tự đồng cấu đồng nhất và tự đồng cấu liên hợp.

3.14. $\mathbb{Q}[\sqrt{2}]$ có ba tự đồng cấu vành là các tự đồng cấu không, tự đồng cấu đồng nhất và tự đồng cấu liên hợp.

3.15. Giả sử $f : \mathbb{Z} \to \mathbb{Z}_{10}$ là một đồng cấu vành. Đặt $f(1) = \overline{a} \in \mathbb{Z}_{10}$. Ta có

$$\overline{a} = f(1) = f(1).f(1) = \overline{a}.\overline{a}.$$

Do đó $a^2 - a \vdots 10$. Mặt khác do $a^2 - a$ luôn là một số chẵn nên $a^2 - a \vdots 10$ khi và chỉ khi nó chia hết cho 5. Do vậy

$$\overline{a} = \overline{0},\ \overline{1},\ \overline{5},\ \overline{6}.$$

Từ đó suy ra có bốn đồng cấu vành từ $\mathbb{Z}$ đến $\mathbb{Z}_{10}$ là các đồng cấu $f(n) = \overline{n\overline{a}}$, với $\overline{a} = \overline{0}.\ \overline{1},\ \overline{5},\ \overline{6}$.

3.16. Giả sử $f : \mathbb{Z}_{15} \to \mathbb{Z}_3$ là một đồng cấu vành. Đặt $f(1) = \overline{a} \in \mathbb{Z}_3$. Ta có

$$\overline{a} = f(1) = f(1).f(1) = \overline{a}.\overline{a}$$

Do đó $a^2 - a \vdots 3$. Do vậy $\overline{a} = \overline{0},\ \overline{1}$.

Với $\overline{a} = \overline{0}$ ta suy ra f là đồng cấu không.

Với $\overline{a} = \overline{1}$ ta có $f(n + 15\mathbb{Z}) = n + 3\mathbb{Z}$ với mọi $n \in \mathbb{Z}$.

3.18. Giả sử $f : \mathbb{Z}_7 \to \mathbb{Z}_4$ là một đồng cấu vành. Đặt $f(\overline{1}) = \overline{a} \in \mathbb{Z}_4$. Ta có

$$\overline{0} = f(\overline{0}) = f(\underbrace{\overline{1} + \overline{1} + ... + \overline{1}}_{7 \text{ lần}}) = 7\overline{a} = \overline{7a}.$$

Do đó $7a \vdots 4$. Vậy $a \vdots 4$, nghĩa là $\overline{a} = \overline{0}$. Từ đó suy ra f là đồng cấu không.

3.19. $End(\mathbb{Z}_2 \times \mathbb{Z}_2)$ có 6 phần tử, đây là vành không giao hoán.

3.20. Chúng ta dễ kiểm tra được rằng $(R, \oplus, \circ)$ là một vành. Hơn nữa ánh xạ

$$\begin{array}{rcl} f : (R, \oplus, \circ) & \to & (R, +, .) \\ r & \mapsto & r + \overline{1} \end{array}$$

là một đẳng cấu vành.

3.21.a) Dựa vào các tiên đề của một vành, ta có thể thử lại được rằng S cùng với ai phép toán đã cho lập thành một vành có đơn vị là $(0, 1)$.

b) Dễ thấy $0 = (0, 0) \in A$. Giả sử $(r_1, n_1), (r_2, n_2) \in A$. Với mọi $x \in R$ ta có

$$r_1x + n_1x = r_2x + n_2x = 0.$$

Do đó

$$\begin{array}{rcl} (r_1 - r_2)x + (n_1 - n_2)x & = & (r_1x + n_1x) - (r_2x + n_2x) \\ & = & 0 - 0 = 0 \end{array}$$

với mọi $x \in R$. Vậy $(r_1 - r_2, n_1 - n_2) \in A$, hay $(r_1, n_1) - (r_2, n_2) \in A$. Lấy (r, n) bất kỳ thuộc A, (s, k) bất kỳ thuộc S ta có:

$$(r, n)(s, k) = (rs + kr + ns, nk).$$

Với mọi $x \in R$ ta có: $rx + nx = 0$. Do đó:

$$\begin{aligned}(rs + kr + ns)x + (nk)x &= (rs)x + (kr)x + (ns)x + (nk)x \\ &= r(sx) + n(sx) + k(rx) + k(nx) \\ &= [r(sx) + n(sx)] + k(rx + nx) \\ &= 0 + k0 = 0\end{aligned}$$

(Chú ý rằng do $(r, n) \in A$ nên ta có $r(sx) + n(sx) = 0$). Vậy $(r, n)(s, k) \in A$. Chứng minh tương tự ta có $(s, k)(r.n) \in A$. Vậy A là iđêan của S.

c) Do S là vành có đơn vị là $(0, 1)$ nên vành thương S/A có đơn vị là $(0, 1) + A$. Xét ánh xạ

$$\begin{aligned}\varphi : R &\to S/A \\ r &\mapsto (r, 0) + A.\end{aligned}$$

Ta dễ thử lại rằng φ là một đồng cấu. Bây giờ ta xác định $\mathrm{Ker}\varphi$. Lấy $r \in \mathrm{Ker}\varphi$. Khi đó $(r, 0) \in A$. Từ đó với $e \in R$ ta có

$$re + 0e = 0 \Rightarrow r = 0.$$

Vậy φ là một đơn cấu, do đó S/A chứa vành con $\mathrm{Im}\varphi$ đẳng cấu với R.

d) Lấy $a, b \in S/A$ sao cho $ab = 0$. Giả sử $a = (r, n) + A, b = (s, k) + A$. Ta có:

$$ab = (rs + kr + ns, nk) + A = 0.$$

Suy ra $(rs + kr + ns, nk) \in A$. Do đó, với $e \in R$ ta có:

$$\begin{aligned}& (rs + kr + ns)e + (nk)e = 0 \\ \Rightarrow\ & (rs)e + (kr)e + (ns)e + (nk)e = 0 \\ \Rightarrow\ & (re)(se) + (ke)(re) + (ne)(se) + (ne)(ke) = 0 \\ \Rightarrow\ & (re + ne)(se + ke) = 0.\end{aligned}$$

Do R không có ước của không nên $re + ne = 0$ hoặc $se + ke = 0$.

Nếu $re + ne = 0$ thì với mọi $x \in R$ ta có:

$$rx + nx = r(ex) + n(ex) = (re + ne)x = 0x = 0.$$

Vậy $(r, n) \in A$.

Tương tự nếu $se + ke = 0$ thì ta cũng suy ra $(s, k) \in A$. Vậy S/A là vành không có ước của không.

3.22. Chúng ta dễ thử lại rằng $R \times \mathbb{Z}$ là một vành, có đơn vị là phần tử $(0,1)$. Hơn nữa, ánh xạ

$$\begin{aligned} f : R &\to R \times \mathbb{Z} \\ r &\mapsto (r,0) \end{aligned}$$

còn là một đơn cấu vành. Do đó R đẳng cấu với vành con $\mathrm{Im}f$ của vành $R \times \mathbb{Z}$.

Chú ý. Bài tập này chứng tỏ rằng mọi vành có thể nhúng được vào một vành có đơn vị.

3.23. a) Giả sử $f : \mathbb{Q} \to \mathbb{Q}$ là một tự đồng cấu. Ta có

$$f(1) = f(1.1) = f(1).f(1)$$

Do đó $f(1) = 0$ hoặc $f(1) = 1$.

Nếu $f(1) = 0$ thì với mọi $r \in \mathbb{Q}$ ta có

$$f(r) = f(r.1) = f(r).f(1) = 0$$

nghĩa là f là đồng cấu không.

Nếu $f(1) = 1$ thì ta dễ chỉ ra được rằng $f(n) = n$ với mọi $n \in \mathbb{Z}$. Với $q \in \mathbb{Z}^*$ ta có

$$1 = f(1) = f(q.\frac{1}{q}) = f(q).f(\frac{1}{q}) = q.f(\frac{1}{q})$$

Suy ra $f(\frac{1}{q}) = \frac{1}{q}$. Do đó với mọi số hữu tỷ $r = \frac{p}{q}$ ta có:

$$f(r) = f(\frac{p}{q}) = f(p.\frac{1}{q}) = f(p).f(\frac{1}{q}) = p.\frac{1}{q} = r.$$

Vậy f là tự đồng cấu đồng nhất của $\mathbb{Q}$.

Tóm lại có hai tự đồng cấu của $\mathbb{Q}$ là đồng cấu không và tự đồng cấu đồng nhất.

b) Chứng minh như câu a) ta cũng có, nếu $f : \mathbb{R} \to \mathbb{R}$ là một đồng cấu thì $f(1) = 0$ hoặc $f(1) = 1$.

Nếu $f(1) = 0$ thì ta cũng suy ra được f là đồng cấu không.

Nếu $f(1) = 1$ thì ta có $f(a) = a$ với mọi $a \in \mathbb{Q}$.

Ta thấy rằng nếu r là một số thực dương thì $f(r) \geq 0$. Thật vậy ta có

$$f(r) = f(\sqrt{r}.\sqrt{r}) = [f(\sqrt{r})]^2 \geq 0.$$

Bây giờ giả sử r là một số thực tuỳ ý sao cho $f(r) \neq r$. Do tính trù mật khắp nơi của trường số hữu tỷ $\mathbb{Q}$ trong $\mathbb{R}$ nên tồn tại số hữu tỷ q sao cho

$$r < q < f(r) \qquad (1)$$

hoặc

$$f(r) < q < r \qquad (2).$$

Nếu (1) xảy ra thì $q - r > 0$. Do đó

$$f(q - r) = f(q) - f(r) \geq 0 \Rightarrow q \leq f(r)$$

Điều này mâu thuẫn với (1).
Nếu (2) xảy ra thì $r - q > 0$, do đó

$$f(r - q) = f(r) - f(q) \geq 0 \Rightarrow f(r) \leq q$$

điều này mâu thuẫn với (2).
Vậy với mọi $r \in \mathbb{R}$ ta có $f(r) = r$, nghĩa là f là ánh xạ đồng nhất.
Tóm lại tập hợp các tự đồng cấu của $\mathbb{R}$ là $\{0, id_{\mathbb{R}}\}$.

c) Giả sử $f : \mathbb{C} \to \mathbb{C}$ là một tự đồng cấu sao cho $f(a) = a$ với mọi $a \in \mathbb{R}$. Khi đó với mọi số thực $z = a + bi$ ta có:

$$f(z) = f(a) + f(b).f(i) = a + bf(i).$$

Mặt khác ta có:

$$-1 = f(-1) = f(i.i) = f(i).f(i)$$

Do đó $f(i) = i$ hoặc $f(i) = -i$.

Nếu $f(i) = i$ thì f là ánh xạ đồng nhất của $\mathbb{C}$. Nếu $f(i) = -i$ thì f là ánh xạ liên hợp của $\mathbb{C}$.

3.24. Giả sử $f : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2})$. Từ

$$f(1) = f(1.1) = f(1).f(1)$$

ta suy ra $f(1) = 0$ hoặc $f(1) = 1$.

Nếu $f(1) = 0$ thì f là đồng cấu không.

Nếu $f(1) = 1$ thì $f(r) = r$ với mọi $r \in \mathbb{Q}$. Do đó với mọi

$$x = a + b\sqrt[3]{2} + c\sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2})$$

ta có

$$f(x) = a + bf(\sqrt[3]{2}) + cf(\sqrt[3]{4}).$$

Mặt khác, ta có: $2 = f(2) = [f(\sqrt[3]{2})]^3$. Do đó $f(\sqrt[3]{2})$ là một căn bậc ba của 2 (gồm có một giá trị thực và hai giá trị phức). Bởi vì $f(\sqrt[3]{2}) \in \mathbb{Q}(\sqrt[3]{2})$ là một số thực nên $f(\sqrt[3]{2}) = \sqrt[3]{2}$. Từ đó suy ra f là tự đồng cấu đồng nhất của $\mathbb{Q}(\sqrt[3]{2})$.
Tóm lại các tự đồng cấu của $\mathbb{Q}(\sqrt[3]{2})$ là $\{0, id_{\mathbb{Q}(\sqrt[3]{2})}\}$.

3.26. a) Chúng ta dễ thử lại được rằng $\mathbb{Q}(\sqrt{d})$ là một trường con của trường số thực $\mathbb{R}$, với $d = 7, 11$.

b) Giả sử tồn tại một đẳng cấu vành $f : \mathbb{Q}(\sqrt{11}) \to \mathbb{Q}(\sqrt{7})$. Khi đó chúng ta suy ra $f(1) = 1$, và do đó $f(11) = 11$. Ta có

$$11 = f(11) = [f(\sqrt{11})]^2.$$

Do đó $f(\sqrt{11}) = \pm\sqrt{11}$. Điều này mâu thuẫn vì $\sqrt{11} \notin \mathbb{Q}(\sqrt{7})$.

3.27. a) Giả sử X là vành có p phần tử với đơn vị là e. Khi đó nhóm $(X, +)$ là một nhóm có cấp nguyên tố nên nó là nhóm xyclic sinh bởi một phần tử bất kỳ khác không. Bởi vậy

$$X = \langle e \rangle = \{0, e, 2e, ..., (p-1)e\}.$$

với $pe = 0$ và $e^2 = 1$. Từ đó có thể suy ra ánh xạ

$$\begin{array}{rcl} f : \mathbb{Z}_p & \to & X \\ \overline{k} & \mapsto & ke \end{array}$$

là một đẳng cấu vành. Vậy $\mathbb{Z}_p \cong X$.

b) Nếu m không là nguyên tố thì $m = m_1.m_2$ với $1 < m_1, m_2 < m$. Giả sử $(m_1, m_2) > 1$. Khi đó $\mathbb{Z}_m$ và $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$ là hai vành có cùng m phần tử nhưng không đẳng cấu vì ta thấy nhóm cộng của $\mathbb{Z}_m$ là nhóm xyclic nhưng nhóm cộng của $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$ không xyclic.

3.29. a) Từ tính chất phân phối giữa phép cộng và phép nhân trong vành R ta suy ra h_a là một tự đồng cấu nhóm của nhóm cộng aben R.

b) Với mọi $a, b, x \in R$ ta có

$$\begin{array}{rcl} (h_a + h_b)(x) & = & h_a(x) + h_b(x) = a.x + b.x = (a+b).x = h_{a+b}(x); \\ (h_a \circ h_b)(x) & = & h_a(h_b(x)) = h_a(b.x) = a.(b.x) = (a.b).x = h_{ab}(x). \end{array}$$

Từ đó suy ra

$$h_a + h_b = h_{a+b},\ h_a \circ h_b = h_{ab}.$$

Vậy h là một đồng cấu vành.

c) Ta có

$$\begin{aligned} \mathrm{Ker}h &= \{a \in R \mid h_a = 0\} \\ &= \{a \in R \mid h_a(x) = 0 \ \ \forall x \in R\} \\ &= \{a \in R \mid a.x = 0 \ \ \forall x \in R.\} \end{aligned}$$

Nếu R có đơn vị là 1 thì với $a \in \mathrm{Ker}h$ ta suy ra $a.1 = 0$, nghĩa là $a = 0$. Vậy Ker $h = 0$, và do đó h là một đơn cấu.

3.30. Xét tương ứng

$$\begin{aligned} \overline{f} : X/A &\to Y/B \\ x + A &\mapsto f(x) + B \end{aligned}$$

Tương ứng trên là một ánh xạ. Thật vậy, giả sử $x + A = x' + A$. Khi đó $x - x' \in A$, và do đó

$$f(x) - f(x') = f(x - x') \in f(A) \subset B.$$

Bởi vậy $f(x) + B = f(x') + B$. Chúng ta dễ thử lại rằng $\overline{f}$ là một đồng cấu vành. Mặt khác ta có:

$$\begin{aligned} \overline{f} \circ p(x) &= \overline{f}(p(x)) = \overline{f}(x + A) \\ = \ f(x) + B &= p'(f(x)) = p' \circ f(x). \end{aligned}$$

Vậy $\overline{f}$ là đồng cấu thoả mãn $\overline{f} \circ p = p' \circ f$.

Bây giờ giả sử $\varphi : X/A \to Y/B$ là đồng cấu sao cho $\varphi \circ p = p' \circ f$. Khi đó ta có:

$$\begin{aligned} \varphi(x + A) &= \varphi(p(x)) = (\varphi \circ p)(x) = (p' \circ f)(x) \\ &= (\overline{f} \circ p)(x) = \overline{f}(p(x)) = \overline{f}(x + A) \end{aligned}$$

Vậy $\varphi = \overline{f}$.

Ta cũng có thể lập luận như sau: Ta có

$$\varphi \circ p = p' \circ f = \overline{f} \circ p.$$

Do p là một toàn ánh nên giản ước cho p ta được $\varphi = \overline{f}$. Điều đó cho ta tính duy nhất của $\overline{f}$.

