Jean-Marie Monier

Giáo trình Toán - Tập 5

ĐẠI SỐ 1

Giáo trình và
600 bài tập có lời giải

NHÀ XUẤT BẢN GIÁO DỤC

DUNOD

Giáo trình Toán - Tập 5

ĐẠI SỐ 1

Cuốn sách này được xuất bản trong khuôn khổ Chương trình Đào tạo Kỹ sư Chất lượng cao tại Việt Nam, với sự trợ giúp của Bộ phận Văn hóa và Hợp tác của Đại Sứ quán Pháp tại nước Cộng hòa Xã hội chủ nghĩa Việt Nam.

Cours de mathématiques - 5

ALGÈBRE 1

Cet ouvrage, publié dans le cadre du Programme de Formation d'Ingénieurs d'Excellence au Vietnam, bénéficie du soutien du Service Culturel et de Coopération de l'Ambassade de France en République Socialiste du Vietnam.

Jean - Marie Monier

Giáo trình Toán
Tập 5

ĐẠI SỐ 1

Giáo trình và 600 bài tập có lời giải

(Tái bản lần thứ năm)

Người dịch :
Nguyễn Tường - Nguyễn Văn Nghị

Hiệu đính :
Nguyễn Văn Thường

NHÀ XUẤT BẢN GIÁO DỤC

Cours de mathématiques - 5

ALGÈBRE 1

Cours et 600 exercices corrigés

1re année MPSI. PCSI. PTSI

Jean-Marie Monier
Professeur en classe de Spéciales
au lycée la Martinière-Monplaisir à Lyon

Lời nói đầu

Bộ giáo trình Toán mới này, với nhiều bài tập có lời giải, được biên soạn dành cho sinh viên giai đoạn I các trường đại học công nghệ quốc gia (năm thứ 1 và thứ 2, mọi chuyên ngành), cho sinh viên giai đoạn I đại học khoa học, và cho các thí sinh dự thi tuyển giáo sư trung học phổ thông.

Bố cục của bộ giáo trình như sau:

Tập1 : Giải tích 1
Tập2 : Giải tích 2 } Giải tích năm thứ 1 (xuất bản lần thứ 2, 6/1996)

Tập 3 : Giải tích 3
Tập4 : Giải tích 4 } Giải tích năm thứ 2 (xuất bản lần thứ 2, 6/1997)

Tập 5: Đại số 1: Đại số năm thứ 1

Tập 6: Đại số 2: Đại số năm thứ 2

Tập 7: Hình học: Hình học năm thứ 1 và năm thứ 2.

Để kiểm chứng mức độ lĩnh hội kiến thức, trong mỗi chương độc giả sẽ thấy nhiều bài tập có lời giải in ở cuối sách. Trừ một vài trường hợp đặc biệt, các bài tập này đều khác với những bài đã có trong bộ bài tập có lời giải gồm tám tập mới xuất bản.

Nhiều vấn đề ở ranh giới của chương trình được đề cập ở cuối chương, dưới dạng các bổ sung có giải.

Tác giả rất mong nhận được những lời phê bình và gợi ý của độc giả. Xin vui lòng gửi các ý kiến đến Nhà xuất bản Dunod, 5, phố Laromiguière, 75005 Paris.

Jean-Marie Monier

Lời cảm ơn

Tôi xin bày tỏ tại đây lòng biết ơn đến các bạn đồng nghiệp đã vui lòng nhận kiểm tra lại từng phần của bản thảo hoặc của bản đánh máy, là: Robert AMBLARD, Bruno ARSAC, Chantal AURAY, Henri BAROZ, Alain BERNARD, Jean-Philippe BERNE, Mohamed BERRAHO, Isabelle BIGEARD, Jacques BLANC, Gérard BOURGIN, Gérard-Pierre BOUVIER, Gérard CASSAYRE, Gilles CHAFFARD, Jean-Paul CHRISTIN, Yves COUTAREL, Gilles DEMEUSOIS, Catherine DONY, Hermin DURAND, Jean FEYLER, Marguerite GAUTHIER, Daniel GENOUD, Christian GIRAUD, André GRUZ, André LAFFONT, Jean-Marc LAPIERRE, Annie MICHEL, Rémy NICOLAÏ, Michel PERNOUD, Jean REY, Sophie RONDEAU, René ROY, Nathalie và Philippe SAUNOIS, Patrice SCHWARTZ, Gérard SIBERT, Mimoun TAÏBI.

Tôi xin bày tỏ niềm thương tiếc chân thành ông Alain GOURET quá cố.

Cuối cùng, tôi cảm ơn sâu sắc Nhà xuất bản Dunod, Gisèle Maïus và Michel Mounic, mà trình độ chuyên môn và tính kiên trì đã tạo điều kiện hoàn thành các tập sách này.

Jean-Marie Monier

Mục lục tập 5

PHẦN THỨ NHẤT - GIÁO TRÌNH

PHẦN THỨ HAI
CHỈ DẪN VÀ TRẢ LỜI CÁC BÀI TẬP

Phần thứ nhất

GIÁO TRÌNH

Chương 1

Ngôn ngữ của lý thuyết tập hợp

Mục đích chương này là trình bày một bảng từ vựng và các tính chất của lý thuyết tập hợp "ngây thơ", có thể sử dụng được và được sử dụng trong mọi lĩnh vực của Toán học, mà không che giấu một cách vô ích hiệu lực tổng quát của chúng, nhưng cũng không phát triển vô bổ.

Chúng tôi cho rằng độc giả đã biết những tính chất sơ cấp của tập hợp các số tự nhiên $\mathbb{N} = \{0, 1, 2, ...\}$.

1.1 Tập hợp

1.1.1 Một số yếu tố lôgic

Một **khẳng định** (hoặc: **tính chất**) p có thể đúng (Đ) hoặc sai (S) (đúng hoặc sai, chứ không phải đồng thời đúng và sai). Một **bảng chân lý** ghi lại hai khả năng đó:

p
Đ
S

Một **định lý** (hoặc: **mệnh đề**) là một khẳng định đúng.

Phủ định của một khẳng định p là một khẳng định được ký hiệu là không p (hoặc: $\neg p$) được xác định bởi bảng chân lý bên.

p	không p
Đ	S
S	Đ

Các phép **liên kết lôgic** và (**hội**), hoặc (**tuyển**), $\Rightarrow$ (**kéo theo**), $\Leftrightarrow$ (**tương đương lôgic**) được xác định bởi:

p	q	p và q	p hoặc q	$p \Rightarrow q$	$p \Leftrightarrow q$
Đ	Đ	Đ	Đ	Đ	Đ
Đ	S	S	Đ	S	S
S	Đ	S	Đ	Đ	S
S	S	S	S	Đ	Đ

"và" có thể ký hiệu là: $\wedge$; "hoặc" là: $\vee$. Cách ký hiệu $\begin{cases} p \\ q \end{cases}$ có thể tiện lợi hơn là: p và q.

Trong phép kéo theo $p \Rightarrow q$, p được gọi là **giả thiết**, q là **kết luận**.

Phép kéo theo $q \Rightarrow p$ được gọi là **đảo** (hoặc: **khẳng định đảo**) của phép kéo theo $p \Rightarrow q$.

Ta có thể diễn tả $p \Rightarrow q$ bằng một trong các cách sau đây:

muốn có p, cần có q
muốn có q, thì có p là đủ
nếu p, thì q
p là một điều kiện đủ để có q
q là một điều kiện cần để có p

Tương đương lôgic $p \Leftrightarrow q$ có thể diễn tả bởi:

muốn có p, cần và đủ là có q
p là điều kiện cần và đủ (ĐKCĐ) để có q
p khi và chỉ khi q (hoặc: nếu và chỉ nếu q)

Một **định lý lôgic** (cũng gọi **mệnh đề hằng đúng**) là một khẳng định đúng với bất kỳ các trị chân lý của các phần tử hợp thành. Sau đây là một số ví dụ trong số các định lý lôgic có ích nhất:

(p hoặc p) $\Leftrightarrow p$
(p và p) $\Leftrightarrow p$
p hoặc (không p): **luật bài trung**
không (p và (không p))
$p \Rightarrow p$
$p \Leftrightarrow p$
không (không p) $\Leftrightarrow p$
(p và ($p \Rightarrow q$)) $\Rightarrow q$: **quy tắc suy diễn**, hoặc **tam đoạn luận**
($p \Rightarrow q$) $\Leftrightarrow$ ((không p) hoặc q)
($p \Rightarrow q$) $\Leftrightarrow$ ((không q) $\Rightarrow$ (không p)): **nguyên lý phản đảo**
(không (p hoặc q)) $\Leftrightarrow$ ((không p) và (không q))
(không (p và q)) $\Leftrightarrow$ ((không p) hoặc (không q))
(không ($p \Rightarrow q$)) $\Leftrightarrow$ (p và (không q))
((p và q) và r) $\Leftrightarrow$ (p và (q và r)): tính kết hợp của và
((p hoặc q) hoặc r) $\Leftrightarrow$ (p hoặc (q hoặc r)): tính kết hợp của hoặc
((p và q) hoặc r) $\Leftrightarrow$ ((p hoặc r) và (q hoặc r)): tính phân phối của hoặc đối với và
((p hoặc q) và r) $\Leftrightarrow$ ((p và r) hoặc (q và r)): tính phân phối của và đối với hoặc
(($p \Rightarrow q$) và ($q \Rightarrow r$)) $\Rightarrow$ ($p \Rightarrow r$): tính bắc cầu của phép kéo theo.

Theo quy ước, ta viết $p \Rightarrow q \Rightarrow r$ thay cho: ($p \Rightarrow q$) và ($q \Rightarrow r$).

Ta hãy chứng minh định lý về sự phủ định của một phép kéo theo như một ví dụ:

p	q	$p \Rightarrow q$	không $(p \Rightarrow q)$	không q	p và (không q)	(không $(p \Rightarrow q)$) $\Leftrightarrow$ (p và (không q))
Đ	Đ	Đ	S	S	S	Đ
Đ	S	S	Đ	Đ	Đ	Đ
S	Đ	Đ	S	S	S	Đ
S	S	Đ	S	Đ	S	Đ

Suy luận phản chứng

Để chứng minh rằng $p \Rightarrow q$ là đúng, ta giả thiết p là đúng và q là sai, và ta chứng minh rằng điều đó dẫn đến mâu thuẫn.

Việc đó quy về chứng minh rằng (p và (không q)) là sai, tức là ((không p) hoặc q là đúng, đó chính là $p \Rightarrow q$.

Bài tập

◊ Chứng minh các định lý lôgic sau:

a) $(p \Leftrightarrow q) \Leftrightarrow (q \Leftrightarrow p)$

b) $\begin{cases} p \Rightarrow q \\ q \Rightarrow r \\ r \Rightarrow p \end{cases} \Rightarrow \begin{cases} p \Leftrightarrow q \\ p \Leftrightarrow r \\ q \Leftrightarrow r \end{cases}$

c) $(p \Rightarrow (q \Rightarrow r)) \Leftrightarrow ((p \text{ và } q) \Rightarrow r)$

d) $((p \text{ hoặc } q) \Rightarrow r) \Leftrightarrow ((p \Rightarrow r) \text{ và } (q \Rightarrow r))$.

1.1.2 Tập hợp

Ta sẽ chỉ giới hạn trong khái niệm ngây thơ (trực quan) về **tập hợp**, mà không đề cập đến khái niệm về quan hệ "tập hợp hóa". Một tập hợp (hay tập) là một sự tụ tập những đối tượng, chẳng hạn $\{0, 1, 3\}$, $\{x \in \mathbb{R};\ x \geq 2\}$. Ký hiệu $x \in E$ có nghĩa: x **thuộc** (hoặc: **là phần tử của**) E; phủ định của nó được ký hiệu $x \notin E$. Ký hiệu $\varnothing$ chỉ **tập hợp rỗng**, là tập hợp không có một phần tử nào.

Một tập hợp có một phần tử x và chỉ một được gọi **một đơn tử** và được ký hiệu $\{x\}$.

Lượng từ phổ cập $\forall$ đọc là "với mọi" hoặc "với bất kỳ" hoặc "với mỗi".

Lượng từ tồn tại $\exists$ đọc là "tồn tại ít nhất một phần tử". Ký hiệu $\exists!$ có nghĩa: tồn tại một và chỉ một phần tử.

Chữ tác động bởi một lượng từ là câm, có thể được thay thế bởi bất kỳ một chữ nào (chưa mang một ý nghĩa nào):

$$(\forall x \in E, P(x)) \Leftrightarrow (\forall y \in E, P(y))$$
$$(\exists x \in E, P(x)) \Leftrightarrow (\exists y \in E, P(y)).$$

Phủ định một câu lượng hóa

Ta có: $\begin{cases} (\text{không } (\forall x \in E, P(x))) \Leftrightarrow (\exists x \in E, \text{không } P(x)) \\ (\text{không } (\exists x \in E, P(x))) \Leftrightarrow (\forall x \in E, \text{không } P(x)). \end{cases}$

Mọi câu lượng hóa bắt đầu bởi $\exists x \in \varnothing$ là sai. Mọi câu lượng hóa bắt đầu bởi $\forall x \in \varnothing$ là đúng.

Nói chung ta không thể thay đổi thứ tự các lượng từ trong một câu lượng hóa.

Chẳng hạn: $(\forall x \in \mathbb{N}, \exists y \in \mathbb{N}, x \leq y)$ là đúng, nhưng $(\exists y \in \mathbb{N}, \forall x \in \mathbb{N}, x \leq y)$ là sai.

Tuy nhiên, nếu các tập hợp E, E' cố định thì:

$$(\forall x \in E, \forall x' \in E', P(x, x')) \Leftrightarrow (\forall x' \in E', \forall x \in E, P(x, x'))$$

và $$(\exists x \in E, \exists x' \in E', P(x, x')) \Leftrightarrow (\exists x' \in E', \exists x \in E, P(x, x')).$$

1.1.3 Quan hệ bao hàm

♦ **Định nghĩa** Cho hai tập hợp E, F, ta nói rằng E **bao hàm trong** F (hoặc: E là một **bộ phận** của F, hoặc E là một **tập hợp con** (hay **tập con**) của F; hoặc: F **bao hàm** E), và ta ký hiệu $E \subset F$ (hoặc: $F \supset E$), khi và chỉ khi: $\forall x \in E, x \in F$.

Ta ký hiệu tập hợp các bộ phận của E là $\mathfrak{P}(E)$.

VÍ DỤ:

- $\mathfrak{P}(\varnothing) = \{\varnothing\}$
- $\mathfrak{P}(\{0, 1\}) = \{\varnothing, \{0\}, \{1\}, \{0, 1\}\}$.

NHẬN XÉT:

1) $A \in \mathfrak{P}(E) \Leftrightarrow A \subset E$

2) $\{x\} \in \mathfrak{P}(E) \Leftrightarrow x \in E$.

Ta ký hiệu $E \underset{\neq}{\subset} F$ thay cho : $E \subset F$ và $E \neq F$.

Ta ký hiệu $E \not\subset F$ để chỉ phủ định của $E \subset F$, tức là: $\exists x \in E, x \notin F$.

Ta có: $E = F \Leftrightarrow (E \subset F$ và $F \subset E)$.

Vậy: $E \neq F \Leftrightarrow \begin{vmatrix} E \not\subset F \\ \text{hoặc} \\ F \not\subset E \end{vmatrix} \Leftrightarrow \begin{vmatrix} (\exists x \in E, x \notin F) \\ \text{hoặc} \\ (\exists y \in F, y \notin E) \end{vmatrix}$

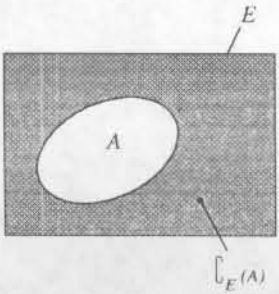
Ta chứng minh dễ dàng các tính chất sau đây đối với mọi tập hợp E, F, G :

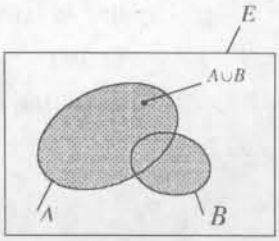
- $\varnothing \subset E, E \subset E$
- $\begin{cases} E \subset F \\ F \subset G \end{cases} \Rightarrow E \subset G$ (tính bắc cầu của quan hệ bao hàm).

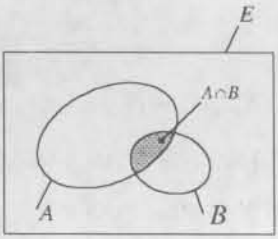
1.1.4 Các phép toán trong $\mathfrak{P}(E)$

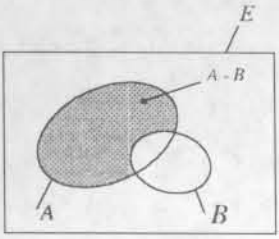
♦ **Định nghĩa 1** Cho E là một tập hợp, $A, B \in \mathfrak{P}(E)$. Ta định nghĩa các bộ phận sau của E:

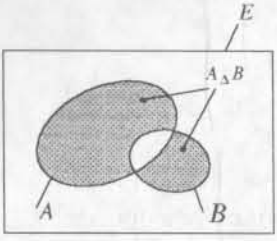
- $\complement_E(A) = \{x \in E; x \notin A\}$, **phần bù của** A **trong** E
- $A \cup B = \{x \in E; x \in A \text{ hoặc } x \in B\}$, **hợp của** A **và** B
- $A \cap B = \{x \in E; x \in A \text{ và } x \in B\}$, **giao của** A **và** B
- $A - B = \{x \in E; x \in A \text{ và } x \notin B\}$, **hiệu** A **trừ** B
- $A \,\Delta\, B = (A - B) \cup (B - A)$, **hiệu đối xứng của** A **và** B.











Để tránh sự lẫn lộn có thể xảy ra với một ý nghĩa khác của "-" (trong các nhóm Abel, các không gian vectơ,...) ta có thể ký hiệu $A \setminus B$ thay cho $A - B$.

Cách ký hiệu $\overline{A}$ thay cho $\complement_E(A)$ có thể tiện lợi, nếu không có nguy cơ lẫn lộn.

Ta sẽ thừa nhận rằng Định nghĩa trên có thể mở rộng ra trường hợp khi A và B không "trực tiếp" là những bộ phận của cùng một tập hợp E. Chẳng hạn, nếu F, G là hai tập hợp, ta thừa nhận rằng có thể định nghĩa $F \cup G$, $F \cap G$, $F - G$, $F \,\Delta\, G$ tương tự như trên đây.

Hai tập hợp F, G được gọi là **rời nhau** khi và chỉ khi $F \cap G = \varnothing$.

Độc giả có thể chứng minh, xem như bài tập, các tính chất sau đây: với mọi bộ phận A, B, C của một tập hợp E:

- $\complement_E(\varnothing) = E$, $\complement_E(E) = \varnothing$, $\complement_E(\complement_E(A)) = A$
- $A \cup \varnothing = \varnothing \cup A = A$ ($\varnothing$ là phần tử trung hòa đối với $\cup$)

  $A \cup A = A$ (mọi phần tử của $\mathfrak{P}(E)$ là lũy đẳng đối với $\cup$)

  $A \cup E = E$ (E hấp thu đối với $\cup$)

  $A \cup B = B \Leftrightarrow A \subset B$

  $A \cup B = B \cup A$ ($\cup$ có tính giao hoán)

  $(A \cup B) \cup C = A \cup (B \cup C)$ ($\cup$ có tính kết hợp)
- $A \cap \varnothing = \varnothing \cap A = \varnothing$ ($\varnothing$ hấp thu đối với $\cap$)

  $A \cap A = A$ (mọi phần tử của $\mathfrak{P}(E)$ là lũy đẳng đối với $\cap$)

  $A \cap E = A$ (E là phần tử trung hòa đối với $\cap$)

  $A \cap B = A \Leftrightarrow A \subset B$

  $A \cap B = B \cap A$ ($\cap$ có tính kết hợp)
- $\complement_E(A \cup B) = \complement_E(A) \cap \complement_E(B)$, $\complement_E(A \cap B) = \complement_E(A) \cup \complement_E(B)$ (các luật De Morgan)
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (phân phối của $\cap$ đối với $\cup$)

  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (phân phối của $\cup$ đối với $\cap$)

  $A \cap (A \cup B) = A \cup (A \cap B) = A$ (các đẳng thức modun)
- $\complement_E(A) = E - A$, $A - \varnothing = A$

  $A - B = \varnothing \Leftrightarrow A \subset B$

  $A - B = A \cap \complement_E(B) = A - (A \cap B)$
- $A \,\Delta\, B = B \,\Delta\, A$ (Δ có tính giao hoán)

  $A \,\Delta\, \varnothing = A$ ($\varnothing$ là phần tử trung hòa đối với Δ)

  $A \,\Delta\, A = \varnothing$ (mọi phần tử của $\mathfrak{P}(E)$ là đối xứng của chính nó đối với Δ)

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

♦ **Định nghĩa 2** Cho E là một tập hợp, $\mathcal{P}$ là một bộ phận của $\mathfrak{P}(E)$. Ta nói rằng $\mathcal{P}$ là một **phân hoạch** của E khi và chỉ khi:

(i) $\forall A \in \mathcal{P},\quad A \neq \varnothing$

(ii) $\forall A \in \mathcal{P}, \forall B \in \mathcal{P},\quad (A \neq B \Rightarrow A \cap B = \varnothing)$

(iii) $\forall x \in E, \exists A \in \mathcal{P},\quad x \in A.$

VÍ DỤ:

1) Với mọi tập khác rỗng E, $\{E\}$ và $\{\{x\}; x \in E\}$ là những phân hoạch của E.

2) Đối với mọi tập E và mọi bộ phận A của E khác $\varnothing$ và khác E, $\{A, \complement_E(A)\}$ là một phân hoạch của E.

3) $\{\mathbb{R}_-^*, \{0\}, \mathbb{R}_+^*\}$ là một phân hoạch của $\mathbb{R}$.

Bài tập

◊ **1.1.2** Cho E là một tập hợp. Chứng minh rằng, với mọi bộ phận A, B, C, D của E thì:

a) $A \subset B \Leftrightarrow \complement_E(A) \supset \complement_E(B) \Leftrightarrow A \cup B = B$
$\Leftrightarrow A \cap B = A \Leftrightarrow A - B = \varnothing \Leftrightarrow \complement_E(A) \cup B = E$

b) $A \cap B \subset (A \cap C) \cup (B \cap \complement_E(C))$

c) $A \cup B = A \cap C \Leftrightarrow B \subset A \subset C$

d) $\begin{cases} A \cap B = A \cap C \\ A \cup B = A \cup C \end{cases} \Leftrightarrow B = C$

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

f) $(A - B) - (A - C) = (A - B) \cap C = (A \cap C) - B$

g) $\begin{cases} A \cap C \subset B \cap C \\ A - C \subset B - C \end{cases} \Leftrightarrow A \subset B$

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

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

j) $A \cap B = C \cap D \Rightarrow (A \cup (B \cap C)) \cap (A \cup (B \cap D)) = A$

k) $(A \cap B = C \cap D, C \cup D = E, C \subset A, D \subset B) \Rightarrow (C = A, D = B).$

◊ **1.1.3** Cho E là một tập hợp, $X, Y, Z, X', Y', Z' \in \mathfrak{P}(E)$. Giả thiết rằng:

$$\begin{cases} X \cup Y \cup Z = E \\ X \cap Y = X' \cap Y', X \cap Z = X' \cap Z', Y \cap Z = Y' \cap Z' \\ X \subset X', Y \subset Y', Z \subset Z'. \end{cases}$$

Chứng minh: $X = X'$, $Y = Y'$, $Z = Z'$.

◊ **1.1.4** Cho E là một tập hợp, $A, B \in \mathfrak{P}(E)$. Giải trong $\mathfrak{P}(E)$ các phương trình sau:

a) $X \cup A = B$

b) $X \cap A = B$

c) $X - A = B$

d) $X \,_{\Delta} A = B$.

◊ **1.1.5** Cho E là một tập hợp, $\mathcal{P}$ là một phân hoạch của E, $\mathcal{A}$ là một bộ phận của $\mathcal{P}$, $\mathcal{B} = \complement_{\mathcal{P}}(\mathcal{A})$. Ta ký hiệu:

$$F = \{x \in E;\ \exists A \in \mathcal{A},\ x \in A\}, \quad G = \{x \in E;\ \exists B \in \mathcal{B},\ x \in B\}.$$

a) Chứng minh rằng $\mathcal{A}$ (tương ứng: $\mathcal{B}$) là một phân hoạch của F (tương ứng: G).

b) Chứng minh: $G = \complement_E(F)$.

◊ **1.1.6** Cho E là một tập hợp, $n \in \mathbb{N}^*$, $A_0, ..., A_n$ là những bộ phận của E sao cho:

$$\varnothing = A_0 \underset{\neq}{\subset} A_1 \underset{\neq}{\subset} A_2 \ldots \underset{\neq}{\subset} A_n = E.$$

Ta ký hiệu $B_1 = A_1 - A_0, ..., B_n = A_n - A_{n-1}$.

Chứng minh rằng $\{B_1, ..., B_n\}$ là một phân hoạch của E.

1.2 Quan hệ

1.2.1 Đại cương

♦ **Định nghĩa 1** Với hai phần tử x, y, tập hợp $\{\{x\}, \{x, y\}\}$ được gọi là **cặp** (x, y).

Đây là một cách định nghĩa (x, y) như là việc cho hai phần tử x, y (không nhất thiết khác nhau) theo một thứ tự nhất định: x trước, y sau.

♦ **Mệnh đề 1** Với mọi phần tử x, y, x', y', ta có:

$$(x, y) = (x', y') \Leftrightarrow \begin{cases} x = x' \\ y = y' \end{cases}.$$

Chứng minh:

- Phép kéo theo $\Leftarrow$ là hiển nhiên.
- Giả sử $(x, y) = (x', y')$, tức là: $\{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\}$.

Nếu $x \neq x'$, thì $\{x\} \neq \{x'\}$, vậy $\{x\} = \{x', y'\}$ và $\{x, y\} = \{x'\}$, suy ra $x = y'$ và $x' = y$.
Nhưng khi đó $\{\{x\}, \{x, x'\}\} = \{\{x'\}, \{x', x\}\}$, suy ra $\{x\} = \{x'\}$, $x = x'$, mâu thuẫn.

Vậy ta có $x = x'$, suy ra $\{x, y\} = \{x', y'\} = \{x, y'\}$, và vì vậy $y = y'$. ■

Vậy ta có thể nói rằng cặp (x, y) là cách cho x và y "trong thứ tự đó".

♦ **Định nghĩa 2** Cho hai tập hợp E, F. Ta gọi tập hợp các cặp (x, y) sao cho $x \in E$ và $y \in F$ là **tích Descartes của** E và F :

$$E \times F = \{(x, y);\ x \in E \text{ và } y \in F\}.$$

Tập hợp $E \times E$ thường được ký hiệu E^2.

Trong thực hành, đáng lẽ viết $\forall (x, y) \in E^2$, ..., ta có thể viết: $\forall x, y \in E$, ...

Từ định nghĩa dễ dàng suy ra:

♦ **Mệnh đề 2** Với mọi tập hợp E, F, G, H:

1) $E \times F = \varnothing \Leftrightarrow (E = \varnothing$ hoặc $F = \varnothing)$
2) $E \times F = F \times E \Leftrightarrow (E = \varnothing$ hoặc $F = \varnothing$ hoặc $E = F)$
3) $(E \times F) \cup (E \times G) = E \times (F \cup G)$
4) $(E \times F) \cup (G \times F) = (E \cup G) \times F$
5) $(E \times F) \cap (G \times H) = (E \cap G) \times (F \cap H)$.

NHẬN XÉT:

Có thể $(E \times F) \cup (G \times H) \neq (E \cup G) \times (F \cup H)$, chẳng hạn như trong ví dụ sau: $E = F = \{0\}, G = H = \{1\}$. ■

Cho $n \in \mathbb{N}^*$, $E_1, ..., E_n$ là những tập hợp. Với mọi x_1 thuộc E_1, ..., x_n thuộc E_n, ta ký hiệu $(x_1, ..., x_n) = (... ((x_1, x_2), x_3), ..., x_n)$, gọi là **một bộ-n**, và ký hiệu là $\prod_{i=1}^{n} E_i$ (hoặc $E_1 \times ... \times E_n$) ; **tích Descartes của** E_1, ..., E_n, là tập hợp các bộ-n $(x_1, ..., x_n)$ trong đó $x_1 \in E_1, ..., x_n \in E_n$. Một bộ-3 được gọi là một **bộ ba**.

Rõ ràng rằng với mọi $(x_1, ..., x_n)$ và mọi $(y_1, ..., y_n)$ thuộc $\prod_{i=1}^{n} E_i$, ta có:

$$(x_1, ..., x_n) = (y_1, ..., y_n) \Leftrightarrow (\forall i \in \{1, ..., n\}, x_i = y_i).$$

♦ **Định nghĩa 3** Cho hai tập hợp E, F.