3.31. a) Chúng ta dễ thử được p là một đồng cấu vành.

b) Giả sử p là một toàn cấu. Khi đó mỗi cặp $(x+I,\ y+J)$, với $x, y \in R$ đều tồn tại phần tử $a \in R$ sao cho

$$p(a) = (x + I,\ y + J).$$

Khi đó ta có

$$a - x = u \in I, \quad y - a = v \in J.$$

Bây giờ chọn $y = x + 1$ ta có:

$$u + v = y - x = 1$$

và do đó $1 \in I + J$, từ đó suy ra $R = I + J$.

Đảo lại, nếu $R = I + J$ thì tồn tại $u \in I,\ v \in J$ sao cho $1 = u + v$. Lấy phần tử bất kỳ $(x+I, y+J)$ thuộc $(R/I)\times(R/J)$. Đặt $a = xv+yu$. Ta có:

$$\begin{aligned} x - a &= x(1 - v) - yu \\ &= xu - yu = (x - y)u \in I. \end{aligned}$$

Từ đó $x + I = a + I$. Hoàn toàn tương tự ta có $y + J = a + J$. Điều này chứng tỏ

$$p(a) = (x + I, y + J).$$

Vậy p là một toàn cấu.

c) Mở rộng: Giả sử $I_1, I_2, ..., I_n$, với $n > 2$, là những iđêan của R. Khi đó ánh xạ

$$\begin{aligned} p : R &\to \prod_{k-i}^{n} (R/I_k) \\ a &\mapsto (a + I_k) \end{aligned}$$

là một toàn cấu khi và chỉ khi với mọi $1 \leq i \neq j \leq n$ ta có: $I_i + I_j = R$.

3.32. Xét ánh xạ

$$\begin{aligned} f : R &\to (R/A) \times (R/B) \\ x &\mapsto (x + A, x + B) \end{aligned}$$

Theo Bài tập 3.31 ta có f là một toàn cấu vành. Hơn nữa

$$\begin{aligned} x \in \mathrm{Ker} f &\Leftrightarrow (x + A, x + B) = (0, 0) \\ &\Leftrightarrow x \in A \cap B. \end{aligned}$$

Vậy $\mathrm{Ker} f = A \cap B$.

Mặt khác do $A + B = R$ nên theo Bài tập 2.7 ta có: $A \cap B = AB$. Từ đó theo định lý đồng cấu vành ta có

$$R/AB \cong (R/A) \times (R/B).$$

3.33. a) $\Rightarrow$ b) Giả sử tồn tại đồng cấu $h : R \to Y$ sao cho $g = h \circ f$. Khi đó với mọi $x \in \mathrm{Ker} f$ ta có

$$g(x) = h(f(x)) = h(0) = 0$$

do đó $x \in \mathrm{Ker} g$. Vậy $\mathrm{Ker}\ f \subseteq \mathrm{Ker} g$.

b) $\Rightarrow$ a) Giả sử $\mathrm{Ker}\ f \subseteq \mathrm{Ker} g$. Khi đó với mỗi $a \in R$, do f là một toàn cấu nên tồn tại $x \in V$ sao cho $f(x) = a$.
Chúng ta nhận xét rằng $g(x)$ không phụ thuộc vào việc chọn phần tử x, mà chỉ phụ thuộc vào a. Thật vậy giả sử $x' \in V$ sao cho $f(x') = a$. Khi đó ta có

$$f(x - x') = f(x) - f(x') = a - a = 0$$

Do đó $x - x' \in \mathrm{Ker} f \subseteq \mathrm{Ker} g$. Suy ra $g(x - x') = 0$, nghĩa là

$$g(x) = g(x').$$

Xét ánh xạ

$$\begin{aligned} h : R &\to Y \\ a &\mapsto g(x) \end{aligned}$$

trong đó $f(x) = a$.

Chúng ta có thể kiểm tra lại được h chính là một đồng cấu thoả mãn $g = h \circ f$.

c) Giả sử tồn tại đồng cấu $\varphi : R \to Y$ sao cho $g = \varphi \circ f$. Khi đó với mỗi $a \in R$, tồn tại $x \in V$ sao cho $a = f(x)$. Khi đó ta có

$$\begin{aligned} \varphi(a) &= \varphi(f(x)) = (\varphi \circ f)(x) \\ &= g(x) = h(f(x)) = h(a) \end{aligned}$$

Do đó $\varphi = h$.

d) Giả sử h là một đơn ánh. Khi đó

$$\begin{aligned} x \in \mathrm{Ker} g &\Leftrightarrow g(x) = 0 \Leftrightarrow h(f(x)) = 0 \\ &\Leftrightarrow f(x) \in \mathrm{Ker} h = \{0\} \Leftrightarrow x \in \mathrm{Ker} f. \end{aligned}$$

Vậy $\mathrm{Ker} f = \mathrm{Ker} g$.

Đảo lại, giả sử $\mathrm{Ker} f = \mathrm{Ker} g$. Lấy $a \in \mathrm{Ker} h$, khi đó do f là một toàn cấu nên tồn tại $x \in V$ sao cho $a = f(x)$. Ta có

$$g(x) = h(f(x)) = h(a) = 0$$

do đó $x \in \mathrm{Ker} g = \mathrm{Ker} f$. Suy ra $a = f(x) = 0$, nghĩa là $\mathrm{Ker} h = \{0\}$. vậy h là một đơn ánh.

e) Nếu h là một toàn cấu thì do f cũng là một toàn cấu nên ta có $g = h \circ f$ cũng là một toàn ánh.

Đảo lại, nếu g là một toàn ánh thì với mọi $y \in Y$, tồn tại $x \in V$ sao cho $y = g(x)$. Khi đó ta có

$$y = g(x) = h(f(x))$$

Do đó h cũng là một toàn ánh.

4. Trường các thương

4.1. Gọi K là trường các thương của miền nguyên $\mathbb{Z}(\sqrt{2})$. Do K chứa $\mathbb{Z}$ nên K phải chứa trường các thương của $\mathbb{Z}$, nghĩa là K chứa $\mathbb{Q}$. Mặt khác do $\sqrt{2} \in K$ nên $\mathbb{Q}(\sqrt{2}) \subset K$.

Do K là trường cực tiểu chứa $\mathbb{Z}(\sqrt{2})$ và $\mathbb{Q}(\sqrt{2})$ là một trường chứa $\mathbb{Z}(\sqrt{2})$ nên ta có $K \subset \mathbb{Q}(\sqrt{2})$. Vậy $K = \mathbb{Q}(\sqrt{2})$.
Lập luận tương tự, trường các thương của các miền nguyên $\mathbb{Z}(i)$, $\mathbb{Z}(\sqrt[3]{2})$ tương ứng là $\mathbb{Q}(i), \mathbb{Q}(\sqrt[3]{2})$.

4.2. a) Chúng ta dễ thử lại được A là một vành con của R. Do R là một trường nên A là một miền nguyên.

b) Gợi ý: Xét ánh xạ

$$\begin{aligned} \varphi : \mathbb{Z} &\to A \\ n &\mapsto ne \end{aligned}$$

4.3. Đặt $A = \left\{ \frac{m}{n} \in \mathbb{Q} | \ (n,p) = 1 \right\}$.

Chúng ta có thể thử lại rằng A là một vành con của $\mathbb{Q}$. Hơn nữa do $1 \in A$ nên A là một miền nguyên.

Gọi $\overline{A}$ là trường các thương của A. Do $A \supset \mathbb{Z}$ nên $\overline{A} \supset \mathbb{Q}$. Mặt khác do $A \subset \mathbb{Q}$ nên $\overline{A} \subset \mathbb{Q}$. Vậy $\overline{A} = \mathbb{Q}$.

4.5. Giả sử I là hạt nhân của một đồng cấu vành $\varphi : R \to K$ trong đó K, là một trường. Khi đó

$$R/I \cong \varphi(R)$$

là một vành con của trường K nên nó là một miền nguyên. Từ đó suy ra I là một iđêan nguyên tố của vành R.

Đảo lại, giả sử I là một iđêan nguyên tố của vành R. Khi đó, I là hạt nhân của phép chiếu chính tắc $p : R \to R/I$. Do I là iđêan nguyên tố nên R/I là một miền nguyên.

Gọi Q là trường các thương của R/I và $\mu : R/I \to Q$ là phép nhúng chính tắc. Khi đó

$$\varphi = \mu \circ p : R \to Q$$

là một đồng cấu vành. Hơn nữa:

$$\mathrm{Ker}\varphi = \mathrm{Ker}(\mu \circ p) = \mathrm{Ker}p = I.$$

4.6. 1) Trường hợp R có đặc số 0. Trên nhóm cộng $R \oplus \mathbb{Z}$ xác định phép nhân cho bởi:

$$(r,k)(r',k') = (rr' + kr' + k'r, kk') \cdot$$

với $r, r' \in R$; $k, k' \in \mathbb{Z}$. Thử lại rằng S là vành có đơn vị $(0,1)$, có đặc số 0 và ánh xạ $R \to S$ cho bởi $r \mapsto (r,0)$ là một đơn cấu vành (một phép nhúng).

2) Nếu đặc số của R bằng $n > 0$ thì ta đặt $S = R \oplus \mathbb{Z}_n$ và xác định phép toán trên S bởi

$$(r,\overline{k})(r',\overline{k'}) = (rr' + k'r + kr', \overline{kk'})$$

Chú ý rằng do vành R có đặc số n nên tương ứng trên không phụ thuộc vào việc chọn đại diện k, k' của các lớp $\overline{k}, \overline{k'}$. Hơn nữa nhóm

cộng S cùng với phép nhân được định nghĩa như trên là một vành có đặc số n, đồng thời ánh xạ $R \to S$ cho bởi $r \mapsto (r.0)$ là một đơn cấu vành.

5. Vành và trường sắp thứ tự

5.1. a) Giả sử $a + x < a + y$. Cộng cả hai vế của bất đẳng thức trên cho $-a$ ta được:

$$\begin{aligned}(-a) + (a + x) < (-a) + (a + y) &\Rightarrow [(-a) + a] + x < [(-a) + a] + y \\ &\Rightarrow 0 + x < 0 + y \Rightarrow x < y.\end{aligned}$$

Các phần còn lại được chứng minh tương tự như trường hợp các số thực.

5.2. Giả sử $a, b \in A \cap P$. Khi đó ta có $a, b \in A$ và $a, b \in P$. Do A là vành con của R nên ta có

$$a + b,\ a.b \in A.$$

Mặt khác, P là tập các phần tử dương của vành sắp thứ tự R nên ta có

$$a + b,\ a.b \in P.$$

Vậy $a + b,\ a.b \in A \cap P$. Hơn nữa, ta có

$$(A \cap P) \cap (-(A \cap P)) \subset P \cap (-P) = \emptyset$$

Suy ra $(A \cap P) \cap (-(A \cap P)) = \emptyset$. Ta có

$$(A \cap P) \cup 0 \cup (-(A \cap P)) \subset A$$

và

$$A \subset A \cap R = A \cap (P \cup 0 \cup (-P))$$

nghĩa là

$$A \subset (A \cap P) \cup 0 \cup (-(A \cap P)).$$

Vậy $A = (A \cap P) \cup 0 \cup (-(A \cap P))$. Từ những lập luận trên ta suy ra A là một vành sắp thứ tự với tập con dương là $A \cap P$.

5.4. Trước hết chúng ta thấy rằng tồn tại $z = \dfrac{x+y}{2}$ thoả mãn điều kiện $x < z < y$. Bây giờ, ta giả sử trong R chỉ tồn tại hữu hạn phần tử $z_1, z_2, ..., z_n$ sao cho

$$x < z_1 < z_2 < ... < z_n < y.$$

Đặt $z_{n+1} = \dfrac{z_n + y}{2}$. Khi đó $z_{n+1} \in R$ và thoả mãn

$$x < z_{n+1} < y \text{ và } z_{n+1} \neq z_1, z_2, ..., z_n.$$

Mâu thuẫn này chứng tỏ trong R tồn tại vô số phần tử z thoả mãn $x < z < y$.

5.5. Giả sử có thể trang bị một quan hệ thứ tự trên vành $\mathbb{Z}_n$ để $\mathbb{Z}_n$ trở thành một vành sắp thứ tự. Khi đó ta có: $\bar{1} > \bar{0}$. Từ đó suy ra

$$\underbrace{\bar{1} + \bar{1} + ... \bar{1}}_{n \text{ lần}} > \bar{0} \Rightarrow \bar{0} > \bar{0}$$

Điều này là vô lý. Vậy không thể trang bị cho tập hợp $\mathbb{Z}_n$ một quan hệ thứ tự để $\mathbb{Z}_n$ trở thành một vành sắp thứ tự.

Chương V

VÀNH ĐA THỨC VÀ VÀNH ƠCLIT

1. Vành đa thức

1.1. $(2x^3 + 4x^2 + x)(3x^2 + 3x + 2) = x^3 + 5x^2 + 2x$.

Vành $\mathbb{Z}_6[x]$ có ước của không. Chẳng hạn $3x$ và $2x + 2$ là hai đa thức khác không nhưng $3x(2x + 2) = 0$.

1.2. Ta có: $x^3 + px + 5 = (x - 5)(x^2 + 5x + 6) + (p - 2)x$. Do đó để $x^3 + px + 5$ chia hết cho $(x^2 + 5x + 6)$ ta phải có $\overline{p - 2} = \bar{0}$, nghĩa là $p = 2 + 7t,\ t \in \mathbb{Z}$.

1.3. a) Giả sử:

$$f(x) = (x - 1)^2 p(x) + 2x = (x - 2)^2 q(x) + 3x \quad (1)$$

với $p(x), q(x) \in \mathbb{Z}[x]$. Từ (1) ta suy ra: $f(1) = 2,\ f(2) = 6$ (2). Hơn nữa ta có:

$$f'(x) = 2(x - 1)p(x) + (x - 1)^2 p'(x) + 2.$$

Do đó: $f'(1) = 2$ (3).
Cũng từ đẳng thức (1) ta suy ra:

$$f'(x) = 2(x - 2)q(x) + (x - 2)^2 q'(x) + 3.$$

Do vậy: $f'(2) = 3$ (4).

Chúng ta có thể chứng minh được rằng không tồn tại một đa thức $f(x)$ có bậc nhỏ hơn 3 thoả mãn các điều kiện (2), (3), (4). Bây giờ ta tìm đa thức $f(x)$ có bậc ba thoả mãn các điều kiện (2), (3), (4). Bằng những tính toán cụ thể ta được:

$$f(x) = -3x^3 + 14x^2 - 17x + 8.$$

Dây chính là đa thức có bậc nhỏ nhất của $\mathbb{Z}[x]$ thoả mãn các yêu cầu của đề bài.

b) Bạn đọc tự giải câu này.

1.4. $\frac{3}{2}x^2 + \frac{5}{4}x - \frac{15}{8}$ và $\frac{45}{8}x + \frac{7}{8}$.

1.5. $x^3 - 2x^2 + 5x - 15$ và $32x^2 + 15$.

1.6. $x^4 + x^3 + x^2 + x$ và 1.

1.7. $2x^2 + x + 1$ và $x^2 + 2$.

1.8. Cả ba đa thức đã cho đều là bất khả quy trên $\mathbb{Z}[x]$.

1.9. Trong đa thức $f(x)$, thay x bởi $x + a$ ta được đa thức $f(x + a) \in A[x]$. Ta có $f(x)$ khác 0, khác ước của 1 khi $f(x + a)$ khác 0, khác ước của 1. Hơn nữa:

$$f(x) = b(x)g(x) \Leftrightarrow f(x + a) = b(x + a)g(x + a)$$

và bậc của $f(x)$ bằng bậc của $f(x + a)$. Từ đó suy ra điều phải chứng minh.

1.10. Đa thức $f(x) = \sum_{i=0}^{n} a_i x^i$ có bậc $n > 1$ và bất khả quy trên A nên suy ra $a_0 \neq 0$. Do đó $g(x) = \sum_{i=0}^{n} a_{n-i} x^i$ khác 0 và khác ước của 1. Giả sử rằng:

$$g(x) = (b_p + b_{p-1}x + \cdots + b_0 x^p)(c_q + c_{q-1}x + \cdots + c_0 x^q).$$

Khi đó:

$$f(x) = (b_0 + b_1 x + \cdots + b_p x^p)(c_0 + c_1 x + \cdots + c_q x^q).$$

Từ đó suy ra điều phải chứng minh.

1.11. Vì p là số nguyên tố nên $(\mathbb{Z}_p^*, .)$ là một nhóm cấp $p - 1$. Theo Định lý Lagrange, với mọi $x \in \mathbb{Z}_p^*$ ta có $x^{p-1} = 1$, do đó $x^p = x$, hay $x^p - x = 0$. Vậy với mọi $x \in \mathbb{Z}_p$, hàm $x \mapsto x^p - x$ là hàm không.

Đa thức $x^5 - x$ xác định một hàm không trên $\mathbb{Z}_5$. Do đó hai đa thức $x^2 - x + 1$ và $x^5 + x^2 - 2x + 1$ cùng xác định một hàm $x^2 - x + 1$.