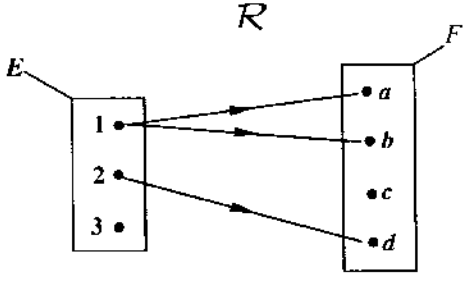
Mọi bộ ba (E, Γ, F), trong đó Γ là một bộ phận của $E \times F$ gọi là **quan hệ** (hoặc: **tương ứng**) từ E đến F. Ta ký hiệu $x \mathcal{R} y$ thay cho $(x, y) \in \Gamma$.

E được gọi là **tập nguồn** của $\mathcal{R}$

F được gọi là **tập đích** của $\mathcal{R}$

Γ được gọi là **đồ thị** của $\mathcal{R}$.

Ta có thể biểu diễn một quan hệ bằng một **biểu đồ (hình tên)** trong đó mũi tên đi từ x đến y khi và chỉ khi $x \mathcal{R} y$. Ví dụ:



Đồ thị của $\mathcal{R}$ là: $\{(1, a), (1, b), (2, d)\}$. ■

Hai quan hệ $\mathcal{R}$, $\mathcal{S}$ là bằng nhau khi và chỉ khi:

$$\begin{cases} \mathcal{R} \text{ và } \mathcal{S} \text{ có cùng một tập nguồn, ký hiệu là } E \\ \mathcal{R} \text{ và } \mathcal{S} \text{ có chung một tập đích, ký hiệu là } F \\ \forall (x, y) \in E \times F, (x \mathcal{R} y \Leftrightarrow x \mathcal{S} y) \end{cases}$$ ■

Nếu $\mathcal{R}$ là một quan hệ từ E đến F, ta ký hiệu $\not\mathcal{R}$ (hoặc: không $\mathcal{R}$) là quan hệ từ E đến F xác định bởi:

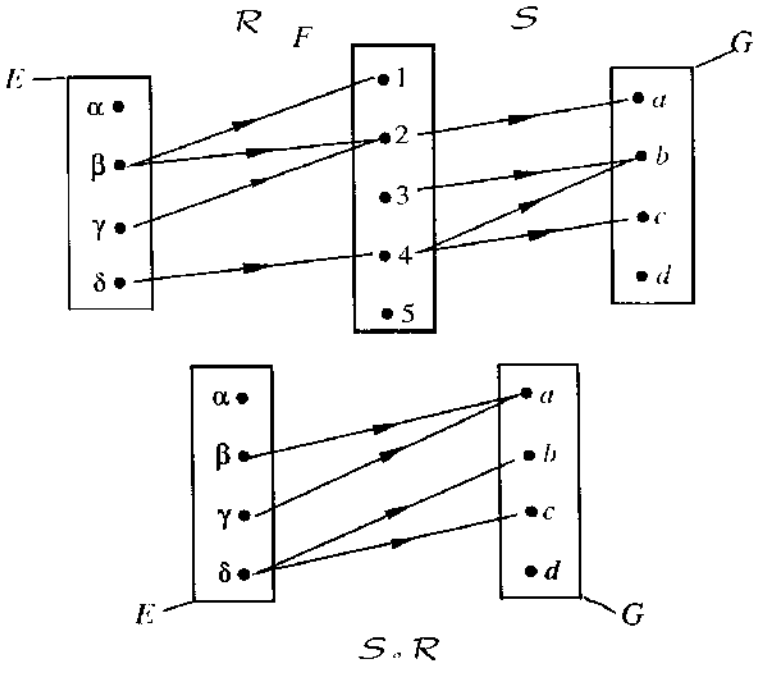
$$\forall (x, y) \in E \times F, (x \not\mathcal{R} y \Leftrightarrow (\text{không } (x \mathcal{R} y))).$$

♦ **Định nghĩa 4** Cho E, F, G là ba tập hợp, $\mathcal{R}$ (tương ứng: $\mathcal{S}$) là một quan hệ từ E đến F (tương ứng: từ F đến G). Ta định nghĩa quan hệ **hợp** (hoặc: **tích**) của $\mathcal{R}$ và $\mathcal{S}$, ký hiệu là $\mathcal{S} \circ \mathcal{R}$, từ E đến G bởi:

$$\forall (x, z) \in E \times G, \left(x \; \mathcal{S} \circ \mathcal{R} \; z \Leftrightarrow \left(\exists y \in F, \begin{cases} x \mathcal{R} y \\ y \mathcal{S} z \end{cases} \right) \right).$$

VÍ DỤ:

1)



2) $E = F = G$ là tập hợp các đường thẳng của một mặt phẳng afin Euclide $\mathcal{R} = \mathcal{S} = \perp$, tính trực giao.

Thế thì $\mathcal{S} \circ \mathcal{R} = /\!/$ (tính song song), vì với mọi đường thẳng D, D'' của E:

$$D /\!/ D'' \Leftrightarrow \left(\exists D' \in E, \begin{cases} D \perp D' \\ D' \perp D'' \end{cases} \right)$$

Vậy trong trường hợp này ta có thể viết: $\perp \circ \perp = /\!/$.

♦ **Mệnh đề 3** **(Tính kết hợp của phép hợp các quan hệ)**

Cho E, F, G, H là những tập hợp, $\mathcal{R}$ (tương ứng: $\mathcal{S}$, tương ứng: $\mathcal{T}$) là một quan hệ từ E đến F (tương ứng: F đến G, tương ứng: G đến H). Thế thì ta có:

$$(\mathcal{T} \circ \mathcal{S}) \circ \mathcal{R} = \mathcal{T} \circ (\mathcal{S} \circ \mathcal{R}).$$

Chứng minh:

Trước tiên, $(\mathcal{T} \circ \mathcal{S}) \circ \mathcal{R}$ và $\mathcal{T} \circ (\mathcal{S} \circ \mathcal{R})$ có chung một tập nguồn (E) và một tập đích (H).

Giả sử $(x, t) \in E \times H$. Ta có:

$$x\,(\mathcal{T} \circ \mathcal{S}) \circ \mathcal{R}\,t \Leftrightarrow \left(\exists y \in F \begin{cases} x\mathcal{R}y \\ y\,\mathcal{T} \circ \mathcal{S}\,t \end{cases}\right) \Leftrightarrow \left(\exists y \in F, \exists z \in G, \begin{cases} x\mathcal{R}y \\ y\mathcal{S}z \\ z\,\mathcal{T}t \end{cases}\right)$$

$$\Leftrightarrow \left(\exists z \in G \begin{cases} x\ \mathcal{S} \circ \mathcal{R}\ z \\ z\,\mathcal{T}\ t \end{cases}\right) \Leftrightarrow x\ \mathcal{T} \circ (\mathcal{S} \circ \mathcal{R})\ t.$$

♦ **Định nghĩa 5** Cho E, F là hai tập hợp, $\mathcal{R}$ là một quan hệ từ E đến F. Ta định nghĩa **quan hệ ngược** của $\mathcal{R}$, ký hiệu là $\mathcal{R}^{-1}$, từ F đến E, bởi:

$$\forall (x, y) \in E \times F, \quad (y\mathcal{R}^{-1}x \Leftrightarrow x\mathcal{R}y).$$

Chẳng hạn quan hệ ngược của $\leq$ trong $\mathbb{N}$ là $\geq$.

♦ **Mệnh đề 4**

1) Với mọi quan hệ $\mathcal{R}$: $(\mathcal{R}^{-1})^{-1} = \mathcal{R}$.

2) Cho E, F, G là những tập hợp, $\mathcal{R}$ (tương ứng: $\mathcal{S}$) là một quan hệ từ E đến F (tương ứng: F đến G). Ta có:

$$(\mathcal{S} \circ \mathcal{R})^{-1} = \mathcal{R}^{-1} \circ \mathcal{S}^{-1}.$$

Chứng minh:

1) Dễ dàng.

2) Với mọi (x, z) thuộc $E \times G$:

$$z\,(\mathcal{S} \circ \mathcal{R})^{-1}\,x \Leftrightarrow x\ \mathcal{S} \circ \mathcal{R}\,z \Leftrightarrow \left(\exists y \in F \begin{cases} x\mathcal{R}y \\ y\mathcal{S}z \end{cases}\right)$$

$$\Leftrightarrow \left(\exists y \in F, \begin{cases} z\mathcal{S}^{-1}y \\ y\mathcal{R}^{-1}x \end{cases}\right) \Leftrightarrow z\ \mathcal{R}^{-1} \circ \mathcal{S}^{-1}\ x.$$

♦ **Định nghĩa 6** Một quan hệ $\mathcal{R}$ từ E đến F được gọi là một **quan hệ hai ngôi** khi và chỉ khi $F = E$. Lúc đó ta nói rằng $\mathcal{R}$ là một quan hệ hai ngôi trong E.

Phần lớn các quan hệ được dùng trong Toán học là những quan hệ hai ngôi ($\leq$ trong $\mathbb{R}$, tính chia hết trong $\mathbb{N}$ hoặc $\mathbb{Z}$, bao hàm trong $\mathfrak{P}(E)$), hoặc các ánh xạ (xem 1.3 dưới đây).

♦ **Định nghĩa 7** Cho E là một tập hợp, $\mathcal{R}$ là một quan hệ hai ngôi trong E, $A \in \mathfrak{P}(E)$). Quan hệ hai ngôi trong A, ký hiệu là $\mathcal{R}_A$, xác định bởi:

$$\forall (x, y) \in A^2, (x\mathcal{R}_A y \Leftrightarrow x\mathcal{R}y)$$

được gọi là **quan hệ sinh bởi** $\mathcal{R}$ **trên** (hoặc: **trong**) A.

VÍ DỤ:

Quan hệ cảm sinh trên tập hợp P các số nguyên tố ($P = \{2, 3, 5, 7, 11, ...\}$), bởi tính chia hết trong $\mathbb{Z}$, là quan hệ bằng nhau.

♦ **Định nghĩa 8** Một quan hệ hai ngôi $\mathcal{R}$ trong một tập hợp E được gọi là:

phản xạ khi và chỉ khi: $\forall x \in E,\ x\mathcal{R}x$

đối xứng khi và chỉ khi: $\forall (x, y) \in E^2,\ (x\mathcal{R}y \Rightarrow y\mathcal{R}x)$

phản đối xứng khi và chỉ khi: $\forall (x, y) \in E^2,\ \left(\begin{cases} x\mathcal{R}y \\ y\mathcal{R}x \end{cases} \Rightarrow x = y\right)$

bắc cầu khi và chỉ khi: $\forall (x, y, z) \in E^3,\ \left(\begin{cases} x\mathcal{R}y \\ y\mathcal{R}z \end{cases} \Rightarrow x\mathcal{R}z\right)$.

VÍ DỤ:

1) Quan hệ $\leq$ trong $\mathbb{N}$ là phản xạ, không đối xứng, phản đối xứng, bắc cầu.

2) Quan hệ $\perp$ trong tập hợp các đường thẳng của mặt phẳng afin Euclide là đối xứng, nhưng không phản xạ, không phản đối xứng, không bắc cầu.

1.2.2 Quan hệ tương đương

♦ **Định nghĩa 1** Cho $\mathcal{R}$ là một quan hệ hai ngôi trong một tập hợp E. Ta nói rằng $\mathcal{R}$ là một **quan hệ tương đương** khi và chỉ khi: $\mathcal{R}$ là phản xạ, đối xứng và bắc cầu.

♦ **Định nghĩa 2** Cho $\mathcal{R}$ là một quan hệ hai ngôi trong một tập hợp E. Với mọi x thuộc E, **lớp tương đương** của x (**modulo** $\mathcal{R}$) là tập hợp, ký hiệu là $\mathrm{cl}_{\mathcal{R}}(x)$ (hoặc $\hat{x}$, hoặc $\overline{x}$, hoặc $\dot{x}$) được xác định bởi:

$$\mathrm{cl}_{\mathcal{R}}(x) = \{y \in E;\ x\mathcal{R}y\}.$$

Mỗi phần tử của $\mathrm{cl}_{\mathcal{R}}(x)$ được gọi là **một đại diện của** $\mathrm{cl}_{\mathcal{R}}(x)$.

Tập thương của E bởi $\mathcal{R}$, và ký hiệu là $E/\mathcal{R}$, là tập hợp các lớp tương đương modulo $\mathcal{R}$, tức là:

$$E/\mathcal{R} = \{\mathrm{cl}_{\mathcal{R}}(x);\ x \in E\}.$$

VÍ DỤ:

1) Quan hệ bằng nhau trong một tập hợp bất kỳ E là một quan hệ tương đương. Với mỗi x thuộc E, ta có $\mathrm{cl}_{=}(x) = \{x\}$, và $E/_{=} = \{\{x\};\ x \in E\}$.

2) Trong một tập hợp E, quan hệ $\mathcal{R}$ xác định bởi: $\forall (x, y) \in E^2,\ x\mathcal{R}y$ là một quan hệ tương đương. Với mọi x thuộc E, ta có $\mathrm{cl}_{\mathcal{R}}(x) = E$, và $E/\mathcal{R} = \{E\}$.

3) Với mọi n thuộc $\mathbb{N}^*$, quan hệ "là đồng dư với ... modulo n", được xác định bởi:

$$\forall (x, y) \in \mathbb{Z}^2, (x \equiv y[n] \Leftrightarrow n \mid x - y)$$

là một quan hệ tương đương (xem dưới đây, 4.1.2, Mệnh đề). Với mọi x thuộc $\mathbb{Z}$, lớp của x được gọi là lớp modulo n của x, và được ký hiệu là $\hat{x}$ (hoặc $\bar{x}$, hoặc $\dot{x}$), và : $\hat{x} = \{x + kn; k \in \mathbb{Z}\}$.

4) Trong tập hợp d các đường thẳng afin của một mặt phẳng afin P, quan hệ song song là một quan hệ tương đương. Với mọi D thuộc d, lớp modulo song song của D được gọi là phương của D.

◆ **Mệnh đề** Cho một tập hợp E.

1) Với mọi quan hệ tương đương $\mathcal{R}$ trong E, tập thương $E/\mathcal{R}$ là một phân hoạch của E.

2) Với mọi phân hoạch $\mathcal{P}$ của E, quan hệ $\mathcal{R}$ xác định trong E bởi:

$$\forall (x, y) \in E^2, \left(x \mathcal{R} y \Leftrightarrow \left(\exists P \in \mathcal{P}, \begin{cases} x \in P \\ y \in P \end{cases} \right) \right)$$

là một quan hệ tương đương trong E, và $\mathcal{P} = E/\mathcal{R}$.

Chứng minh:

1) Giả sử $\mathcal{R}$ là một quan hệ tương đương trong E.

- $(\forall x \in E, \mathrm{cl}_{\mathcal{R}}(x) \neq \varnothing)$, vì $x \in \mathrm{cl}_{\mathcal{R}}(x)$.
- Giả sử $(x, y) \in E^2$ sao cho $\mathrm{cl}_{\mathcal{R}}(x) \cap \mathrm{cl}_{\mathcal{R}}(y) \neq \varnothing$.

Vậy tồn tại $z \in \mathrm{cl}_{\mathcal{R}}(x) \cap \mathrm{cl}_{\mathcal{R}}(y)$. Khi đó ta có $x \mathcal{R} z$ và $y \mathcal{R} z$, vì vậy (do tính đối xứng và bắc cầu) $x \mathcal{R} y$. Suy ra $\mathrm{cl}_{\mathcal{R}}(x) \subset \mathrm{cl}_{\mathcal{R}}(y)$. Thật vậy, giả sử $t \in \mathrm{cl}_{\mathcal{R}}(x)$; ta có $x \mathcal{R} t$ và $x \mathcal{R} y$, do đó $y \mathcal{R} t$, tức là $t \in \mathrm{cl}_{\mathcal{R}}(y)$. Hơn nữa, vì x và y có những vai trò đối xứng nên: $\mathrm{cl}_{\mathcal{R}}(x) = \mathrm{cl}_{\mathcal{R}}(y)$.

- Vì $(\forall x \in E, x \in \mathrm{cl}_{\mathcal{R}}(x))$, nên hợp các phần tử của $E/\mathcal{R}$ là E.

2) Ngược lại, giả sử $\mathcal{P}$ là một phân hoạch của E và $\mathcal{R}$ là quan hệ được xác định trong E bởi:

$$\forall (x, y) \in E^2, \left(x \mathcal{R} y \Leftrightarrow \left(\exists P \in \mathcal{P}, \begin{cases} x \in P \\ y \in P \end{cases} \right) \right).$$

a) • Vì $(\forall x \in E, \exists P \in \mathcal{P}, x \in P)$, nên ta có: $\forall x \in E, x \mathcal{R} x$, vậy $\mathcal{R}$ phản xạ.

• Với mọi (x, y) thuộc E^2:

$$x R y \Leftrightarrow \left(\exists P \in \mathcal{P}, \begin{cases} x \in P \\ y \in P \end{cases} \right) \Leftrightarrow \left(\exists P \in \mathcal{P}, \begin{cases} y \in P \\ x \in P \end{cases} \right) \Leftrightarrow y \mathcal{R} x ;$$

vậy $\mathcal{R}$ đối xứng.

• Giả sử $(x, y, z) \in E^3$ sao cho $x \mathcal{R} y$ và $y \mathcal{R} z$. Tồn tại $P, Q \in \mathcal{P}$ sao cho: $\begin{cases} x \in P \\ y \in P \end{cases}$ và $\begin{cases} y \in Q \\ z \in Q \end{cases}$. Vì $P \cap Q \neq \varnothing$ và $\mathcal{P}$ là một phân hoạch, nên ta có $P = Q$ và $\begin{cases} x \in P \\ z \in P \end{cases}$, suy ra $x \mathcal{R} z$. Như thế, $\mathcal{R}$ bắc cầu.

b) α) Giả sử $x \in E$. Tồn tại $P \in \mathcal{P}$ sao cho $x \in P$, và khi đó ta có $\mathrm{cl}_{\mathcal{R}}(x) = P$. Thật vậy:

- Với mọi y thuộc P, $\begin{cases} x \in P \\ y \in P \end{cases}$, vậy $x\mathcal{R}y$.
- Với mọi y thuộc $\mathrm{cl}_{\mathcal{R}}(x)$, tồn tại $Q \in \mathcal{P}$ sao cho $\begin{cases} x \in Q \\ y \in Q \end{cases}$, và $Q = P$ (vì $P \in \mathcal{P}$, $Q \in \mathcal{P}$, $P \cap Q \neq \varnothing$), vậy $y \in P$.

Điều này chứng tỏ rằng: $E/\mathcal{R} \subset \mathcal{P}$.

β) Ngược lại, giả sử $P \in \mathcal{P}$. Tồn tại $x \in P$ và khi đó ta có: $\mathrm{cl}_{\mathcal{R}}(x) = P$ theo α). Điều này chứng tỏ rằng: $\mathcal{P} \subset E/\mathcal{R}$.

NHẬN XÉT:

1) Nếu $\mathcal{R}$ là một quan hệ tương đương trong E, thì với mọi (x, y) thuộc E^2:

$$x\mathcal{R}y \Leftrightarrow \mathrm{cl}_{\mathcal{R}}(x) = \mathrm{cl}_{\mathcal{R}}(y) \Leftrightarrow x \in \mathrm{cl}_{\mathcal{R}}(y) \Leftrightarrow y \in \mathrm{cl}_{\mathcal{R}}(x).$$

2) Mệnh đề trên nêu bật song ánh (xem 1.3.2, Định nghĩa 1) giữa tập hợp các quan hệ tương đương trên E và tập hợp các phân hoạch của E.

Bài tập

◊ **1.2.1** Cho E là một tập hợp, $\mathcal{R}$ là một quan hệ phản xạ trong E sao cho:

$$\forall (x, y, z) \in E^3, \left(\begin{cases} x\mathcal{R}y \\ y\mathcal{R}z \end{cases} \Rightarrow z\mathcal{R}x \right).$$

Kiểm chứng rằng $\mathcal{R}$ là một quan hệ tương đương.

◊ **1.2.2** Cho E là một tập hợp, $\mathcal{R}$ là một quan hệ phản xạ và bắc cầu trong E, $\mathcal{S}$ là một quan hệ xác định trong E bởi:

$$x\mathcal{S}y \Leftrightarrow (x\mathcal{R}y \text{ và } y\mathcal{R}x)$$

Kiểm chứng rằng $\mathcal{S}$ là một quan hệ tương đương.

◊ **1.2.3** Xét trong $\mathbb{R}$ quan hệ $\mathcal{R}$ xác định bởi:

$$x\mathcal{R}y \Leftrightarrow x^2 - y^2 = x - y.$$

a) Kiểm chứng rằng $\mathcal{R}$ là một quan hệ tương đương.

b) Với mọi x thuộc $\mathbb{R}$, tính $\mathrm{cl}_{\mathcal{R}}(x)$

◊ **1.2.4** Cho $\mathcal{R}$ là một quan hệ được xác định trong $\mathbb{R}$ bởi:

$$(x^3 + 2)(y^2 + 1) = (y^3 + 2)(x^2 + 1).$$

a) Kiểm chứng rằng $\mathcal{R}$ là một quan hệ tương đương.

b) Với mọi x thuộc $\mathbb{R}$, xác định số phần tử của $\mathrm{cl}_{\mathcal{R}}(x)$.

1.2.3 Quan hệ thứ tự

1) Đại cương

♦ **Định nghĩa 1** Cho $\mathcal{R}$ là một quan hệ hai ngôi trong một tập hợp E.

Ta nói rằng $\mathcal{R}$ là một **quan hệ thứ tự** khi và chỉ khi: $\mathcal{R}$ phản xạ, phản đối xứng và bắc cầu.

Ta thường nói **thứ tự** thay cho: quan hệ thứ tự. Một quan hệ thứ tự thường được ký hiệu $\leq$ (chẳng hạn, $\leq$ thông thường trong $\mathbb{R}$), hoặc $\preccurlyeq$.

Một **tập hợp được sắp thứ tự** (hay: **được sắp**) là một cặp $(E, \preccurlyeq)$ trong đó $\preccurlyeq$ là một thứ tự trên E.

♦ **Định nghĩa 2** Cho $(E, \preccurlyeq)$ là một tập hợp được sắp thứ tự.

1) Hai phần tử x, y của E được gọi là **so sánh được** (đối với $\preccurlyeq$) khi và chỉ khi:

$$x \preccurlyeq y \quad \text{hoặc} \quad y \preccurlyeq x.$$

2) Ta nói rằng $\preccurlyeq$ là một **quan hệ thứ tự toàn phần** (hoặc: là một **thứ tự toàn phần**) khi và chỉ khi mọi phần tử của E đều so sánh được từng đôi, tức là:

$$\forall (x, y) \in E^2, (x \preccurlyeq y \text{ hoặc } y \preccurlyeq x).$$

VÍ DỤ:

1) $\leq$ thông thường trong $\mathbb{R}$ là một thứ tự toàn phần.

2) Nếu E là một tập hợp có ít nhất hai phần tử, thì quan hệ bao hàm trong $\mathfrak{P}(E)$ là một thứ tự không toàn phần. ■

Cho $(E, \preccurlyeq)$ là một tập hợp được sắp. Ta định nghĩa trong E một quan hệ, ký hiệu là $\prec$, gọi là **thứ tự nghiêm ngặt ứng với** $\preccurlyeq$, xác định bởi:

$$\forall (x, y) \in E^2, \left(x \prec y \Leftrightarrow \begin{cases} x \preccurlyeq y \\ x \neq y \end{cases} \right).$$

Ta chú ý rằng (nếu E khác rỗng), $\prec$ không phải là một quan hệ thứ tự, vì nó không phản xạ.

Quan hệ ngược (xem 1.2.1, Định nghĩa 5) của một thứ tự $\preccurlyeq$ trong E là một thứ tự ký hiệu là $\succcurlyeq$; nói khác đi:

$$\forall (x, y) \in E^2, (x \succcurlyeq y \Leftrightarrow y \preccurlyeq x).$$

Nếu $\preccurlyeq$ là một thứ tự trên E, thì với mỗi bộ phận A của E, quan hệ cảm sinh bởi $\preccurlyeq$ trong A (xem 1.2.1, Định nghĩa 7) là một thứ tự, được gọi là **thứ tự cảm sinh** bởi $\preccurlyeq$ trong A.

2) Các phần tử đặc biệt của một tập hợp được sắp thứ tự

♦ **Định nghĩa 1** Cho $(E, \preccurlyeq)$ là một tập hợp được sắp thứ tự.

1) Cho $A \in \mathfrak{P}(E)$, $x \in E$. Ta nói rằng x là **một chặn trên** (hoặc: **cận trên**) (tương ứng: **chặn dưới** (hoặc: **cận dưới**)) của A trong E khi và chỉ khi:

$$\forall a \in A,\ a \preccurlyeq x \text{ (tương ứng: } \forall a \in A,\ x \preccurlyeq a).$$

2) Cho $A \in \mathfrak{P}(E)$. Ta nói rằng A **bị chặn trên** (tương ứng: **bị chặn dưới**) trong E khi và chỉ khi A có ít nhất một chặn trên (tương ứng: chặn dưới) trong E, tức là:

$$\exists x \in E,\ \forall a \in A,\ a \preccurlyeq x \quad \text{(tương ứng: } \exists x \in E,\ \forall a \in A,\ x \preccurlyeq a).$$

3) Cho $A \in \mathfrak{P}(E)$, $\alpha \in E$. Ta nói rằng α là một phần tử **lớn nhất** (tương ứng: **bé nhất**) của A khi và chỉ khi:

$$\begin{cases} \alpha \in A \\ \forall a \in A, \quad a \preccurlyeq \alpha \end{cases} \qquad \left(\text{tương ứng: } \begin{cases} \alpha \in A \\ \forall a \in A, \quad \alpha \preccurlyeq a \end{cases} \right).$$

4) Cho $A \in \mathfrak{P}(E)$, $x \in A$. Ta nói rằng x là **một phần tử cực đại** (tương ứng: **cực tiểu**) của A khi và chỉ khi:

$$\forall a \in A,\ (x \preccurlyeq a \Rightarrow x = a) \text{ (tương ứng: } \forall a \in A,\ (a \preccurlyeq x \Rightarrow x = a)).$$

Ta có thể ký hiệu tập hợp các chặn trên (tương ứng: chặn dưới) của A trong E là $\mathrm{Maj}_E(A)$ (tương ứng: $\mathrm{Min}_E(A)$). Với $(a, b) \in E^2$, ta nói rằng b là **một chặn trên của** a (hoặc a là **một chặn dưới của** b) khi và chỉ khi $a \preccurlyeq b$.

NHẬN XÉT:

1) Nếu α, β là những phần tử lớn nhất của A, thì $\alpha \preccurlyeq \beta$ (vì $\alpha \in A$ và β là một phần tử lớn nhất của A), và tương tự $\beta \preccurlyeq \alpha$, suy ra $\alpha = \beta$. Như thế, một bộ phận A của E có nhiều nhất một phần tử lớn nhất. Nếu A có một phần tử lớn nhất (tương ứng: bé nhất) thì nó được ký hiệu $\mathrm{Max}(A)$ (tương ứng: $\mathrm{Min}(A)$).

2) Một bộ phận A của E có thể có hoặc không có phần tử lớn nhất. Chẳng hạn, trong $(\mathbb{R}, \leq)$, $\mathbb{R}_-$ có một phần tử lớn nhất (là 0), nhưng $\mathbb{R}_+$ không có phần tử lớn nhất.

3) Một bộ phận A của E có thể không có phần tử cực đại, hoặc có một, hoặc có nhiều. Chẳng hạn:

- trong $(\mathbb{R}, \leq)$, $\mathbb{R}_+$ không có phần tử cực đại
- trong $(\mathbb{R}, \leq)$, $[0; 1]$ có một phần tử cực đại và chỉ một, đó là 1 và đó cũng là phần tử lớn nhất của $[0; 1]$
- trong $(\mathbb{N} - \{0, 1\}, |)$, $\mathbb{N} - \{0, 1\}$ có vô số phần tử cực tiểu, đó là các số nguyên tố.

4) Nếu $(E, \preccurlyeq)$ được sắp thứ tự toàn phần, thì E có nhiều nhất một phần tử cực đại, đó cũng là phần tử lớn nhất của E. Thật vậy, nếu x là phần tử cực đại của E, thì vì $\preccurlyeq$ là thứ tự toàn phần trong E, nên ta có:

$$\forall a \in A, (a \preccurlyeq x \text{ hoặc } x \preccurlyeq a)$$

và như vậy: $\forall a \in E, (a \preccurlyeq x \text{ hoặc } x = a)$, tức là: $\forall a \in E, a \preccurlyeq x$.

Vậy khái niệm phần tử cực đại chỉ có ích trong trường hợp $\preccurlyeq$ là thứ tự không toàn phần.

◆ **Định nghĩa 2** Cho $(E, \preccurlyeq)$ là một tập hợp được sắp thứ tự, $A \in \mathfrak{P}(E)$.