1.12. Gọi $B = \mathrm{Ker}\varphi$, thế thì B là một idêan trong $K[x]$. Giả sử $f(x), g(x) \in K[x]$ sao cho $f(x)g(x) \in B$. Ta phải chứng minh $f(x) \in B$ hoặc $g(x) \in B$. Do

$$f(u)g(u) = 0$$

trong F nên $f(u) = 0$ hoặc $g(u) = 0$. Từ đó $f(x) \in B$ hoặc $g(x) \in B$.

Cuối cùng, ta phải chỉ ra $B \neq K[x]$. Thật vậy, trong $K[x]$, ta xét đa thức

$$h(x) = x + 1 - u.$$

Khi đó $h(u) = 1 \neq 0$ nên $h(x) \notin B$.

Nếu K là vành con có chứa đơn vị của miền nguyên F thì kết quả trên vẫn đúng.

1.13. a) Việc chứng minh $I[x]$ là một iđêan của $\mathbb{Z}[x]$ dành cho bạn đọc. Xét ánh xạ

$$\begin{aligned} \varphi : \mathbb{Z}[x] &\to (\mathbb{Z}/I)[x] \\ f(x) = \sum_{i=0}^{n} a_i x^i &\mapsto \sum_{i=0}^{n} \overline{a}_i x^i, \end{aligned}$$

với $\overline{a}_i = a_i + I$. Bạn đọc hãy kiểm tra rằng φ là một đồng cấu vành. Có thể thấy rằng φ là một toàn cấu. Bây giờ ta tìm hạt nhân của φ.

$$\begin{aligned} f(x) \in \mathrm{Ker}\varphi &\Rightarrow \sum_{i=0}^{n} \overline{a}_i x^i = 0 \Rightarrow \overline{a}_i = 0 \\ &\Rightarrow a_i \in I \Rightarrow f(x) \in I[x]. \end{aligned}$$

Từ đó, $\mathrm{Ker}\varphi \subset I[x]$. Bao hàm ngược lại là hiển nhiên, do đó $\mathrm{Ker}\varphi = I[x]$. Bây giờ điều phải chứng minh được suy ra từ Định lý đồng cấu.

b) Từ đẳng cấu

$$\mathbb{Z}[x]/I[x] \cong (\mathbb{Z}/I)[x] \quad (*)$$

suy ra rằng nếu I là iđêan nguyên tố thì $\mathbb{Z}/I$ là miền nguyên và do đó $(\mathbb{Z}/I)[x]$ là miền nguyên. Từ đó suy ra $I[x]$ là iđêan nguyên tố của $\mathbb{Z}[x]$.

$I[x]$ không là iđêan tối đại của $\mathbb{Z}[x]$ bởi vì nếu ngược lại thì vế trái của hệ thức $(*)$ là một trường, còn vế phải không là trường.

1.14. Xét ánh xạ

$$\begin{aligned} \varphi : \mathbb{Z}[x] &\longrightarrow \mathbb{Z}_n \\ a_o + a_1 x + \ldots + a_n x^n &\longmapsto \overline{a_o} \end{aligned}$$

trong đó $\overline{a_o} = a_o + n\mathbb{Z}$. Dễ chứng minh được φ là một đồng cấu vành.

Hơn nữa, φ còn là một toàn cấu có $\text{Ker}\varphi = I$. Theo định lý đồng cấu ta có

$$\mathbb{Z}[x]/I \cong \mathbb{Z}_n.$$

Từ đó suy ra I là một iđêan nguyên tố khi và chỉ khi $\mathbb{Z}_n$ là một miền nguyên. Điều này xảy ra khi và chỉ khi n là một số nguyên tố.

1.15. 4 nghiệm đó là $\pm\overline{1}$ và $\pm\overline{4}$.

1.16. 6 nghiệm đó là: $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}$.

1.17. Đặt $f(x) = (x+1)^{2n} - x^{2n} - 2x - 1$. Ta có:

$$f(-\frac{1}{2}) = f(-1) = f(0) = 0$$

nên $f(x)$ chia hết cho $2x+1$, $x+1$ và x.

1.18. Xét đa thức

$$f(x) = (x-a_1)(x-a_2)...(x-a_n) - 1,$$

với a_i là những số nguyên phân biệt. Khi đó:

$$f(x) = g(x)h(x),$$

với $g(x), h(x)$ là những đa thức trên $\mathbb{Z}$ và không khả nghịch. Ta có:

$$f(a_i) = -1 = g(a_i)h(a_i).$$

Do $g(a_i)$ và $h(a_i)$ là những số nguyên nên các dẳng thức trên kéo theo:

$$g(a_i) + h(a_i) = 0.$$

Điều này xảy ra tại n giá trị phân biệt a_i. Mặt khác:

$$\deg(g(x) + h(x)) \leq \max(\deg g(x), \deg h(x)) < \deg f(x) = n$$

nên ta có $g(x) + h(x) = 0$. Do đó:

$$f(x) = -[g(x)]^2.$$

Đẳng thức này không thể xảy ra do dấu của các hệ số cao nhất ở mỗi vế là khác nhau.

1.19. Giả sử $f(x)$ khả quy trong $\mathbb{Q}[x]$. Khi đó: $f(x) = g(x)h(x)$, với $g(x), h(x)$ là những đa thức với hệ số nguyên có bậc lớn hơn hoặc bằng 1, đồng thời ta có thể giả sử hệ tử cao nhất của hai đa thức này bằng 1. Suy ra: $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$, với $\overline{f}, \overline{g}, \overline{h} \in \mathbb{Z}_p[x]$. Hơn nữa:

$$\deg(\overline{g}) = \deg(g) \geq 1; \quad \deg(\overline{h}) = \deg(h) \geq 1.$$

Suy ra $\overline{f}(x)$ khả quy trên $\mathbb{Z}_p$, trái với giả thiết.

1.20. a) Giả sử $\dfrac{p}{q}$ là nghiệm của đa thức $f(x)$. Khi đó ta có:

$$f(\frac{p}{q}) = a_n(\frac{p}{q})^n + a_{n-1}(\frac{p}{q})^{n-1} + \cdots + a_1\frac{p}{q} + a_0 = 0.$$

$$\Rightarrow \ a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} + a_0 q^n = 0$$

$$\Leftrightarrow \ a_n p^n = -q(a_{n-1}p^{n-1} + \cdots + a_0 q^{n-1})$$

suy ra q là ước của $a_n p^n$. Kết hợp với giả thiết: $(p, q) = 1$ ta được q là ước của a_n.

Chứng minh tương tự ta có p là ước của a_0.

b) Ta có:

$$f(m) = f(m) - f(\frac{p}{q}) = \sum_{k=0}^{n} a_k[m^k - (\frac{p}{q})^k]$$

$$\Rightarrow q^n f(m) = \sum_{k=0}^{n} a_k q^{n-k}[(mq)^k - p^k] \ \vdots \ mq - p.$$

Mặt khác do $(p, q) = 1$ nên ta có: $(mq - p, q^n) = 1$. Từ đó suy ra $f(m) \ \vdots \ mq - p$, nghĩa là: $p - mq \mid f(m)$. Đặc biệt $p - q$ là ước của $f(1)$ và $p + q$ là ước của $f(-1)$.

1.21. Giả sử $\alpha \in F$ là một nghiệm của đa thức

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \ a_i \in R.$$

Khi đó $\alpha = \dfrac{p}{q}$ với $p, q \in R$ và $(p, q) = 1$. Do α là nghiệm của $f(x)$ nên lý luận hoàn toàn tương tự Bài tập 1.20 ta có $q \mid 1$, nghĩa là tồn tại $u \in R$ sao cho $uq = i$. Khi đó, $\alpha = \dfrac{p}{q} = pu \in R$.

1.22. Giả sử $f(x)$ là đa thức có bậc nhỏ nhất với hệ tử cao nhất nhận u làm nghiệm. Giả sử $f(x)$ không bất khả quy,

$$f(x) = g(x)h(x),$$

trong đó $\deg(h) < \deg(f)$, $\deg(g) < \deg(f)$ và $h(x), g(x)$ có hệ tử cao nhất bằng 1. Khi đó

$$f(u) = h(u)g(u) = 0.$$

Suy ra $h(u) = 0$ hoặc $g(u) = 0$, nghĩa là $h(x)$ hoặc $g(x)$ nhận u làm nghiệm, trái với giả thiết về $f(x)$.

1.23. Đặt $I = \{g(x) \in K[x] \mid g(u) = 0\}$. Dễ thấy $I \neq \emptyset$. Hơn nữa, với mọi $f(x), g(x) \in I$ ta có:

$$f(u) = 0, g(u) = 0.$$

Do đó: $f(u) - g(u) = 0$ và $f(u)h(u) = 0$ với mọi $h(x) \in K[x]$.

1.24. Ta có

$$\mathrm{Ker}\psi = \{q(x).(x^2 + 1) \mid q(x) \in Q[x]\}$$

và $\mathrm{Im}\psi = \mathbb{C}$ (do $\psi(a + bx) = (a + bi)$ nên ψ là toàn ánh).

1.25. Ta có

$$\mathrm{Ker}\psi = \{q(x).(x^2 - 2x + 4) \mid q(x) \in Q[x]\}$$

và $\mathrm{Im}\psi = \mathbb{C}$ (do $a + bi = \psi(a - \dfrac{b}{\sqrt{3}} + \dfrac{b}{\sqrt{3}}x)$ nên ψ là toàn ánh).

1.26. $\sqrt{2} + \sqrt{3}$ là nghiệm của đa thức $x^4 - 10x^2 + 1$. Mặt khác, nếu đa thức này có nghiệm hữu tỷ $\dfrac{p}{q}$, $(p, q) = 1$ thì p là ước của 1 và q là ước của 1. Do đó các nghiệm hữu tỷ (nếu có) của đa thức này chỉ có thể là ± 1. Mặt khác ta thấy ± 1 không phải là nghiệm của đa thức trên. Do đó $\sqrt{2} + \sqrt{3}$ là số vô tỷ.

1.27. $8x + 2$ và $14x + 97$.

1.28. $-x^2 + 3x + 5$ và $2x^2 + 16x + 16$.

1.29. $x^2 + x$ và x^2.

1.30. $(a + c)x + (b + d)$ và $(bc + ad)x + (bd - ac)$.

1.31. Xét đồng cấu vành: $\psi : \mathbb{R}[x] \to \mathbb{C}$ được xác định bởi $\psi(p(x)) = p(i\sqrt{5})$. Hạt nhân của đồng cấu này là tập các đa thức chứa nhân tử $x^2 + 5$. Đó là iđêan $(x^2 + 5)$. $\text{Im}\psi = \mathbb{C}$ (do $a + bi = \psi(a + \frac{b}{\sqrt{5}}x)$ nên ψ là toàn ánh). Vì vậy, theo định lý đồng cấu vành ta có: $\mathbb{R}[x]/(x^2 + 5) \cong \mathbb{C}$.

1.32. Xét đồng cấu vành: $\psi : \mathbb{Z}[x] \to \mathbb{C}$ được xác định bởi $\psi(p(x)) = p(i)$. Ta có: $\text{Ker}\psi = (x^2 + 1)$, $\text{Im}\psi = \mathbb{Z}[i]$. Do đó

$$\mathbb{Z}[x]/(x^2 + 1) \cong \mathbb{Z}[i].$$

1.33. Xét đồng cấu vành: $\psi : \mathbb{Q}[x] \to \mathbb{R}$ được xác định bởi $\psi(p(x)) = p(\sqrt{7})$. Ta có: $\text{Ker}\psi = (x^2 - 7)$, $\text{Im}\psi = \mathbb{Q}(\sqrt{7})$. Do đó

$$\mathbb{Q}[x]/(x^2 - 7) \cong \mathbb{Q}(\sqrt{7}).$$

1.34. Xét đồng cấu vành: $\psi : \mathbb{Z}[x] \to \mathbb{Q}$ được xác định bởi $\psi(p(x)) = p(\frac{1}{2})$. Ta có:

$$\text{Ker}\psi = (2x - 1), \text{Im}\psi = \{\frac{a}{b} \in \mathbb{Q} \mid a \in \mathbb{Z}, b = 2^r, r \geq 0\}.$$

Do đó: $\mathbb{Z}[x]/(2x - 1) \cong \{\frac{a}{b} \in \mathbb{Q} \mid a \in \mathbb{Z}, b = 2^r, r \geq 0\}$.

1.35. Xét đồng cấu vành: $\psi : \mathbb{Z}_{14} \to \mathbb{Z}_7$ được xác định bởi $\psi(\overline{n}) = \overline{2n}$. Ta có: $\text{Ker}\psi = (7)$, $\text{Im}\psi = \mathbb{Z}_7$. Do đó $\mathbb{Z}_{14}/(7) \cong \mathbb{Z}_7$.

1.36. Xét đồng cấu vành: $\psi : \mathbb{Z}_{14} \to \mathbb{Z}_2$ được xác định bởi $\psi(\overline{n}) = \overline{7n}$. Ta có: $\text{Ker}\psi = (2)$, $\text{Im}\psi = \mathbb{Z}_2$. Do đó $\mathbb{Z}_{14}/(2) \cong \mathbb{Z}_2$.

1.37. Xét đồng cấu vành: $\psi : R[x, y] \to R[x, y]$ được xác định bởi

$$\psi(f(x, y)) = f(-y, y).$$

Ta có: $\text{Ker}\psi = (x + y)$. $\text{Im}\psi = R[y]$. Do đó $\mathbb{R}[x, y]/(x + y) \cong \mathbb{R}[y]$.

1.38. Xét đồng cấu vành: $\psi : R \times S \to S$ được xác định bởi $\psi((r, s)) = s$. Ta có: $\text{Ker}\psi = ((0, 1))$, $\text{Im}\psi = S$. Do đó:

$$(R \times S)/((1, 0)) \cong S.$$

1.39. Xét đồng cấu vành $\psi : \mathbb{R}[x, y] \longrightarrow \mathbb{R}$, $f(x, y) \mapsto f(0, 0)$. Khi đó ψ là một đồng cấu vành có: $\text{Ker}\psi = I$.

1.40. $\{p(x) \in \mathbb{Q}[x] | p(0) = 3\}$ không phải là một iđêan của $\mathbb{Q}[x]$.

1.41. Xét ánh xạ:

$$\begin{aligned} \varphi : A[x] &\to (A/I)[x] \\ f(x) = \sum_{i=0}^{n} a_i x^i &\mapsto \overline{f}(x) = \sum_{i=0}^{n} \overline{a_i} x^i \end{aligned}$$

trong đó $\overline{a_i} = a_i + I \in A/I$.

Rõ ràng φ là một đồng cấu vành và là một toàn ánh. Hơn nữa, ta có:

$$f(x) = \sum_{i=0}^{n} a_i x^i \in \mathrm{Ker}\varphi$$

khi và chỉ khi $\sum_{i=0}^{n} \overline{a_i} x^i = 0 \Leftrightarrow \overline{a_i} = 0$, với mọi $i = 0, 1, \ldots, n$. Nghĩa là $a_i \in I$. Do đó $\mathrm{Ker}\varphi = I[x]$ là một iđêan của $A[x]$ và ta có:

$$A[x]/I[x] \cong (A/I)[x]$$

Ta có: I là một iđêan nguyên tố của $A \Leftrightarrow A/I$ là một miền nguyên $\Leftrightarrow (A/I)[x]$ là một miền nguyên $\Leftrightarrow A[x]/I[x]$ là một miền nguyên $\Leftrightarrow I[x]$ là một iđêan nguyên tố của $A[x]$.

Nếu iđêan I là tối đại thì iđêan $I[x]$ là không là tối đại vì vành đa thức $(A/I)[x]$ không phải là một trường.

2. Thuật toán chia trong miền nguyên

2.1. Xét đa thức: $f(x) = ax^2 + bx + c \in \mathbb{R}[x]$, $a \neq 0$ với $\Delta = b^2 - 4ac < 0$. Nếu $f(x)$ khả quy thì tồn tại hai đa thức $g(x)$ và $h(x)$ thuộc $\mathbb{R}[x]$ với $\deg g(x) = \deg h(x) = 1$ sao cho:

$$f(x) = g(x)h(x).$$

Khi đó $g(x)$ và $h(x)$ lại có nghiệm thực. Các nghiệm này đồng thời cũng là nghiệm của $f(x)$. Vậy $f(x)$ có hai nghiệm thực, do đó $\Delta \geq 0$ (trái giả thiết). Vậy $f(x)$ là bất khả quy trong $\mathbb{R}[x]$.

Điều này không còn đúng khi thay trường số thực $\mathbb{R}$ bởi trường số

phức $\mathbb{C}$, vì mỗi đa thức bậc hai trên $\mathbb{C}$ được phân tích thành tích của hai nhị thức bậc nhất.

2.2. a) Giả sử $f(x) = ax + b \in F[x]$, $a \neq 0$, có sự phân tích trong $F[x]$ là

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

với $g(x)$ và $h(x)$ thuộc $F[x]$ sao cho: $\deg g(x) + \deg h(x) = 1$. Khi đó nếu $\deg g(x) = 1$ thì $\deg h(x) = 0$, nghĩa là $h(x) = d \in F$ và $d \neq 0$. Như vậy

$$g(x) = d^{-1}f(x)$$

tức là $g(x)$ và $f(x)$ liên kết với nhau.

Nếu $\deg g(x) = 0$ thì hoàn toàn tương tự $f(x)$ và $h(x)$ liên kết với nhau. Vậy $f(x)$ là đa thức bất khả quy.

Điều trên đây không còn đúng nữa nếu F không là một trường. Chẳng hạn đa thức $f(x) = 2x + 4 \in \mathbb{Z}[x]$ có $f(x) = 2(x + 2)$, nhưng 2 và $x + 2$ đều không là ước của 1 trong $\mathbb{Z}[x]$. Điều đó chứng tỏ $f(x)$ khả quy.

b) Giả sử $f(x) \in F[x]$ là đa thức có bậc bằng 2 hoặc 3. Ta sẽ chứng tỏ rằng $f(x)$ khả quy trên F khi và chỉ khi $f(x)$ có nghiệm trong F.

Thật vậy, điều kiện đủ là hiển nhiên. Bây giờ giả sử $f(x)$ khả quy trên F, nghĩa là tồn tại những phần tử $g(x), h(x) \in F[x]$ không khả nghịch sao cho

$$f(x) = g(x).h(x).$$

Do F là một trường và $g(x), h(x) \in F[x]$ không khả nghịch nên hai đa thức $g(x), h(x)$ có bậc lớn hơn hoặc bằng 1. Mặt khác ta có:

$$\deg g(x) + \deg h(x) = \deg f(x) \leq 3.$$

Do đó nếu ta giả sử $\deg g(x) \leq \deg h(x)$ thì ta suy ra $\deg g(x) = 1$. Do đó $g(x)$ có nghiệm trong F, từ đó suy ra $f(x)$ có nghiệm trong F.

2.3. $f(x) = 2x + 8 = 2(x + 4)$, do đó $f(x)$ khả quy trong $\mathbb{Z}[x]$.
Hai đa thức $g(x) = 2x^2 + 1$ và $h(x) = x^2 + 4x - 2$ bất khả quy trong $\mathbb{Z}[x]$.

2.4. Trên $\mathbb{Z}$ và $\mathbb{Q}$, ta có: $f(x) = (x - 2)(x^2 - 2)(x^2 + x + 1)$. Còn trên $\mathbb{Z}[\sqrt{2}]$ và $\mathbb{R}$ thì $f(x) = (x - 2)(x - \sqrt{2})(x + \sqrt{2})(x^2 + x + 1)$.

2.5. $x^3 + x^2 + x + 1 = (x + 1)(x^2 + 1)$ nên nó khả quy trên $\mathbb{Q}[x]$.

2.6. $x^4 + x^2 - 6 = (x^2 + 3)(x^2 - 2)$ nên nó khả quy trong $\mathbb{Q}[x]$.

2.7. Dễ thấy đa thức $4x^3 + 3x^2 + x + 1$ không có nghiệm trong $\mathbb{Z}_5$, do vậy theo Bài tập 2.2, đa thức này bất khả quy trên $\mathbb{Z}_5$.

2.8. $x^4 - 2x^3 + x^2 + 1$ khả quy trong $\mathbb{R}[x]$ vì mọi đa thức có bậc lớn hơn 2 đều khả quy trong $\mathbb{R}[x]$.

2.9. $5 = (1 - 2i)(1 + 2i)$ nên không bất khả quy trong $\mathbb{Z}[i]$.

2.10. Do a là luỹ linh nên tồn tại $n \in \mathbb{N}$ sao cho $a^n = 0$. Khi đó:

$$\begin{aligned} 1 &= 1 - a^n x^n = 1 - (ax)^n \\ &= (1 + ax)(1 - ax + (ax)^2 - \cdots + (-1)^{n-1}(ax)^{n-1}) \end{aligned}$$

Do vậy: $1 + ax$ khả nghịch.

3. Vành chính

3.1. a) Do F là miền nguyên nên ta có:

$$\deg(f.g) = \deg(f) + \deg(g)$$

với $f(x), g(x) \in F[x]$. Suy ra $F[x]$ cũng là miền nguyên.

Giả sử I là một iđêan của $F[x]$. Chọn $p(x)$ là đa thức có bậc nhỏ nhất trong I. Do F là một trường nên trong $F[x]$ có phép chia với dư. Vì vậy với mỗi đa thức $f(x) \in I$ đều tồn tại $q(x), r(x) \in F[x]$ sao cho

$$f(x) = p(x)q(x) + r(x)$$

với $\deg r < \deg p$ nếu $r(x) \neq 0$.

Rõ ràng $p(x)q(x)$ và $f(x)$ đều thuộc I nên $r(x) \in I$. Theo cách chọn $p(x)$ thì $r(x) = 0$. Điều này chứng tỏ

$$I = p(x)F[x] = (p(x)).$$

b) Giả sử $p(x)$ bất khả quy trên F. Gọi I là iđêan chính sinh bởi $p(x)$. Giả sử B là iđêan chứa I. Theo câu a), vì $F[x]$ là vành chính nên B là iđêan chính, giả sử B sinh bởi $g(x)$. Do $B \supset I$ nên $g(x) \mid p(x)$. Kết hợp với tính chất $p(x)$ là đa thức bất khả quy ta được $g(x)$ hoặc là phần tử bất khả quy, hoặc liên kết với $p(x)$. Do đó hoặc $B = F[x]$ hoặc $B = I$. Điều này chứng tỏ I là tối đại.

Để chứng minh vành $E = F[x]/(p(x))$ là trường ta chỉ cần chứng minh mọi phần tử của E có nghịch đảo là đủ. Giả sử $\overline{f(x)}$ là phần tử khác không của E. Thế thì $f(x) \notin I$. Do I là tối đại nên iđêan sinh bởi I và $f(x)$ phải trùng với $F[x]$:

$$F[x] = f(x)F[x] + I.$$

Từ đó suy ra tồn tại $g(x) \in F[x]$ và $s(x) \in I$ sao cho

$$1 = f(x)g(x) + s(x).$$

Điều này kéo theo: $1 = \overline{f}\ \overline{g}$.

3.2. a) Giả sử hai đa thức bất khả quy $p(x), q(x)$ trên trường $F[x]$ có nghiệm chung là u. Khi đó do $p(x)$ và $q(x)$ là nguyên tố cùng nhau và vì vậy tồn tại hai đa thức $r(x), s(x) \in F[x]$ sao cho

$$r(x)p(x) + s(x)q(x) = 1.$$

Thay $x = u$ ta được $0 = 1$ (Vô lý).
b) Hiển nhiên.

3.3. Nếu $f(x)$ là đa thức bất khả quy trên trường F có bậc $n \geq 1$ thì với mọi đa thức $g(x)$ có bậc nhỏ hơn n ta đều có $(f(x), g(x)) = 1$. Do đó

$$(f(x), g(x)h(x)) = 1,$$

với mọi $f(x), g(x)$ có bậc nhỏ hơn n. Nghĩa là không tồn tại hai đa thức khác không có bậc nhỏ hơn n mà tích của chúng chia hết cho $f(x)$.

3.4. 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.

3.5. 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 $a \in A \backslash Ap$. Vì $a \notin Ap$ nên a không chia hết cho p, và vì vậy 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 $1 = au + pv \in I$, khi đó $I = A$. Điều đó chứng tỏ Ap là một iđêan tối đại.

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 tồn tại những phần tử không khả nghịch a, b sao cho: $p = a.b$. 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

$$Ap \subsetneq Aa \subsetneq A,$$

trái với giả thiết về tính tối đại của iđêan Ap. Vậy p phải là phần tử bất khả quy trong A.

3.6. 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 iđêan nguyên tố của A, nên mọi iđêan tối đại đều là iđêan nguyên tố.

Bây giờ ta chứng minh rằng nếu A là một vành chính thì mọi iđêan nguyên tố khác không đều là tối đại. Thật vậy, giả sử $I \neq 0$ là một iđêan nguyên tố của vành chính A. Vì A là vành chính nên tồn tại $a \in A$ sao cho $I = (a)$. Do I là nguyên tố nên $I \neq A$, do đó a không là ước của 1.

Bây giờ ta chứng minh a là phần tử bất khả quy trong A. Thật vậy, giả sử $a = uv$ với u và v thuộc A. Thế thì ta có

$$(a) \subset (u) \text{ và } (a) \subset (v).$$

Mặt khác vì $uv = a \in (a)$ nên hoặc $u \in (a)$ hoặc $v \in (a)$ suy ra

$$(u) \subset (a) \text{ hoặc } (v) \subset (a).$$

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.

3.7. Nếu K là một trường thì K chỉ có hai iđêan là K và 0. Khi đó K là iđêan chính sinh bởi 1 và 0 là iđêan chính sinh bởi 0. Vậy K là một vành chính.

3.8. 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 $\mathbb{Z}/6\mathbb{Z}$ là vành có ước của không, do đó nó không phải là miền nguyên, vì vậy không là vành chính.

3.9. a) Giả sử I là iđêan của vành R/A. Gọi $p : R \to R/A$ là toàn cấu chính tắc. Khi đó $p^{-1}(I)$ là iđêan của vành R. Vì R là vành chính nên $p^{-1}(I) = (b)$. Suy ra $I = (\bar{b})$.

b) Theo a), mọi iđêan của vành R/A đều là iđêan chính, do đó R/A là vành chính khi và chỉ khi là miền nguyên, điều đó tương đương với A là iđêan nguyên tố.

3.10. Vành con của một vành chính có thể không phải là một vành chính. Chẳng hạn, $m\mathbb{Z}$ $(m > 1)$ là vành con của vành chính $\mathbb{Z}$ nhưng không phải là vành chính vì $m\mathbb{Z}$ không có đơn vị.

3.11. 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 ta có: $1 = 1 + 0\sqrt{3}i \in A$. Giả sử $a + b\sqrt{3}i$ và $c + d\sqrt{3}i$ là hai phần tử của A, thế thì:

$$(a + b\sqrt{3}i) - (c + d\sqrt{3}i) = (a - c) + (b - d)\sqrt{3}i \ \in A,$$

$$(a + b\sqrt{3}i)(c + d\sqrt{3}i) = (ac - 3bd) + (ad + bc)\sqrt{3}i \ \in A.$$

b) Với mỗi số phức $\alpha = a + b\sqrt{3}i$, 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,

$$N(\alpha.\beta) = (\alpha.\beta)(\overline{\alpha.\beta}) = \alpha.\overline{\alpha}\beta.\overline{\beta} = N(\alpha)N(\beta).$$

Từ đó ta có nhận xét rằng: $\alpha \in A$, α khả nghịch khi và chỉ khi $N(\alpha) = 1$. Ta có:

$$N(2) = 4;\ N(1 + \sqrt{3}i) = 4;\ N(1 - \sqrt{3}i) = 4$$

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. Nghĩa 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 $\beta = -1 + 0\sqrt{3}i$, và do đó 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 $\gamma = \pm 1$ và 2 liên kết với β. 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 số 4 có hai sự phân tích thành tích những phần tử khả quy:

$$4 = 2.2 = (1 + \sqrt{3}i)(1 - \sqrt{3}i)$$

3.12. 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, dễ nhận thấy rằng đối với một số hữu tỷ α, bao giờ cũng tìm thấy một số nguyên a sao cho

$$|\alpha - a| \leq \frac{1}{2}.$$

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

$$|x - z| \leq \frac{3}{4} < 1. \quad (*)$$

Bây giờ hãy lấy một iđêan I không tầm thường của A. Tập hợp

$$X = \{|z|^2 \mid 0 \neq z \in I\}$$

là một bộ phận khác rỗng của $\mathbb{N}$ và không chứa 0. 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

$$\left|\frac{v}{u} - z\right| < 1 \text{ hay } |v - zu|^2 < |u|^2.$$

Nhưng $u, v \in I,\ z \in A$, vậy $v - zu \in I$. Mặt khác $|u|^2$ là phần tử bé nhất của X, nên $v - zu = 0$, hay $v = zu$. Từ đó $I = Au$. Vậy A là vành chính.

3.13. Dễ kiểm tra A là một vành con chứa đơn vị của $\mathbb{Q}$, do đó nó là một miền nguyên.

Giả sử I là một iđêan khác không của A. Khi đó tồn tại $\frac{p}{q} \in I$, $p, q \neq 0$. Khi đó $p = \frac{p}{q}q \in I$. Như vậy I có chứa những số nguyên khác không và do đó chứa những số nguyên dương. Giả sử p là số nguyên dương nhỏ nhất thuộc I. Ta viết $p = 2^r p'$, trong đó $(2, p') = 1$. Khi đó

$$2^r = \frac{1}{p'}p \in I.$$

Do cách chọn p suy ra $p = 2^r$. Ta sẽ chứng minh rằng $I = (2^r)$. Thật vậy, với mọi $\frac{m}{n} \in I$ ta viết $\frac{m}{n} = 2^s\frac{m'}{n}$, trong đó m' và n lẻ. Khi đó:

$$2^s = \frac{m}{n}.\frac{n}{m'} \in I \Rightarrow s \geq r$$

do $p = 2^r$ là số nguyên dương nhỏ nhất thuộc I. Vậy

$$\frac{m}{n} = 2^r.2^{s-r}\frac{m'}{n} \in (2^r).$$

Hay $I = (2^r)$. Chú ý rằng nếu $r = 0$ thì ta có $I = A$

3.14. Trong vành $\mathbb{Z}[x]$, xét iđêan I sinh bởi x và 2:

$$I = \{u(x).x + 2.v(x) \mid u(x), v(x) \in \mathbb{Z}[x]\}.$$

Nhận xét rằng nếu $h(x) \in I$ thì hệ 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 và 2 thuộc I, 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.

Xét ánh xạ $\varphi : \mathbb{Z}[x] \to \mathbb{C},\ f(x) \mapsto f(i\sqrt{2})$. Đây là một đồng cấu vành. Hơn nữa, $\mathrm{Ker}\varphi = (x^2+2)$ và $\mathrm{Im}\varphi = \mathbb{Z}[i\sqrt{2}]$. Do đó theo Định lý đồng cấu vành ta có:

$$\mathbb{Z}[x]/(x^2+2) \cong \mathbb{Z}[i\sqrt{2}].$$

Mà $\mathbb{Z}[i\sqrt{2}]$ là một vành chính (xem Bài tập 3.12) nên $\mathbb{Z}[x]/(x^2+2)$ là một vành chính.

3.15. a) Trước hết nếu A là một trường thì $A[x]$ là một miền nguyên. Nếu I là một iđêan khác 0 của $A[x]$ thì ta có thể chọn $p(x)$ là một đa thức có bậc thấp nhất trong I, từ đó chứng minh được I là iđêan chính sinh bởi $p(x)$ và 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

$$I = \{x.f(x) + a.g(x) \mid f(x), g(x) \in A[x]\}$$

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

$$1 \in I \ \text{ và } \ 1 = 0.x + a.b.$$

Điều đó chứng tỏ b là nghịch đảo của a. Vậy a khả nghịch, do đó A là một trường.

b) Kết quả của phần a) không còn đúng nếu thay $K[x]$ bởi vành $K[c]$, với c là phần tử đại số trên K. Ta chỉ cần lấy $K = \mathbb{Z}$, $c = 1$ là đại số trên $\mathbb{Z}$, khi đó $\mathbb{Z}[1] = \mathbb{Z}$ là một vành chính, tuy nhiên $K = \mathbb{Z}$ không phải là một trường.

3.16. a) Giả sử A là iđêan của $K \times \mathbb{Z}$. Khi đó, ta có thể chứng minh được rằng $A = I \times J$, trong đó

$$I = \{x \in K \mid \exists\, n \in \mathbb{Z}, (x,n) \in A\}$$

$$J = \{n \in \mathbb{Z} \mid \exists\, x \in K, (x,n) \in A\}$$

là những iđêan theo thứ tự của vành K và $\mathbb{Z}$. Do K và $\mathbb{Z}$ là những vành chính nên I, J là những iđêan chính, $I = (a), J = (m)$. Khi đó A là iđêan chính sinh bởi (a, m).

$K \times \mathbb{Z}$ không là vành chính vì nó có ước của không:

$$(1,0)(0,1) = (0,0).$$

b) Giả sử K là vành đơn. Vì K giao hoán và có đơn vị $1 \neq 0$ nên suy ra K là trường và do đó $K[x]$ là vành chính.

Ngược lại, giả sử $K[x]$ là vành chính. Nếu K không là trường thì tồn tại phần tử khác không $a \in K$, mà a không khả nghịch. Khi đó ta có thể chứng minh được rằng iđêan sinh bởi a và x không phải là iđêan chính trong $K[x]$.

3.17. Ta có $K[x]$ không phải là một trường. Vì vậy, theo Bài tập 3. 15, vành đa thức $K[x][y]$ không phải là một vành chính, nghĩa là vành đa thức hai ẩn $K[x,y]$ không phải là một vành chính.