1) Nếu tập hợp $\text{Maj}_E(A)$ các chặn trên (hoặc: cận trên) của A trong E có một phần tử bé nhất M, thì M được gọi là **biên trên** (hoặc: **cận trên đúng**) của A (**trong** E) và được ký hiệu $\text{Sup}_E(A)$, hoặc $\text{Sup}(A)$.

2) Nếu tập hợp $\text{Min}_E(A)$ các chặn dưới (hoặc: cận dưới) của A trong E có một phần tử lớn nhất m, thì m được gọi là **biên dưới** (hoặc: **cận dưới đúng**) của a (**trong** E) và được ký hiệu $\text{Inf}_E(A)$ hoặc $\text{Inf}(A)$.

Nếu A gồm hai phần tử x, y, hoặc một họ các phần tử $(x_i)_{i \in I}$, thì ta sẽ ký hiệu $\text{Sup}_E(x, y)$, $\text{Inf}_E(x, y)$, $\sup\limits_{i \in I} x_i$, $\inf\limits_{i \in I} x_i$ thay cho $\text{Sup}_E(A)$, $\text{Inf}_E(A)$.

NHẬN XÉT:

Cho $(E, \preccurlyeq)$ là một tập được sắp thứ tự, $A \in \mathfrak{P}(E)$, $M \in E$. Muốn cho M là biên trên (nếu tồn tại) của A trong E, cần và đủ là:

$$\begin{cases} \forall a \in A, & a \preccurlyeq M \\ \forall x \in E, & ((\forall a \in A, a \preccurlyeq x) \Rightarrow M \preccurlyeq x) \end{cases}$$

VÍ DỤ:

1) $E = \mathbb{R}$, $\leq$ thông thường, $A =]0; 1[$.

Ta có: • $\text{Maj}_E(A) = [1; +\infty[$, vậy $\text{Sup}_E(A)$ tồn tại và $\text{Sup}_E(A) = 1$.

• $\text{Min}_E(A) =]-\infty; 0]$, vậy $\text{Inf}_E(A)$ tồn tại và $\text{Inf}_E(A) = 0$.

Ta chú ý rằng, theo ví dụ trên, biên trên (tương ứng: biên dưới) của A trong E, nếu tồn tại, có thể không thuộc A.

2) $E = \mathbb{Q}$, $\leq$ thông thường, $A = \{x \in \mathbb{Q}_+; x^2 < 2\}$.

Ta có: $\text{Maj}_E(A) = \{x \in \mathbb{Q}_+; x^2 \geq 2\} = \{x \in \mathbb{Q}_+; x^2 > 2\}$, tập này không có phần tử bé nhất (tức là: $\sqrt{2} \notin \mathbb{Q}$); vậy A không có biên trên trong E.

3) $E = \mathfrak{P}(F)$, trong đó F là một tập hợp, $\subset$ là quan hệ bao hàm. Với mọi (X, Y) thuộc E^2, ta có:

$$\text{Sup}_{\mathfrak{P}(F)}(X, Y) = X \cup Y \quad \text{và} \quad \text{Inf}_{\mathfrak{P}(F)}(X, Y) = X \cap Y.$$

4) $E = \mathbb{N} - \{0; 1\}$, $|$ là tính chia hết. Với mọi (x, y) thuộc E^2, ta có (xem 4.2.2, Mệnh đề 3) :

$$\text{Sup}(x, y) = x \vee y = \text{BCNN}(x, y), \quad \text{Inf}(x, y) = x \wedge y = \text{UCLN}(x, y).$$

NHẬN XÉT:

1) • $\mathrm{Sup}_E(\varnothing)$ là phần tử bé nhất của E (nếu tồn tại)

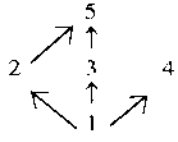
• $\mathrm{Inf}_E(\varnothing)$ là phần tử lớn nhất của E (nếu tồn tại).

2) Với mọi bộ phận khác rỗng A của E, nếu $\mathrm{Inf}_E(A)$ và $\mathrm{Sup}_E(A)$ tồn tại, thì:

$$\mathrm{Inf}_E(A) \leq \mathrm{Sup}_E(A).$$

Bài tập

◊ **1.2.5** Cho $E = \{1, 2, 3, 4, 5\}$, $\mathcal{R}$ là quan hệ thứ tự xác định trong E bởi biểu đồ bên (theo quy ước không có tính phản xạ và tính bắc cầu), $A = \{2, 3\}$, $B = \{2, 4\}$, $C = \{1, 2, 5\}$.



Với mỗi bộ phận A, B, C, khảo sát sự tồn tại và trị có thể có của tập hợp các chặn trên của chúng trong E, của tập hợp các phần tử cực đại, biên trên, và phần tử lớn nhất của chúng.

◊ **1.2.6** a) Cho $(E, \preccurlyeq)$ là một tập hợp được sắp thứ tự, A, B là hai bộ phận của E sao cho $A \subset B$. Chứng minh rằng, nếu A và B có các biên trên (cận trên đúng) trong E thì $\mathrm{Sup}_E(A) \preccurlyeq \mathrm{Sup}_E(B)$.

b) Cho ba ví dụ về các tập hợp được sắp thứ tự $(E, \preccurlyeq)$ và các bộ phận A, B của E sao cho $A \subset B$ và thỏa mãn:

1) $\begin{cases} A \text{ có biên trên trong } E \\ B \text{ không có biên trên trong } E \end{cases}$

2) $\begin{cases} A \text{ không có biên trên trong } E \\ B \text{ có biên trên trong } E \end{cases}$

3) $\begin{cases} A \text{ và } B \text{ có biên trên trong } E \\ \mathrm{Sup}_E(A) \neq \mathrm{Sup}_E(B). \end{cases}$

◊ 1.2.7 Thứ tự tích

Cho $(E, \preccurlyeq)$, $(F, \preccurlyeq)$ là hai tập hợp được sắp thứ tự, $\mathcal{P}$ là quan hệ xác định trong $E \times F$ bởi:

$$(x, y)\,\mathcal{P}\,(x', y') \Leftrightarrow \begin{cases} x \preccurlyeq x' \\ y \preccurlyeq y' \end{cases}.$$

a) Chứng minh $\mathcal{P}$ là một thứ tự trên $E \times F$, gọi là *thứ tự tích* của các thứ tự trên E và trên F.

b) Lấy $E = F = \mathbb{R}$, được trang bị thứ tự thông thường.

α) Với mọi cặp (x, y) của $\mathbb{R}^2$, xác định tập hợp các chặn trên đối với $\mathcal{P}$ của (x, y) trong $\mathbb{R}^2$.

β) Thứ tự $\mathcal{P}$ có là một thứ tự toàn phần trong $\mathbb{R}^2$ không?

γ) Xác định tập hợp các phần tử cực đại của $A = \{(x, y) \in \mathbb{R}^2 ; x + y \geq 0\}$ đối với thứ tự $\mathcal{P}$.

δ) Trong $\mathbb{R}^2$ thì $(\mathbb{R}_-^*)^2$ có biên trên đối với $\mathcal{P}$ hay không? và nếu có, hãy xác định biên trên đó.

◊ 1.2.8 Thứ tự từ điển

Cho $(E, \preccurlyeq)$, $(F, \preccurlyeq)$ là hai tập hợp được sắp thứ tự, $\mathcal{L}$ là quan hệ xác định trong $E \times F$ bởi:

$$(x, y)\,\mathcal{L}\,(x', y') \Leftrightarrow \left| \begin{array}{l} x \prec x' \\ \text{hoặc} \\ (x = x' \text{ và } y \preccurlyeq y') \end{array} \right. .$$

a) Chứng minh rằng $\mathcal{L}$ là một thứ tự trên $E \times F$, gọi là *thứ tự từ điển* (của các thứ tự trên E và trên F).

b) Chứng minh rằng nếu $\preccurlyeq$ của E và của F là thứ tự toàn phần, thì $\mathcal{L}$ là một thứ tự toàn phần.

c) Lấy $E = F = \mathbb{R}$, được trang bị thứ tự thông thường.

α) Với mọi cặp (x, y) thuộc $\mathbb{R}^2$, hãy xác định tập hợp các chặn trên đối với $\mathcal{L}$ của (x, y) trong $\mathbb{R}^2$.

β) $\mathbb{R}_-^* \times \mathbb{R}$ có biên trên đối với $\mathcal{L}$ trong $\mathbb{R}^2$ hay không? và nếu có, hãy xác định nó.

1.3 Ánh xạ

1.3.1 Các định nghĩa

♦ **Định nghĩa 1** Cho hai tập hợp E, F.

Hàm từ E **đến** F là một quan hệ f từ E đến F thỏa mãn:

$$\forall(x, y, y') \in E \times F \times F, \left(\begin{cases} x\ f\ y \\ x\ f\ y' \end{cases} \Rightarrow y = y'\right).$$

Khi đó ta thường ký hiệu $y = f(x)$ hơn là $x\ f\ y$.

Tập hợp (hoặc **miền**) **xác định** của hàm f, ký hiệu Def(f) là tập hợp các phần tử x của E sao cho tồn tại $y \in F$ thỏa mãn $y = f(x)$.

Với mọi x thuộc E, nếu tồn tại phần tử y của F sao cho $y = f(x)$, thì y được gọi là **ảnh của** x **bởi** f (hay: **qua** f).

Với mọi y thuộc F, một phần tử x của E sao cho $y = f(x)$ (có thể không tồn tại phần tử x, tồn tại một, tồn tại nhiều) được gọi là một **tạo ảnh của** y **bởi** f (hay: **qua** f).

Như vậy, một quan hệ là một hàm khi và chỉ khi mỗi phần tử của tập nguồn có quan hệ với nhiều nhất một phần tử của tập đích.

♦ **Mệnh đề 1** Nếu f là một hàm từ E đến F và g là một hàm từ F đến G, thì quan hệ $g \circ f$ (xem 1.2.1, Định nghĩa 4) là một hàm từ E đến G.

Chứng minh:

Giả sử $(x, z, z') \in E \times G \times G$ sao cho: $\begin{cases} x\,(g \circ f)\,z \\ x\,(g \circ f)\,z' \end{cases}$. Tồn tại $(y, y') \in F^2$ sao cho:

$\begin{cases} x\ f\ y \text{ và } y\ g\ z \\ x\ f\ y' \text{ và } y'\ g\ z' \end{cases}$.

Vì $\begin{cases} x\ f\ y \\ x\ f\ y' \end{cases}$ và vì f là một hàm, nên ta có: $y = y'$. Sau đó, do $\begin{cases} y\ g\ z \\ y\ g\ z' \end{cases}$ và g là một hàm, nên ta kết luận $z = z'$.

♦ **Định nghĩa 2** Một hàm f từ E đến F được gọi là một **ánh xạ** khi và chỉ khi Def(f) = E. Tập hợp các ánh xạ từ E vào F được ký hiệu là F^E.

Nói khác đi, một quan hệ $\mathcal{R}$ từ E đến F là một ánh xạ khi và chỉ khi, với mọi x thuộc E, tồn tại một và chỉ một phần tử y của F sao cho $x \mathcal{R} y$. Ký hiệu F^E sẽ được lý giải dưới đây (3.5.1).

Một ánh xạ f từ E đến F được ký hiệu $\underset{x \mapsto f(x)}{f : E \to F}$, trong đó chữ x là câm.

NHẬN XÉT:

Hai ánh xạ f, g là bằng nhau khi và chỉ khi chúng có chung một tập nguồn (ký hiệu E), chung một tập đích, và: $\forall x \in E,\ f(x) = g(x)$.

◆ **Mệnh đề 2** Nếu $f : E \to F$, $g : F \to G$ là hai ánh xạ, thì hàm hợp $g \circ f$ là một ánh xạ.

Chứng minh:
Theo Mệnh đề 1, $g \circ f$ đã là một hàm. Cho $x \in E$. Vì f là một ánh xạ nên tồn tại $y \in F$ sao cho $y = f(x)$. Ngoài ra, vì g là một ánh xạ, nên tồn tại $z \in G$ sao cho $z = g(y)$. Vậy theo định nghĩa của $g \circ f$ ta có : $z = (g \circ f)(x)$.

NHẬN XÉT:
Nếu $f : E \to F$, $g : F \to G$ là hai ánh xạ, thì ta có:

$$\forall x \in E, (g \circ f)(x) = g(f(x)).$$

◆ **Mệnh đề 3** **(Tính kết hợp của phép hợp các ánh xạ)**
Với mọi ánh xạ $f : E \to F$, $g : F \to G$, $h : G \to H$, ta có:

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

Chứng minh:
Đó là một trường hợp riêng của 1.2.1, Mệnh đề 3.

NHẬN XÉT:
Phép hợp các ánh xạ không giao hoán, tức là có thể $g \circ f \neq f \circ g$. Chẳng hạn, $f : \underset{x \mapsto x+1}{\mathbb{R} \to \mathbb{R}}$ và $g : \underset{y \mapsto y^2}{\mathbb{R} \to \mathbb{R}}$ không giao hoán đối với $\circ$, vì:

$$\forall x \in \mathbb{R}, \quad \begin{cases} (g \circ f)(x) = g(x+1) = (x+1)^2 \\ (f \circ g)(x) = f(x^2) = x^2 + 1 \end{cases},$$

và đặc biệt $(g \circ f)(1) \neq (f \circ g)(1)$.

VÍ DỤ:

1) Với tập hợp E bất kỳ, ta ký hiệu $\mathrm{Id}_E : \underset{x \mapsto x}{E \to E}$, gọi là **ánh xạ đồng nhất** (hoặc **phép đồng nhất**) của E.

2) Cho E là một tập hợp, $A \in \mathfrak{P}(E)$; **ánh xạ nhúng chính tắc từ** A **vào** E là ánh xạ, ký hiệu $i_{A,E}$ (hoặc i_A), xác định bởi:

$$i_{A,E} : \underset{x \mapsto x}{A \to E}.$$

3) Cho E là một tập hợp, $f : E \to E$ là một ánh xạ. Ta ký hiệu $f^0 = \mathrm{Id}_E$, $f^1 = f$, và với mọi n thuộc $\mathbb{N} - \{0, 1\}$, $f^n = f \circ f^{n-1}$, nếu không có nguy cơ bị lẫn với các phép toán khác (f^{-1} có thể chỉ $\frac{1}{f}$, $f^{(n)}$ có thể chỉ đạo hàm cấp n của f...).

4) Cho E, F là hai tập hợp, $a \in F$. **Ánh xạ hằng a** là ánh xạ thường được ký hiệu cũng là a, xác định bởi: $a : \underset{x \mapsto a}{E \to E}$.

5) Cho E là một tập hợp. Với tập con A tùy ý của E, ta định nghĩa **hàm đặc trưng** (hoặc: **hàm chỉ**) của A, ký hiệu χ_A (hoặc: φ_A) như sau:

$$\chi_A : E \to \{0, 1\}$$
$$x \mapsto \begin{cases} 1 & \text{nếu } x \in A \\ 0 & \text{nếu } x \in \complement_E(A) \end{cases}$$

6) Cho $n \in \mathbb{N}^*$, E_1, ..., E_n là những tập hợp. Với mỗi i thuộc $\{1, ..., n\}$, ta định nghĩa **ánh xạ chiếu chính tắc thứ i**, ký hiệu là p_i, như sau:

$$p_i : E_1 \times ... \times E_n \to E_i$$
$$(x_1, ..., x_n) \mapsto x_i$$

Chẳng hạn, với $n = 2$:

$$p_1 : E_1 \times E_2 \to E_1 \quad \text{và} \quad p_2 : E_1 \times E_2 \to E_2.$$
$$(x_1, x_2) \mapsto x_1 \qquad (x_1, x_2) \mapsto x_2$$

NHẬN XÉT:

Với mọi ánh xạ $f : E \to F$, ta có:

$$f \circ \mathrm{Id}_E = f \quad \text{và} \quad \mathrm{Id}_F \circ f = f.$$

♦ **Định nghĩa 3** Một bộ phận A của một tập hợp E được gọi là **ổn định đối với** một ánh xạ $f : E \to E$ khi và chỉ khi: $\forall a \in A, f(a) \in A$.

Bài tập

◊ **1.3.1** Cho E là một tập hợp. Với mọi bộ phận A của E, ta ký hiệu: $\varphi_A : E \to \{0, 1\}$

$$x \mapsto \begin{cases} 1 \text{ nếu } x \in A \\ 0 \text{ nếu } x \in \overline{A} \end{cases}$$

là hàm đặc trưng của A (xem Ví dụ 5), trong đó $\overline{A} = \complement_E(A)$.

Chứng minh các công thức sau đối với mọi bộ phận A, B của E:

1) $A \subset B \Leftrightarrow \varphi_A \leq \varphi_B$ 2) $A = B \Leftrightarrow \varphi_A = \varphi_B$

3) $\varphi_A^2 = \varphi_A$ 4) $\varphi_{A \cap B} = \varphi_A \varphi_B$

5) $\varphi_{\overline{A}} = 1 - \varphi_A$ 6) $\varphi_{A \cup B} = \varphi_A + \varphi_B - \varphi_A \varphi_B$

7) $\varphi_{A - B} = \varphi_A (1 - \varphi_B)$

8) $\varphi_{A \Delta B} = \varphi_A + \varphi_B - 2\varphi_A \varphi_B = (\varphi_A - \varphi_B)^2 = |\varphi_A - \varphi_B|$.

◊ **1.3.2** Cho E, F là hai tập hợp, $\mathcal{U}$ là tập hợp các cặp (X, f) tạo thành bởi một bộ phận khác rỗng X của E và một ánh xạ f từ X vào F. Ta định nghĩa trong $\mathcal{U}$ một quan hệ, ký hiệu $\mathcal{R}$, là:

$$(X, f) \mathcal{R} (X', f') \Leftrightarrow \begin{cases} X \subset X' \\ \forall x \in X, \quad f(x) = f'(x) \end{cases}$$

a) Chứng minh rằng $\mathcal{R}$ là một quan hệ thứ tự trong $\mathcal{U}$.

b) Các phần tử cực đại (tương ứng : cực tiểu) của $\mathcal{U}$ đối với $\mathcal{R}$ là gì?

◊ **1.3.3** Cho E, F, G, E', F', G' là những tập hợp, $\begin{array}{ccc} E & \xrightarrow{f} & F \\ u\downarrow & & \downarrow v \\ E' & \xrightarrow[f']{} & F' \end{array}$, $\begin{array}{ccc} F & \xrightarrow{g} & G \\ v\downarrow & & \downarrow w \\ F' & \xrightarrow[g']{} & G' \end{array}$

là những *biểu đồ giao hoán*, tức là sao cho $v \circ f = f' \circ u$ và $w \circ g = g' \circ v$.

Chứng minh rằng biểu đồ $\begin{array}{ccc} E & \xrightarrow{g \circ f} & F \\ u\downarrow & & \downarrow w \\ E' & \xrightarrow[g' \circ f']{} & F'' \end{array}$ có tính giao hoán.

◊ **1.3.4 Nhân tử hóa một ánh xạ**

Cho E, F, G là ba tập hợp khác rỗng.

a) Cho $f : E \to F$, $g : E \to G$ là hai ánh xạ. Chứng minh rằng, để tồn tại $h : F \to G$ sao cho

biểu đồ $\begin{array}{ccc} E & \xrightarrow{g} & G \\ f\downarrow & \nearrow_{h} & \\ F & & \end{array}$ là giao hoán (tức là: $h \circ f = g$), điều kiện cần và đủ là:

$\forall (x, x') \in E^2, (f(x) = f(x') \Rightarrow g(x) = g(x'))$.

b) Cho hai ánh xạ $g : E \to G$, $h = F \to G$. Chứng minh rằng, để tồn tại $f : E \to F$ sao cho

biểu đồ $\begin{array}{ccc} E & \xrightarrow{g} & G \\ f\downarrow & \nearrow_{h} & \\ F & & \end{array}$ là giao hoán (tức là: $h \circ f = g$), cần và đủ là:

$\forall x \in E, \exists y \in F, g(x) = h(y)$.

1.3.2 Đơn ánh, toàn ánh, song ánh

♦ **Định nghĩa 1** Một ánh xạ $f : E \to F$ được gọi là ánh xạ:

- **đơn ánh** khi và chỉ khi: $\forall (x, x') \in E^2, (f(x) = f(x') \Rightarrow x = x')$
- **toàn ánh** khi và chỉ khi: $\forall y \in F, \exists x \in E, y = f(x)$
- **song ánh** khi và chỉ khi: f là toàn ánh và đơn ánh, tức là:

$$\forall y \in F, \exists! x \in E, \quad y = f(x).$$

Ta cũng nói **đơn ánh** (tương ứng: **toàn ánh**, tương ứng: **song ánh**) thay cho ánh xạ đơn ánh (tương ứng: ánh xạ toàn ánh, tương ứng: ánh xạ song ánh).

NHẬN XÉT:

1) Một ánh xạ $f : E \to F$ là đơn ánh khi và chỉ khi :

$$\forall (x, x') \in E^2, \quad (x \neq x' \Rightarrow f(x) \neq f(x')).$$

Nói khác đi, $f : E \to F$ là đơn ánh khi và chỉ khi mọi phần tử của F có *nhiều nhất* một tạo ảnh bởi f trong E.

2) Một ánh xạ $f : E \to F$ là toàn ánh khi và chỉ khi mọi phần tử của F có *ít nhất* một tạo ảnh bởi f trong E.

VÍ DỤ:

1) Nếu $A \subset E$, ánh xạ nhúng chính tắc $i_A : \begin{matrix} A \to E \\ x \mapsto x \end{matrix}$ là một đơn ánh, cũng được gọi **đơn ánh chính tắc** từ A vào E.

2) Cho E là một tập hợp, $\mathcal{R}$ là một quan hệ tương đương trong E. Ánh xạ $s : \begin{matrix} E \to E/\mathcal{R} \\ x \mapsto \mathrm{cl}_{\mathcal{R}}(x) \end{matrix}$ là một toàn ánh, được gọi **toàn ánh chính tắc từ E lên $E/\mathcal{R}$**.

♦ Định nghĩa 2

1) Một song ánh bất kỳ từ E vào E gọi là một **hoán vị** của E.

2) **Đối hợp** (hoặc: **ánh xạ đối hợp**) của E là một ánh xạ $f : E \to E$ bất kỳ sao cho $f \circ f = \mathrm{Id}_E$.

♦ **Mệnh đề 1** Hợp của hai đơn ánh (tương ứng: toàn ánh, tương ứng: song ánh) là một đơn ánh (tương ứng: toàn ánh, tương ứng: song ánh).

Chứng minh:

Cho hai ánh xạ $f : E \to F$, $g : F \to G$.

1) Giả sử f và g là đơn ánh.

Với mọi (x, x') thuộc E^2 ta có:

$$(g \circ f)(x) = (g \circ f)(x') \Leftrightarrow g(f(x)) = g(f(x')) \Rightarrow f(x) = f(x') \Rightarrow x = x',$$

vậy $g \circ f$ là đơn ánh.

2) Giả sử f và g là toàn ánh.

Cho $z \in G$. Vì g là toàn ánh nên tồn tại $y \in F$ sao cho $z = g(y)$. Rồi, vì f là toàn ánh nên tồn tại $x \in E$ sao cho $y = f(x)$. Vậy ta có $z = g(f(x)) = (g \circ f)(x)$, điều này chứng tỏ $g \circ f$ là toàn ánh.

3) (f và g là song ánh) $\Rightarrow \begin{cases} f \text{ và } g \text{ là đơn ánh} \\ f \text{ và } g \text{ là toàn ánh} \end{cases} \Rightarrow \begin{cases} g \circ f \text{ là đơn ánh} \\ g \circ f \text{ là toàn ánh} \end{cases}$

$\Rightarrow (g \circ f$ là song ánh).

♦ **Mệnh đề 2** Cho $f : E \to F$, $g : F \to G$.

1) Nếu $g \circ f$ là đơn ánh, thì f là đơn ánh.

2) Nếu $g \circ f$ là toàn ánh, thì g là toàn ánh.

Chứng minh:

1) Giả sử $g \circ f$ là đơn ánh. Với mọi (x, x') thuộc E^2 ta có:

$$f(x) = f(x') \Rightarrow g(f(x)) = g(f(x')) \Leftrightarrow (g \circ f)(x) = (g \circ f)(x') \Rightarrow x = x',$$

vậy f là đơn ánh.

2) Giả sử $g \circ f$ là toàn ánh. Cho $z \in G$, tồn tại $x \in E$ sao cho $z = (g \circ f)(x) = g(f(x))$, chứng tỏ g là toàn ánh.

♦ **Mệnh đề 3** Cho một ánh xạ $f : E \to F$. Để quan hệ ngược của f là một ánh xạ, cần và đủ là: f là song ánh. Hơn nữa, nếu f là song ánh thì ánh xạ ngược f^{-1} của f là một song ánh.

Chứng minh:

1) Ta nhớ lại rằng quan hệ ngược f^{-1} của f (xem 1.2.1, Định nghĩa 5) được định nghĩa bởi:

$$\forall (x, y) \in E \times F, \quad y f^{-1} x \Leftrightarrow x f y \Leftrightarrow y = f(x).$$

Ta có: (f là song ánh) $\Leftrightarrow (\forall y \in F, \exists! x \in E, \quad y = f(x))$

$\Leftrightarrow (\forall y \in F, \exists! x \in E, \quad y f^{-1} x) \Leftrightarrow (f^{-1}$ là một ánh xạ).

2) Nếu f là song ánh thì f^{-1} là một ánh xạ như trên đã nói) và vì $(f^{-1})^{-1} = f$ là một ánh xạ, nên f^{-1} là song ánh.

♦ **Mệnh đề 4** Nếu $f : E \to F$ và $g : F \to G$ là những song ánh, thì $g \circ f : E \to G$ là song ánh và $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Chứng minh: Do Mệnh đề 1 và 1.2.1, Mệnh đề 4.

NHẬN XÉT:

Từ nay, ta sẽ không sử dụng tới quan hệ ngược của một quan hệ, ngoại trừ trường hợp khi quan hệ đó là một song ánh. Vậy ký hiệu f^{-1} sẽ chỉ ánh xạ ngược của f với giả thiết f là song ánh. Tuy nhiên, ta sẽ sử dụng ký hiệu $f^{-1}(A')$ (nghịch ảnh của một tập con A' của tập đích) đối với một ánh xạ f bất kỳ, xem 1.3.5, Định nghĩa.

♦ **Mệnh đề 5** Cho $f : E \to F$ là một ánh xạ. Muốn cho f là song ánh, điều kiện cần và đủ là tồn tại một ánh xạ $g : F \to E$ sao cho:

$$\begin{cases} g \circ f = \mathrm{Id}_E \\ f \circ g = \mathrm{Id}_F \end{cases}.$$

Hơn nữa, với các giả thiết đó, ta có: $g = f^{-1}$.

Chứng minh:

1) Nếu f là song ánh thì f^{-1} tồn tại như là một ánh xạ, và rõ ràng ràng:

$$\begin{cases} f^{-1} \circ f = \mathrm{Id}_E \\ f \circ f^{-1} = \mathrm{Id}_F \end{cases}.$$

2) Ngược lại, nếu tồn tại $g : F \to E$ sao cho $\begin{cases} g \circ f = \mathrm{Id}_E \\ f \circ g = \mathrm{Id}_F \end{cases}$, thì, theo Mệnh đề 2, vì Id_E là đơn ánh và Id_F là toàn ánh, ta suy ra f là đơn ánh và toàn ánh, do đó là song ánh. Tương tự đối với g. Cuối cùng:

$$g = g \circ (f \circ f^{-1}) = (g \circ f) \circ f^{-1} = \mathrm{Id}_E \circ f^{-1} = f^{-1}.$$

♦ **Hệ quả** Một ánh xạ $f : E \to E$ là đối hợp khi và chỉ khi:

$$\begin{cases} f \text{ là song ánh} \\ f^{-1} = f \end{cases}.$$

Bài tập

◊ **1.3.5** Cho E, F là hai tập hợp, $f : E \to F$, $g : F \to E$ là hai ánh xạ sao cho $f \circ g \circ f$ là song ánh. Chứng minh f và g đều là song ánh.

◊ **1.3.6** Cho E, F, G là ba tập hợp, $f : E \to F$, $g : F \to G$ là hai ánh xạ. Chứng minh:

a) Nếu $g \circ f$ là đơn ánh và f là toàn ánh, thì g là đơn ánh.

b) Nếu $g \circ f$ là toàn ánh và g là đơn ánh, thì f là toàn ánh.

◊ **1.3.7** Cho hai tập hợp khác rỗng E, F, $f : E \to F$. Chứng minh (sử dụng bài tập 1.3.4):

a) f là đơn ánh khi và chỉ khi tồn tại một toàn ánh $h : F \to E$ sao cho $h \circ f = \mathrm{Id}_E$.

b) f là toàn ánh khi và chỉ khi tồn tại một đơn ánh $g : F \to E$ sao cho $f \circ g = \mathrm{Id}_F$.

◊ **1.3.8** Cho hai tập hợp khác rỗng E, F. Chứng minh rằng hai tính chất sau đây là tương đương:

(i) Tồn tại một đơn ánh từ E vào F.

(ii) Tồn tại một toàn ánh từ F vào E.

◊ **1.3.9** Cho $f : \mathbb{N} \to \mathbb{N}$ và $g : \mathbb{N} \to \mathbb{N}$

$$x \mapsto 2x \qquad y \mapsto \begin{cases} \dfrac{y}{2} & \text{nếu } y \text{ là chẵn} \\ \dfrac{y-1}{2} & \text{nếu } y \text{ là lẻ.} \end{cases}$$

a) Khảo sát các tính chất đơn ánh, toàn ánh, song ánh của f và của g.

b) Xác định $g \circ f$ và $f \circ g$.

◊ **1.3.10 Tích của hai quan hệ tương đương**

Giả sử E, F là hai tập hợp, $\mathcal{R}$ (tương ứng: $\mathcal{S}$) là một quan hệ tương đương trong E (tương ứng: F), $\mathcal{T}$ là một quan hệ xác định trong $E \times F$ bởi:

$$(x, y)\ \mathcal{T}\ (x', y') \Leftrightarrow \begin{cases} x \mathcal{R} x' \\ y \mathcal{S} y' \end{cases}.$$

a) Hãy kiểm chứng rằng $\mathcal{T}$ là một quan hệ tương đương trong $E \times F$.

b) Nêu rõ một song ánh giữa $E/\mathcal{R} \times F/\mathcal{S}$ và $(E \times F)/\mathcal{T}$.

◊ **1.3.11*** Trong $E = \mathbb{R}^{\mathbb{R}}$ ta định nghĩa một quan hệ $\mathcal{R}$ bởi:

$$f \mathcal{R} g \Leftrightarrow \left(\exists \varphi \in E, \begin{cases} \varphi \text{ là song ánh} \\ \varphi \circ f = g \circ \varphi \end{cases} \right).$$

a) Chứng minh rằng $\mathcal{R}$ là một quan hệ tương đương trong E.

b) Có hay không ch $\mathcal{R}$ sh (các hàm hypebolic)? cos $\mathcal{R}$ sin?

c) Tìm một điều kiện cần và đủ đối với $(p, q) \in \mathbb{R}^2$ để $f : \begin{matrix} \mathbf{R} \to \mathbf{R} \\ x \mapsto x^2 \end{matrix}$ và $g : \begin{matrix} \mathbf{R} \to \mathbf{R} \\ x \mapsto x^2 + px + q \end{matrix}$ là tương đương.

1.3.3 Thu hẹp và thác triển của ánh xạ

♦ **Định nghĩa 1** Cho E, F là hai tập hợp, $f : E \to F$ là một ánh xạ, $A \in \mathfrak{P}(E)$. **Thu hẹp của** f **vào** A là ánh xạ, ký hiệu là $f|_A$, xác định bởi:

$$f|_A : \begin{array}{c} A \to F \\ x \mapsto f(x) \end{array}.$$

Ký hiệu $\mathrm{i} : A \to E$ là ánh xạ nhúng chính tắc, vậy ta có: $f|_A = f \circ \mathrm{i}$.

♦ **Định nghĩa 2** Cho E, F là hai tập hợp, $f : E \to F$ là một ánh xạ, E' là một tập hợp sao cho $E \subset E'$. **Thác triển** (hoặc: **mở rộng**) **của** f **trên** E' là một ánh xạ $g : E' \to F$ sao cho: $\forall x \in E,\ g(x) = f(x)$.

Ký hiệu $\mathrm{i} : E \to E'$ là ánh xạ nhúng chính tắc, g là một thác triển của f trên E' khi và chỉ khi $g \circ \mathrm{i} = f$.

NHẬN XÉT:

Nếu đã cho $f : E \to F$ và E', f có (trừ ngoại lệ) nhiều hơn một thác triển trên E'. Chẳng hạn $f : \begin{array}{c} \mathbb{R}^* \to \mathbb{R} \\ x \mapsto \frac{\sin x}{x} \end{array}$ có vô số thác triển trên $\mathbb{R}$, chúng là các ánh xạ

$$\begin{array}{c} \mathbb{R} \to \mathbb{R} \\ x \mapsto \begin{cases} \frac{\sin x}{x} & \text{nếu } x \neq 0 \\ \alpha & \text{nếu } x = 0 \end{cases} \end{array}, \alpha \in \mathbb{R}.$$

Trong các thác triển này, có một ánh xạ dáng chú ý là $g : \begin{array}{c} \mathbb{R} \to \mathbb{R} \\ x \mapsto \begin{cases} \frac{\sin x}{x} & \text{nếu } x \neq 0 \\ 1 & \text{nếu } x = 0 \end{cases} \end{array}$ vì đó là thác triển duy nhất liên tục tại 0.

♦ **Định nghĩa 3** Cho E, F là hai tập hợp, $f : E \to F$ là một ánh xạ, $A \in \mathfrak{P}(E)$, $B \in \mathfrak{P}(E)$ sao cho:

$$\forall a \in A, \quad f(a) \in B$$

Ánh xạ cảm sinh bởi f **trên** A **(ở nguồn) và** B **(ở đích)** là ánh xạ $\begin{array}{c} A \to B \\ x \mapsto f(x) \end{array}$

Đặc biệt, cho $f : E \to E$ là một ánh xạ và A là một bộ phận của E ổn định đối với f; ánh xạ cảm sinh bởi f trên A ở nguồn và A ở đích được gọi là **ánh xạ cảm sinh bởi** f **trên** A và thường được ký hiệu f_A. Vậy ta có $f_A : \begin{array}{c} A \to A \\ x \mapsto f(x) \end{array}$

1.3.4 Thứ tự và ánh xạ

1) Tính đơn điệu

◆ **Định nghĩa** Cho $(E, \preccurlyeq)$, $(F, \preccurlyeq)$ là hai tập hợp được sắp thứ tự. Một ánh xạ $f : E \to F$ được gọi là ánh xạ:

- **tăng** khi và chỉ khi: $\forall (x, y) \in E^2, (x \preccurlyeq y \Rightarrow f(x) \preccurlyeq f(y))$
- **giảm** khi và chỉ khi: $\forall (x, y) \in E^2, (x \preccurlyeq y \Rightarrow f(y) \preccurlyeq f(x))$
- **đơn điệu** khi và chỉ khi: f là tăng hoặc giảm.
- **tăng nghiêm ngặt** khi và chỉ khi: $\forall (x, y) \in E^2, (x \prec y \Rightarrow f(x) \prec f(y))$.
- **giảm nghiêm ngặt** khi và chỉ khi: $\forall (x, y) \in E^2, (x \prec y \Rightarrow f(y) \prec f(x))$.
- **đơn điệu nghiêm ngặt** khi và chỉ khi: f là tăng nghiêm ngặt hoặc giảm nghiêm ngặt.

VÍ DỤ:

1) Ánh xạ $f : \begin{matrix} \mathbb{N}^* \to \mathbb{N}^* \\ x \mapsto x^2 \end{matrix}$ tăng nghiêm ngặt nếu ta trang bị cho $\mathbb{N}^*$ (nguồn và đích) thứ tự | (tính chia hết).

2) Ánh xạ : $E : \begin{matrix} \mathbb{R} \to \mathbb{Z} \\ x \mapsto E(x) \end{matrix}$ (phần nguyên) là tăng, nhưng không tăng nghiêm ngặt (đối với thứ tự ≤ thông thường).

3) Với mọi tập hợp E, ánh xạ $\begin{matrix} \mathfrak{P}(E) \to \mathfrak{P}(E) \\ X \mapsto \complement_E(X) \end{matrix}$ là giảm nghiêm ngặt đối với thứ tự bao hàm.

4) Ánh xạ $\begin{matrix} \mathbb{R} \to \mathbb{R} \\ x \mapsto x^2 \end{matrix}$ không đơn điệu (đối với thứ tự thông thường).

2) Thứ tự cảm sinh trên F^X bởi một thứ tự của F

Ta chứng minh dễ dàng mệnh đề sau:

◆ **Mệnh đề** Cho X là một tập hợp, $(F, \preccurlyeq)$ là một tập hợp được sắp thứ tự.

Quan hệ trong F^X, cũng được ký hiệu là $\preccurlyeq$, được xác định bởi:

$$f \preccurlyeq g \Leftrightarrow (\forall x \in X,\ f(x) \preccurlyeq g(x))$$

là một quan hệ thứ tự trên F^X.

NHẬN XÉT:

Dù thứ tự trên F là toàn phần thì thứ tự trên F^X cũng có thể không toàn phần. Ví dụ như, với $X = F = \{0, 1\}$, được sắp bởi thứ tự ≤ thông thường, các phần tử f, g của F^X xác định bởi $f(0) = 0, f(1) = 1, g(0) = 1, g(1) = 0$ không so sánh với nhau được đối với ≤.

Bài tập

◊ **1.3.12** Cho E là một tập hợp, $(F, \preccurlyeq)$ là một tập được sắp thứ tự, $f : E \to F$ là một đơn ánh. Ta định nghĩa trong E một quan hệ $\mathcal{R}$ bởi: $x \mathcal{R} y \Leftrightarrow f(x) \preccurlyeq f(y)$.

Chứng minh rằng $\mathcal{R}$ là một quan hệ thứ tự trên E.

◊ **1.3.13** Cho $(E, \preccurlyeq)$, $(F, \preccurlyeq)$, $(G, \preccurlyeq)$ là ba tập được sắp thứ tự, $f : E \to F$, $g : F \to G$ là hai ánh xạ.

a) Nếu f và g đơn điệu (tương ứng: đơn điệu nghiêm ngặt), thì có thể nói gì về $g \circ f$?

b) Cho một ví dụ trong đó f tăng và là song ánh, nhưng f^{-1} không tăng.

c) Chứng minh rằng, nếu f tăng và là đơn ánh, thì f tăng nghiêm ngặt.

d) Chứng minh rằng, nếu f là tăng nghiêm ngặt và nếu thứ tự $\preccurlyeq$ của E là toàn phần, thì f là đơn ánh.

◊ **1.3.14** Cho E là một tập hợp, $f : \mathfrak{P}(E) \to \mathfrak{P}(E)$ là một ánh xạ. Chứng minh rằng hai tính chất sau là tương đương:

(i) $\forall X, Y \in \mathfrak{P}(E), f(X \cup Y) \supset f(f(X)) \cup f(Y) \cup Y$

(ii) $\forall X, Y \in \mathfrak{P}(E), \begin{cases} f(X) \supset X \\ f(f(X)) = f(X) \\ X \subset Y \Rightarrow f(X) \subset f(Y) \end{cases}$.

(Lưu ý rằng $f(X)$ không chỉ ảnh bởi f của một bộ phận X, xem 1.3.5, Định nghĩa dưới đây, mà chỉ ảnh của một phần tử X của tập nguồn của f).

◊ **1.3.15** Cho $(E, \preccurlyeq)$, $(F, \preccurlyeq)$ là hai tập được sắp thứ tự, $f : E \to F$, $g : F \to E$ đều tăng, $A = \{x \in E; (g \circ f)(x) = x\}$, $B = \{y \in F; (f \circ g)(y) = y\}$.

a) Chứng minh rằng : $\begin{cases} \forall x \in A, f(x) \in B \\ \forall y \in B, g(y) \in A \end{cases}$. Ta ký hiệu f' : $\begin{matrix} A \to B \\ x \mapsto f(x) \end{matrix}$ và g' : $\begin{matrix} B \to A \\ y \mapsto g(y) \end{matrix}$.

b) Chứng minh rằng f' và g' là những song ánh tăng nghiêm ngặt và là ánh xạ ngược của nhau (A và B được trang bị các thứ tự cảm sinh bởi các thứ tự của E và F).

1.3.5 Ảnh và nghịch ảnh của các bộ phận qua một ánh xạ

◆ **Định nghĩa** Cho E, E' là hai tập hợp, $f : E \to E'$ là một ánh xạ.

1) Với mọi bộ phận A của E, ta định nghĩa **ảnh của A bởi f**, ký hiệu là $f(A)$:

$$f(A) = \{x' \in E'; \exists a \in A, x' = f(a)\}.$$

2) Với mọi bộ phận A' của E', ta định nghĩa **nghịch ảnh của A' bởi f**, ký hiệu là $f^{-1}(A')$:

$$f^{-1}(A') = \{x \in E; f(x) \in A'\}.$$

NHẬN XÉT :

1) Ta có: • Với mọi A thuộc $\mathfrak{P}(E)$ và x' thuộc E' : $x' \in f(A) \Leftrightarrow (\exists a \in A, x' = f(a))$

• Với mọi A' thuộc $\mathfrak{P}(E')$ và x thuộc E : $x \in f^{-1}(A') \Leftrightarrow f(x) \in A'$.

Điều này chứng tỏ tính toán với các nghịch ảnh "đơn giản" hơn là tính toán với các ảnh.

2) Ký hiệu $f^{-1}(A')$ (trong đó A' là một bộ phận của E') không giả thiết f là song ánh. Độc giả có thể chứng minh rằng, nếu $f : E \to E'$ là song ánh, thì, với mọi A' thuộc $\mathfrak{P}(E')$, ảnh của A' bởi f^{-1} cũng là nghịch ảnh của A' bởi f.

Ta có thể chứng minh, xem như bài tập, các kết quả sau đây:

Mệnh đề Cho E, E' là hai tập hợp, $f : E \to E'$ là một ánh xạ.

1) Với mọi bộ phận A, B của E, ta có:

- $A \subset B \Rightarrow f(A) \subset f(B)$
- $f(A \cup B) = f(A) \cup f(B)$
- $f(A \cap B) \subset f(A) \cap f(B)$.

2) Với mọi bộ phận A', B' của E', ta có:

- $A' \subset B' \Rightarrow f^{-1}(A') \subset f^{-1}(B')$
- $f^{-1}(A' \cup B') = f^{-1}(A') \cup f^{-1}(B')$
- $f^{-1}(A' \cap B') = f^{-1}(A') \cap f^{-1}(B')$
- $f^{-1}(\complement_{E'}(A')) = \complement_E(f^{-1}(A'))$.

3) • $\forall A \in \mathfrak{P}(E), A \subset f^{-1}(f(A))$

• $\forall A' \in \mathfrak{P}(E'), f(f^{-1}(A')) \subset A'$.

Bài tập

◊ **1.3.16** Cho E, F là hai tập hợp, $f : E \to F, g : F \to E$ là hai ánh xạ thỏa mãn $f \circ g = \mathrm{Id}_F$. Chứng minh: $(g \circ f)(E) = g(F)$.

◊ **1.3.17** Cho hai tập hợp $E, E', f : E \to E'$. Chứng minh:

$$\forall A' \in \mathfrak{P}(E'), \quad f(f^{-1}(A')) = A' \cap f(E).$$

◊ **1.3.18** Cho hai tập hợp $E, E', f : E \to E'$. Chứng minh f là song ánh khi và chỉ khi: $\forall A \in \mathfrak{P}(E), \quad f(\complement_E(A)) = \complement_{E'}(f(A))$.

◊ **1.3.19** Cho hai tập hợp $E, E', f : E \to E'$. Chứng minh rằng các tính chất sau đây là tương đương:

(i) f là toàn ánh

(ii) $\forall y \in E', f(f^{-1}(\{y\})) = \{y\}$

(iii) $\forall A' \in \mathfrak{P}(E'), f(f^{-1}(A')) = A'$

(iv) $\forall A' \in \mathfrak{P}(E'), (f^{-1}(A') = \varnothing \Rightarrow A' = \varnothing)$.

◊ **1.3.20** Cho hai tập hợp $E, E', f: E \to E'$.

a) Chứng minh: $\forall A', B' \in \mathfrak{P}(E'),\ f^{-1}(A' \,\Delta\, B') = f^{-1}(A') \,\Delta\, f^{-1}(B')$.

b) Chứng minh f là đơn ánh khi và chỉ khi: $\forall A, B \in \mathfrak{P}(E),\ f(A \,\Delta\, B) = f(A) \,\Delta\, f(B)$.

◊ **1.3.21** Cho E là một tập hợp, $\mathcal{A}$ là một tập con của E^E, $F = \{X \in \mathfrak{P}(E), \forall f \in \mathcal{A},\ f(X) \subset X\}$.

Chứng minh rằng trong F mọi tập con khác rỗng của F có một biên trên và một biên dưới đối với thứ tự bao hàm.

1.3.6 Họ

◆ **Định nghĩa 1** Cho một tập hợp E. **Họ phần tử của** E là một ánh xạ bất kỳ có tập đích là E.

Một họ phần tử của một tập hợp E được ký hiệu $(x_i)_{i \in I}$ thay vì $\underset{i \mapsto x(i)}{I \to E}$; tập nguồn I của họ được gọi là **tập chỉ số** của họ.

Chẳng hạn, một dãy là một họ mà tập chỉ số là $\mathbb{N}$.

Một họ $(x_i)_{i \in I}$ được gọi là **hữu hạn** khi và chỉ khi I là một tập hợp hữu hạn. Nếu $I = \{1, ..., p\}$ trong đó $p \in \mathbb{N}^*$, thì $(x)_{i \in I}$ cũng được ký hiệu là $(x_i)_{1 \le i \le p}$ và được xem như trùng với bộ - p $(x_1, ..., x_p)$ (xem 1.2.1).

Họ con của một họ $(x_i)_{i \in I}$ những phần tử thuộc E là một họ $(x_j)_{j \in J}$, trong đó J là một bộ phận của I. Ký hiệu $\varphi : \underset{j \mapsto j}{J \to I}$ là ánh xạ nhúng chính tắc và f là họ $(x_i)_{i \in I}$ (tức là : $f : \underset{i \mapsto x_i}{I \to E}$), thì họ con $(x_j)_{j \in J}$ là $f \circ \varphi : \underset{j \mapsto x_j}{J \to E}$. Chẳng hạn một dãy trích từ một dãy $(x_n)_{n \in \mathbb{N}}$ là một họ con của $(x_n)_{n \in \mathbb{N}}$ mà tập chỉ số là vô hạn.

◆ **Định nghĩa 2** Cho một tập hợp E, $(A_i)_{i \in I}$ là một họ những bộ phận của E. Ta định nghĩa:

- **Hợp của họ** $(A_i)_{i \in I}$, ký hiệu là $\bigcup_{i \in I} A_i$, bởi:

$$\bigcup_{i \in I} A_i = \{x \in E;\ \exists i \in I, x \in A_i\}$$

- **Giao của họ** $(A_i)_{i \in I}$, ký hiệu là $\bigcap_{i \in I} A_i$, bởi:

$$\bigcap_{i \in I} A_i = \{x \in E;\ \forall i \in I, x \in A_i\}.$$

Như thế, với mỗi x thuộc E, ta có:

- $x \in \bigcup_{i \in I} A_i \Leftrightarrow (\exists i \in I, x \in A_i)$
- $x \in \bigcap_{i \in I} A_i \Leftrightarrow (\forall i \in I, x \in A_i)$.

Trường hợp đặc biệt, theo định nghĩa ta có: $\bigcup_{i \in \varnothing} A_i = \varnothing$ và $\bigcap_{i \in \varnothing} A_i = E$.

◆ **Định nghĩa 3** Cho một tập hợp E. Một họ $(A_i)_{i\in I}$ những bộ phận của E được gọi là một **phân hoạch** của E khi và chỉ khi:

(i) $\forall i \in I, A_i \neq \varnothing$

(ii) $\forall (i,j) \in I^2, (i \neq j \Rightarrow A_i \cap A_j = \varnothing)$

(iii) $\bigcup_{i\in I} A_i = E$.

Định nghĩa này là hoàn toàn tương thích với định nghĩa đã thấy ở 1.1.4, Định nghĩa 2, bởi vì muốn cho $(A_i)_{i\in I}$ là một phân hoạch theo định nghĩa trên, cần và đủ là $\{A_i; i \in I\}$ là một phân hoạch của E theo nghĩa của 1.1.4, Định nghĩa 2.

Chẳng hạn, $\{[n; n+1[; n \in \mathbb{Z}\}$ và $([n; n+1[)_{n\in\mathbb{Z}}$ là những phân hoạch của $\mathbb{R}$.

Bài tập

◊ **1.3.22** Cho tập hợp E. Chứng minh các công thức sau, đối với mọi họ những bộ phận của E và mọi bộ phận của E:

a) $\complement_E\left(\bigcup_{i\in I} A_i\right) = \bigcap_{i\in I} \complement_E(A_i)$, $\complement_E\left(\bigcap_{i\in I} A_i\right) = \bigcup_{i\in I} \complement_E(A_i)$

b) $\left(\bigcup_{i\in I} A_i\right) \cap B = \bigcup_{i\in I} (A_i \cap B)$, $\left(\bigcap_{i\in I} A_i\right) \cup B = \bigcap_{i\in I} (A_i \cup B)$

c) $\left(\bigcup_{i\in I} A_i\right) \cap \left(\bigcup_{j\in J} B_j\right) = \bigcup_{(i,j)\in I\times J} (A_i \cap B_j)$, $\left(\bigcap_{i\in I} A_i\right) \cup \left(\bigcap_{j\in J} B_j\right) = \bigcap_{(i,j)\in I\times J} (A_i \cup B_j)$

d) $(\forall i \in I, A_i \subset B_i) \Rightarrow \begin{cases} \bigcup_{i\in I} A_i \subset \bigcup_{i\in I} B_i \\ \bigcap_{i\in I} A_i \subset \bigcap_{i\in I} B_i \end{cases}$

e) $\bigcap_{i\in I} (A_i - B_i) = \left(\bigcap_{i\in I} A_i\right) - \left(\bigcup_{i\in I} B_i\right)$.

◊ **1.3.23** Cho E, E' là hai tập hợp, $f : E \to E'$ là một ánh xạ.

a) Với mỗi họ $(A'_i)_{i\in I}$ những bộ phận của E', chứng minh:

$$f^{-1}\left(\bigcup_{i\in I} A'_i\right) = \bigcup_{i\in I} f^{-1}(A'_i), \qquad f^{-1}\left(\bigcap_{i\in I} A'_i\right) = \bigcap_{i\in I} f^{-1}(A'_i).$$

b) Với mọi họ $(A_i)_{i\in I}$ những bộ phận của E, chứng minh:

$$f\left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I} f(A_i), \qquad f\left(\bigcap_{i\in I} A_i\right) \subset \bigcap_{i\in I} f(A_i).$$

c) Chứng minh rằng, nếu f là đơn ánh, thì, với mọi họ $(A_i)_{i\in I}$ những bộ phận của E:

$$f\left(\bigcap_{i\in I} A_i\right) = \bigcap_{i\in I} f(A_i).$$

◊ **1.3.24** Cho một tập hợp E, $f,\ g : E \to E$.

a) Giả sử $A \in \mathfrak{P}(E)$.

α) Chứng minh rằng, nếu A ổn định đối với f và đối với g, thì A ổn định đối với $g \circ f$.

β) Suy ra rằng, nếu A ổn định đối với f, thì dãy $(f^n(A))_{n \in \mathbb{N}}$ là dãy giảm, trong đó $f^0 = \mathrm{Id}_E$, $f^1 = f$, $f^n = f \circ \ldots \circ f$ (n nhân tử).

γ) Chứng minh rằng, nếu A ổn định đối với f và nếu tồn tại $n \in \mathbb{N}^*$ sao cho $f^n(A) = A$, thì $f(A) = A$.

b) Cho $(A_i)_{i \in I}$ là một họ những bộ phận của E. Chứng minh rằng, nếu mọi A_i ($i \in I$) đều ổn định đối với f, thì $\bigcup_{i \in I} A_i$ và $\bigcap_{i \in I} A_i$ ổn định đối với f.

◊ **1.3.25** a) Cho E, E' là hai tập hợp, $f : E \to E'$ là một toàn ánh. Chứng minh rằng, với mọi phân hoạch $(A'_i)_{i \in I}$ của E', họ $(f^{-1}(A'_i))_{i \in I}$ là một phân hoạch của E.

b) Cho một ví dụ về các tập E, E', toàn ánh $f : E \to E'$ và phân hoạch $(A_i)_{i \in I}$ của E, sao cho $(f(A_i))_{i \in I}$ không phải là một phân hoạch của E'.

Bổ sung

◊ C 1.1* Tính tương thích giữa các quan hệ tương đương và ánh xạ

A Tính tương thích

Cho E, F là hai tập hợp, $\mathcal{R}$ (tương ứng: $\mathcal{S}$) là một quan hệ tương đương trong E (tương ứng: F), $f : E \to F$ là một ánh xạ. Ta nói rằng f **tương thích** với $\mathcal{R}$ và $\mathcal{S}$ khi và chỉ khi:

$$\forall (x, x') \in E^2, \quad (x \mathcal{R} x' \Rightarrow f(x) \, \mathcal{S} \, f(x')).$$

1) Cho E, F là hai tập hợp, $\mathcal{R}$ (tương ứng: $\mathcal{S}$) là một quan hệ tương đương trong E (tương ứng: F), $p : E \to E/\mathcal{R}$ (tương ứng: $q : F \to F/\mathcal{S}$) là toàn ánh chính tắc, $f : E \to F$ là một ánh xạ.

Chứng minh rằng điều kiện cần và đủ để tồn tại $\varphi : E/\mathcal{R} \to F/\mathcal{S}$ sao cho biểu đồ sau giao hoán (tức là: $\varphi \circ p = q \circ f$), là f phải tương thích với $\mathcal{R}$ và $\mathcal{S}$ và, nếu f tương thích với $\mathcal{R}$ và $\mathcal{S}$, thì φ là duy nhất.

$$\begin{array}{ccc} E & \xrightarrow{\ f\ } & F \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle q} \\ E/\mathcal{R} & \xrightarrow[\ \varphi\ ]{} & F/\mathcal{S} \end{array}$$

Nếu f tương thích với $\mathcal{R}$ và $\mathcal{S}$, ta ký hiệu $\widetilde{f}$ là ánh xạ duy nhất từ $E/\mathcal{R}$ vào $F/\mathcal{S}$ sao cho $\widetilde{f} \circ p = q \circ f$; ta nói rằng $\widetilde{f}$ thu được từ f bằng cách **chuyển sang các tập thương**.

2) a) Cho E, F, G là ba tập hợp, $\mathcal{R}$ (tương ứng: $\mathcal{S}$, tương ứng: $\mathcal{T}$) là một quan hệ tương đương trong E (tương ứng: F, tương ứng: G), $f : E \to F$ là một ánh xạ tương thích với $\mathcal{R}$ và $\mathcal{S}$, $g : F \to G$ là một ánh xạ tương thích với $\mathcal{S}$ và $\mathcal{T}$. Chứng minh $g \circ f : E \to G$ tương thích với $\mathcal{R}$ và $\mathcal{T}$, và $\widetilde{g \circ f} = \widetilde{g} \circ \widetilde{f}$.

b) Cho E là một tập hợp và $\mathcal{R}$ là một quan hệ tương đương trong E. Kiểm chứng rằng Id_E tương thích với $\mathcal{R}$ và $\mathcal{R}$, và $\widetilde{\mathrm{Id}_E} = \mathrm{Id}_{E/\mathcal{R}}$

B Phân tích chính tắc của một ánh xạ

1) Cho E, F là hai tập hợp, $f : E \to F$ là một ánh xạ.

a) Chứng minh rằng quan hệ $\mathcal{R}_f$ xác định trong E bởi:

$$x \, \mathcal{R}_f \, x' \Leftrightarrow f(x) = f(x')$$

là một quan hệ tương đương.

b) Ta ký hiệu $i : f(E) \to F$ là đơn ánh chính tắc và $p : E \to E/\mathcal{R}_f$ là toàn ánh chính tắc.

Chứng minh tồn tại một ánh xạ $\hat{f} : E/\mathcal{R}_f \to f(E)$ duy nhất sao cho $f = i \circ \hat{f} \circ p$, và $\hat{f}$ là song ánh.

Ta nói rằng hệ thức $f = i \circ \hat{f} \circ p$ là **dạng phân tích chính tắc** của f.

2) *Ví dụ*

a) Xác định dạng phân tích chính tắc của ánh xạ phần nguyên E : $\begin{array}{c} \mathbf{R} \to \mathbf{R} \\ x \mapsto \mathrm{E}(x) \end{array}$.

b) Cho E là một tập hợp, $A \in \mathfrak{P}(E)$,

$$f : \begin{array}{c} \mathfrak{P}(E) \to \mathfrak{P}(E) \\ X \mapsto X \cap A \end{array}, \quad g : \begin{array}{c} \mathfrak{P}(E) \to \mathfrak{P}(E) \\ X \mapsto X \cup A \end{array}.$$

Xác định các dạng phân tích chính tắc của f và g.

Chương 2

Cấu trúc đại số

2.1 Luật hợp thành trong

♦ **Định nghĩa 1** **Luật hợp thành trong** (viết tắt: **lhtt**) trên một tập hợp E là mọi ánh xạ từ $E \times E$ vào E.

Một lhtt trên E thường được ký hiệu là $*$: $E \times E \to E$, hoặc $\top$, $\perp$, $+$, $\cdot$, $\circ$, ...
$(x, y) \mapsto x*y$

Đôi khi ta nói **luật** thay cho luật hợp thành trong.

VÍ DỤ:

1) Phép cộng và phép nhân là những lhtt trong $\mathbb{N}$.