3.18. Theo Bài tập 3.15, $\mathbb{Z}_n[x]$ là một vành chính khi và chỉ khi $\mathbb{Z}_n$ là một trường. Điều này xảy ra khi và chỉ khi n là một số nguyên tố.

3.19. a) Lấy phần tử khác không $\alpha \in K$. Khi đó $\alpha = \overline{g(x)} = g(x) + I$ với $g(x) \notin I$, nghĩa là $g(x)$ không là bội của $f(x)$. Mặt khác do $f(x)$ là đa thức bậc hai và $f(a) \neq 0$ với mọi $a \in \mathbb{Z}_3$ nên $f(x)$ bất khả qui trên $\mathbb{Z}_3$. Từ đó $(g(x), f(x)) = 1$. Bởi vậy, tồn tại $u(x), v(x) \in \mathbb{Z}_3[x]$ sao cho

$$g(x)u(x) + f(x)v(x) = 1$$

Chuyển qua lớp ta có

$$\overline{g(x)f(x)} = 1 \quad (\text{do } \overline{f(x)} = 0).$$

Vậy $\alpha = \overline{g(x)}$ khả nghịch và do đó K là một trường.

Giả sử α là phần tử tuỳ ý của K, $\alpha = \overline{g(x)}$ với $g(x) \in \mathbb{Z}_3[x]$. Do $\mathbb{Z}_3$ là trường nên $\mathbb{Z}_3[x]$ là miền nguyên, bởi vậy theo phép chia với dư ta có

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

trong đó $r(x) = ax + b$, $a, b \in \mathbb{Z}_3$ và không nhất thiết khác không. Từ đó

$$\alpha = \overline{r(x)} = ax + b + I.$$

Trong K có $0 = \overline{f(x)} = \overline{x}^2 + 1$. Bởi vậy $f(x)$ có hai nghiệm là $i = \overline{x}$ và $-i$.

b) Xét ánh xạ

$$\begin{aligned} \varphi : \mathbb{Z}_3 &\to K \\ a &\mapsto \overline{a} = a + I \end{aligned}$$

φ là đơn cấu, vì thế $\mathbb{Z}_3 \cong \mathrm{Im}\varphi$ và có thể xem $\mathbb{Z}_3$ như là trường con của K. Phần tử đơn vị của $\mathbb{Z}_3$ có cấp 3 nên đặc số của K là 3.

3.20. $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$.

3.21. $x^5 + 1 = (x+1)(x^4 - x^3 + x^2 - x + 1)$.

3.22. $x^4 + 1 = x^4 + \overline{5}x^2 + \overline{6} = (x^2+2)(x^2+3)$.

3.23. $2x^3 + x^2 + 4x + 2 = (2x+1)(x^2+2)$.

3.24. $2x^3 + x^2 + 4x + 2 = (2x+1)(x + i\sqrt{2})(x - i\sqrt{2})$.

3.25. $x^8 - 16 = (x \pm \sqrt{2})(x \pm i\sqrt{2})(x - 1 \pm i)(x + 1 \pm i)$.

3.26. $x^8 - 16 = (x - \sqrt{2})(x + \sqrt{2})(x^2+2)(x^2 - 2x + 2)(x^2 + 2x + 2)$.

3.27. $x^8 - 16 = (x^2 - 2)(x^2+2)(x^2 - 2x + 2)(x^2 + 2x + 2)$.

3.28. $x^8 - 16 = (x^2 - 2)(x^2+2)(x^2 - 2x + 2)(x^2 + 2x + 2)$.

3.29. $6 = 6 + 0.\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ nhưng $6 = 2.3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$ nên $\mathbb{Z}[\sqrt{-5}]$ không có tính chất nhân tử hoá duy nhất.

3.30. a) Đặt $d = (a, b)$ và $e = (ca, cb)$. Khi đó $cd \mid ca$ và $cd \mid cb$. Vì vậy $cd \mid e$. Tức là $e = cdk$. Đặt $dk = d_1$ ta có $d \mid d_1$.

Mặt khác, ta có

$$e = cd_1 \mid (ca, cb).$$

Vậy $d_1 \mid (a, b)$ do đó $d_1 \mid d$. Vậy $d = d_1$. Từ đó suy ra $cd_1 = cd$, tức là $e = cd$ hay $(ca, cb) = c(a, b)$.

b) Nếu $(a, b) = 1$ thì $(ac, bc) = c$. Do đó

$$1 = (a, c) = (a, (ac, bc)) = ((a, ac), bc) = (a, bc).$$

3.31. Do R là một miền nguyên thoả mãn điều kiện có ƯCLN nên ta giả sử $d = (a, p)$. Do p là bất khả quy nên d khả nghịch hoặc d liên kết với p. Nếu d khả nghịch thì ta có a và p nguyên tố cùng nhau. Nếu d liên kết với p thì a chia hết cho p.

3.32. Ta chỉ cần chứng minh rằng nếu R là vành thoả mãn điều kiện có ƯCLN thì mọi phần tử bất khả quy đều là nguyên tố.

Thật vậy, giả sử p là phần tử bất khả quy và $p \mid ab$. Vì p là bất khả quy và (a, p) là một ước của p nên hoặc là $(a, p) = p$ hoặc là $(a, p) = 1$.

Tương tự, ta có $(b,p) = p$ hoặc $(b,p) = 1$. Nếu $(a,p) = 1$ và $(b,p) = 1$ thì theo Bài tập 3.31, ta có $(ab,p) = 1$, mâu thuẫn với giả thiết $p \mid ab$. Vậy hoặc $(a,p) = p$ hoặc $(b,p) = p$, tức là $p \mid a$ hoặc $p \mid b$.

3.33. Giả sử ngược lại rằng p không chia hết a_i với mọi $i = 1, 2, ..., n$. Khi đó theo Bài tập 3.31, $(p, a_i) = 1$ với mọi i, và do đó

$$(p, a_1 a_2 ... a_n) = 1.$$

Điều này trái với giả thiết $p|a_1, a_2, ..., a_n$. Vậy tồn tại a_k sao cho $p \mid a_k$.

3.34. Giả sử $a \in R, a \neq 0$, không khả nghịch. Xét một dây chuyền giảm những ước của miền nguyên R

$$a = a_1, a_2, ..., a_n, ...$$

Theo giả thiết dây chuyền này dừng tại phần tử a_s nào đó. Điều này có nghĩa a_s là một phần tử bất khả quy, và hơn nữa nó là một ước của a.

3.35. Giả sử $a \in R, a \neq 0$, không khả nghịch. Nếu a là phần tử bất khả quy thì kết quả là hiển nhiên. Nếu a không là phần tử bất khả quy thì a có một ước bất khả quy là p_1 và $a = p_1 a_1$ với a_1 là ước thực sự của a. Tiếp tục lập luận như trên ta được

$$a = a_0 = p_1 a_1, a_1 = p_2 a_2, ..., a_{n-1} = p_n a_n,$$

với p_i bất khả quy và a_i là ước thực sự của a_{i-1}, $(i = 1, 2, ..., n)$. Theo giả thiết dãy giảm những ước

$$a = a_0, a_1, a_2, ..., a_n, ...$$

dừng tại phần tử a_m nào đó. Điều này có nghĩa a_m là phần tử bất khả quy, và ta được

$$a = p_1 p_2 ... p_m a_m$$

là sự phân tích của a thành tích những nhân tử bất khả quy. Bây giờ giả sử

$$a = p_1 p_2 ... p_n = q_1 q_2 ... q_m, \qquad (1)$$

là hai sự phân tích của a thành tích những nhân tử bất khả quy. Giả sử $m < n$. Từ đẳng thức (1) suy ra

$$p_1 | q_1 q_2 ... q_m,$$

do đó p_1 phải là ước của một q_i nào đó. Bằng cách đánh số lại các chỉ số ta có thể giả thiết $p_1 \mid q_1$. Do q_1 là phần tử bất khả quy nên q_1 liên kết với p_1 hay $q_1 = u_1 p_1$, với $u_1 | 1$. Như vậy

$$p_1 p_2 ... p_n = u_1 p_1 q_2 ... q_m$$

Sau khi giản ước cho p_1 ta được

$$p_2 ... p_n = u_1 q_2 ... q_m$$

Tiếp tục lập luận trên sau hữu hạn bước ta được

$$1 = u_1 ... u_n q_{n+1} ... q_m.$$

Vì $q_{n+1}, ..., q_m$ là những phần tử bất khả quy nên đẳng thức này không thể xảy ra. Lập luận tương tự cho trường hợp $n < m$. Vậy ta có $n = m$ và ta có p_i liên kết với q_i với một cách đánh số thích hợp cho các chỉ số.

3.36. Nếu $a = p_1 q_2 ... q_m$ là sự phân tích của a thành tích của những nhân tử bất khả quy trong vành R thì m được gọi là *độ dài* của sự phân tích của a và ký hiệu bởi $l(a)$.

Xét một dãy chuyền giảm những ước của vành nhân tử hoá R,

$$a_1, a_2, ..., a_n, ...$$

Khi đó ta có dãy giảm các số tự nhiên:

$$l(a_1), l(a_2), ..., l(a_n), ...$$

Hiển nhiên dãy này dừng, và do đó dãy trên cũng dừng.

Bây giờ ta chứng tỏ vành nhân tử hoá R thoả mãn điều kiện có UCLN. Giả sử a, b là hai phần tử tuỳ ý thuộc R. Nếu $a = 0$ hoặc nếu $b \mid 1$ thì $(a, b) = b$. Nếu a, b cùng khác không và không khả nghịch thì chúng có các biểu diễn

$$a = p_1^{\alpha_1} ... p_k^{\alpha_k} \quad , \quad b = p_1^{\beta_1} ... p_k^{\beta_k},$$

trong đó $p_i (i = 1, 2, ..., n)$ là những phần tử bất khả quy, đôi một khác nhau và $\alpha_i, \beta_i \geq 0$. Khi đó rõ ràng ta có

$$(a, b) = p_1^{\delta_1} ... p_k^{\delta_k} \text{ với } \delta_i = \min(\alpha_i, \beta_i).$$

3.37. a) Hiển nhiên ta có trường số phức $\mathbb{C}$ là một vành nhân tử hoá. Nhưng vành con

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

là miền nguyên, không phải là vành nhân tử hoá. Nhận xét rằng $\alpha \in \mathbb{Z}[\sqrt{-5}]$ khả nghịch khi và chỉ khi $\alpha = \pm 1$.

Dễ thấy các phương trình $a^2 + 5b^2 = 3$ và $a^2 + 5b^2 = 7$ không có nghiệm nguyên nên $N(\alpha) \neq 3, \neq 7$ với mọi $\alpha \in \mathbb{Z}[\sqrt{-5}]$. Giả sử $3 = \alpha.\beta$. Khi đó

$$N(\alpha)N(\beta) = N(3) = 9.$$

Do $N(\alpha) \neq 3$, $N(\beta) \neq 3$ nên $N(\alpha) = 1$ hoặc $N(\beta) = 1$, nghĩa là $\alpha = \pm 1$ hoặc $\beta = \pm 1$. Vậy 3 là phần tử bất khả quy.

Tương tự, ta chứng minh được $7, 1 + 2\sqrt{-5}, 1 - 2\sqrt{-5}$ cũng là những phần tử bất khả quy.

Trong vành $\mathbb{Z}[\sqrt{-5}]$ ta có:

$$21 = 3.7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

nên $\mathbb{Z}[\sqrt{-5}]$ không là vành nhân tử hoá.

b) Xét ánh xạ $\varphi : \mathbb{Z}[x] \to \mathbb{Z}[\sqrt{-5}]$, $f(x) \mapsto f(\sqrt{-5})$. Dễ thấy φ là toàn cấu vành. Do đó

$$\mathbb{Z}[x]/\mathrm{Ker}\varphi \cong \mathbb{Z}[\sqrt{-5}].$$

Ta có $\mathbb{Z}[x]$ là vành nhân tử hoá, song vành thương $\mathbb{Z}[x]/\mathrm{Ker}\varphi$ không phải là vành nhân tử hoá (mặc dù là miền nguyên) vì $\mathbb{Z}[\sqrt{-5}]$ không là vành nhân tử hoá.

3.38. a) Giả sử

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

$$g(x) = b_0 + b_1x + \cdots + b_mx^m$$

là hai đa thức nguyên bản và

$$f(x)g(x) = c_0 + c_1x + \cdots + c_{m+n}x^{m+n}.$$

Nếu tích này không là đa thức nguyên bản thì tồn tại một số nguyên tố p là ước chung của tất cả các hệ số $c_0, c_1, ..., c_{m+n}$. Vì tất cả các hệ tử của $f(x)$ không thể chia hết cho p (do $f(x)$ là nguyên bản)

nên trong các hệ số $a_0, a_1, ..., a_k$ sẽ có một hệ tử đầu tiên, giả sử a_i, không chia hết cho p.

Tương tự, giả sử b_j là hệ tử đầu tiên của $g(x)$ không chia hết cho p. Khi đó:

$$c_{i+j} = a_0b_{i+j} + \cdots + a_{i-1}b_{j+1} + a_ib_j + a_{i+1}b_{j-1} + \cdots + a_{i+j}b_0$$

Vì c_{i+j} chia hết cho p, và theo giả thiết, tất cả các số hạng của vế phải, trừ a_ib_j đều chia hết cho p, nên a_ib_j phải chia hết cho p. Vì p là nguyên tố nên a_i hoặc b_j phải chia hết cho p. Nhưng điều này đã không xảy ra. Vậy $f(x)g(x)$ là đa thức nguyên bản.

b) Ta chứng minh khẳng định tương đương: Nếu đa thức $f(x) \in A[x]$ bất khả quy trong $A[x]$ thì nó cũng bất khả quy trong $\overline{A}[x]$.

Thật vậy, giả sử ngược lại rằng đa thức $f(x) \in A[x]$ khả quy trong $\overline{A}[x]$, tức là

$$f(x) = f_1(x)f_2(x),$$

với $f_1(x), f_2(x) \in \overline{A}[x]$ và $\deg(f_1, f_2) < \deg(f)$.

Ta có $f_i(x) = \dfrac{a_i}{b_i} f_i^*(x)$, $(i = 1, 2)$, trong đó $(a_i, b_i) = 1$ và $f_i^*(x)$ là một đa thức nguyên bản. Từ đó

$$f(x) = \frac{a_1a_2}{b_1b_2} f_1^*(x)f_2^*(x).$$

Giả sử $\dfrac{a_1a_2}{b_1b_2} = \dfrac{q}{r}$ với $(q, r) = 1$. Khi đó ta có:

$$f(x) = \frac{q}{r} f_1^*(x)f_2^*(x)$$

Nếu c_i là một hệ tử nào đó của tích $f_1^*(x)f_2^*(x)$ thì c_iq phải chia hết cho r, vì $f(x) \in A[x]$. Vì $(q, r) = 1$ nên r phải chia hết c_i. Vậy r là một ước chung của các hệ tử của tích $f_1^*(x)f_2^*(x)$.

Nhưng theo chứng minh a) thì tích $f_1^*(x)f_2^*(x)$ là một đa thức nguyên bản nên r khả nghịch. Do vậy $r^{-1} \in A$, từ đó:

$$f(x) = (r^{-1}qf_1^*(x))(f_2^*(x))$$

với $r^{-1}qf_1^*(x), f_2^*(x) \in A[x]$ là những đa thức có bậc nhỏ hơn bậc của $f(x)$. Vậy $f(x)$ là khả quy trên $A[x]$, trái với giả thiết.

3.39. Trước hết chúng ta có nhận xét rằng:

"Nếu $f(x) \in \mathbb{Z}[x]$ là đa thức bất khả quy trong $\mathbb{Z}[x]$ thì $f(x)$ là một đa thức nguyên bản, đồng thời nó bất khả quy trong $\mathbb{Q}[x]$".

Kết luận thứ hai của nhận xét trên được suy ra từ Bài tập 3.38. Bây giờ ta giả sử:

$$f(x) = a_o + a_1 x + ... + a_n x^n \in \mathbb{Z}[x]$$

bất khả quy trong $\mathbb{Z}[x]$ nhưng không nguyên bản. Khi đó tồn tại số nguyên dương $d > 1$ là ước chung của các hệ số $a_o, a_1, ..., a_n$. Do đó:

$$f(x) = d.q(x)$$

với $q(x) \in \mathbb{Z}[x]$ là đa thức có bậc bằng với bậc của $f(x)$, do đó nó không khả nghịch.

Mặt khác do d là số nguyên dương lớn hơn 1 nên d cũng không khả nghịch trong $\mathbb{Z}[x]$. Từ đó suy ra $f(x)$ khả quy trong $\mathbb{Z}[x]$, trái giả thiết. Vậy các kết luận của nhận xét trên đã được chứng minh.