2) Với tập hợp X bất kỳ, phép hợp và phép giao là những lhtt trong $\mathfrak{P}(X)$.

♦ **Định nghĩa 2** **Phỏng nhóm** (magma) là một cặp $(E, *)$ trong đó E là một tập hợp và $*$ là một lhtt trong E.

♦ **Định nghĩa 3** Một lhtt $*$ trong một tập hợp E được gọi là **kết hợp** khi và chỉ khi: $\forall (x, y, z) \in E^3, (x * y) * z = x * (y * z)$.

Thay cho câu "$*$ là kết hợp", ta cũng nói: phỏng nhóm $(E, *)$ là kết hợp.

VÍ DỤ:

1) Phép cộng và phép nhân trong $\mathbb{C}$ là kết hợp.

2) Lhtt $*$: $\mathbb{Q}^2 \to \mathbb{Q}$, $(x,y) \mapsto \frac{x+y}{2}$ không kết hợp, vì $((-1) * 0) * 1 = \frac{1}{4}$ và $(-1) * (0 * 1) = -\frac{1}{4}$.

♦ **Ký hiệu** Cho E là một tập hợp, $*$ hoặc $\cdot$ hoặc $+$ là một lhtt kết hợp trong E, $n \in \mathbb{N}^*$, $x_1, ..., x_n \in E$, $x \in E$. Ta ký hiệu:

$$\underset{i=1}{\overset{n}{*}} x_i = x_1 * x_2 * ... * x_n,$$

$$\prod_{i=1}^{n} x_i = x_1 x_2 ... x_n, \quad \sum_{i=1}^{n} x_i = x_1 + x_2 + ... + x_n,$$

$$x^n = x * x * .... * x, \quad x^n = xx ... x, \quad nx = x + x + ... + x$$

(n hạng tử hoặc nhân tử) (đặc biệt: $x^1 = x$).

Ta nói rằng hai phần tử x, y của một phỏng nhóm $(E, *)$ là **giao hoán** (hoặc: **có thể hoán vị**) khi và chỉ khi: $x * y = y * x$.

◆ **Định nghĩa 4** Một lhtt $*$ trong một tập hợp E được gọi là **giao hoán** khi và chỉ khi: $\forall (x, y) \in E^2, \quad x * y = y * x$.

VÍ DỤ:

1) Phép cộng và phép nhân trong $\mathbb{C}$ là giao hoán.

2) Phép trừ trong $\mathbb{C}$ là không giao hoán.

Ta chứng minh dễ dàng (bằng lập luận quy nạp) Mệnh đề sau:

◆ **Mệnh đề 1** Cho E là một tập hợp được trang bị một lhtt kết hợp và giao hoán, ký hiệu là $+$. Thế thì:

1) $\forall n \in \mathbb{N}^*, \forall (x_1, ..., x_n) \in E^n, \forall (y_1, ...y_n) \in E^n,$

$$\sum_{i=1}^{n} (x_i + y_i) = \sum_{i=1}^{n} x_i + \sum_{i=1}^{n} y_i$$

2) $\forall (n, p) \in (\mathbb{N}^*)^2, \forall (x_{ij})_{1 \le i \le n,\ 1 \le j \le p} \in E^{np}, \quad \sum_{i=1}^{n} \left(\sum_{j=1}^{p} x_{ij} \right) = \sum_{j=1}^{p} \left(\sum_{i=1}^{n} x_{ij} \right).$

3) $\forall n \in \mathbb{N}^*, \forall \sigma \in \mathfrak{S}_n, \forall (x_1, ..., x_n) \in E^n, \quad \sum_{i=1}^{n} x_{\sigma(i)} = \sum_{i=1}^{n} x_i$.

(Xem 3.3.1, về nhóm đối xứng $\mathfrak{S}_n$).

◆ **Định nghĩa 5** Cho $(E, *)$ là một phỏng nhóm, $a \in E$.

1) Ta nói rằng a là **chính quy** (hoặc: **giản ước được**) **trái** đối với $*$, khi và chỉ khi:

$$\forall (x, y) \in E^2, \quad (a * x = a * y \Rightarrow x = y).$$

2) Ta nói rằng a là **chính quy** (hoặc: **giản ước được**) **phải** đối với $*$, khi và chỉ khi:

$$\forall (x, y) \in E^2, \quad (x * a = y * a \Rightarrow x = y).$$

3) Ta nói rằng a là **chính quy** (hoặc: **giản ước được**) đối với $*$ khi và chỉ khi a là chính quy trái và phải đối với $*$, tức là:

$$\forall (x, y) \in E^2, \quad \begin{cases} a * x = a * y \Rightarrow x = y \\ x * a = y * a \Rightarrow x = y \end{cases}.$$

VÍ DỤ:

1) Trong $\mathbb{C}$ mọi phần tử đều chính quy đối với $+$.

2) Các phần tử chính quy của $\mathbb{C}$ đối với $\bullet$ là các số phức $\neq 0$.

3) Với $n \in \mathbb{N}^*$, các phần tử chính quy của $\mathbf{M}_n(\mathbb{C})$ là các ma trận thuộc $\mathbf{M}_n(\mathbb{C})$ có định thức $\neq 0$ (xem 9.4, Mệnh đề 2) 4)).

◆ **Định nghĩa 6** Cho $(E, *)$ là một phỏng nhóm, $e \in E$.

1) Ta nói rằng e là **trung hòa trái** đối với $*$ khi và chỉ khi: $\forall x \in E, e * x = x$.

2) Ta nói rằng e là **trung hòa phải** đối với $*$ khi và chỉ khi: $\forall x \in E, x * e = x$.

3) Ta nói rằng e là **trung hòa** đối với $*$ khi và chỉ khi e vừa là trung hòa trái vừa là trung hòa phải đối với $*$, tức là: $\forall x \in E, e * x = x * e = x$.

Ta cũng nói phần tử trung hòa thay cho trung hòa.

VÍ DỤ:

1) 0 là trung hòa đối với + trong $\mathbb{N}$.

2) Đối với lhtt $*$: $\mathbb{N}^2 \to \mathbb{N}$, $(x, y) \mapsto y$, mọi phần tử của $\mathbb{N}$ là trung hòa trái và không có một phần tử nào của $\mathbb{N}$ là trung hòa phải.

◆ **Ký hiệu** Nếu $(E, *)$ là một phỏng nhóm có một phần tử trung hòa ký hiệu là e, thì, với mọi x thuộc E, ta ký hiệu: $x^0 = e$.

◆ **Mệnh đề 2 (Tính duy nhất của phần tử trung hòa, nếu nó tồn tại)** Nếu e, e' là hai phần tử trung hòa đối với $*$ trong E, thì $e = e'$.

Chứng minh:

Tổng quát hơn, nếu e là phần tử trung hòa trái và nếu e' là phần tử trung hòa phải, thì $e = e'$, vì $e * e' = e'$ (do e là phần tử trung hòa trái) và $e * e' = e$ (do e' là phần tử trung hòa phải).

◆ **Định nghĩa 7** **Vị nhóm** là một phỏng nhóm $(E, *)$ thỏa mãn:

$$\begin{cases} * \text{ là kết hợp} \\ E \text{ có phần tử trung hòa đối với } *. \end{cases}$$

VÍ DỤ:

- $(\mathbb{N}, +)$ và $(\mathbb{N}, \times)$ là những vị nhóm.
- Với mọi tập hợp X, $(\mathfrak{P}(X), \cap)$, $(\mathfrak{P}(X), \cup)$ là những vị nhóm.
- Với mọi tập hợp X, $(X^X, \circ)$ là một vị nhóm.

◆ **Định nghĩa 8** Cho $(E, *)$ là một phỏng nhóm có phần tử trung hòa e.

Một phần tử x của E được nói là **khả đối xứng** (hay: **khả nghịch**) đối với $*$ khi và chỉ khi tồn tại ít nhất một phần tử y của E sao cho $x * y = y * x = e$; một phần tử y như thế (nếu tồn tại) được gọi là **một đối xứng** của x đối với $*$.

◆ **Mệnh đề 3** Cho $(E, *)$ là một vị nhóm, và $x \in E$. Nếu x khả đối xứng đối với $*$, thì x có một và chỉ một đối xứng đối với $*$.

Chứng minh:

Giả sử $y, z \in E$ sao cho $\begin{cases} x * y = y * x = e \\ x * z = z * x = e \end{cases}$.

♦ **Ký hiệu** Cho $(E, *)$ là một vị nhóm, x là một phần tử của E khả đối xứng đối với $*$. Đối xứng của x được ký hiệu là x^{-1}, và cũng gọi là **nghịch đảo** của x. Khi luật ký hiệu là $+$, thì đối xứng của x (nếu nó tồn tại) được ký hiệu $-x$ và cũng gọi **đối** của x.

♦ **Mệnh đề 4** Cho $(E, *)$ là một vị nhóm, $x, y \in E$. Nếu x và y khả đối xứng đối với $*$, thì $x * y$ khả đối xứng đối với $*$ và:

$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

Chứng minh:

$(y^{-1} * x^{-1}) * (x * y) = (y^{-1} * (x^{-1} * x)) * y = y^{-1} * y = e$ và tương tự: $(x * y) * (y^{-1} * x^{-1}) = e$.

♦ **Định nghĩa 9** Cho E là một tập hợp, $*$, $\top$ là hai luật hợp thành trong E.

1) Ta nói rằng $\top$ **phân phối trái** (tương ứng: **phải**) **trên** (hoặc: **đối với**) $*$ khi và chỉ khi:

$$\forall (x, y, z) \in E^3, \quad x \top (y * z) = (x \top y) * (x \top z)$$

(tương ứng: $(y * z) \top x = (y \top x) * (z \top x)$).

2) Ta nói rằng $\top$ là **phân phối trên** (hoặc: **đối với**) $*$ khi và chỉ khi $\top$ vừa phân phối trái vừa phân phối phải đối với $*$.

VÍ DỤ:

1) Trong $\mathbb{R}$, phép nhân phân phối đối với phép cộng.

2) Với tập hợp bất kỳ X, mỗi một trong hai luật $\cup$, $\cap$ phân phối đối với luật kia trong $\mathfrak{P}(X)$.

♦ **Định nghĩa 10** Cho hai phỏng nhóm $(E, *)$, $(F, \top)$, **đồng cấu phỏng nhóm** (hoặc: **đồng cấu**) từ $(E, *)$ vào $(F, \top)$ là mọi ánh xạ $f : E \to F$ sao cho:

$$\forall (x, y) \in E^2, \quad f(x * y) = f(x) \top f(y).$$

Một **tự đồng cấu của một phỏng nhóm** $(E, *)$ là một đồng cấu phỏng nhóm từ $(E, *)$ vào $(E, *)$.

Một **đẳng cấu phỏng nhóm** là một đồng cấu song ánh của phỏng nhóm.

Một **tự đẳng cấu của một phỏng nhóm** $(E, *)$ là một tự đồng cấu song ánh của phỏng nhóm $(E, *)$.

Ta có thể ký hiệu một đồng cấu phỏng nhóm là $f : (E, *) \to (F, \top)$.

VÍ DỤ:

1) Ánh xạ $\ln : \begin{array}{ccc} \mathbb{R}_+^* & \to & \mathbb{R} \\ x & \mapsto & \ln x \end{array}$ là một đẳng cấu từ phỏng nhóm $(\mathbb{R}_+^*, \times)$ lên phỏng nhóm $(\mathbb{R}, +)$.

2) Cho E là một tập hợp, $*$, $\top$ là hai lhtt trong E. Muốn cho $\top$ phân phối trái (tương ứng: phải) đối với $*$, điều kiện cần và đủ là ánh xạ $\gamma_a : \begin{array}{ccc} E & \to & E \\ x & \mapsto & a \top x \end{array}$ (tương ứng $\delta_a : \begin{array}{ccc} E & \to & E \\ x & \mapsto & x \top a \end{array}$) là một tự đồng cấu của phỏng nhóm $(E, *)$, với mọi a thuộc E.

♦ **Mệnh đề 5**

1) Nếu $f : (E, *) \to (F, \top)$ và $g : (F, \top) \to (G, \perp)$ là hai đồng cấu phỏng nhóm, thì $g \circ f : E \to G$ là một đồng cấu phỏng nhóm từ $(E, *)$ vào $(G, \perp)$.

2) Với mọi phỏng nhóm $(E, *)$, $\mathrm{Id}_E : \underset{x \mapsto x}{E \to E}$ là một tự đẳng cấu của phỏng nhóm $(E, *)$.

3) Nếu $f : (E, *) \to (F, \top)$ là một đẳng cấu phỏng nhóm, thì $f^{-1} : F \to E$ là một đẳng cấu của phỏng nhóm $(F, \top)$ lên phỏng nhóm $(E, *)$.

Chứng minh:

1) $\forall (x, y) \in E^2$, $(g \circ f)(x * y) = g(f(x) \top f(y)) = (g \circ f)(x) \perp (g \circ f)(y)$.

2) Hiển nhiên.

3) Vì f là song ánh, nên ánh xạ ngược $f^{-1} : F \to E$ tồn tại, và với mọi (u, v) thuộc F^2 ta có: $u \top v = f(f^{-1}(u)) \top f(f^{-1}(v)) = f(f^{-1}(u) * f^{-1}(v))$,
do đó bằng cách hợp bằng f^{-1}, ta được: $f^{-1}(u \top v) = f^{-1}(u) * f^{-1}(v)$.

♦ **Định nghĩa 11** Cho X là một tập hợp, $(E, *)$ là một phỏng nhóm. Ta có thể trang bị E^X một luật hợp thành trong, vẫn ký hiệu là $*$, được xác định bởi:

$$\forall f, g \in E^X, \quad \forall x \in X, \quad (f * g)(x) = f(x) * g(x),$$

và được gọi là **khuyếch** ra E^X của luật $*$ trên E.

VÍ DỤ:
Nếu $f, g : \mathbb{R} \to \mathbb{R}$, thì $f + g : \underset{x \mapsto f(x)+g(x)}{\mathbb{R} \to \mathbb{R}}$

♦ **Định nghĩa 12** Cho $(E, *)$ là một phỏng nhóm. Ta có thể trang bị cho $\mathfrak{P}(E)$ một lhtt, vẫn ký hiệu là $*$, được xác định bởi:

$$\forall A, B \in \mathfrak{P}(E), \ A*B = \{x \in E; \exists (a, b) \in A \times B, x = a*b\} = \{a*b; (a, b) \in A \times B\},$$

và được gọi là **khuyếch ra** $\mathfrak{P}(E)$ của luật $*$ trên E.

VÍ DỤ:
Trong $\mathbb{R}$, $\{1, 2\} + \{4, 9\} = \{5, 6, 10, 11\}$, $]-\infty; 0[+]0; +\infty[= \mathbb{R}$.
Với $A = \mathfrak{P}(E)$ và $a \in A$, ta có thể ký hiệu $a * A$ thay cho $\{a\} * A$; ví dụ như, trong $(\mathbb{Z}, \cdot)$ thông thường, với mọi x thuộc $\mathbb{Z}$, $x\mathbb{Z} = \{xn; n \in \mathbb{Z}\}$.

♦ **Định nghĩa 13** Cho $(E, *)$ là một phỏng nhóm. Một bộ phận A của E được nói là **ổn định** đối với $*$ khi và chỉ khi $A * A \subset A$, tức là:

$$\forall (x, y) \in A^2, \quad x * y \in A.$$

Nếu A là một bộ phận của E ổn định đối với $*$, thì lhtt trong A được xác định bởi $\underset{(x,y) \mapsto x*y}{A \times A \to A}$ được gọi là **lhtt cảm sinh trên** A bởi luật $*$ trên E, và cũng được ký hiệu là $*$.

♦ **Định nghĩa 14** **Tích của hai phỏng nhóm** $(E, \top)$, $(F, \perp)$ là một phỏng nhóm $(E \times F, *)$, trong đó $*$ là lhtt trong $E \times F$ được xác định bởi:

$$\forall (x, y), (x', y') \in E \times F, \quad (x, y) * (x', y') = (x \top x', y \perp y').$$

VÍ DỤ:

$\mathbb{R}^2$, được trang bị lhtt + và xác định bởi:

$$\forall (x, y), (x', y') \in \mathbb{R}^2, \quad (x, y) + (x', y') = (x + x', y + y')$$

là tích của phỏng nhóm $(\mathbb{R}, +)$ với chính nó.

Bài tập

◊ **2.1.1** Cho $*$ là lhtt xác định trong $\mathbb{R}$ bởi:

$$x * y = xy + (x^2 - 1)(y^2 - 1).$$

a) Kiểm chứng $*$ giao hoán, không kết hợp và có phần tử trung hòa.

b) Giải các phương trình sau (với ẩn $x \in \mathbb{R}$):

1) $2 * x = 5$ 2) $x * x = 1$.

◊ **2.1.2** Cho $*$ là một lhtt trong $\mathbb{R}$ thỏa mãn:

$$\forall (a, b, c) \in \mathbb{R}^3, \quad \begin{cases} 0 * a = -a \\ a * (b * c) = c * (b * a) \end{cases}.$$

Chứng minh: $\forall (a, b, c) \in \mathbb{R}^3, \quad a * (b * c) = (a * b) * (-c)$.

Cho một ví dụ về luật $*$ như thế.

◊ **2.1.3** Cho $(E, *)$ là một phỏng nhóm kết hợp, $a \in E$, $\top$ là lhtt xác định trong E bởi: $x \top y = x * a * y$. Chứng minh $\top$ có tính kết hợp.

◊ **2.1.4** Cho $(E, \cdot)$ là một phỏng nhóm, $(x, y) \in E^2$; ta giả thiết $\cdot$ là kết hợp và $xy = yx$. Chứng minh:

$$\forall (n, p) \in (\mathbb{N}^*)^2, \quad x^n y^p = y^p x^n.$$

◊ **2.1.5** Cho $(E, *)$ một vị nhóm; chứng minh rằng mọi phần tử của E khả đối xứng đối với $*$ đều chính quy đối với $*$. Cho một ví dụ trong đó khẳng định đảo sai.

◊ **2.1.6** Cho một phỏng nhóm $(E, *)$. Với mọi $a \in E$, ta ký hiệu $\gamma_a : \underset{x \mapsto a*x}{E \to E}$ và $\delta_a : \underset{x \mapsto x*a}{E \to E}$, theo thứ tự được gọi là **tịnh tiến sang trái** và **tịnh tiến sang phải** theo a.

a) Chứng minh rằng, với mọi a thuộc E, γ_a (tương ứng: δ_a) là đơn ánh khi và chỉ khi a là phần tử chính quy trái (tương ứng: phải).

b) Chứng minh rằng $*$ là kết hợp khi và chỉ khi: $\forall (a, b) \in E^2, \quad \gamma_a \circ \delta_b = \delta_b \circ \gamma_a$.

◊ **2.1.7** Cho $(E, *)$ là một phỏng nhóm kết hợp, hữu hạn. Ta giả thiết tồn tại một phần tử x của E chính quy đối với $*$. Chứng minh rằng $*$ có phần tử trung hòa và x là khả đối xứng.

◊ **2.1.8** Cho một phỏng nhóm $(E, *)$. Một phần tử x của E được nói là **lũy đẳng** nếu và chỉ nếu: $x * x = x$.

a) Chứng minh rằng, nếu $*$ là kết hợp và nếu x và y là lũy đẳng và giao hoán, thì $x * y$ là lũy đẳng.

b) Chứng minh rằng, nếu $*$ là kết hợp, có phần tử trung hòa và nếu x là lũy đẳng và khả đối xứng, thì x^{-1} là lũy đẳng.

◊ **2.1.9** Cho một tập hợp E, một lht kết hợp $*$ trong E, một lht $\top$ trong E phân phối đối với $*$.

a) Chứng minh rằng, nếu $x, x', y, y' \in E$ là những phần tử sao cho $x \top x'$ và $y \top y'$ đều chính quy đối với $*$, thì $x \top y'$ và $y \top x'$ giao hoán đối với $*$ (tính $(x * y) \top (x' * y')$ bằng hai cách khác nhau).

b) Suy ra rằng, nếu $\top$ có phần tử trung hòa, thì hai phần tử chính quy đối với $*$ là giao hoán được đối với $*$.

c) Chứng minh rằng, nếu $\top$ có phần tử trung hòa và nếu tất cả các phần tử của E là chính quy đối với $*$, thì $*$ là giao hoán.

◊ **2.1.10** a) Khảo sát (tính kết hợp, giao hoán, tồn tại phần tử trung hòa) luật $*$ xác định trong $]0; +\infty[$ bởi: $x * y = \sqrt{x^2 + y^2}$.

b) Với $(n, a) \in \mathbb{N}^* \times]0; +\infty[$, tính $a * \ldots * a$ (n nhân tử).

◊ **2.1.11** a) Khảo sát (tính kết hợp, giao hoán, tồn tại phần tử trung hòa, tồn tại phần tử đối xứng) luật $*$ xác định trong $\mathbb{R}$ bởi: $x * y = x + y - xy$.

b) Với $(n, a) \in \mathbb{N}^* \times \mathbb{R}$, tính $a * \ldots * a$ (n nhân tử).

◊ **2.1.12** Cho $(E, *)$, $(F, \top)$ là hai phỏng nhóm, $f : E \to F$ là một đồng cấu phỏng nhóm.

a) Chứng minh rằng, nếu một bộ phận A của E ổn định đối với $*$, thì $f(A)$ ổn định đối với $\top$.

b) Chứng minh rằng, nếu một bộ phận B của F ổn định đối với $\top$, thì $f^{-1}(B)$ ổn định đối với $*$.

◊ **2.1.13** Cho X là một tập hợp, $(E, *)$ là một phỏng nhóm, $*$ là luật hợp thành trong trong E^X được xác định bởi (xem Định nghĩa 11):

$$\forall f, g \in E^X, \forall x \in X, \quad (f * g)(x) = f(x) * g(x).$$

Chứng minh rằng, nếu $*$ (trong E) có một trong những tính chất sau, thì $*$ (trong E^X) cũng có tính chất đó:

1) tính kết hợp 2) tính giao hoán 3) tồn tại phần tử trung hòa

4) tồn tại phần tử trung hòa và, với mọi phần tử, tồn tại phần tử đối xứng.

◊ **2.1.14** Cho một phỏng nhóm $(E, *)$; ta cũng ký hiệu $*$ là khuếch của $*$ ra $\mathfrak{P}(E)$ (xem Định nghĩa 12).

a) Chứng minh:

1) $\forall A, B, A', B' \in \mathfrak{P}(E)$, $\begin{cases} A \subset A' \\ B \subset B' \end{cases} \Rightarrow A * B \subset A' * B'$

2) Nếu $*$ có tính kết hợp (tương ứng: giao hoán) trong E, thì $*$ cũng kết hợp (tương ứng: giao hoán) trong $\mathfrak{P}(E)$.

3) Nếu $*$ có phần tử trung hòa e trong E, thì $\{e\}$ là phần tử trung hòa đối với $*$ trong $\mathfrak{P}(E)$.

b) Nếu $*$ có phần tử trung hòa và mọi phần tử của E đều khả đối xứng đối với $*$, thì ta có thể khẳng định rằng mọi phần tử của $\mathfrak{P}(E)$ là khả đối xứng đối với $*$ không?

◊ **2.1.15** Cho $(E, *)$ là một phỏng nhóm kết hợp, $(a, b) \in E^2$. Chứng minh rằng $\{a\} * E$, $E * \{b\}$, $\{a\} * E * \{b\}$, $E * \{a\} * E$ ổn định đối với $*$.

◊ **2.1.16** Cho một phỏng nhóm $(E, *)$. Với $A, B, C \in \mathfrak{P}(E)$, so sánh:

a) $A * (B \cup C)$ và $(A * B) \cup (A * C)$

b) $A * (B \cap C)$ và $(A * B) \cap (A * C)$.

◊ **2.1.17** Cho $(E, *)$ là một phỏng nhóm kết hợp và giao hoán, và A là tập hợp các phần tử của E không chính quy đối với $*$. Chứng minh: $E * A \subset A$; đặc biệt, A ổn định đối với $*$.

◊ **2.1.18** Cho $(E, *)$ là một phỏng nhóm kết hợp. Chứng minh:

a) Với bộ phận ổn định A tùy ý, $A * A$ ổn định.

b) Với bộ phận A bất kỳ của E, **hoán tập của** A (được định nghĩa là:

$$A^C = \{x \in E;\ \forall a \in A,\ a * x = x * a\}$$

cũng ổn định.

◊ **2.1.19** Cho $(E, *)$ là một phỏng nhóm, $A = \{x \in E;\ \forall (y, z) \in E^2,\ (x * y) * z = x * (y * z)\}$.

a) Chứng minh rằng A ổn định đối với $*$.

b) Chứng minh rằng luật cảm sinh bởi $*$ trong A có tính kết hợp.

◊ **2.1.20** Cho $(E, *)$ là một phỏng nhóm, $C = \{x \in E,\ \forall y \in E,\ x * y = y * x\}$ được gọi là **tâm** của $(E, *)$. Ta giả thiết $*$ là kết hợp.

a) Chứng minh C ổn định đối với $*$.

b) Chứng minh rằng luật cảm sinh bởi $*$ trong C có tính giao hoán.

◊ **2.1.21** Cho $(E, \top)$, $(F, \perp)$ là hai phỏng nhóm, $*$ là luật tích, được định nghĩa là (xem Định nghĩa 14): $(x, y) * (x', y') = (x \top x', y \perp y')$.

Chứng minh rằng nếu $\top$ và $\perp$ có một trong những tính chất sau, thì $*$ cũng có tính chất đó:

1) tính kết hợp 2) tính giao hoán 3) tồn tại phần tử trung hòa

4) tồn tại phần tử trung hòa và mọi phần tử đều có phần tử đối xứng.

◊ **2.1.22** Cho X là một tập hợp, $E = X^X$ được trang bị luật $\circ$, $f \in E$. Chứng minh:

a) f là đơn ánh khi và chỉ khi f chính quy trái đối với $\circ$ trong E.

b) f là toàn ánh khi và chỉ khi f chính quy phải đối với $\circ$ trong E.

◊ **2.1.23** Cho $(E, *)$ là một phỏng nhóm và $\leq$ là một quan hệ thứ tự trong E. Ta giả thiết rằng, với mọi (a, b, x) thuộc E^3:

(i) $a * b \leq a$ (ii) $a * b \leq b$ (iii) $\left.\begin{matrix} x \leq a \\ x \leq b \end{matrix}\right\} \Rightarrow x \leq a * b$.

Chứng minh:

a) $*$ giao hoán

b) Mọi phần tử của E đều lũy đẳng đối với $*$ (xem bài tập 2.1.8)

c) $\forall (a, b, c) \in E^3,\ (a \leq b \Rightarrow a * c \leq b * c)$

d) $\forall (a, b, c, d) \in E^4,\ \left(\left\{\begin{matrix} a \leq b \\ c \leq d \end{matrix}\right.\right) \Rightarrow a * c \leq b * d$

e) $*$ có tính kết hợp.

2.2 Nhóm

2.2.1 Đại cương

♦ **Định nghĩa 1** Ta nói rằng một tập hợp G có trang bị một luật hợp thành trong $*$ là một **nhóm** khi và chỉ khi:

$$\begin{cases} * \text{ có tính kết hợp} \\ G \text{ có phần tử trung hòa đối với } * \\ \text{Mọi phần tử của } G \text{ có phần tử đối xứng đối với } * \end{cases}$$

Nếu hơn nữa $*$ có tính giao hoán, thì ta nói rằng G là một **nhóm Abel** (hoặc: **nhóm giao hoán**).

VÍ DỤ:

1) $(\mathbb{C}, +)$ là một nhóm Abel.

2) Tập hợp các phép đẳng cự vectơ của một mặt phẳng vectơ Euclide là một nhóm đối với $\circ$.

Các ký hiệu được sử dụng nhiều nhất là như sau:

Luật	Tích hai phần tử	Phần tử trung hòa	Phần tử đối xứng của một phần tử x	Tích của x với phần tử đối xứng của y
$*$	$x * y$	e , 1	x^{-1}	$x * y^{-1}$
$\circ$	$x \circ y$	1, 1	x^{-1}	$x \circ y^{-1}$
$\cdot$	xy	1	x^{-1}	xy^{-1}
$+$	$x + y$	0	$-x$	$x - y$

♦ **Mệnh đề**

Trong một nhóm, mọi phần tử đều chính quy.

Chứng minh:

Với bất kỳ (x, y, z) thuộc G^3:

$(x * y = x * z \Rightarrow x^{-1} * (x * y) = x^{-1} * (x * z) \Rightarrow (x^{-1} * x) * y = (x^{-1} * x) * z \Rightarrow y = z)$.

Lập luận tương tự với phép nhân bên phải.

♦ **Định nghĩa 2** Nếu $(G, *)$ là một nhóm hữu hạn, thì bản số của G được gọi là **cấp** của G.

Chẳng hạn, với mọi n thuộc $\mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z}, +)$ (xem 4.1.2, Mệnh đề 3) là một nhóm hữu hạn cấp n.

Bài tập

◊ **2.2.1** Cho $(G, \cdot)$ là một nhóm sao cho: $\forall x \in G, x^2 = e$. Chứng minh rằng G giao hoán.

◊ **2.2.2** Cho $(G, \cdot)$ là một nhóm hữu hạn, A, B là hai bộ phận của G sao cho:

$$\mathrm{Card}(A) + \mathrm{Card}(B) > \mathrm{Card}(G).$$

Chứng minh : $G = AB$ (tức là: $\forall x \in G, \exists (a, b) \in A \times B, x = ab$).

◊ **2.2.3** Cho $(G, \cdot)$ là một nhóm hữu hạn cấp chẵn, S là tập hợp các phần tử cấp 2 của G, tức là: $S = \{x \in G : x^2 = e \text{ và } x \neq e\}$.

a) Chứng minh rằng quan hệ $\mathcal{R}$ xác định trong G bởi: $x \mathcal{R} y \Leftrightarrow (y = x$ hoặc $y = x^{-1})$ là một quan hệ tương đương.

b) Suy ra rằng $\mathrm{Card}(S)$ lẻ.

◊ **2.2.4** Chứng minh rằng $\mathcal{A} = \{f_{a,b} : \underset{x \mapsto ax+b}{\mathbb{R} \to \mathbb{R}} ; (a, b) \in \mathbb{R}^* \times \mathbb{R}\}$ là một nhóm đối với $\circ$. Nó có giao hoán không?

2.2.2 Nhóm con

◆ **Định nghĩa 1** Cho $(G, *)$ là một nhóm, $H \in \mathfrak{P}(G)$. Ta nói rằng H là một **nhóm con** của G khi và chỉ khi:

(i) $\forall (x, y) \in H^2, x * y \in H$

(ii) $e \in H$

(iii) $\forall x \in H, x^{-1} \in H$

(trong đó e là phần tử trung hòa của G và x^{-1} là phần tử đối xứng của x trong G).

VÍ DỤ:

1) Với mọi n thuộc $\mathbb{N}$, $n\mathbb{Z} = (\{na; a \in \mathbb{Z}\})$ là một nhóm con cộng của $\mathbb{Z}$.

2) Tập hợp các phép dẳng cự vectơ thuận của một mặt phẳng Euclide P là một nhóm con đối với $\circ$ của nhóm các phép dẳng cự vectơ của P.

◆ **Mệnh đề 1** Cho $(G, *)$ là một nhóm, $H \in \mathfrak{P}(G)$. Để H là một nhóm con của G, điều kiện cần và đủ là:

$$\begin{cases} H \text{ ổn định đối với } * \\ H \text{ là một nhóm đối với luật cảm sinh bởi luật } * \text{ của } G. \end{cases}$$

Chứng minh:

1) Giả sử H là một nhóm con của G. Theo (i), $*$ là lhtt trong H.

Luật $*$ trong H có tính kết hợp (vì nó kết hợp trong G), có e là phần tử trung hòa theo (ii), và mọi phần tử của H có phần tử đối xứng đối với $*$ trong H theo (iii). Như thế $(H, *)$ là một nhóm.

2) Ngược lại, giả sử H ổn định đối với $*$ và $(H, *)$ là một nhóm.

- Rõ ràng (i) được thỏa mãn.
- Ký hiệu e' là phần tử trung hòa của H. Ta có $e' * e' = e' = e' * e$, vậy (do tính chính quy của e' trong G), $e' = e$. Như thế $e \in H$.
- Giả sử $x \in H$. Vì $(H, *)$ là một nhóm nên x có phần tử đối xứng y đối với $*$ trong H: $x * y = y * x = e$.

Suy ra y là đối xứng của x đối với $*$ trong G, vậy (xem 2.1, Mệnh đề 3) $x^{-1} = y \in H$.

♦ **Mệnh đề 2** Cho G là một nhóm, $(H_i)_{i \in I}$ là một họ những nhóm con của G. Thế thì $\bigcap_{i \in I} H_i$ là một nhóm con của G.

Chứng minh:

Ký hiệu $H = \bigcap_{i \in I} H_i$.

1) Với mọi (x, y) thuộc G^2:

$(x, y) \in H^2 \Rightarrow (\forall i \in I, (x \in H_i \text{ và } y \in H_i)) \Rightarrow (\forall i \in I, x * y \in H_i) \Rightarrow x * y \in H$.

2) $(\forall i \in I, e \in H_i)$, vậy $e \in H$.

3) Với mọi x thuộc G: $x \in H \Rightarrow (\forall i \in I, x \in H_i) \Rightarrow (\forall i \in I, x^{-1} \in H_i) \Rightarrow x^{-1} \in H$.

Mệnh đề trên dẫn đến Định nghĩa sau:

♦ **Định nghĩa 2** Cho $(G, *)$ là một nhóm, $A \in \mathfrak{P}(G)$. Giao của tất cả các nhóm con của G có chứa A là một nhóm con của G, được gọi là **nhóm con sinh bởi** A và được ký hiệu $< A >$.

Vậy ta có: $< A > = \bigcap_{\substack{H \text{ là nhóm con của } G \\ A \subset H}} H$.

Với mọi a thuộc G, ta có thể ký hiệu $< a >$ thay cho $< \{a\} >$.

♦ **Mệnh đề 3** Cho $(G, *)$ là một nhóm, $A \in \mathfrak{P}(G)$; $< A >$ là nhóm con bé nhất của G (theo nghĩa bao hàm) có chứa A.

Chứng minh:

1) Theo Mệnh đề 2, $< A >$ là một nhóm con của G có chứa A.

2) Giả sử H là một nhóm con của G chứa A. Theo định nghĩa của $< A >$, ta có: $< A > \subset H$. Như thế $< A >$ được bao hàm trong mọi nhóm con của G chứa A.

♦ **Mệnh đề 4** Cho $(G, *)$ là một nhóm, $A \in \mathfrak{P}(G)$.

1) $< \varnothing > = \{e\}$, trong đó e là phần tử trung hòa của G.

2) Với mọi bộ phận khác rỗng A của G, $\{A\}$ là tập hợp các hợp thành bội của các phần tử của A và các phần tử đối xứng của các phần tử của A.

Chứng minh.

1) Hiển nhiên.

2) Ta ký hiệu $A^{-1} = \{y \in G;\ y^{-1} \in A\} = \{x^{-1};\ x \in A\}$, $B = A \cup A^{-1}$, H là tập hợp các hợp thành bội của các phần tử của B, tức là:

$$H = \{x \in G;\ \exists n \in \mathbb{N}^*, \exists (b_1, ..., b_n) \in B^n, x = \underset{i=1}{\overset{n}{*}} b_i\}.$$

Ta sẽ chứng minh H là nhóm con chứa A nhỏ nhất của G.

a) Ta chứng minh H là một nhóm con của G.

- Giả sử $(x, y) \in H^2$. Tồn tại $n, p \in \mathbb{N}^*, b_1, ..., b_n, c_1, ..., c_p \in B$ sao cho $x = \underset{i=1}{\overset{n}{*}} b_i$ và $y = \underset{j=1}{\overset{p}{*}} c_j$. Ký hiệu $d_k = \begin{cases} b_k & \text{nếu } 1 \le k \le n \\ c_{k-n} & \text{nếu } n+1 \le k \le n+p \end{cases}$, ta có:

$$x * y = b_1 * ... * b_n * c_1 * ... * c_p = d_1 * ... * d_n * d_{n+1} * ... * d_{n+p} = \underset{k=1}{\overset{n+p}{*}} d_k \in H.$$

- Vì $A \neq \emptyset$, nên tồn tại $a \in A$, vậy $e = a * a^{-1} \in H$.

- Giả sử $x \in H$. Tồn tại $n \in \mathbb{N}^*$, $b_1, ..., b_n \in B$ sao cho $x = \underset{i=1}{\overset{n}{*}} b_i$.

Vậy $b_1^{-1}, ..., b_n^{-1} \in B$ và $x^{-1} = \underset{i=1}{\overset{n}{*}} b_{n+1-i}^{-1} = b_n^{-1} * \cdots * b_1^{-1} \in H$.

b) $A \subset H$ vì $A \subset B \subset H$.

c) Giả sử L là một nhóm con của G sao cho $A \subset L$.

Khi đó ta có: $\forall x \in A$, $(x \in L$ và $x^{-1} \in L)$, từ đây $B \subset L$, rồi $H \subset L$.

Vì H là nhóm con chứa A nhỏ nhất của G, nên ta kết luận (xem Mệnh đề 3): $H = < A >$.

♦ Định nghĩa 3

1) Một nhóm G được nói là **nhóm đơn** khi và chỉ khi tồn tại $a \in G$ sao cho $G = < a >$.

2) Nếu G là một nhóm đơn thì một phần tử bất kỳ a của G thỏa mãn $G = < a >$ được gọi là **phần tử sinh** của G.

3) Một nhóm G được gọi là **nhóm xyclic** khi và chỉ khi nó là nhóm đơn và hữu hạn.

VÍ DỤ:

1) $(\mathbb{Z}, +)$ là một nhóm đơn, mà một phần tử sinh là 1 (hoặc -1).

2) $(\mathbb{Z}_{/3\mathbb{Z}}, +)$ là một nhóm đơn, mà một phần tử sinh, chẳng hạn là $\hat{2}$.

3) $(\mathbb{R}, +)$ không phải là một nhóm đơn.

Dưới đây ta sẽ khảo sát (bài tập 4.1.32) việc phân loại các nhóm đơn.

Bài tập

◊ **2.2.5** Cho G là một nhóm, H, K là hai nhóm con của G. Chứng minh:

$$H \cup K = G \Leftrightarrow (H = G \text{ hoặc } K = G).$$

◊ **2.2.6** Cho $G = \mathbb{R}^* \times \mathbb{R}$ và $*$ là luật trong G xác định bởi:

$$(x, y) * (x', y') = (xx', xy' + y).$$

a) Chứng minh $(G, *)$ là một nhóm không giao hoán.

b) Chứng minh $\mathbb{R}_+^* \times \mathbb{R}$ là một nhóm con của G.

◊ **2.2.7** Cho $(G, \bullet)$ là một nhóm. Bộ phận của G xác định bởi:

$C = \{x \in G;\ \forall y \in G,\ xy = yx\}$, được gọi là **tâm** của G.

Chứng minh C là một nhóm con của G.

◊ **2.2.8** Cho $G = \mathbb{R}^* \times \mathbb{R}$ và $*$ là luật trong G xác định bởi:

$$(x, y) * (x', y') = \left(xx', xy' + \frac{y}{x'}\right).$$

a) Chứng minh rằng $(G, *)$ là một nhóm.

b) Chỉ ra tâm của G (xem bài tập 2.2.7).

c) Chứng minh rằng $\mathbb{R}^* \times \{1\}$, $\{1\} \times \mathbb{R}$, $\mathbb{Q}^* \times \mathbb{Q}$ là những nhóm con của G.

d) Chứng minh rằng, với bất kỳ k thuộc $\mathbb{R}$, tập hợp $H_k = \left\{\left(x, k\left(x - \frac{1}{x}\right)\right); x \in \mathbb{R}^*\right\}$ là một nhóm con giao hoán của G.

◊ **2.2.9** Cho G là một nhóm hữu hạn.

Chứng minh rằng, với bất kỳ nhóm con H của G, nếu $\text{Card}(H) > \frac{1}{2}\text{Card}(G)$, thì $H = G$.

◊ **2.2.10** Cho $(G, \top)$, $(G', \perp)$ là hai nhóm, $*$ là luật tích (xem 2.1, Định nghĩa 14) được xác định trong $G \times G'$ bởi: $(x, y) * (x', y') = (x \top x', y \perp y')$.

a) Chứng minh $(G \times G', *)$ là một nhóm.

b) Chứng minh rằng, nếu H (tương ứng: H') là một nhóm con của G (tương ứng: G') thì $H \times H'$ là một nhóm con của $G \times G'$.

◊ **2.2.11*** Cho (G) là một nhóm của $(\mathbb{C}, +)$ sao cho: $\forall x \in]0; 1[, x + ix^2 \in G$.

Chứng minh $G = \mathbb{C}$.

2.2.3 Đồng cấu nhóm

♦ **Định nghĩa 1** Cho $(G, *)$, $(G', \top)$ là hai nhóm, $f : G \to G'$ là một ánh xạ. Nếu f là một đồng cấu (tương ứng: tự đồng cấu, tương ứng: đẳng cấu, tương ứng: tự đẳng cấu) phồng nhóm, thì f được gọi là **đồng cấu** (tương ứng: **tự đồng cấu**, tương ứng: **đẳng cấu**, tương ứng: **tự đẳng cấu**) **nhóm**.

♦ **Mệnh đề 1** Cho $f : (G, *) \to (G', \top)$ là một đồng cấu nhóm. Thế thì:

1) $f(e) = e'$

2) $\forall x \in G, \quad f(x^{-1}) = (f(x))^{-1}$

trong đó e (tương ứng: e') là phần tử trung hòa của G (tương ứng: G').

Chứng minh:

1) $f(e) \top f(e) = f(e * e) = f(e) = f(e) \top e'$, vậy do tính chính quy của $f(e)$ trong G': $f(e) = e'$.

2) $\begin{cases} f(x) \top f(x^{-1}) = f(x * x^{-1}) = f(e) = e' \\ f(x^{-1}) \top f(x) = f(x^{-1} * x) = f(e) = e' \end{cases}$, vậy $f(x^{-1}) = (f(x))^{-1}$.

♦ **Định nghĩa 2** Cho $(G, *)$, $(G', \top)$ là hai nhóm, $f : (G, *) \to (G', \top)$ là một đồng cấu nhóm. Ta có:

- **Hạt nhân** của f, và ký hiệu $\mathrm{Ker}(f)$ là:

$$\mathrm{Ker}(f) = \{x \in G; f(x) = e'\} = f^{-1}(\{e'\}).$$

trong đó e' là phần tử trung hòa của G'.

- **Ảnh** của f, và ký hiệu $\mathrm{Im}\ (f)$, là:

$$\mathrm{Im}(f) = \{y \in G'; \exists x \in G, y = f(x)\} = f(G).$$

♦ **Mệnh đề 2** Nếu $f : (G, *) \to (G', \top)$ là một đồng cấu nhóm, thì $\mathrm{Ker}(f)$ (tương ứng: $\mathrm{Im}(f)$) là một nhóm con của G (tương ứng: G').

Chứng minh:

1) • Giả sử $(x, y) \in (\mathrm{Ker}(f))^2$. Ta có: $f(x * y) = f(x) \top f(y) = e' \top e' = e'$, vậy $x * y \in \mathrm{Ker}(f)$.

• $f(e) = e'$, vậy $e \in \mathrm{Ker}(f)$.

• Nếu $x \in \mathrm{Ker}(f)$, thì $f(x^{-1}) = (f(x))^{-1} = e'^{-1} = e'$, vậy $x^{-1} \in \mathrm{Ker}(f)$.

2) • Giả sử $(x', y') \in (\mathrm{Im}(f))^2$. Vậy tồn tại $(x, y) \in G^2$ sao cho $x' = f(x)$, $y' = f(y)$, suy ra: $x' \top y' = f(x) \top f(y) = f(x * y) \in \mathrm{Im}(f)$.

• $e' = f(e) \in \mathrm{Im}(f)$.

• Nếu $x' \in \mathrm{Im}(f)$, thì tồn tại $x \in G$ sao cho $x' = f(x)$, và ta có:

$x'^{-1} = (f(x))^{-1} = f(x^{-1}) \in \mathrm{Im}(f)$.

Tổng quát hơn, xem bài tập 2.2.12.

♦ **Định nghĩa 3** Một nhóm $(G, *)$ được gọi là **đẳng cấu với** một nhóm $(G', \top)$ khi và chỉ khi tồn tại một đẳng cấu nhóm từ $(G, *)$ lên $(G', \top)$.

VÍ DỤ:

$(\mathbb{R}_+^*, \times)$ đẳng cấu với $(\mathbb{R}, +)$ vì $\ln : \mathbb{R}_+^* \to \mathbb{R}$, $x \mapsto \ln x$ là một đẳng cấu nhóm.

NHẬN XÉT:

Quan hệ "đẳng cấu với" giữa các nhóm là một quan hệ tương đương trên mọi tập hợp các nhóm (nhưng không tồn tại tập hợp tất cả các nhóm).

♦ **Mệnh đề 3 (Chuyển cấu trúc nhóm)**

Cho $(G, *)$ là một nhóm, $(E, \top)$ là một phỏng nhóm. Nếu tồn tại một đẳng cấu phỏng nhóm từ $(G, *)$ lên $(E, \top)$, thì $(E, \top)$ là một nhóm đẳng cấu với nhóm $(G, *)$.

Ta cũng nói **truyền** thay cho chuyển.

Chứng minh:

Giả sử tồn tại một đẳng cấu phỏng nhóm $f : (G, *) \to (E, \top)$. Ta ký hiệu e là phần tử trung hòa của G.

Giả sử $x, y, z \in E$, $X = f^{-1}(x)$, $Y = f^{-1}(y)$, $Z = f^{-1}(z)$.

1) $(x \top y) \top z = (f(X) \top f(Y)) \top f(Z) = f(X * Y) \top f(Z) = f((X * Y) * Z)$

$= f(X * (Y * Z)) = f(X) \top f(Y * Z) = f(X) \top (f(Y) \top f(Z)) = x \top (y \top z)$,

vậy $\top$ có tính kết hợp trong E.

2) $\begin{cases} x \top f(e) = f(X) \top f(e) = f(X * e) = f(X) = x \\ f(e) \top x = f(e) \top f(X) = f(e * X) = f(X) = x \end{cases}$,

vậy $f(e)$ là phần tử trung hòa đối với $\top$ trong E.

3) $\begin{cases} x \top f(X^{-1}) = f(X) \top f(X^{-1}) = f(X * X^{-1}) = f(e) \\ f(X^{-1}) \top x = f(X^{-1}) \top f(X) = f(X^{-1} * X) = f(e) \end{cases}$,

vậy tồn tại phần tử đối xứng của x đối với $\top$ trong E.

VÍ DỤ:

Xét luật $*$ xác định trong $\mathbb{R}$ bởi:

$$\forall (x, y) \in \mathbb{R}^2, \quad x * y = x\sqrt{1 + y^2} + y\sqrt{1 + x^2}.$$

Rõ ràng ánh xạ sh : $\mathbb{R} \to \mathbb{R}$ (sin hypecbolic) là song ánh và thỏa mãn:

$$\forall (u, v) \in \mathbb{R}^2, \quad \mathrm{sh}(u + v) = \mathrm{sh}u * \mathrm{sh}v.$$

Vậy $(\mathbb{R}, *)$ là một nhóm, đẳng cấu với $(\mathbb{R}, +)$, vì ánh xạ sh là một đẳng cấu nhóm từ $(\mathbb{R}, +)$ lên $(\mathbb{R}, *)$.

Bài tập

◊ **2.2.12** Cho (G, T), $(G', \perp)$ là hai nhóm, $f : G \to G'$ là một đồng cấu nhóm.

a) Chứng minh rằng, với mọi nhóm con H của G, $f(H)$ là một nhóm con của G'.

b) Chứng minh rằng với mọi nhóm con H' của G', $f^{-1}(H')$ là một nhóm con của G.

◊ **2.2. 13** Chứng minh rằng tập hợp các tự đẳng cấu của một phỏng nhóm $(E, *)$ là một nhóm đối với $\circ$.

◊ **2.2.14** Cho G, G' là hai nhóm, e là phần tử trung hòa của G, $f : G \to G'$ là một đồng cấu nhóm. Chứng minh f là đơn ánh khi và chỉ khi $\mathrm{Ker}(f) = \{e\}$.

◊ **2.2.15** Cho G là một nhóm hữu hạn, f là một tự đẳng cấu của G sao cho:

$$\mathrm{Card}\{x \in G ; f(x) = x^{-1}\} > \frac{1}{2}\mathrm{Card}(G).$$

Chứng minh: $f^2 = \mathrm{Id}_G$.

◊ **2.2.16*** Cho $(G, \bullet)$ là một nhóm, H, K là hai nhóm con hữu hạn của G. Chứng minh rằng bộ phận HK của G là hữu hạn và: $\mathrm{Card}(HK) = \dfrac{\mathrm{Card}(H).\mathrm{Card}(K)}{\mathrm{Card}(H \cap K)}$.

◊ **2.2.17*** Cho $(G, \bullet)$ là một nhóm sao cho $f : \begin{matrix} G \to G \\ x \mapsto x^3 \end{matrix}$ là một tự đồng cấu toàn ánh của nhóm G. Chứng minh rằng G là nhóm Abel.

◊ **2.2.18** Cho $(G, \bullet)$ là một nhóm sao cho tồn tại $n \in \mathbb{N}^*$ thỏa mãn $f_n : \begin{matrix} G \to G \\ x \mapsto x^n \end{matrix}$ là một tự đồng cấu toàn ánh của nhóm G. Chứng minh rằng:

$$\forall (x, y) \in G^2, \quad x^{n-1}y = yx^{n-1}.$$

◊ **2.2.19** Cho G là một nhóm đơn (tương ứng: xyclic), $f : G \to G'$ là một đồng cấu nhóm toàn ánh. Chứng minh rằng G' là nhóm đơn (tương ứng: xyclic).

◊ **2.2.20** Chứng minh rằng các nhóm $(\mathbb{Q}, +)$ và $(\mathbb{Q}_+^*, \times)$ không đẳng cấu với nhau.

◊ **2.2.21** Chứng minh rằng các nhóm $(\mathbb{R}^*, \times)$ và $(\mathbb{C}^*, \times)$ không đẳng cấu với nhau.

2.3 Vành

2.3.1 Các định nghĩa

◆ **Định nghĩa** Cho A là một tập hợp có trang bị hai luật hợp thành trong kí hiệu là $+, \cdot$.

1) Ta nói rằng $(A, +, \cdot)$ (hoặc : A) là một **giả vành** khi và chỉ khi :

$$\begin{cases} (A, +) \text{ là một nhóm Abel} \\ \cdot \text{ kết hợp} \\ \cdot \text{ phân phối đối với } +. \end{cases}$$

2) Ta nói rằng A là một **vành** khi và chỉ khi :

$$\begin{cases} (A, +, \cdot) \text{ là một giả vành} \\ A \text{ có phần tử trung hòa đối với } \cdot \end{cases}$$

3) Ta nói rằng A là một **vành giao hoán** khi và chỉ khi :

$$\begin{cases} A \text{ là một vành} \\ \cdot \text{ giao hoán} \end{cases}$$

VÍ DỤ:

1) $(\mathbf{Z}, +, \bullet)$ là một vành giao hoán

2) $(K[X], +, \bullet)$ là một vành giao hoán.

3) Với mọi n thuộc $\mathbf{N}^* - \{0,1\}$, $\mathbf{M}_n(K)$ là một vành không giao hoán (xem 8.1.4).

4) Với mọi tập hợp X, $(\mathfrak{P}(X), \Delta, \cap)$ là một vành giao hoán (xem bài tập 2.3.6 dưới đây).

2.3.2 Các phép toán trong một vành

Cho $(A, +, \cdot)$ là một vành. Ta ký hiệu :

0 là phần tử trung hòa đối với $+$

$-x$ là đối xứng của phần tử x của A đối với $+$

1 (hoặc 1_A) là phần tử trung hòa đối với $\cdot$.

Ta chứng minh dễ dàng các công thức sau :

1) $\forall x \in A, 0 \cdot x = x \cdot 0 = 0$ (ta nói rằng 0 có tính **hấp thu** đối với $\cdot$)

2) $\forall x \in A, (-1_A) \cdot x = x \cdot (-1_A) = -x$

3) $\forall (x, y) \in A^2, \begin{cases} (-x)y = x(-y) = -xy \\ (-x)(-y) = xy \end{cases}$

4) $\forall (x, y, z) \in A^3, \begin{cases} (x - y)z = xz - yz \\ z(x - y) = zx - zy \end{cases}$

5) $\forall n \in \mathbb{N}^*, \forall a \in A, (1-a)\sum_{k=0}^{n-1} a^k = \left(\sum_{k=0}^{n-1} a^k\right)(1-a) = 1 - a^n$

6) $\forall p \in \mathbb{N}, \forall a \in A, (1+a)\sum_{k=0}^{2p}(-1)^k a^k = \left(\sum_{k=0}^{2p}(-1)^k a^k\right)(1+a) = 1 + a^{2p+1}$

7) $\forall a \in A, \forall n \in \mathbb{N}^*, \forall (x_1, ..., x_n) \in A^n, \left(\sum_{i=1}^{n} a x_i = a\sum_{i=1}^{n} x_i, \sum_{i=1}^{n} x_i a = \left(\sum_{i=1}^{n} x_i\right)a\right)$

8) $\forall n, p \in \mathbb{N}^*, \forall (x_1, ..., x_n) \in A^n, (y_1, ..., y_p) \in A^p,$

$$\sum_{i=1}^{n}\left(\sum_{j=1}^{p} x_i y_i\right) = \sum_{j=1}^{p}\left(\sum_{i=1}^{n} x_i y_j\right) = \left(\sum_{i=1}^{n} x_i\right)\left(\sum_{j=1}^{p} y_j\right).$$

♦ **Ký hiệu** Cho một vành $(A, +, \cdot)$. Với mọi (n, x) thuộc $\mathbb{Z} \times A$, ta ký hiệu :

$$\begin{cases} nx = x + ... + x \ (n \text{ hạng tử}) & \text{nếu } n \in \mathbb{N}^* \\ nx = 0 & \text{nếu } n = 0 \\ nx = -(-nx) & \text{nếu } n \in \mathbb{Z}^* \end{cases}$$

Độc giả chứng minh dễ dàng các công thức sau :

1) $\forall (n, p) \in \mathbb{Z}^2, \forall x \in A, \quad (n+p)x = nx + px$

2) $\forall n \in \mathbb{Z}, \forall x \in A, \ n(-x) = (-n)x = -(nx)$, ký hiệu là $-nx$

3) $\forall n \in \mathbb{Z}, \forall (x, y) \in A^2, \quad \begin{cases} n(x+y) = nx + ny \\ n(x-y) = nx - ny \end{cases}$

4) $\forall (n, p) \in \mathbb{Z}^2, \forall x \in A, \quad (np)x = n(px)$

5) $\forall n \in \mathbb{Z}, \forall (x, y) \in A^2, \quad n(xy) = (nx)y = x(ny)$

6) $\forall n \in \mathbb{Z}, \forall x \in A, \ nx = (n1_A)x = x(n1_A)$.

Đôi khi ta ký hiệu n thay cho $n1_A$, với $n \in \mathbb{Z}$, nếu không gây ra lẫn lộn.

♦ **Định lý (Công thức nhị thức Newton)**

Cho một vành $(A, +, \cdot)$, $n \in \mathbb{N}$, $(x, y) \in A^2$ sao cho $xy = yx$. Ta có :

$$(x + y)^n = \sum_{k=0}^{n} C_n^k x^k y^{n-k}$$

(trong đó quy ước $x^0 = y^0 = 1_A$).

Ở lớp cuối cấp trung học phổ thông độc giả đã biết đến các hệ số C_n^p. Dưới đây, ở 3.3.3, ta sẽ nghiên cứu các hệ số đó.

Chứng minh :

Phương pháp thứ 1

Quy nạp theo n.

Với $n = 0$ công thức là hiển nhiên.

Chú ý rằng các lũy thừa của x và của y giao hoán với nhau (xem bài tập 2.1.4). Giả thiết công thức đúng với n. x, y cố định. Ta có :

$$(x+y)^{n+1} = (x+y)^n(x+y) = \left(\sum_{k=0}^{n} C_n^k x^k y^{n-k}\right)(x+y)$$

$$= \left(\sum_{k=0}^{n} C_n^k x^k y^{n-k}\right)x + \left(\sum_{k=0}^{n} C_n^k x^k y^{n-k}\right)y$$

$$= \sum_{k=0}^{n} C_n^k x^{k+1} y^{n-k} + \sum_{k=0}^{n} C_n^k x^{n-k} y^{n-k+1}$$

$$= \sum_{\substack{l=0 \\ (l=k+1)}}^{n+1} C_n^{l-1} x^l y^{n+1-l} + \sum_{k=0}^{n+1} C_n^k x^k y^{n+1-k}$$

$$= \sum_{k=0}^{n+1} \left(C_n^{k-1} + C_n^k\right) x^k y^{n+1-k} = \sum_{k=0}^{n+1} C_{n+1}^k x^k y^{n+1-k}$$

Phương pháp thứ 2

Bằng cách "khai triển tường minh" $(x+y)^n$ thành tổng của các hạng tử có dạng $x^k y^{n-k}$, $0 \le k \le n$; trong tổng này, số các hạng tử $x^k y^{n-k}$, với $k \in \{0, ..., n\}$ cố định, bằng số k nhân tử lấy trong n nhân tử, tức là C_n^k.

Bài tập

◊ **2.3.1** Cho A là một vành sao cho : $\forall x \in A$, $x^2 = x$.

1) Chứng minh : $\forall x \in A$, $2x = 0$.

2) Suy ra A giao hoán.

3) Chứng minh rằng, với bất kỳ (x, y, z) thuộc A^3 : $(x+y)z = 0 \Leftrightarrow \begin{cases} x(y+1)z = 0 \\ (x+1)yz = 0 \end{cases}$.