Trở lại bài toán: Do $p(x) \in \mathbb{Z}[x]$ bất khả quy trong $\mathbb{Z}[x]$ nên nó bất khả quy trong $\mathbb{Q}[x]$. Vì vậy, theo giả thiết $p(x) \mid f(x).g(x)$ ta suy ra trong vành $\mathbb{Q}[x]$: hoặc $p(x) \mid f(x)$ hoặc $p(x) \mid g(x)$. Không mất tính chất tổng quát, ta có thể giả sử $p(x) \mid f(x)$, nghĩa là tồn tại đa thức $q(x) \in \mathbb{Q}[x]$ sao cho

$$f(x) = p(x).q(x) \qquad (1).$$

Ta biểu diễn $q(x)$ dưới dạng

$$q(x) = \frac{a}{b}.q^*(x)$$

trong đó $a, b \in \mathbb{Z}$, $(a, b) = 1$ và $q^*(x) \in \mathbb{Z}[x]$ là đa thức nguyên bản. Khi đó ta có:

$$p(x).q^*(x) = \frac{b}{a} f(x) \qquad (2).$$

Giả sử $f(x) = c_o + c_1 x + ... + c_n x^n \in \mathbb{Z}[x]$. Trong đẳng thức (2), vế trái là đa thức với hệ số nguyên, do đó $\frac{bc_i}{a}$ cũng là những số nguyên với mọi $i = 0, 1, ..., n$. Kết hợp với giả thiết $(a, b) = 1$ ta suy ra $a \mid c_i$

với mọi $i = 0, 1, ..., n$. Đặt $c_i = a.d_i, d_i \in \mathbb{Z}$. Từ đẳng thức (2) ta suy ra:

$$p(x).q^*(x) = bd_o + bd_1x + ... + bd_nx^n \qquad (3).$$

Theo bài tập 3.38, $p(x).q^*(x)$ là đa thức nguyên bản, do đó các hệ số $bd_o, bd_1, ..., bd_n$ nguyên tố cùng nhau. Từ đó suy ra $b = \pm 1$. Kết hợp với dẳng thức (2) ta có:

$$ap(x)q^*(x) = \pm f(x)$$

nghĩa là trong vành $\mathbb{Z}[x]$, $p(x)$ là ước của $f(x)$.

3.40. Giả sử A là vành Gauss, K là trường các thương của A, $f(x)$ là đa thức khác không và không khả nghịch của $A[x]$. Giả sử

$$f(x) = f_1(x)...f_n(x)$$

là sự phân tích của $f(x)$ thành các nhân tử bất khả quy trong $K[x]$. Ta có:

$$f_i(x) = \frac{a_i}{b_i} f_i^*(x)$$

với $f_i^*(x) \in A[x]$ là các đa thức nguyên bản. Suy ra

$$f(x) = \frac{a}{b} f_1^*(x)...f_n^*(x) \text{ với } a, b \in A, \ (a, b) = 1.$$

Theo Bài tập 3.38, $f_1^*(x)...f_n^*(x)$ là đa thức nguyên bản nên b khả nghịch. Do đó $f(x)$ liên kết với $af_1^*(x)...f_n^*(x) = p_1...p_kf_1^*(x)...f_n^*(x)$.

Các đa thức $f_i^*(x)$ là nguyên bản và bất khả quy trong $A[x]$ nên chúng là các đa thức bất khả quy trong $A[x]$ (theo Bài tập 3.38), còn $p_1, ..., p_k$ là các phần tử bất khả quy của A nên cũng là các phần tử bất khả quy của $A[x]$.

Bây giờ, giả sử

$$f(x) = p_1...p_kf_1(x)...f_n(x) = q_1...q_lg_1(x)...g_m(x)$$

là hai sự phân tích của $f(x)$ thành các đa thức bất khả quy trong $A[x]$. Khi đó các đa thức $f_i(x), g_j(x)$ đều nguyên bản nên các đa thức $f_(x)...f_n(x), g_1(x)...g_m(x)$ là các đa thức nguyên bản. Suy ra

$$p_1...p_k \sim q_1...q_l$$

nên $k = l$ và $p_i \sim q_i$ (nhắc lại rằng $\sim$ là ký hiệu chỉ sự liên kết của hai phần tử). Ta cũng có:

$$f_1(x)...f_n(x) \sim g_1(x)...g_m(x).$$

Do $f_i(x), g_j(x)$ là các đa thức nguyên bản, bất khả quy trong $A[x]$ nên cũng là các đa thức bất khả quy trong $A[x]$. Do sự phân tích duy nhất của các phần tử trong vành $A[x]$ nên ta có $n = m$ và $f_i(x) \sim g_i(x)$. Vậy $A[x]$ là vành nhân tử hoá.

Kết quả sẽ không còn đúng nếu thay giả thiết "vành Gauss" bằng giả thiết "vành chính". Ví dụ: vành số nguyên $\mathbb{Z}$ là vành chính nhưng vành đa thức $\mathbb{Z}[x]$ không phải là vành chính.

4. Vành Ơclit (Euclide)

4.1. a) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ là một miền nguyên. Khi đó nó là một vành Ơclit cùng với ánh xạ

$$\begin{aligned} \varphi : \mathbb{Z}[\sqrt{2}] &\to \mathbb{N} \\ a + b\sqrt{2} &\mapsto |a^2 - 2b^2| \end{aligned}$$

b) $\mathbb{Z}[i\sqrt{2}] = \{a + b\sqrt{2}i \mid a, b \in \mathbb{Z}\}$ là miền nguyên và cùng với ánh xạ

$$\begin{aligned} \delta : \mathbb{Z}[i\sqrt{2}] &\to \mathbb{N} \\ a + bi\sqrt{2} &\mapsto a^2 + 2b^2 \end{aligned}$$

là một vành Ơclit.

c) Xét ánh xạ: $\varphi : \mathbb{Z}[x] \to \mathbb{C},\ f(x) \mapsto f(i\sqrt{2})$. Ta có

$$\mathrm{Ker}\psi = (x^2 + 2), \mathrm{Im}\psi = \mathbb{Z}[i\sqrt{2}].$$

Do đó theo Định lý đồng cấu vành ta có:

$$\mathbb{Z}[x]/(x^2 + 2) \cong \mathbb{Z}[i\sqrt{2}].$$

Theo b) ta có $\mathbb{Z}[i\sqrt{2}]$ là một vành Ơclit nên $\mathbb{Z}[x]/(x^2 + 2)$ cũng là vành Ơclit.

d) Trước hết ta có nhận xét rằng:

$$A = \left\{ \frac{2a+b}{2} + \frac{b}{2}\sqrt{-11} \mid a, b \in \mathbb{Z} \right\}$$
$$= \left\{ \frac{m}{2} + \frac{n}{2}\sqrt{-11} \mid m, n \in \mathbb{Z} \text{ và có cùng tính chẵn, lẻ} \right\}$$

Mặt khác, nếu $\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{-11} \in A$ thì ta có

$$N(\alpha) = |\alpha|^2 = \frac{m^2 + 11n^2}{4} \in \mathbb{N}.$$

Ta sẽ chứng minh A cùng với ánh xạ $N : A^* \to \mathbb{N}$, $\alpha \mapsto N(\alpha)$ là một vành Oclit.

Nếu $\alpha \mid \beta$ thì $N(\alpha) \mid N(\beta)$, do đó $N(\alpha) \leq N(\beta)$.

Giả sử $\alpha, \beta \in A, \beta \neq 0$. Khi đó do

$$\alpha, \beta \in \mathbb{Q}(\sqrt{-11}) \text{ nên } \frac{\alpha}{\beta} = r + s\sqrt{-11} \in \mathbb{Q}(\sqrt{-11}).$$

Giả sử n là số nguyên gần $2s$ nhất, ta có:

$$|2s - n| \leq \frac{1}{2}.$$

Mặt khác với $k = [2r]$ thì $2r \leq k < 2r + 1$. Do đó

$$|2r - k| < 1, \ |2r - (k+1)| \leq 1.$$

Trong hai số k và $k+1$ có một số cùng tính chẵn, lẻ với n, ta gọi số đó là m. Hiển nhiên $|2r - m| \leq 1$.

Đặt $q = \frac{m}{2} + \frac{n}{2}\sqrt{-11} \in A$, ta có: $\alpha = \beta q + \gamma$, với $\gamma = \alpha - \beta q \in A$ và

$$N(\gamma) = N(\alpha - \beta q) = N(\beta)N(\frac{\alpha}{\beta} - q)$$
$$= N(\beta)N\left((r - \frac{m}{2}) + (s - \frac{n}{2})\sqrt{-11}\right)$$
$$= N(\beta)N\left((r - \frac{m}{2})^2 + (s - \frac{n}{2})^2.11\right) \leq N(\beta)\left((\frac{1}{2})^2 + 11(\frac{1}{4})^2\right)$$
$$= \frac{15}{16}N(\beta) < N(\beta).$$

Vậy A là vành Ơclit.

4.2. Theo Bài tập 3.13, A là một vành chính. Với mỗi số hữu tỷ $\frac{m}{n} \in A$ đều tồn tại duy nhất số tự nhiên $r \in \mathbb{N}$ sao cho

$$\frac{m}{n} = 2^r \frac{m'}{n}$$

với $(m', 2) = 1$. Khi đó A cùng với ánh xạ $\varphi : A \to \mathbb{N}$, $\varphi(\frac{m}{n}) = r$ là một vành Ơclit.

4.3. Giả sử A là một trường. Khi đó A cùng với ánh xạ

$$\delta : A^* \longrightarrow \mathbb{N},\ a \mapsto \delta(a) = n_0$$

với n_0 là một số tự nhiên cho trước, là một vành Ơclit.

4.4. $\mathbb{C}$ là vành Ơclit, $\mathbb{Z}[\sqrt{-5}]$ là vành con chứa đơn vị của $\mathbb{C}$ nhưng không là vành Ơclit.

4.5. Nếu R/A là vành Ơclit thì R/A là miền nguyên, do đó A là iđêan nguyên tố. Ngược lại, nếu A là iđêan nguyên tố trong vành Ơclit R thì $A = 0$ hoặc A tối đại, do đó $R/A \cong R$ hoặc R/A là trường. Trong cả hai trường hợp R/A là vành Ơclit.

4.6. Giả sử A là một vành Ơclit với ánh xạ Ơclit:

$$\delta : A^* \longrightarrow \mathbb{N}$$

Nếu A là một trường thì với mọi $x \in A^*$ ta có $1 = xx^{-1}$. Vậy $\delta(1) \geq \delta(x)$; mặt khác $x = 1.x$ nên $\delta(x) \geq \delta(1)$. Từ đó $\delta(x) = \delta(1)$ với mọi $x \in A^*$.

Bây giờ giả sử δ là một ánh xạ hằng. Đối với hai phần tử $x = 1$ và $y \neq 0$ ta có q và r thuộc A sao cho

$$1 = yq + r$$

và $\delta(r) < \delta(y)$ nếu $r \neq 0$. Do δ là ánh xạ hằng, nên $r = 0$, nghĩa là mọi $y \neq 0$ đều có nghịch đảo.

4.7. Dùng thuật toán Ơclit ta được $(f(x), g(x)) = 1$.

4.8. $(a, b) = 3$, $s = -5$, $t = 4$.

4.9. $(a, b) = 7$, $s = -72$, $t = 131$.

4.10. $(a,b) = 1,\ s = -(2x+1)/3,\ t = (2x+2)/3.$

4.11. $(a,b) = x^3 + 4x - 2,\ s = 1,\ t = -x.$

4.12. $(a,b) = 2x + 1,\ s = 1,\ t = 2x + 1.$

4.13. $(a,b) = 1,\ s = x^2 - x + 1,\ t = 4x^3 + x^2 + 4x + 3.$

4.14. $(a,b) = 1,\ s = 1,\ t = -1 + 2i.$

4.15. $\mathbb{Z}[x]$ cùng với ánh xạ $\delta(f(x)) = \deg f(x)$ với mỗi đa thức khác 0 không là vành Óclit, thật vậy: với hai phần tử $x, 2 \in \mathbb{Z}[x]$, không tồn tại hai đa thức $q(x), r(x) \in \mathbb{Z}[x]$ sao cho:

$$x = 2.q(x) + r(x)$$

trong đó bậc của $r(x)$ bằng 0 nếu $r(x) \neq 0$.

Ta lưu ý rằng $\mathbb{Z}[x]$ không phải là một vành chính nên với bất kỳ định nghĩa nào của $\delta(f(x))$, $\mathbb{Z}[x]$ cũng không là vành Óclit.

4.16. Với mọi $a + bi \in \mathbb{Z}[i]$ ta có:

$$N(a+bi) = a^2 + b^2 = 1 \Leftrightarrow a = \pm 1, b = 0 \text{ hoặc } a = 0, b = \pm 1$$

Như vậy $N(a + bi) = 1$ khi và chỉ khi $a + bi = \pm 1$ hoặc $a + bi = \pm i$.

Giả sử $\alpha \in \mathbb{Z}[i], \alpha \neq 0$ và $N(\alpha)$ nguyên tố trong $\mathbb{Z}$. Giả sử $\alpha = \beta.\gamma$ với $\beta, \gamma \in \mathbb{Z}[i]$. Vì:

$N(\alpha) = N(\beta)N(\gamma)$ nguyên tố và $N(\alpha), N(\beta) > 0$ nên ta có $N(\alpha) = 1$ hoặc $N(\beta) = 1$. Theo nhận xét trên ta có $\beta|1$ hoặc $\alpha|1$. Nghĩa là α bất khả quy và do đó nguyên tố trong $\mathbb{Z}[i]$.

Đảo lại không đúng: 3 nguyên tố trong $\mathbb{Z}[i]$ nhưng $N(3) = 9$ không nguyên tố trong $\mathbb{Z}$.

4.17. *a*) $\Rightarrow$ *b*). Giả sử R là một trường. Khi đó $R[x]$ cùng với ánh xạ:

$$\begin{aligned} \varphi : R[x] &\to \mathbb{N} \\ f(x) &\mapsto \deg(f(x)) \end{aligned}$$

là một vành Óclit.

b) $\Rightarrow$ *c*). Hiển nhiên.

c) $\Rightarrow$ *a*). Xem bài tập 3.15.

4.18. Giả sử tồn tại miền nguyên R để vành đa thức hai ẩn $R[x, y]$ là một vành Óclit. Ta có:

$$R[x][y] = R[x, y]$$

là vành Oclit, theo Bài tập 4.17 ta suy ra $R[x]$ phải là một trường. Tuy nhiên điều này không bao giờ xảy ra vì phần tử $x \in R[x]$ không có nghịch đảo.

4.19. $\mathbb{Z}_2[x]/(x^3+1) = \{0, 1, x, a, b, c, d, e\}$ trong đó

$$a = x+1, b = x^2, c = x^2+1, d = x^2+x, e = x^2+x+1.$$

Trong bảng cộng và nhân ta thay x^3 bởi 1, x^4 bởi x, ta được:

$\cdot$	0	1	x	a	b	c	d	e
0	0	0	0	0	0	0	0	0
1	0	1	x	a	b	c	d	e
x	0	x	b	d	1	a	c	e
a	0	a	d	c	c	d	a	0
b	0	b	1	c	x	d	a	e
c	0	c	a	d	d	a	c	0
d	0	d	c	a	a	c	d	0
e	0	e	e	0	e	0	0	b

$+$	0	1	x	a	b	c	d	e
0	0	1	x	a	b	c	d	e
1	1	0	a	x	c	b	e	d
x	x	a	0	1	d	e	b	c
a	a	x	1	0	e	d	c	b
b	b	c	d	e	0	1	x	a
c	c	c	e	d	1	0	a	x
d	d	e	b	c	x	a	0	1
e	e	d	c	b	a	x	1	0

Các ước của không trong vành này là: a, c, d, e. Do đó vành này không là trường.

4.20. Tương tự Bài tập 4.19 với

$$\mathbb{Z}_3[x]/(x^2+2x+2) = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}.$$

4.21. $(x-\sqrt{2})(x+\sqrt{2})$.

4.22. x^3+x^2+2 là đa thức bất khả quy trong $\mathbb{Z}_3[x]$. Ta có

$$\mathbb{Z}_3[x]/(x^3+x^2+2) = \{a_0 + a_1x + a_2x^2 \mid a_i \in \mathbb{Z}_3\}.$$

4.23. $x^4 - 2$ là đa thức trong $\mathbb{Q}[x]$. Ta có

$$\mathbb{Q}[x]/(x^4 - 2) = \{a_0 + a_1x + a_2x^2 + a_3x^3 \mid a_i \in \mathbb{Q}\} \simeq \mathbb{Q}[\sqrt[4]{2}].$$

4.24. $x^7 + 4x^3 - 3ix + 1$ là đa thức khả quy trong $\mathbb{C}[x]$ vì các đa thức bất khả quy trong $\mathbb{C}[x]$ là các đa thức bậc nhất.

4.25. $x^2 - 3$ là đa thức bất khả quy trong $\mathbb{Q}(\sqrt{2})[x]$. Ta có

$$\mathbb{Q}(\sqrt{2})[x]/(x^2 - 3) = \{a_0 + a_1x | a_i \in \mathbb{Q}(\sqrt{2})\} \cong \mathbb{Q}[\sqrt{2}, \sqrt{3}].$$

4.26. $3x^5 - 4x^3 + 2$ là đa thức bất khả quy trong $\mathbb{Q}[x]$. Ta có

$$Q[x]/(3x^5 - 4x^3 + 2) = \{a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 \mid a_i \in \mathbb{Q}\}.$$

4.27. Giả sử vành A cùng với ánh xạ $\delta : A^* \to \mathbb{N}$ là một vành Oclit. Khi đó $\delta(A^*)$ có thể là một tập hữu hạn hoặc vô hạn. Vì $\mathbb{N}$ là tập sắp thứ tự tốt và $\delta(A^*)$ là một tập con khác rỗng 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

$$\delta(A^*) = \{n_0, n_1, ..., n_{m-1}\} \text{ với } n_0 < n_1 < \cdots < n_{m-1}$$

ta có thể lập một ánh xạ $\delta' : A^* \longrightarrow \mathbb{N}$ như sau: $\delta'(a) = i$ nếu $\delta(a) = n_i$.

Bây giờ xét trường hợp tập hợp $\delta(A^*)$ vô hạn. Do mọi bộ phận khác rỗng của $\mathbb{N}$ đều có phần tử bé nhất nên $\delta(A^*)$ là dãy tăng các số tự nhiên sau đây

$$\delta(A^*) = \{n_0, n_1, ..., n_k, ...\} \text{ với } n_i < n_{i+1}, i = 0, 1, 2, ...$$

Khi đó ta lập ánh xạ $\delta' : A^* \longrightarrow \mathbb{N}$ bằng cách đặt $\delta'(a) = i$ nếu $\delta(a) = n_i$.

Ta chứng minh δ' là ánh xạ Oclit. Giả sử $a|b$, với a và b thuộc A. Thế thì $\delta(a) \leq \delta(b)$. Giả sử $\delta(a) = n_i$ và $\delta(a) = n_k$, với $n_i \leq n_k$. Suy ra $i \leq k$ và 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 $a = bq + r$ và $\delta(r) < \delta(b)$ 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 $\delta'(r) < \delta'(b)$.

4.28. 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 $\delta(A^*)$.

Bây giờ nếu $u|1$ thì $\delta(u) \leq \delta(1)$, suy ra $\delta(u) = \delta(1)$ và là phần tử bé nhất trong $\delta(A^*)$.

Đảo lại, giả sử $u \in A^*$ sao cho $\delta(u) \leq \delta(a)$ với mọi $a \in A^*$. Vì A là vành Oclit nên cho 1 và u ta có v và r thuộc A sao cho:

$$1 = uv + r$$

trong đó $\delta(r) < \delta(u)$ nếu $r \neq 0$. Nhưng điều này không xảy ra vì $\delta(u)$ là phần tử nhỏ nhất của tập $\delta(A^*)$. Vậy $r = 0$ và do đó u là ước của 1.

4.29. Giả sử A là một vành Oclit. Theo Bài tập 4.28, ta có thể lấy ánh xạ Oclit 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 $\delta(x) = 1$, suy ra x không khả nghịch. Giả sử y là một phần tử tuỳ ý của A. Lấy y chia cho x ta được

$$y = xq + r, \text{ trong đó } \delta(r) < \delta(x) = 1 \text{ nếu } r \neq 0.$$

Do đó nếu $r \neq 0$ thì $\delta(r) = 0$, nghĩa là r khả nghịch. Vậy mọi phần tử y của A có dạng $y = xq$, hoặc $y = xq + r$ với r khả nghịch.

Nói cách khác, mọi lớp của $A/(x)$ có một đại diện hoặc bằng 0 hoặc khả nghịch.

4.30. 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

$$N(y) = |y|^2 = \left(a + \frac{b}{2}\right)^2 + \frac{19b^2}{4} = a^2 + ab + 5b^2 \in \mathbb{N}.$$

Mặt khác, nếu 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 $u = a + b\dfrac{1+i\sqrt{19}}{2}$ khả nghịch, nghĩa là tồn tại phần tử v sao cho: $uv = 1$. Thế thì

$$N(u)N(v) = N(uv) = N(1) = 1.$$

Theo nhận xét 1),

$$N(u) = 1 = \left(a + \frac{b}{2}\right)^2 + \frac{19b^2}{4} \quad \text{hay} \quad (2ab)^2 + 19b^2 = 4.$$

Suy ra $b = 0$ và $4a^2 = 4$ hay $a = \pm 1$.

Bây giờ ta chứng minh bài toán bằng phản chứng. Để cho gọn, ta đặt

$$u = a + b\frac{1+i\sqrt{19}}{2} \text{ và } A = \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right] = \mathbb{Z}[u].$$

Giả sử $A = \mathbb{Z}[u]$ là một vành Oclit. Ta phải có $x = a + bu$ 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

$$ma + (mb)u, \quad \text{hoặc} \quad ma \pm 1 + (mb)u.$$

Như vậy y không chạy khắp $\mathbb{Z}[u]$ (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 $2 = xq$ hoặc $2 = xq \pm 1$.

Nếu $2 = xq \pm 1$ thì $3 = xq$ ($1 = xq$ không xảy ra vì x không khả nghịch). Từ đó $N(x)N(q) = 9$. Do $N(x) \geq 5$ nên $N(x) = 9$ và $N(q) = 1$. Theo nhận xét 1), $q = \pm 1$ và $x = \pm 3$, mâu thuẫn với khẳng định x phải có phần ảo.

Nếu $2 = xq$ thì $N(x)N(q) = 4$. Nhưng $N(x) \geq 5$ nên trường hợp này không xảy ra.

Chương VI

PHÂN TÍCH ĐA THỨC TRÊN CÁC TRƯỜNG SỐ

1. Phân tích các đa thức thực và phức

1.1. Giả sử $f(x)$ chia hết cho $g(x)$ trong $\mathbb{C}[x]$, nghĩa là $f(x) = g(x)q(x)$, $\alpha \in \mathbb{C}$ là một nghiệm của $g(x)$. Từ $g(\alpha) = 0$ suy ra $f(\alpha) = 0$ và nếu α là nghiệm bội cấp $k \geq 1$ của $g(x)$ thì $g(x) = (x-\alpha)^k h(x)$. Do đó $f(x) = (x-\alpha)^k h(x)q(x)$, nghĩa là α là nghiệm bội lớn hơn hoặc bằng k của $f(x)$.

Đảo lại, nếu mọi nghiệm bội cấp $k_i \geq 1$ của $g(x)$ đều là nghiệm bội với cấp lớn hơn hoặc bằng k_i của $f(x)$ thì ta có:

$$g(x) = a.(x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}\cdots(x-\alpha_n)^{k_n},$$

$$f(x) = b.(x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}\cdots(x-\alpha_n)^{k_n}q(x).$$

Điều này chứng tỏ $f(x) = b.a^{-1}.g(x)q(x)$. Vậy $f(x)$ chia hết cho $g(x)$.

1.2. Đa thức $g(x) = x^2 + x + 1$ là một đa thức bậc hai không có nghiệm hữu tỷ nên nó là đa thức bất khả quy trên $\mathbb{Q}[x]$. Đa thức này có hai nghiệm phức là ε và ε^2, là hai căn nguyên thuỷ bậc ba của đơn vị (vì $x^3 - 1 = (x-1)g(x)$). Mặt khác, dễ kiểm tra rằng đa thức $f(x) = x^{3k} + x^{3l+1} + x^{3n+2}$ cũng nhận ε và ε^2 làm nghiệm. Khi đó theo Bài tập 1.1 tồn tại đa thức $h(x) \in \mathbb{C}[x]$ sao cho $f(x) = g(x)h(x)$. Nhưng $f(x)$ và $g(x) \in \mathbb{Q}[x]$ nên suy ra $h(x) \in \mathbb{Q}[x]$. Vậy đa thức $f(x)$ chia hết cho đa thức $g(x)$.

1.3. Không thể định nghĩa được một thuật toán chia trong $\mathbb{R}[x, y]$. Và do đó không thể chia $x^3 + 3xy + y + 4$ cho $xy + y^3 + 2$.

1.4. Vì K là một trường, $f(x)$ và $g(x)$ nguyên tố cùng nhau nên nếu xem $yf(x) + g(x)$ như một đa thức bậc nhất một ẩn đối với y thì $yf(x)+g(x)$ là đa thức nguyên bản, do đó bất khả quy trên $K[x]$. Suy ra $yf(x) + g(x)$ bất khả quy trong $K[x, y] = K[x][y]$.

1.5. Trước hết chúng ta có nhận xét rằng: nếu $\varphi : \mathbb{C} \to \mathbb{C}$ là một ánh xạ đa thức trên $\mathbb{C}$ thì tồn tại duy nhất đa thức $f(x) \in \mathbb{C}[x]$ sao cho $\varphi(a) = f(a)$ với mọi $a \in \mathbb{C}$. Sự tồn tại của $f(x) \in \mathbb{C}[x]$ dựa theo định nghĩa của ánh xạ đa thức. Bây giờ giả sử $g(x) \in \mathbb{C}[x]$ cũng thoả mãn điều kiện $\varphi(a) = g(a)$ với mọi $a \in \mathbb{C}$. Khi đó ta có $f(a) = g(a)$ với mọi $a \in \mathbb{C}$. Đặt $h(x) = f(x)-g(x) \in \mathbb{C}[x]$. Nếu $h(x)$ không là đa thức 0 thì $h(x)$ là một đa thức có bậc không vượt quá $\max(\deg f(x), \deg g(x))$, đồng thời

$$h(a) = f(a) - g(a) = 0$$

với mọi $a \in \mathbb{C}$. Điều này không thể xảy ra vì trong trường $\mathbb{C}$, một đa thức bậc n có không quá n nghiệm. Vậy $h(x)$ là đa thức không, nghĩa là $f(x) = g(x)$.

Từ nhận xét trên suy ra tồn tại một song ánh giữa tập $\mathbb{C}[x]$ và tập các ánh xạ đa thức trên $\mathbb{C}$.

b) Mệnh đề a) không còn đúng khi thay $\mathbb{C}$ bởi một trường K tuỳ ý. Chẳng hạn chọn $K = \mathbb{Z}_3$ thì trên $\mathbb{Z}_3$, tồn tại hai đa thức khác nhau nhưng có giá trị đồng nhất với nhau tại mọi $x \in \mathbb{Z}_3$, chẳng hạn hai đa thức: 0 và $x^3 - x$.

2. Phân tích các đa thức nguyên và hữu tỷ

2.1. Do $\frac{r}{s}, (r, s) = 1$, là một nghiệm hữu tỷ của đa thức $p(x)$ với hệ số nguyên nên ta có: $p(x) = (x - \frac{r}{s})q(x)$. Giả sử

$$q(x) = b_{n-1}x^{n-1} + \cdots + b_1x + b_0$$

trong đó $b_i \in \mathbb{Q}$. Khi đó:

$$p(x) = (b_{n-2} + \frac{r}{s}b_{n-1})x^{n-1} + \cdots + (b_0 - \frac{r}{s}b_1)x + \frac{r}{s}b_0$$

Do $p(x)$ là đa thức với hệ số nguyên nên ta có: $\frac{r}{s}b_0 \in \mathbb{Z}$. Mà $(r, s) = 1$ nên $s|b_0$. Lại do $b_0 - \frac{r}{s}b_1 \in \mathbb{Z}$, mà $b_0 \in \mathbb{Z}$ nên $\frac{r}{s}b_1 \in \mathbb{Z}$ suy ra $s|b_1$. Cứ

tiếp tục lập luận như vậy ta được $s|b_i$ với mọi $i = 0, 1, \ldots, n-1$. Do đó $p(x)$ có thể viết lại được dưới dạng:

$$p(x) = (sx - r)g(x)$$

với $g(x)$ là đa thức thu được từ $q(x)$ bằng cách chia các hệ số b_i của $q(x)$ cho s.

2.2. Nếu $\frac{r}{s}, (r, s) = 1$, là một nghiệm của đa thức nguyên $p(x)$ thì theo Bài tập 2.1, $p(x)$ được viết dưới dạng $p(x) = (sx - r)q(x)$, trong đó $q(x)$ là đa thức với hệ số nguyên. Thay $x = 1$ vào đẳng thức trên ta được $p(1) = (s - r)q(1)$, trong đó $q(1) \in \mathbb{Z}$. Do đó $(r - s) \mid p(1)$. Như vậy, phân số tối giản $\frac{r}{s}$ không thể là một nghiệm của đa thức nguyên $p(x)$ trừ khi $(r - s) \mid p(1)$. Do đó để tìm nghiệm hữu tỷ của một đa thức nguyên ta chỉ cần kiểm tra các phân số tối giản $\frac{r}{s}$, trong đó r là ước của hệ tử tự do, s là ước của hệ tử cao nhất thoả mãn $(r - s) \mid p(1)$.

2.3. Ta có $\frac{\sqrt{2}}{\sqrt[3]{5}}$ là một nghiệm của đa thức $25x^6 - 8$. Mặt khác nếu đa thức này có nghiệm hữu tỷ $\frac{p}{q}$ thì p là ước của 8 và q là ước của 25. Do đó các nghiệm hữu tỷ (nếu có) của đa thức này chỉ có thể là $\pm 1, \pm 2, \pm 4, \pm 8, \pm\frac{1}{5}, \pm\frac{1}{25}, \pm\frac{2}{5}, \pm\frac{2}{25}, \pm\frac{4}{5}, \pm\frac{4}{25}, \pm\frac{8}{5}, \pm\frac{8}{25}$. Song dễ kiểm tra các giá trị này không phải là nghiệm của đa thức $25x^6 - 8$. Do đó $\frac{\sqrt{2}}{\sqrt[3]{5}}$ là số vô tỷ.

2.4. Đa thức $f(x) = x^3 - 3n^2x + n^3$ có bậc 3 nên $f(x)$ bất khả quy trong $\mathbb{Q}[x]$ khi và chỉ khi nó không có nghiệm hữu tỷ. Giả sử $f(x)$ có nghiệm hữu tỷ là $q \in \mathbb{Q}$, nghĩa là $q^3 - 3n^2q + n^3 = 0$. Suy ra: $\left(\frac{q}{n}\right)^3 - 3\frac{q}{n} + 1 = 0$. Điều này chứng tỏ $\frac{q}{n}$ là một nghiệm hữu tỷ của đa thức $x^3 - 3x + 1$. Nhưng dễ kiểm tra đa thức $x^3 - 3x + 1$ không có nghiệm hữu tỷ nên điều này là vô lý. Vậy $f(x)$ không có nghiệm hữu tỷ và do đó nó là bất khả quy trong $\mathbb{Q}[x]$.

2.5. b) Tìm nghiệm hữu tỷ của đa thức: $2x^3 + 3x^2 + 6x - 4$.

Ta có các ước của 4 là $\pm 1, \pm 2, \pm 4$; các ước của 2 là $\pm 1, \pm 2$. Do đó

các nghiệm hữu tỷ (nếu có) của đa thức này là $\pm 1, \pm 2, \pm 4, \pm\frac{1}{2}$. Dễ kiểm tra, trong số các giá trị này chỉ có $\frac{1}{2}$ là nghiệm.

a), c), d). Tương tự.

2.6. Giả sử ngược lại rằng đa thức $f(x) \in \mathbb{Z}[x]$ có nghiệm nguyên là a trong khi $f(0)$ và $f(1)$ đều là những số lẻ. Do $f(0)$ là số hạng tự do nên a là ước của $f(0)$ phải là một số lẻ. Lại theo điều kiện cần trong Bài tập 2.2 thì $a-1$ phải là ước của $f(1)$. Song $a-1$ là số chẵn còn $f(1)$ là số lẻ nên điều này là vô lý. Vậy $f(x)$ không có nghiệm nguyên.

2.7. Giả sử x_1 là nghiệm hữu tỷ của $f(x)$. Khi đó: $ax_1^2 + bx_1 + c = 0$. Do đó $(ax_1)^2 + b(ax_1) + ac = 0$, nghĩa là $y_1 = ax_1$ là nghiệm hữu tỷ của tam thức bậc hai: $g(y) = y^2 + by + ac$. Hiển nhiên nghiệm hữu tỷ y_1 là nghiệm nguyên và $g(y)$ còn có nghiệm thứ hai y_2. Ta có:

$$y_1 + y_2 = -b \text{ và } y_1 y_2 = ac.$$

Do $b, y_1 \in \mathbb{Z}$ nên $y_2 = -b - y_1 \in \mathbb{Z}$. Do đó $abc = -y_1 y_2 (y_1 + y_2)$. Vì trong ba số nguyên $y_1, y_2, y_1 + y_2$ có ít nhất một số chẵn nên abc chẵn và vì vậy có ít nhất một trong ba số a, b, c chẵn.