◊ **2.3.2** Cho $(A, +, \cdot)$ là một giả vành, C là **tâm** của A, $C = \{x \in A \ ; \ \forall a \in A, ax = xa\}$.

Giả thiết : $\forall x \in A$, $x^2 - x \in C$.

a) Chứng minh : $\forall (x, y) \in A^2$, $xy + yx \in C$.

b) Suy ra : $\forall (x, y) \in A^2$, $xy = yx$.

◊ **2.3.3** Cho A là một vành. Một phần tử x của A được gọi là **lũy linh** khi và chỉ khi tồn tại $n \in \mathbb{N}^*$ sao cho $x^n = 0$.

a) Chứng minh rằng, nếu x, y là lũy linh và giao hoán, thì $x + y$ cũng là lũy linh.

b) Chứng minh rằng, nếu x là lũy linh và $xy = yx$, thì xy cũng là lũy linh.

c) Giả sử $x \in A$ là lũy linh. Chứng minh rằng $1 - x$ khả nghịch và tính $(1 - x)^{-1}$.

◊ **2.3.4 Đặc số của một vành**

Cho A là một vành, $E = \{n \in \mathbb{N}^* ; n1_A = 0_A\}$.

Nếu $E = \varnothing$ thì ta nói A có **đặc số 0**.

Nếu $E \neq \varnothing$, phần tử nhỏ nhất của E được gọi là **đặc số của** A.

Nói khác đi, đặc số của A là số tự nhiên nhỏ nhất n thuộc $\mathbb{N}^*$ sao cho $n1_A = 0_A$, nếu tồn tại, và bằng 0 nếu trái lại.

Đặc số của $\mathbb{Z}$ là bao nhiêu ? của $\mathbb{Z}/n\mathbb{Z}$ ($n \in \mathbb{N}^*$) là bao nhiêu ?

◊ **2.3.5*** Cho A là một vành, $a \in A$. Ta giả thiết rằng a có ít nhất một nghịch đảo trái và không có nghịch đảo phải nào. Chứng minh a có vô hạn nghịch đảo trái.

2.3.3 Vành con

◆ **Định nghĩa** Cho một vành $(A, +, \cdot)$, $B \in \mathfrak{P}(A)$. Ta nói rằng B là một **vành con** của A khi và chỉ khi :

$$\begin{cases} B \text{ là một nhóm con của } (A,+) \\ \forall (x,y) \in B^2,\ xy \in B \\ 1_A \in B \end{cases}$$

NHẬN XÉT :
Nếu B là một vành con của A, thì B là một vành (đối với các luật cảm sinh bởi các luật trong A) và có cùng phần tử trung hòa đối với $\bullet$ như A.

VÍ DỤ :
1) $\mathbb{Z}$ là một vành con của vành $(\mathbb{Q}, +, \bullet)$.
2) $2\mathbb{Z}$ không phải là một vành con của $(\mathbb{Z}, +, \bullet)$.

◆ **Mệnh đề** Cho một vành $(A, +, \bullet)$, $B \in \mathfrak{P}(A)$. Để B là một vành con của A, cần và đủ là :

$$\begin{cases} \text{(i)}\ \forall (x,y) \in B^2,\ x - y \in B \\ \text{(ii)}\ \forall (x,y) \in B^2,\ xy \in B \\ \text{(iii)}\ 1_A \in B \end{cases}$$

Chứng minh :

1) Rõ ràng rằng, nếu B là một vành con của A, thì các điều kiện (i), (ii), (iii) được thỏa mãn.

2) Ngược lại, giả sử (i), (ii), (iii) thỏa mãn. Thế thì :

$$0_A = 1_A - 1_A \in B$$

$$\forall x \in B,\quad -x = 0 - x \in B$$

$$\forall (x, y) \in B^2,\ x + y = x - (-y) \in B$$

vậy B là một nhóm con của $(A, +)$.

2.3.4 Đồng cấu vành

♦ **Định nghĩa** Cho A, A' là hai vành, $f : A \to A'$ là một ánh xạ. Ta nói rằng f là một **đồng cấu vành** khi và chỉ khi :

$$\begin{cases} \forall (x, y) \in A^2, & f(x+y) = f(x) + f(y) \\ \forall (x, y) \in A^2, & f(xy) = f(x) f(y) \\ f(1_A) = 1_{A'}. \end{cases}$$

Một **tự đồng cấu của một vành** $(A, +, \cdot)$ là một đồng cấu vành từ $(A, +, \cdot)$ vào $(A, +, \cdot)$.

Một **đẳng cấu vành** là một đồng cấu vành song ánh.

Một **tự đẳng cấu của một vành** $(A, +, \cdot)$ là một tự đồng cấu song ánh của vành $(A, +, \cdot)$

♦ **Mệnh đề**

1) Nếu $f : A \to A'$ và $g : A' \to A''$ là hai đồng cấu vành, thì $g \circ f : A \to A''$ là một đồng cấu vành.

2) $\mathrm{Id}_A : A \to A$ là một tự đẳng cấu của vành $(A, +, \cdot)$.

3) Nếu $f : A \to A'$ là một đẳng cấu vành, thì $f^{-1} : A' \to A$ là một đẳng cấu vành.

Chứng minh :

Tương tự như phép chứng minh của 2.1, Mệnh đề 5.

Bài tập

◊ **2.3.6** Cho một tập hợp X.

a) Chứng minh rằng $((\mathbb{Z}/2\mathbb{Z})^X, +, \bullet)$ là một vành giao hoán.

b) Với mọi bộ phận A của X, ta kí hiệu $\theta_A : X \to \mathbb{Z}/2\mathbb{Z}$ là ánh xạ được xác định bởi :

$$\theta_A(x) = \begin{cases} \hat{1} & \text{nếu } x \in A \\ \hat{0} & \text{nếu } x \in \complement_X(A) \end{cases}$$

gọi là *hàm đặc trưng* của A (xem 1.3.1, Ví dụ 5).

Chứng minh rằng ánh xạ $\theta : \underset{A \mapsto \theta_A}{\mathfrak{P}(X) \to (\mathbf{Z}/2\mathbf{Z})^X}$ là một đẳng cấu từ $(\mathfrak{P}(X), \Delta, \cap)$ vào $((\mathbb{Z}/2\mathbb{Z})^X, +, \bullet)$, và suy ra rằng $(\mathfrak{P}(X), \Delta, \cap)$ là một vành giao hoán.

2.3.5 Vành nguyên

♦ Định nghĩa 1

Cho A là một vành, $a \in A$.

1) Ta nói rằng a là một **ước trái của không** trong A khi và chỉ khi :

$$\begin{cases} a \neq 0 \\ \exists b \in A \quad (b \neq 0 \text{ và } ab = 0). \end{cases}$$

2) Ta nói rằng a là **ước phải của không** trong A khi và chỉ khi :

$$\begin{cases} a \neq 0 \\ \exists c \in A \quad (c \neq 0 \text{ và } ca = 0). \end{cases}$$

3) Ta nói rằng a là **một ước của không** trong A khi và chỉ khi a là một ước trái của không trong A hoặc là một ước phải của không trong A.

VÍ DỤ :

1) $\mathbb{Z}$ không có một ước của không nào.

2) Trong $\mathbb{Z}/6\mathbb{Z}$, $\hat{2}$, $\hat{3}$, $\hat{4}$ là những ước của không, còn $\hat{0}$, $\hat{1}$, $\hat{5}$ không phải là ước của không.

3) Trong $M_2(\mathbb{R})$, $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ là một ước trái của không, còn $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ là một ước phải của không, vì : $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = 0.$

4) Trong $\mathbb{R}^{\mathbb{R}}$, $f : \mathbb{R} \to \mathbb{R}$ và $g : \mathbb{R} \to \mathbb{R}$ là những ước của không,

$$x \mapsto \begin{cases} 0 \text{ nếu } x < 0 \\ x \text{ nếu } x \geq 0 \end{cases} \qquad x \mapsto \begin{cases} x & \text{nếu } x \leq 0 \\ \varphi & \text{nếu } x > 0 \end{cases}$$

vì : $f \neq 0, g \neq 0, fg = 0.$

♦ Định nghĩa 2

Một vành A được gọi là **vành nguyên** khi và chỉ khi :

$$\begin{cases} A & \text{giao hoán} \\ A & \text{không có ước của không} \\ A & \neq \{0\}. \end{cases}$$

VÍ DỤ :

1) $(\mathbb{Z}, +, \cdot)$ là vành nguyên.

2) $(\mathbb{Z}/6\mathbb{Z}, +, \cdot)$ không phải là vành nguyên.

2.4 Thể

♦ **Định nghĩa 1** Một tập hợp K có trang bị hai luật $+, \cdot$ được gọi **thể** khi và chỉ khi :

$$\begin{cases} (K, +, \cdot) \text{ là một vành} \\ 0_K \neq 1_K \\ \text{Mọi phần tử thuộc } K\text{-}\{0\} \text{ đều có một nghịch đảo đối với } \cdot \text{ trong } K. \end{cases}$$

Nếu hơn nữa $\cdot$ giao hoán trong K, thì ta nói rằng $(K, +, \cdot)$ là một **thể giao hoán.**

VÍ DỤ :

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ là những thể giao hoán (đối với các luật thông thường $+, \cdot$).

Trong giáo trình này, mọi thể được xét đều giao hoán. Mặt khác, ta có thể chứng minh (định lí Wedderburn) rằng mọi thể hữu hạn đều giao hoán.

NHẬN XÉT :

Mọi thể giao hoán là một vành nguyên.

Khẳng định ngược lại là sai : $\mathbb{Z}$ là một vành nguyên, nhưng không phải là một thể.

♦ **Định nghĩa 2** Cho $(K, +, \cdot)$ là một thể, $L \in \mathfrak{P}(K)$. Ta nói rằng L là một **thể con** của K khi và chỉ khi : $\begin{cases} L \text{ là một vành con của } K \\ \forall x \in L\text{-}\{0\}, x^{-1} \in L \end{cases}$, tức là

$$\begin{cases} \forall (x,y) \in L^2, x - y \in L \\ \forall (x,y) \in L^2, xy \in L \\ 1_K \in L \\ \forall x \in L - \{0\}, \ x^{-1} \in L. \end{cases}$$

VÍ DỤ :

$\mathbb{Q}$ là một thể con của $\mathbb{R}$, và $\mathbb{R}$ là một thể con của $\mathbb{C}$ (đối với các luật thông thường $+, \cdot$).

NHẬN XÉT :

Mọi thể con của một thể K là một thể đối với các luật cảm sinh, và các phần tử trung hòa của L đối với $+$ và $\cdot$ là các phần tử trung hòa của K.

♦ **Định nghĩa 3** Cho K, K' là hai thể, $f : K \to K'$ là một ánh xạ. Nếu f là một đồng cấu (tương ứng : tự đồng cấu, tương ứng : đẳng cấu, tương ứng : tự đẳng cấu) vành, thì f sẽ gọi là **đồng cấu** (tương ứng : **tự đồng cấu,** tương ứng : **đẳng cấu,** tương ứng : **tự đẳng cấu**) **thể.**

VÍ DỤ :

$\mathrm{Id}_{\mathbb{C}} : \underset{z \mapsto z}{\mathbb{C} \to \mathbb{C}}$ và ánh xạ lấy liên hợp $\underset{z \mapsto \bar{z}}{\mathbb{C} \to \mathbb{C}}$ là những tự đẳng cấu của thể $\mathbb{C}$ (đối với các luật thông thường).

CHÚ Ý : Nếu $f : K \to K'$ là một đồng cấu thể thì, với mọi x thuộc K - $\{0\}$:

$$f(x) \neq 0 \text{ và } (f(x))^{-1} = f(x^{-1}).$$

Bài tập

◊ **2.4.1** Cho một thể K, $(x, y) \in (K - \{0\})^2$ sao cho $x + y = -1$ và $x^{-1} + y^{-1} = 1$.

Chứng minh : $xy = -1$ và $x^4 + y^4 = 7$.

(Ở đây ta đã ký hiệu n thay cho $n1_K$, với $n \in \mathbb{Z}$. xem 2.3.2).

◊ **2.4.2** Cho một thể K. Chứng minh rằng đặc số của vành K (xem bài tập 2.3.4) là 0 hoặc là một số nguyên tố. Đặc số của $\mathbb{Q}$ là bao nhiêu ? của $\mathbb{Z}/p\mathbb{Z}$ (p nguyên tố) là bao nhiêu ?

◊ **2.4.3*** Cho K là một thể giao hoán hữu hạn. Chứng minh rằng :

$$\forall x \in K, \exists (a, b) \in K^2, x = a^2 + b^2.$$

(Sử dụng bài tập 2.2.2).

◊ **2.4.4*** Tồn tại hay không một thể K sao cho các nhóm $(K, +)$ và $(K - \{0\}, \times)$ đẳng cấu với nhau ?

Bổ sung

◊ C2.1 Lớp trái trong một nhóm, định lý Lagrange

Cho $(G, \cdot)$ là một nhóm, phần tử trung hòa ký hiệu là e.

1) Giả sử $\mathcal{R}$ là một quan hệ tương đương trong G, tương thích trái với luật của G, tức là sao cho :

$$\forall (x, x', y) \in G^3, \quad (x\mathcal{R}x' \Rightarrow yx\ \mathcal{R}yx')$$

Với $x \in G$, ta ký hiệu $\bar{x}$ là lớp modulo $\mathcal{R}$ của x.

a) Chứng minh rằng $\bar{e}$ là một nhóm con của G.

b) Chứng minh : $\forall (x, x') \in G^2, (x\mathcal{R}x' \Leftrightarrow x^{-1}x' \in \bar{e})$. Vậy : $\forall x \in G, \ \bar{x} = x\bar{e}$.

2) Ngược lại, giả sử H là một nhóm con của G, và $\mathcal{R}_H$ là một quan hệ xác định trong G bởi :

$$\forall (x, x') \in G^2, (x\mathcal{R}_H x' \Leftrightarrow x^{-1}x' \in H).$$

a) Chứng minh rằng $\mathcal{R}_H$ là một quan hệ tương đương trong G, tương thích trái với luật của G, và H là $\bar{e}$, lớp modulo $\mathcal{R}_H$ của e.

b) Chứng minh rằng, với mọi x thuộc G, ánh xạ $y \mapsto xy$ là một song ánh từ $\bar{e}$ lên $\bar{x}$.

3) **Định lý Lagrange**

Chứng minh rằng, nếu G là một nhóm hữu hạn, thì, với mọi nhóm con của H của G, bản số của H chia hết bản số của G.

4) *Ví dụ việc áp dụng định lý Lagrange*

a) Trong một nhóm hữu hạn gồm 24 phần tử, có tồn tại hay không các nhóm con có 10 phần tử ?

b) Cho G là một nhóm, với phần tử trung hòa ký hiệu là e, H, K là hai nhóm con hữu hạn của G sao cho UCLN (Card (H), Card (K)) = 1 (xem 4.2.1, Mệnh đề - Định nghĩa). Chứng minh : $H \cap K = \{e\}$.

◊ C2.2* Nhóm con chuẩn tắc, nhóm thương

I Nhóm con chuẩn tắc

Cho $(G, \cdot)$ là một nhóm, với phần tử trung hòa ký hiệu là e.

1) Giả sử $\mathcal{R}$ là một quan hệ tương đương trong G, tương thích trái và phải với luật của G, tức là sao cho (xem C2.1 1)) :

$$\forall (x, x', y) \in G^3, (x\mathcal{R}x' \Rightarrow \begin{cases} yx\,\mathcal{R}yx' \\ xy\mathcal{R}x'\,y \end{cases})$$

Với $x \in G$, ta ký hiệu $\bar{x}$ là lớp modulo $\mathcal{R}$ của x.

Chứng minh rằng $\bar{e}$ là một nhóm con của G, và : $\forall x \in G, \forall y \in \bar{e}, xyx^{-1} \in \bar{e}$.

2) Một nhóm con H của G là **chuẩn tắc** trong G và ta ký hiệu $H \lhd G$, khi và chỉ khi :

$$\forall x \in H, \forall y \in G, \quad yxy^{-1} \in H.$$

Giả sử H là một nhóm con chuẩn tắc của G. Ta kí hiệu $\mathcal{R}_H$ là quan hệ trong G được xác định bởi :

$$\forall (x, x') \in G^2, (x\mathcal{R}_H x' \ \Leftrightarrow x^{-1}x' \in H).$$

Chứng minh rằng $\mathcal{R}_H$ là một quan hệ tương đương trong G, tương thích trái và phải với luật của G, và H là lớp modulo $\mathcal{R}_H$ của e.

3) a) Chứng minh rằng, nếu G giao hoán thì mọi nhóm con của G đều chuẩn tắc trong G.
b) Cho một ví dụ về một nhóm G và một nhóm con H của G sao cho H không chuẩn tắc trong G.

4) Cho G, G' là hai nhóm, $f : G \to G'$ là một đồng cấu nhóm.
a) Chứng minh rằng, với mọi nhóm con chuẩn tắc H' của G', $f^{-1}(H')$ là một nhóm con chuẩn tắc của G. Đặc biệt, $\mathrm{Ker}(f)$ là một nhóm con chuẩn tắc của G.
b) Cho một ví dụ về các nhóm G, G' với đồng cấu nhóm $f : G \to G'$, và với nhóm con H chuẩn tắc trong G, mà $f(H)$ không phải là một nhóm con chuẩn tắc của G'.
c) Chứng minh rằng, nếu $H \lhd G$ và nếu f là toàn ánh, thì $f(H) \lhd G'$.

5) a) Cho $(G, \cdot)$ là một nhóm. $C(G)$ là **tâm** của G xác định bởi:
$$C(G) = \{a \in G;\ \forall x \in G,\ ax = xa\}.$$
Chứng minh : $C(G) \lhd G$.
b) Cho G là một nhóm hữu hạn với bản số chẵn $2n$ ($n \in \mathbb{N}^*$). Chứng minh rằng mọi nhóm con của G với bản số n đều chuẩn tắc trong G.

II Nhóm thương

Cho G là một nhóm, H là một nhóm con chuẩn tắc của G. Ta ký hiệu $\mathcal{R}_H$ là quan hệ tương đương trong G xác định bởi:
$$\forall (x, x') \in G^2, \quad (x \mathcal{R}_H x' \Leftrightarrow x^{-1}x' \in H).$$
Với $x \in G$, ta ký hiệu $\overline{x}$ là lớp modulo $\mathcal{R}_H$ của x. Ta ký hiệu G/H thay vì $G/\mathcal{R}_H$.

1) Chứng minh: $\forall (x, x', y, y') \in G^4,\ \left(\begin{cases} x \mathcal{R} x' \\ y \mathcal{R} y' \end{cases} \Rightarrow xy \mathcal{R} x'y' \right)$.

2) Suy ra rằng ta có thể định nghĩa một luật hợp thành trong trên G/H, vẫn ký hiệu là $\cdot$, bởi:
$$\forall (x, y) \in G^2, \quad \overline{x} \ \overline{y} = \overline{xy}\ .$$

3) Chứng minh rằng $(G/H, \cdot)$ là một nhóm, được gọi là **nhóm thương** của G theo nhóm con chuẩn tắc H.

4) a) **Nhân tử hóa một đồng cấu nhóm**
Cho G (tương ứng: G') là một nhóm, H (tương ứng: H') là một nhóm con chuẩn tắc của G (tương ứng: G'), $f : G \to G'$ là một đồng cấu nhóm sao cho $f(H) \subset H'$. Chứng minh rằng f tương thích với các quan hệ tương đương $\mathcal{R}_H$ trong G và $\mathcal{R}_{H'}$ trong G' (xem C 1.1 *A*).
Vậy tồn tại (xem C1.1.A 1)) một ánh xạ $\tilde{f} : G/H \to G'/H'$ duy nhất, sao cho biểu đồ
$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ p \downarrow & & \downarrow p' \\ G/H & \xrightarrow[\tilde{f}]{} & G'/H' \end{array}$$
giao hoán, trong đó p, p' là các toàn ánh chính tắc.
Chứng minh $\tilde{f}$ là một đồng cấu nhóm.

b) **Phân tích chính tắc một đồng cấu nhóm**
Cho G, G' là hai nhóm, $f : G \to G'$ là một đồng cấu nhóm. Chứng minh rằng tồn tại một đồng cấu nhóm duy nhất $\hat{f} : G/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ sao cho $f = i \circ \hat{f} \circ p$ (trong đó $\mathrm{Ker}(f) = \{x \in G;\ f(x) = e'\}$, $\mathrm{Im}(f) = \{x' \in G';\ \exists x \in G,\ x' = f(x)\}$, $i : \mathrm{Im}(f) \to G'$ là đơn ánh chính tắc, $p : G \to G/\mathrm{Ker}(f)$ là toàn ánh chính tắc), và $\hat{f}$ là một đẳng cấu nhóm.

Ví dụ: (xem 4.1.2): Xác định i, $\hat{f}$, p khi $G = \mathbb{Z}$, $G' = \mathbb{Z}/n\mathbb{Z}$ ($n \in \mathbb{N}^*$), $f : \underset{k \mapsto \overline{k}}{G \to G'}$ (trong đó $\overline{k}$ là lớp modulo n của k).

◊ C2.3 Vành Boole hữu hạn

Một vành A được gọi là **vành Boole** khi và chỉ khi: $\forall x \in A,\ x^2 = x$.

I *1) Ví dụ*

Cho một tập hợp E.

a) Chứng minh rằng $((\mathbb{Z}/2\mathbb{Z})^E, +, \cdot)$ là một vành Boole (trong đó $\mathbb{Z}/2\mathbb{Z} = \{\hat{0}, \hat{1}\}$ được trang bị phép cộng và phép nhân modulo 2, xem 4.1.2. Mệnh đề 3).

b) Chứng minh rằng $(\mathfrak{P}(E), \Delta, \cap)$ là một vành Boole đẳng cấu với $((\mathbb{Z}/2\mathbb{Z})^E, +, \cdot)$.

2) Cho A là một vành Boole.

a) Chứng minh: $\forall x \in A,\ x + x = 0$.

b) Chứng minh rằng A giao hoán.

c) Chứng minh: $\forall (x, y) \in A^2,\ \ xy(x + y) = 0$.

d) Chỉ trong câu *I* 2) *d)* này ta giả thiết rằng A là vành nguyên. Chứng minh rằng A đẳng cấu với $\{0\}$ hoặc với $\mathbb{Z}/2\mathbb{Z}$ (sử dụng *c)*).

II Cho A là một vành Boole.

1) Chứng minh rằng quan hệ $\leq$ trong A xác định bởi: $\forall (x, y) \in A^2,\ (x \leq y \Leftrightarrow xy = x)$ là một quan hệ thứ tự trong A.

2) a) Chứng minh rằng, với mọi (x, y) thuộc A^2, $\mathrm{Inf}(x, y)$ và $\mathrm{Sup}(x, y)$ tồn tại và tương ứng bằng xy và $x + y + xy$.

b) Ký hiệu $x \wedge y = \mathrm{Inf}(x, y)$ và $x \vee y = \mathrm{Sup}(x, y)$, chứng minh rằng các luật hợp thành trong $\wedge$ và $\vee$ kết hợp, giao hoán, và luật này phân phối đối với luật kia.

3) a) Chứng minh rằng A có một phần tử bé nhất, đó là 0.

b) Chứng minh rằng, với mọi x thuộc A, tồn tại một phần tử duy nhất của A, mà ta sẽ ký hiệu là x^*, sao cho $\begin{cases} x \wedge x^* = 0 \\ x \vee x^* = 1 \end{cases}$, và hãy tính x^* theo x.

c) Chứng minh các công thức sau, với mọi (x, y) thuộc A^2:

1) $0^* = 1$ và $1^* = 0$

2) $x^{**} = x$

3) $(x \vee y)^* = x^* \wedge y^*$ và $(x \wedge y)^* = x^* \vee y^*$

4) $x \leq y \Leftrightarrow y^* \leq x^*$

5) $x \leq y \Leftrightarrow x \wedge y^* = 0 \Leftrightarrow x^* \vee y = 1$.

4) Ta giả thiết rằng trong câu hỏi này A *hữu hạn*. Ta ký hiệu M là tập hợp các phần tử cực đại của $A - \{1\}$ (xem 1.2.3, 2), Định nghĩa 1, 4) và $\phi : A \to \mathfrak{P}(M)$ là ánh xạ xác định bởi:

$$\forall x \in A,\quad \phi(x) = \{m \in M;\ \text{không } (x \leq m)\},$$

a) Chứng minh, với bất kỳ (x, m) thuộc $A \times M$:

$$(\text{không } (x \leq m)) \Leftrightarrow mx \neq x \Leftrightarrow x^* \leq m \Leftrightarrow (1 + m)(1 + x) = 0.$$

b) Chứng minh, với mọi (x, y, m) thuộc $A \times A \times M$:

$$x \wedge y \leq m \Leftrightarrow (x \leq m \text{ hoặc } y \leq m).$$

c) Suy ra, với mọi (x, y) thuộc A^2:

1) $\phi(x) = \varnothing \Leftrightarrow x = 0$

2) $\phi(x^*) = \complement_M(\phi(x))$

3) $\phi(x \wedge y) = \phi(x) \cap \phi(y)$

4) $\phi(x \vee y) = \phi(x) \cup \phi(y)$.

d) Chứng minh rằng ϕ là một đẳng cấu vành.

Chương 3

Số nguyên, số hữu tỷ

3.1 Các tính chất của $\mathbb{N}$

3.1.1 Cấu trúc của $\mathbb{N}$

Ở đây ta nhắc lại các tính chất thường dùng của tập hợp $\mathbb{N}$ **các số tự nhiên**, xem như đã biết. Độc giả nào quan tâm sẽ tìm thấy một cách xây dựng $\mathbb{N}$ (theo tiên đề của Peano) trong giáo trình của J.M. Arnaudiès và H.Fraysse, Tập 1, trang 41-54.

Tập hợp $\mathbb{N} = \{ 0, 1, 2, 3..\}$ được trang bị hai luật hợp thành trong + (phép cộng) và . (phép nhân), thỏa mãn:

+ kết hợp, + giao hoán, + có phần tử trung hòa ký hiệu là 0.

Mọi phần tử của $\mathbb{N}$ đều chính quy đối với +

. kết hợp, . giao hoán, . có phần tử trung hòa, ký hiệu là 1

. phân phối đối với +

Mọi phần tử của $\mathbb{N}^*$ (= $\mathbb{N}$ - {0}), đều chính quy đối với .

Tập hợp $\mathbb{N}$ được trang bị một quan hệ thứ tự toàn phần ≤ thỏa mãn:

Mọi bộ phận khác rỗng của $\mathbb{N}$ có một phần tử bé nhất (ta nói rằng $\mathbb{N}$ là tập hợp **được sắp thứ tự** tốt).

Mọi bộ phận khác rỗng và bị chặn trên của $\mathbb{N}$ có một phần tử lớn nhất.

≤ tương thích với +, tức là: $\forall(a, b, c)\in \mathbb{N}^3, (a \le b \Rightarrow a + c \le b + c)$

≤ tương thích với . , tức là: $\forall(a, b, c) \in \mathbb{N}^3, (a \le b \Rightarrow ac \le bc)$.

Ta suy ra các tính chất sau:

$$\forall(a, b, c, d) \in \mathbb{N}^4, \left(\begin{cases} a \le b \\ c \le d \end{cases} \Rightarrow a + c \le b + d\right)$$

$$\forall(a, b, c) \in \mathbb{N}^3, \quad (a + c \le b + c \Leftrightarrow a \le b)$$

$$\forall(a, b, c, d) \in \mathbb{N}^4, \left(\begin{cases} a \le b \\ c \le d \end{cases} \Rightarrow ac \le bd\right)$$

$$\forall(a, b, c) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}^*, (ac \le bc \Leftrightarrow a \le b)$$

$$\forall(a, b, n) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}^*, (a \le b \Leftrightarrow a^n \le b^n)$$

Cuối cùng, nếu một bộ phận E của $\mathbb{N}$ thỏa mãn $\begin{cases} 0 \in E \\ \forall n \in E, \quad n+1 \in E \end{cases}$,

thì $E = \mathbb{N}$ (**nguyên lý quy nạp**).

3.1.2 Nguyên lý quy nạp

Nguyên lý quy nạp đã nói trên đây ở 3.1.1 cũng có thể diễn tả như sau:

Giả sử $n_0 \in \mathbb{N}$ và $P(n)$ là một tính chất đối với một số tự nhiên $n \geq n_0$. Muốn cho $P(n)$ đúng với mọi n thuộc $\mathbb{N}$ mà $n \geq n_0$ điều kiện cần và đủ là ta có:

$\begin{cases} \bullet\ P(n_0) \text{ đúng} \\ \bullet\ \text{Với mọi } n \text{ thuộc } \mathbb{N} \text{ mà } n \geq n_0, \text{ nếu } P(n) \text{ đúng, thì } P(n+1) \text{ cũng đúng.} \end{cases}$

VÍ DỤ:

Chứng minh: $\forall n \in \mathbb{N}^*,\ 2\sum_{k=1}^{n} k = n(n+1)$.