2.8. a) Dùng tiêu chuẩn Eisenstein với $p = 3$ hoặc $p = 5$.

b) Dùng tiêu chuẩn Eisenstein với $p = 2$.

c) Hướng dẫn: Đặt $t = x + 1$, sau đó áp dụng tiêu chuẩn Eisenstein với $p = 3$.

d) Hướng dẫn: Đặt $x = t + 1$, sau đó áp dụng tiêu chuẩn Eisenstein với $p = 3$.

e) Đặt $y = x - 3$ ta được

$$x^4 - 8x^3 + 12x^2 - 6x + 3 = y^4 + 4y^3 - 6y^2 - 42y - 42$$

Theo tiêu chuẩn Eisenstein với $p = 2$ suy ra đa thức ẩn y bất khả quy. Do đó đa thức ẩn x cũng bất khả quy trong $\mathbb{Q}[x]$.

2.9. Đa thức này bất khả quy trong $\mathbb{Q}[x]$.

2.10. Đa thức này bất khả quy trong $\mathbb{Q}[x]$.

2.11. Đa thức này bất khả quy trong $\mathbb{Q}[x]$.

2.12. Giả sử ngược lại rằng $f(x)$ là khả quy, tức là $f(x)$ có sự phân tích thực sự: $f(x) = g(x)h(x)$ với $g, h \in \mathbb{Z}[x]$, $0 < \deg g, \deg h < 2n$. Vì $f(x)$ không có nghiệm thực nên $g(x), h(x)$ cũng không có nghiệm

thực, do đó chúng không đổi dấu. Giả sử $g(x) > 0, h(x) > 0$ với mọi x. Vì $f(a_i) = 1$ nên $g(a_i) = h(a_i) = 1$ với mọi $i = 1, 2, ..., n$. Suy ra bậc của g và h phải bằng n (vì nếu có đa thức nào có bậc bé hơn n thì đa thức đó đồng nhất bằng 1, vô lý). Vậy $g(x), h(x)$ có dạng:

$$g(x) = 1 + a(x - a_1)(x - a_2) \cdots (x - a_n),$$

$$f(x) = 1 + b(x - a_1)(x - a_2) \cdots (x - a_n),$$

trong đó $a, b \in \mathbb{Z}$. So sánh hệ số cao nhất và hệ số tự do của hai vế của đẳng thức $f(x) = g(x)h(x)$ ta được $ab = 1$ và

$$1 + (-1)^n a_1 \cdots a_n(a + b) + a_1^2 \cdots a_n^2 = 1 + a_1^2 \cdots a_n^2.$$

Suy ra $ab = 1$ và $a + b = 0$. Rõ ràng là không tồn tại những số nguyên như vậy. Do đó $f(x)$ là đa thức bất khả quy.

2.13. Giả sử $f(x) = x^4 + px^2 + q$ có thể phân tích được thành tích của hai đa thức bậc hai:

$$x^4 + px^2 + q = (x^2 + ax + m)(x^2 + bx + n).$$

Khi đó so sánh hệ số ở hai vế ta được

$$\begin{cases} a + b = 0 \\ m + n + ab = p \\ an + bm = 0 \\ mn = q \end{cases}$$

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 tỷ khi và chỉ khi $p^2 - 4q$ là bình phương của một số hữu tỷ.

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 tỷ nên q và $2\sqrt{q} - p$ phải là bình phương của những số hữu tỷ.

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 tỷ.

2.14. a) $x^3 - y^3 = (x - y)(x^2 + xy + y^2)$.

b) $x^4 - y^2 = (x^2 - y)(x^2 + y)$.

c) $x^6 - y^6 = (x - y)(x + y)(x^2 + xy + y^2)(x^2 - xy + y^2)$.

d) $x^7 + 2x^3y + 3x^2 + 9y = y(2x^3 + 9) + x^7 + 3x^2$, trong đó $2x^3 + 9$ và $x^7 + 3x^2$ là nguyên tố cùng nhau nên áp dụng Bài tập 1.4 ta được đa thức đã cho là bất khả quy.

2.15. Ta có y là phần tử nguyên tố trong $\mathbb{Q}[y]$ vì $\mathbb{Q}[y]/(y) \cong \mathbb{Q}$. Xét đa thức $x^3 + 3x^2y^2 + 2x^2y + xy^4 + 7y + y^2$ xem như là đa thức ẩn x lấy hệ tử trong $\mathbb{Q}[y]$. Đa thức này thoả mãn tiêu chuẩn Eisenstein đối với phần tử nguyên tố y nên nó là đa thức bất khả quy trong $\mathbb{Q}[y][x] = \mathbb{Q}[y, x] \cong \mathbb{Q}[x, y]$.

2.16. Giả sử $f(x) = u(x)v(x)$, $u(x), v(x) \in \mathbb{Z}[x]$. Khi đó ta có:

$$\overline{f}(x) = \overline{u}(x)\overline{v}(x), \text{ với } \overline{u}(x), \overline{v}(x) \in \mathbb{Z}_p[x].$$

Do $\deg f = \deg \overline{f}$ nên $\deg u = \deg \overline{u}$ và $\deg v = \deg \overline{v}$.

Nếu $\overline{f}(x)$ bất khả quy trong $\mathbb{Z}_p[x]$ thì $\overline{u}(x)$ hoặc $\overline{v}(x)$ là phần tử khả nghịch trong $\mathbb{Z}_p[x]$, chẳng hạn $\overline{u}(x) \in \mathbb{Z}_p[x], \overline{u}(x) \neq 0$. Thế thì $\deg u = \deg \overline{u} = 0$, nghĩa là $u(x) \in \mathbb{Z}^*$, và do đó khả nghịch trong $\mathbb{Q}$. Vậy $f(x)$ bất khả quy trên $\mathbb{Q}$.

2.17. Ta có ảnh của đa thức $f(x) = x^4 - 15x^3 + 7$ trong $\mathbb{Z}_2[x]$ là $\overline{f}(x) = x^4 + x^3 + 1$. Đa thức này không có nghiệm trong $\mathbb{Z}_2$. Bởi vậy nếu $\overline{f}(x)$ khả quy trên $\mathbb{Z}_2$ thì nó phải có dạng

$$\overline{f}(x) = (x^2 + ax + b)(x^2 + cx + d).$$

Đồng nhất các hệ số của các đa thức ở hai vế ta được

$$a + c = 1, ac + b + d = 0, ad + bc = 0, bd = 1.$$

Do $bd = 1$ nên $b = d = 1$, suy ra $a + c = 1$ và $a + c = 0$. Điều vô lý này chứng tỏ $\overline{f}(x)$ là bất khả quy trên $\mathbb{Z}_2$ và do đó $f(x)$ bất khả quy trên $\mathbb{Q}$.

2.18. a) Nếu $c \in \mathbb{Q}$ là nghiệm của $p(x)$ thì $c \in \mathbb{Z}$ vì hệ số cao nhất của $p(x)$ bằng 1. Nhưng do $c^3 - 3c + 1 = 0$ nên $c^2 - 3 = -\dfrac{1}{c}$. Hiển nhiên,

không có số nguyên c nào thoả mãn quan hệ đó. Vậy $p(x)$ không có nghiệm trong $\mathbb{Q}$ và do bậc của $p(x)$ bằng 3 nên $p(x)$ bất khả quy trên trường $\mathbb{Q}$.

Chỉ cần vẽ đồ thị của hàm số $y = x^3 - 3x + 1$ ta thấy $p(x)$ có ba nghiệm thực.

b) Ta có $c(3 - c^2) = 1$ và $(c + 2)(c^2 - 2c + 1) = 1$.

c) Giả sử $f(c)g(c) \in 2A$, với $f(x), g(x) \in \mathbb{Z}[x]$. Theo phép chia với dư,

$$f(x)g(x) = p(x)q(x) + r(x) \qquad (1)$$

Từ đó $f(c)g(c) = r(c) \in 2A$, bởi vậy $r(x) \in 2\mathbb{Z}[x]$. Lấy các hệ số của các đa thức trong hệ thức (1) theo môđun 2 ta được

$$\overline{f}(x)\overline{g}(x) = \overline{p}(x)\overline{q}(x) \qquad (2)$$

Hiển nhiên $\overline{p}(x)$ bất khả quy trong $\mathbb{Z}_2$. Bởi vậy từ (2) suy ra $\overline{f}(x)$ hoặc $\overline{g}(x)$ chia hết cho $\overline{p}(x)$, chẳng hạn $\overline{f}(x)$. Khi đó

$$f(x) = p(x)q'(x) + r'(x), \text{với } r'(x) \in 2\mathbb{Z}[x].$$

Từ đó, $f(c) = r'(c) \in 2A$.

3. Phân tích đa thức trên trường hữu hạn

3.1. $x^2 + x + 1$ là đa thức bất khả quy bậc 2 duy nhất trên $\mathbb{Z}_2$.

3.2. $x^2 + 3x + 4$.

3.3. $x^2 + 2$.

3.4. Giả sử $f, g \in L_p$ được cho bởi công thức $f(x) = ax + b$ và $g(x) = a'x + b'$, trong đó $a, a' \neq 0$. Khi đó $g \circ f : \mathbb{Z}_p \to \mathbb{Z}_p$ được cho bởi $(g \circ f)(x) = g(f(x)) = g(ax + b) = a'(ax + b) + b' = aa'x + a'b + b'$, trong đó $aa', a'b + b' \in \mathbb{Z}_p, aa' \neq 0$. Do đó $g \circ f$ là một hàm tuyến tính từ $\mathbb{Z}_p \to \mathbb{Z}_p$. Hay $g \circ f \in L_p$.

Hàm đồng nhất $id : \mathbb{Z}_p \to \mathbb{Z}_p$, $x \mapsto 1x + 0$ là phần tử đơn vị của phép toán hợp thành.

Với mỗi $f \in L_p$, $f(x) = ax + b$ thì f có nghịch đảo là phần tử $f^{-1} : \mathbb{Z}_p \to \mathbb{Z}_p, f^{-1}(x) = a'x + b'$, trong đó a' là nghịch đảo của a trong

$\mathbb{Z}_p$ (do $\mathbb{Z}_p$ là một trường), còn $b' = -a'b$. Vậy $(L_p, \circ)$ là một nhóm.

Hơn nữa, mỗi phần tử $f \in L_p$ hoàn toàn được xác định bởi công thức $f(x) = ax + b$, với $a, b \in \mathbb{Z}_p, a \neq 0$. Do đó a nhận $p-1$ giá trị, còn b nhận p giá trị nên L_p có $(p-1)p$ phần tử, hay L_p là nhóm có cấp $p(p-1)$.

3.5. Do p là một số nguyên tố nên $(\mathbb{Z}_p^*, .)$ là một nhóm cấp $p-1$. Do đó với mọi $\overline{a} \in \mathbb{Z}_p^*$ ta có: $\overline{a}^{p-1} = \overline{1}$, hay là: $\overline{a}^{p-1} - \overline{1} = \overline{0}$. Vậy mọi $x = \overline{a} \in \mathbb{Z}_p^*$ là nghiệm của đa thức $x^{p-1} - 1$.

Theo chứng minh trên thì đa thức $x^{p-1} - 1$ có $p-1$ nghiệm là $\overline{1}, \overline{2}, ..., \overline{p-1}$. Do p là số nguyên tố nên $\mathbb{Z}_p$ là một trường. Vì vậy đa thức $x^{p-1} - 1$ bậc $p-1$ có đúng $p-1$ nghiệm như trên. Do đó:

$$x^{p-1} - 1 = (x-1)(x-2)...(x-p+1)$$

3.6. Giả sử n là số nguyên tố. Khi đó, theo Bài tập 3.5 ta có:

$$x^{n-1} - 1 \equiv (x-1)(x-2)...(x-n+1) \pmod{n} \quad (*)$$

Thay $x = 0$ vào đẳng thức (*) ta thu được:

$$(n-1)! \equiv -1 (\mathrm{mod} n).$$

Ngược lại, giả sử $(n-1)! \equiv -1 \pmod{n}$. Ta chứng minh n là số nguyên tố. Thật vậy, nếu n là hợp số thì tồn tại hai số $a, b \in \{2, 3, ..., n-1\}$ sao cho $a.b = n$, nghĩa là $ab \equiv 0 \pmod{n}$. Do đó: $(n-1)! = 1.2...(n-1) \equiv 0 \pmod{n}$, trái với giả thiết.

Tài liệu tham khảo

1. M. F. Atiyah - I. G. Macdonald. *Introduction to Commutative Algebra*, Massachusetts, 1969.

2. G. Birkhoff - S. MacLane. *A Survey of Modern Algebra* (Bản dịch tiếng Việt, NXB Đại học và Trung học chuyên nghiệp, 1979).

3. G. Birkhoff - S. MacLane. *Algebra*, 1967.

4. G. Birkhoff - T. Bartee. *Modern applied algebra*, 1976.

5. A. G. Curos. *Bài giảng đại số đại cương*, nguyên bản tiếng Nga, Matxcơva, 1962.

6. W. J. Gilbert - W. K. Nicholson. *Modern algebra with applications*, Wiley-Interscience, 1976.

7. Trần Văn Hạo - Hoàng Kỳ. *Bài tập Đại số*, NXB Đại học và Trung học chuyên nghiệp, 1980.

8. Bùi Huy Hiền. *Bài tập đại số đại cương*, NXB Giáo dục, 1997.

9. T. W. Hungerford. *Algebra*, Springer, 1974.

10. Ngô Thúc Lanh. *Đại số và số học* tập I, II, NXB Giáo dục, 1986, 1987.

11. S. Lang. *Algebra*, Columbia University, New York (Phần I bản dịch tiếng Việt, NXB Đại học và Trung học chuyên nghiệp, 1974).

12. Hoàng Xuân Sính. *Đại số cao cấp* tập I, NXB Giáo dục, 1995.

Chịu trách nhiệm xuất bản:
Chủ tịch HĐQT kiêm Tổng Giám đốc NGÔ TRẦN ÁI
Phó Tổng Giám đốc kiêm Tổng biên tập NGUYỄN QUÝ THAO

Chịu trách nhiệm nội dung:
Chủ tịch HĐQT kiêm Giám đốc Công ty CP Sách ĐH – DN
TRẦN NHẬT TÂN

Biên tập nội dung và sửa bản in:
ĐỖ HỮU PHÚ

Thiết kế mỹ thuật và trình bày bìa :
BÍCH LA

Thiết kế sách và chế bản :
ĐỖ PHÚ

HƯỚNG DẪN GIẢI BÀI TẬP ĐẠI SỐ ĐẠI CƯƠNG

Mã số: 7B720y9 – DAI

In 1.000 bản (QĐ : 10), khổ 16 x 24 cm. In tại Nhà in Hà Nam

Địa chỉ: Số 29, Quốc lộ 1A, P. Quang Trung, T.P. Phủ Lý, Hà Nam.

Số ĐKKH xuất bản : 04 - 2009/CXB/257 - 2117/GD.

In xong và nộp lưu chiểu tháng 3 năm 2009.

CÔNG TY CỔ PHẦN SÁCH ĐẠI HỌC - DẠY NGHỀ
HEVOBCO
25 HÀN THUYÊN - HÀ NỘI
Website : www.hevobco.com.vn

VƯƠNG MIỆN KIM CƯƠNG
CHẤT LƯỢNG QUỐC TẾ

TÌM ĐỌC SÁCH THAM KHẢO VỀ TOÁN – TIN CỦA NHÀ XUẤT BẢN GIÁO DỤC	
1. Đại số đại cương	Nguyễn Tiến Quang
2. Toán học cao cấp (tập 1, 2, 3)	Nguyễn Đình Trí (Chủ biên)
3. Bài tập Toán học cao cấp (tập 1, 2, 3)	Nguyễn Đình Trí (Chủ biên)
4. Đại số tuyến tính và hình học giải tích	PGS. TS. Trần Trọng Huệ
5. Đồ thị và các thuật toán	PGS. TS. Hoàng Chí Thành
6. Toán rời rạc ứng dụng trong tin học	PGS. TS. Đỗ Đức Giáo
7. Hướng dẫn giải Bài tập Toán rời rạc	PGS. TS. Đỗ Đức Giáo
8. Phương pháp tính	Tạ Văn Đĩnh
9. Toán học tính toán	Doãn Tam Hoè
10. Cấu trúc máy tính	TS. Trần Quang Vinh

Bạn đọc có thể mua sách tại các Công ti Sách - Thiết bị trường học ở các địa phương hoặc các cửa hàng sách của Nhà xuất bản Giáo dục :

- Tại TP. Hà Nội : 187 Giảng Võ ; 232 Tây Sơn ; 23 Tràng Tiền ; 25 Hàn Thuyên.
- Tại TP. Đà Nẵng : 78 Pasteur, Quận Hải Châu.
- Tại TP. Hồ Chí Minh : 104 Mai Thị Lựu, Quận 1 ; Số 5 Bình Thới, Quận 11 ; 240 Trần Bình Trọng, Quận 5.
- Tại TP. Cần Thơ : 5/5, đường 30/4.

Website : www.nxbgd.com.vn

8 934980 936290

Giá: 31.000đ