Công thức là hiển nhiên với $n = 1$. Nếu $2\sum_{k=1}^{n} k = n(n+1)$, thì:

$$2\sum_{k=1}^{n+1} k = \left(2\sum_{k=1}^{n} k\right) + 2(n+1) = n(n+1) + 2(n+1) = (n+1)(n+2).$$

Ta chú ý rằng cũng có thể thu được công thức phải chứng minh bằng cách cộng từng vế:

$$\begin{cases} \sum_{k=1}^{n} k = 1 + 2 + \ldots + (n-1) + n \\ \sum_{k=1}^{n} k = n + (n-1) + \ldots + 2 + 1. \end{cases}$$

Coi như ta đã biết khái niệm phân số (xem 3.7), ta có:

$$\boxed{\forall n \in \mathbb{N}^*,\ \sum_{k=1}^{n} k = \frac{n(n+1)}{2}.}$$

Độc giả có thể chứng minh theo cách tương tự, bằng quy nạp, các công thức kinh điển sau đây với n bất kỳ thuộc $\mathbb{N}^*$: $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$, $\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$.

Tổng quát hơn, để tính $\sum_{k=1}^{n} k^p$, xem bài tập 3.3.19. ■

Trong một lập luận quy nạp, để suy ra $P(n+1)$, ta có thể cần đến không những chỉ $P(n)$, mà còn các $P(k)$ với $n_0 \le k \le n$. Áp dụng nguyên lý quy nạp vào tính chất $Q(n)$ xác định bởi:

$$Q(n) \Leftrightarrow (\forall k \in \{n_0, \ldots, n\}, \quad P(k)),$$

ta được: Muốn cho $P(n)$ là đúng với bất kỳ n thuộc $\mathbb{N}$ mà $n \ge n_0$, cần và đủ là ta có:

- $P(n_0)$ đúng
- Với n bất kỳ thuộc $\mathbb{N}$ sao cho $n \ge n_0$, nếu $P(k)$ đúng với mọi k thuộc $\{n_0, \ldots, n\}$, thì $P(n+1)$ đúng.

Trong trường hợp này, ta nói là đã áp dụng phép **quy nạp mạnh.**

3.1.3 Tính chia hết trong $\mathbb{N}$

♦ **Định nghĩa 1** Cho $(a,b) \in \mathbb{N}^2$. Ta nói rằng a **chia hết** b (trong $\mathbb{N}$), và ký hiệu $a \mid b$, khi và chỉ khi tồn tại $c \in \mathbb{N}$ sao cho $b = ac$.

Một số tự nhiên n được gọi là **chẵn (lẻ)** khi và chỉ khi $2 \mid n$ (tương ứng : $2 \mid n+1$)

NHẬN XÉT:

1) $\forall a \in \mathbb{N}, \quad a \mid 0$.

2) $\forall b \in \mathbb{N}, \quad (0 \mid b \Leftrightarrow b = 0)$.

♦ **Mệnh đề**

Quan hệ $\mid$ là một quan hệ thứ tự không toàn phần trong $\mathbb{N}$.

Chứng minh:

1) Tính phản xạ là hiển nhiên.

2) Giả sử $a \mid b$ và $b \mid a$. Vậy tồn tại $c, d \in \mathbb{N}$ sao cho $b = ac$ và $a = bd$; suy ra $b = bcd$.
Nếu $b \neq 0$, thì $cd = 1$, vậy $c = d = 1$, $a = b$.
Nếu $b = 0$, thì $a = 0$, vậy $a = b$.
Như thế, $\mid$ phản đối xứng.

3) Giả sử $a \mid b$ và $b \mid c$. Vậy tồn tại $d, e \in \mathbb{N}$ sao cho $b = ad$ và $c = be$, từ đây $c = a(de)$ và $de \in \mathbb{N}$, vậy $a \mid c$. Như thế $\mid$ có tính bắc cầu.

4) $2 \not| 3$ và $3 \not| 2$, vậy $|$ là không toàn phần.

Ta chứng minh dễ dàng các tính chất sau, dưới đây ta sẽ trở lại các tính chất đó trong số học của $\mathbb{Z}$ (4.1.1, Mệnh đề 2):

1) $\forall (a, b, c) \in \mathbb{N}^3, (a \mid b \Rightarrow a \mid bc)$

2) $\forall (a, b, c) \in \mathbb{N}^3, \left(\begin{cases} a \mid b \\ a \mid c \end{cases} \Rightarrow a \mid b + c \right)$

3) $\forall (a, b, \alpha, \beta) \in \mathbb{N}^4, \left(\begin{cases} a \mid b \\ \alpha \mid \beta \end{cases} \Rightarrow a\alpha \mid b\beta \right)$

4) $\forall (a, b, n) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}^*, (a \mid b \Rightarrow a^n \mid b^n)$.

Để thuận tiện, nếu $a \mid b$ và $a \neq 0$, ta có thể ký hiệu phần tử duy nhất c của $\mathbb{N}$ sao cho $b = ac$ là $\frac{a}{b}$, coi như đã đi trước việc khảo sát $\mathbb{Q}$ (3.7).

♦ **Định nghĩa 2** Một phần tử p của $\mathbb{N}$ được gọi là **nguyên tố** khi và chỉ khi:

$$\begin{cases} p \geq 2 \\ \forall a \in \mathbb{N}, (a \mid p \Rightarrow (a = 1 \text{ hoặc } a = p)). \end{cases}$$

Dưới đây (4.4.3, Định lý 2), ta sẽ chứng minh rằng tập hợp các số nguyên tố $\mathbb{P} = \{2, 3, 5, 7, 11 \ldots\}$ là vô hạn.

Bài tập

◊ **3.1.1** Chứng minh: $\forall (a, b, c) \in (\mathbb{N}^*)^3, (ab < c \Rightarrow a + b \leq c)$.

◊ **3.1.2** Giải trong $\mathbb{N}^3$: $10x + 15y + 6z = 133$.

◊ **3.1.3** Chứng minh rằng với mọi n thuộc $\mathbb{N}$:

(i) $1^{2n} + 2^{2n} + 3^{2n} \geq 2.7^n$.

(ii) $1^{2n+1} + 2^{2n+1} + 3^{2n+1} \geq 6^{n+1}$

và khảo sát các trường hợp đẳng thức.

Các bài tập 3.1.4 *và* 3.1.5 *minh họa nguyên lý quy nạp.*

◊ **3.1.4** Chứng minh:

a) $\forall n \in \mathbb{N} - \{0, 1\}, \sum_{k=1}^{n} \frac{1}{k^2} > \frac{3n}{2n+1}$

b) $\forall n \in \mathbb{N}^*, \quad 4^n (n!)^3 < (n+1)^{3n}$

c) $\forall n \in \mathbb{N}^*, \quad 1!3! \ldots (2n+1)! \geq ((n+1)!)^{n+1}$

d) $\forall n \in \mathbb{N}^*, \quad \sqrt{\frac{3}{4n+3}} < \prod_{k=1}^{n} \frac{4k+1}{4k+3} < \sqrt{\frac{5}{4n+5}}$.

◊ **3.1.5** Cho $n \in \mathbb{N} - \{0, 1\}$, E là một tập hợp, $(A_i)_{1 \leq i \leq n}$ là một họ những bộ phận của E. Chứng minh rằng $\Delta_{i=1}^{n} A_i$ (trong đó Δ là hiệu đối xứng) là tập hợp các phần tử của E thuộc đúng một số lẻ A_i.

◊ **3.1.6** Chứng minh $f : \mathbb{N} \times \mathbb{N}^* \to \mathbb{N}$ là đơn ánh.
$(x, y) \mapsto (x + y)^2 + y$

◊ **3.1.7** Tìm các cặp ánh xạ (f, g) từ $\mathbb{N}^*$ vào $\mathbb{N}^*$ sao cho:

$$\forall (x, y) \in (\mathbb{N}^*)^2, \quad (f(x))^{g(y)} + (f(y))^{g(x)} = x + y .$$

◊ **3.1.8** Tìm tất cả các bộ ba ánh xạ (f, g, h) từ $\mathbb{N}^*$ vào $\mathbb{N}^*$ sao cho:

$$\forall (x,y,z) \in (\mathbb{N}^*)^3, \quad (f(x))^{g(y)} + (g(y))^{h(z)} + (h(z))^{f(x)} = x + y + z .$$

◊ **3.1.9*** Tìm tất cả các ánh xạ $f : \mathbb{N} \to \mathbb{N}$ tăng nghiêm ngặt và thỏa mãn:

$$\begin{cases} f(2) = 2 \\ \forall (p,q) \in \mathbb{N}^2, f(pq) = f(p) f(q) \end{cases}$$

◊ **3.1.10** Tính $\sum_{k=1}^{n} k(n+1-k)$ với $n \in \mathbb{N}^*$.

◊ **3.1.11*** Với $(n, p) \in \mathbb{N}^* \times \mathbb{N}$, ta ký hiệu $S_p(n) = \sum_{k=1}^{n} k^p$. Tìm tất cả các bộ ba (p, q, r) thuộc $(\mathbb{N}^*)^3$ sao cho : $r \geq 2$ và: $\forall n \in \mathbb{N}^*, S_p(n) = (S_q(n))^r$.

3.2 Tập hợp hữu hạn, tập hợp vô hạn

Chủ đích của ta ở đây không phải là xây dựng một lý thuyết về bản số, mà chỉ rút ra các tính chất cơ bản của các tập hữu hạn. Phần lớn các tính chất này có thể xem như là hiển nhiên một cách trực quan.

Ta không đề cập đến vấn đề **đếm được** (cùng lực lượng với $\mathbb{N}$), mà độc giả có thể tham khảo trong Giáo trình của J.M.Arnaudiès và H.Fraysse (Tập 1, trang 59-61).

3.2.1 Tập hợp cùng lực lượng

♦ **Định nghĩa** Ta nói rằng một tập hợp E **cùng lực lượng** (hay: **đẳng lực**) với một tập hợp F khi và chỉ khi tồn tại một song ánh từ E lên F.

Ví dụ:

1) $\{2, 4\}$ đẳng lực với $\{1, 2\}$.

2) $\mathbb{N}^*$ đẳng lực với $\mathbb{N}$ vì ánh xạ $\mathbb{N}^* \to \mathbb{N}$, $n \mapsto n-1$ là một song ánh.

♦ **Mệnh đề** Quan hệ "cùng lực lượng" (hay "đẳng lực") là một quan hệ tương đương giữa các tập hợp.

Chứng minh:

1) Với tập hợp E bất kỳ, $\mathrm{Id}_E : E \to E$ là một song ánh.

2) Nếu $f : E \to F$ là một song ánh, thì f^{-1} là một song ánh từ F lên E (xem 1.3.2, Mệnh đề 3).

3) Nếu $f : E \to F$, $g : F \to G$ là một song ánh thì $g \circ f : E \to G$ là một song ánh (xem 1.3.2, Mệnh đề 1).

Ta ký hiệu $E \simeq F$ để chỉ E đẳng lực với F.

3.2.2 Tập hợp hữu hạn

Ở đây ta ký hiệu $F_0 = \varnothing$ và, với mọi n thuộc $\mathbb{N}^*$, $F_n = \{1, ..., n\} = \{k \in \mathbb{N}, 1 \le k \le n\}$.

Độc giả cũng có thể gặp ký hiệu $[\![1; n]\!]$ để chỉ F_n.

♦ **Định nghĩa 1** Một tập hợp E được gọi là **hữu hạn** khi và chỉ khi tồn tại $n \in \mathbb{N}$ sao cho E đẳng lực với F_n.

♦ **Mệnh đề 1** Nếu một tập hợp E là hữu hạn, thì mọi tập hợp E' đẳng lực với E đều hữu hạn.

Chứng minh:

Nếu $E \simeq F_n$ và $E' \simeq E$ thì $E' \simeq F_n$ vì $\simeq$ có tính bắc cầu.

Ta có thể xem Mệnh đề sau đây là hiển nhiên theo trực giác :

♦ **Mệnh đề 2** Cho $(n, p) \in \mathbb{N}^2$.

1) Tồn tại một đơn ánh từ F_n vào F_p khi và chỉ khi $n \leq p$.

2) Tồn tại một toàn ánh từ F_n lên F_p khi và chỉ khi $n \geq p$.

3) Tồn tại một song ánh từ F_n lên F_p khi và chỉ khi $n = p$.

Theo điểm 3) của Mệnh đề 2 trên đây, ta có thể phát biểu Định nghĩa sau:

♦ **Định nghĩa 2** Cho E là một tập hợp hữu hạn. Tồn tại một số tự nhiên n duy nhất thuộc $\mathbb{N}$ sao cho E đẳng lực với F_n ; n được gọi là **bản số** của E và được ký hiệu Card(E) hoặc #(E).

Từ mệnh đề 2 ta suy ra Mệnh đề 3 sau:

♦ **Mệnh đề 3** Cho hai tập hợp E, E' .

1) Nếu E' hữu hạn thì tồn tại một đơn ánh từ E vào E' khi và chỉ khi

$$E \text{ hữu hạn và } \#(E) \leq \#(E').$$

2) Nếu E hữu hạn thì tồn tại toàn ánh từ E lên E' khi và chỉ khi

$$E' \text{ hữu hạn và } \#(E) \geq \#(E').$$

3) Nếu E hoặc E' hữu hạn thì tồn tại một song ánh từ E lên E' khi và chỉ khi

$$E \text{ và } E' \text{ đều hữu hạn và } \#(E) = \#(E').$$

♦ **Mệnh đề 4** Nếu E là một tập hợp hữu hạn, thì mọi bộ phận F của E đều hữu hạn, và ta có: $\#(F) \leq \#(E)$.

Chứng minh :

Chỉ cần áp dụng Mệnh đề 3.1 vào đơn ánh chính tắc $F \to E$.

♦ **Mệnh đề 5** Nếu E, F là hai tập hợp hữu hạn, thì $E \cup F$ hữu hạn và:

$$\#(E \cup F) + \#(E \cap F) = \#(E) + \#(F).$$

Chứng minh:

1) Giả sử A, B là hai tập hợp hữu hạn, rời nhau; ta ký hiệu: $a = \#(A)$, $b = \#(B)$. Tồn tại một song ánh $\alpha : F_a \to A$ và một song ánh β: $F_b \to B$. Rõ ràng ánh xạ γ: $F_{a+b} \to A \cup B$ xác định bởi: $\forall n \in F_{a+b}$, $\gamma(n) = \begin{cases} \alpha(n) & \text{nếu } 1 \leq n \leq a \\ \beta(n-a) & \text{nếu } a+1 \leq n \leq a+b \end{cases}$

là một song ánh. Suy ra $A \cup B$ hữu hạn và : $\#(A \cup B) = \#(A) + \#(B)$.

2) Áp dụng 1) đối với $(E, F - E)$ thay cho (A, B), ta kết luận $E \cup F$ hữu hạn và

$$\#(E \cup F) + \#(E \cap F) = \#(E \cup (F - E)) + \#(E \cap F) = (\#(E) + \#(F - E)) + \#(E \cap F)$$

$$= \#(E) + (\#(F - E) + \#(E \cap F)) = \#(E) + \#(F).$$

Về việc mở rộng ra cho trường hợp n tập hợp hữu hạn (**công thức cái sàng**), xem bài tập 3.2.7.

♦ **Hệ quả 1** Cho E là một tập hợp hữu hạn, $F \in \mathfrak{P}(E)$. Nếu $\#(F) = \#(E)$, thì $F = E$.

Chứng minh:

Nếu $\#(F) = \#(E)$, thì do $\#(E) = \#(F) + \#(E - F)$, nên ta suy ra $\#(E - F) = 0$, $E - F = \varnothing$, $F = E$.

♦ **Hệ quả 2** Cho $n \in \mathbb{N}^*$ và $E_1, ..., E_n$ là những tập hợp hữu hạn. Nếu $E_1, ..., E_n$ rời nhau từng đôi thì : $\#\left(\bigcup_{i=1}^{n} E_i\right) = \sum_{i=1}^{n} \#(E_i)$.

Chứng minh:

Quy nạp theo n.

Tính chất đang xét đúng với $n = 1$, $n = 2$ (xem Mệnh đề 5).

Nếu nó đúng với n, và nếu $E_1, ..., E_{n+1}$ là những tập hợp hữu hạn rời nhau từng đôi thì $E_1, ..., E_n$ rời nhau từng đôi và $\left(\bigcup_{i=1}^{n} E_i\right) \cap E_{n+1} = \varnothing$, suy ra :

$$\#\left(\bigcup_{i=1}^{n+1} E_i\right) = \#\left(\bigcup_{i=1}^{n} E_i\right) + \#(E_{n+1}) = \sum_{i=1}^{n} \#(E_i) + \#(E_{n+1}) = \sum_{i=1}^{n+1} \#(E_i).$$

♦ **Mệnh đề 6** Cho E, E' là hai tập hợp hữu hạn có cùng một bản số, và $f : E \to E'$ là một ánh xạ. Các tính chất sau là tương đương:

(i) f là đơn ánh (ii) f là toàn ánh (iii) f là song ánh.

Chứng minh:

1) (i) $\Rightarrow$ (ii), và (i) $\Rightarrow$(iii):

Nếu f là đơn ánh, thì $\tilde{f} : E \to f(E)$, $x \mapsto f(x)$ là song ánh, vậy $\#(f(E)) = \#(E) = \#(E')$, suy ra $f(E) = E'$ (xem Hệ quả 1), f là toàn ánh, và như vậy f là song ánh.

2) (ii) $\to$ (i), và (ii) $\to$ (iii):

Giả sử f là toàn ánh và không đơn ánh. Vậy tồn tại $x_1, x_2 \in E$ sao cho: $x_1 \neq x_2$ và $f(x_1) = f(x_2)$. Ánh xạ $g : E - \{x_2\} \to E'$, $x \mapsto f(x)$ là toàn ánh, vậy (xem Mệnh đề 3, 2)) :

$$\#(E - \{x_2\}) \geq \#(E').$$

Nhưng $\#(E - \{x_2\}) = \#(E) - 1$ và $\#(E') = \#(E)$, mâu thuẫn.

Như thế f là đơn ánh, do đó song ánh.

3) (iii) $\Rightarrow$ (i), và (iii) $\Rightarrow$ (ii) là tầm thường.

◆ **Mệnh đề 7** Nếu E , F là hai tập hợp hữu hạn, thì $E \times F$ hữu hạn và $\#(E \times F) = \#(E).\#(F)$.

Chứng minh:

Ký hiệu $n = \#(E)$, $p = \#(F)$, rõ ràng rằng $F_n \times F_p$ hữu hạn, có bản số np và $E \times F$ đẳng lực với $F_n \times F_p$.

Ta cũng có thể chú ý rằng: $E \times F = \bigcup_{f \in F} (E \times \{f\})$,và áp dụng Hệ quả 2. ■

Ta suy ra dễ dàng (do quy nạp theo n), với mọi n thuộc $\mathbb{N}^*$ và mọi tập hữu hạn $E_1, ..., E_n$, rằng tập hợp $\prod_{i=1}^{n} E_i$ hữu hạn và $\#\left(\prod_{i=1}^{n} E_i\right) = \prod_{i=1}^{n} \#(E_i)$. ■

Đặc biệt, với n bất kỳ thuộc $\mathbb{N}^*$ và tập hợp hữu hạn E bất kỳ, E^n hữu hạn và:

$$\#(E^n) = (\#(E))^n.$$

◆ **Hệ quả** Nếu E, F là hai tập hợp hữu hạn, thì F^E hữu hạn và:

$$\#(F^E) = (\#(F))^{\#(E)}.$$

Chứng minh:

Chỉ cần chú ý rằng F^E đẳng lực với $F^{\#(E)}$ và áp dụng kết quả trên đây.

NHẬN XÉT:

1) Công thức trên lý giải cho ký hiệu tổng quát F^E dùng để chỉ tập hợp các ánh xạ từ E vào F.

2) Nếu $E = \emptyset$, thì F^E được tạo thành bởi một ánh xạ duy nhất, đó là ánh xạ rỗng, có đồ thị $\emptyset$, và như vậy $\#(F^E) = 1$; ta lại được $(\#(F))^{\#(E)} = (\#(F))^0 = 1$. Đặc biệt: $0^0 = 1$.

Cần chú ý không lẫn lộn ký hiệu đại số 0^0 này với một giới hạn mà ta có thể gặp.

3.2.3 Tập hợp vô hạn

♦ **Định nghĩa** Một tập hợp được gọi là **vô hạn** khi và chỉ khi nó không hữu hạn.

Bằng cách lập luận phản đảo, hoặc phản chứng, từ 3.2.2 ta suy ra các kết quả sau:

♦ **Mệnh đề 1** Nếu một tập hợp E vô hạn, thì mọi tập hợp E' đẳng lực với E đều vô hạn.

♦ **Mệnh đề 2** Cho hai tập hợp E , E'.

1) Nếu E vô hạn và nếu tồn tại một đơn ánh từ E vào E', thì E' vô hạn.

2) Nếu E' vô hạn và nếu tồn tại một toàn ánh từ E lên E', thì E vô hạn.

♦ **Mệnh đề 3** Nếu một tập hợp có ít nhất một bộ phận vô hạn thì chính tập hợp đó cũng vô hạn.

♦ **Mệnh đề 4** Nếu E vô hạn và F khác rỗng, thì $E \times F$ vô hạn.

Cuối cùng, ta có thể xem các kết quả sau như là "tất nhiên":

♦ **Mệnh đề 5** $\mathbb{N}$ là vô hạn.

♦ **Mệnh đề 6** Nếu E vô hạn, thì tồn tại một đơn ánh từ $\mathbb{N}$ vào E.

Bài tập

◊ **3.2.1** Cho một tập hợp hữu hạn E. Chứng minh $\mathfrak{P}(E)$ là hữu hạn và: $\#(\mathfrak{P}(E)) = 2^{\#(E)}$.

◊ **3.2.2** Cho một tập hợp E, chứng minh rằng nếu $\mathfrak{P}(E)$ hữu hạn thì E hữu hạn.

◊ **3.2.3** Chứng minh rằng mọi dãy giảm với hạng tử thuộc $\mathbb{N}$ là dãy dừng.

◊ **3.2.4** Cho hai tập hợp $E, F, f : E \to F$ là một ánh xạ.

a) Giả sử A là một bộ phận hữu hạn của E, chứng minh $f(A)$ hữu hạn và : $\#(f(A)) \leq \#(A)$.

b) Giả sử B là một bộ phận hữu hạn của F, ta có thể khẳng định rằng $f^{-1}(B)$ hữu hạn hay không? Xét trường hợp f là đơn ánh.

◊ **3.2.5** Cho E là một tập hợp, $f : E \to E$ là một phép đối hợp, $A = \{x \in E;\ f(x) \neq x\}$. Giả thiết A hữu hạn, chứng minh $\#(A)$ chẵn.

◊ **3.2.6** Chứng minh rằng $f : \mathbb{N}^2 \to \mathbb{N}$, xác định bởi:

$$f(x, y) = \frac{(x+y)(x+y+1)}{2} + x$$

là song ánh (giả thiết độc giả đã học qua về tập $\mathbb{Q}$).

◊ **3.2.7*** **Công thức sàng**

Cho $n \in \mathbb{N}^*$, $E_1, \ldots, E_n$ là những tập hữu hạn. Chứng minh :

$$\#\left(\bigcup_{i=1}^{n} E_i\right) = \sum_{k=1}^{n} (-1)^{k-1} \sum_{I \in \mathfrak{P}_k(\{1,\ldots,n\})} \#\left(\bigcap_{i \in I} E_i\right),$$

trong đó $\mathfrak{P}_k(\{1, \ldots, n\})$ chỉ tập hợp các bộ phận có k phần tử của $\{1, \ldots, n\}$, chẳng hạn:

$$\#(E_1 \cup E_2 \cup E_3) = \#(E_1) + \#(E_2) + \#(E_3) - (\#(E_1 \cap E_2) + \#(E_1 \cap E_3) + \#(E_2 \cap E_3)) + \#(E_1 \cap E_2 \cap E_3).$$

◊ **3.2.8** Cho E là một tập hợp hữu hạn, $n = \#(E)$, $\mathcal{R}$ là một quan hệ tương đương trong E, $N = \#(E/\mathcal{R})$, ν là số các cặp (x, y) thuộc E^2 thỏa mãn $x \mathcal{R} y$.

a) Ký hiệu $E_1, \ldots, E_N$ là các phần tử của $E/\mathcal{R}$, chứng minh : $\nu = \sum_{i=1}^{N} (\#(E_i))^2$.

b) Suy ra : $n^2 \leq N\nu$.

◊ **3.2.9*** Cho $(a_n)_{n \in \mathbb{N}}$, $(b_n)_{n \in \mathbb{N}}$ là hai dãy có hạng tử thuộc $\mathbb{N}$. Chứng minh :

$$\exists (p, q) \in \mathbb{N}^2,\ (p \neq q,\ a_p \leq a_q,\ b_p \leq b_q).$$

◊ **3.2.10** Cho $(n, p) \in \mathbb{N}^2$, sao cho $n \geq p^2 + 1$, $(x_1, \ldots, x_n) \in \mathbb{N}^n$. Chứng minh :

ít nhất $p + 1$ số $x_1, \ldots, x_n$ bằng nhau
hoặc
ít nhất $p + 1$ số $x_1, \ldots, x_n$ khác nhau từng đôi.

◊ **3.2.11** Cho một tập hợp E. Chứng minh rằng, để cho E hữu hạn, cần và đủ là mọi bộ phận khác rỗng của $\mathfrak{P}(E)$ đều có ít nhất một phần tử cực đại (đối với quan hệ bao hàm).

3.3 Giải tích tổ hợp

Trong mục 3.3 này ta sẽ ký hiệu $F_n = \{1, ..., n\}$, với $n \in \mathbb{N}^*$.

3.3.1 Hoán vị

Ta nhớ lại rằng hoán vị của F_n là mọi song ánh từ F_n vào F_n (Định nghĩa 2).

♦ **Ký hiệu** Ta ký hiệu $\mathfrak{S}_n$ là tập hợp các hoán vị của $\{1, ..., n\}$.

Việc cho một phần tử σ của $\mathfrak{S}_n$ được xác định bởi việc cho liên tiếp $\sigma(1)(\sigma(1) \in F_n)$, $\sigma(2)(\sigma(2) \in F_n - \{\sigma(1)\})$, ..., $\sigma(n)$... Suy ra: $\text{Card}(\mathfrak{S}_n) = n(n-1)...1$.

Tích $\prod_{k=1}^{n} k$ được gọi là **giai thừa** (của) n, và ký hiệu là $n!$.

Như vậy ta được: $\text{Card}(\mathfrak{S}_n) = n!$

3.3.2 Chỉnh hợp

♦ **Định nghĩa** Cho $n, p \in \mathbb{N}^*$ sao cho $p \le n$. **Chỉnh hợp** p phần tử của F_n là mọi bộ - p $(x_1, ..., x_p)$ thuộc $(F_n)^p$ sao cho $x_1, ..., x_p$ từng đôi khác nhau.

VÍ DỤ:

1) (1,4,2) là một chỉnh hợp ba phần tử của F_5.

2) (3,2,2,5) không phải là một chỉnh hợp (vì 2 được lặp lại).

Việc cho một chỉnh hợp p phần tử của F_n quy về việc cho một đơn ánh từ F_p vào F_n. Chính xác hơn, ánh xạ $f \mapsto (f(1), ..., f(p))$ là một song ánh của tập hợp các đơn ánh từ F_p vào F_n, lên tập hợp các chỉnh hợp p phần tử của F_n.

Việc cho một chỉnh hợp $(x_1, ..., x_p)$ quy về việc cho liên tiếp x_1 (trong F_n), x_2 (trong $F_n - \{x_1\}$), ..., x_p (trong $F_n - \{x_1, ..., x_{p-1}\}$). Suy ra số các chỉnh hợp p phần tử của F_n là: $n(n-1)\cdot ... \cdot (n-p+1)$.

Ta ký hiệu số chỉnh hợp p phần tử của F_n là $A_n^p = n(n-1)...(n-p+1) = \dfrac{n!}{(n-p)!}$;

theo quy ước : $A_n^p = 0$ nếu $p > n$.

Đặc biệt: $A_n^n = n!$

NHẬN XÉT:

Chúng ta vừa đếm, bằng một công thức đơn giản, các đơn ánh từ F_p vào $F_n (p \le n)$. Ngược lại, không có một công thức "đơn giản" cho số các toàn ánh từ F_n lên $F_p (n \ge p)$, xem bài tập 3.3.18.

3.3.3 Tổ hợp

◆ **Định nghĩa** Cho $(n, p) \in \mathbb{N}^2$. Mọi bộ phận có bản số p của F_n gọi là **tổ hợp** p phần tử của F_n (hoặc: **khối-p** của F_n).

Giả sử $p \le n$. Ta ký hiệu tập hợp các chỉnh hợp p phần tử của F_n là $\mathcal{A}(n, p)$ và tập hợp các tổ hợp p phần tử của F_n là $\mathcal{C}(n, p)$. Ánh xạ $\mathcal{A}(n,p) \to \mathcal{C}(n,p)$, $(x_1,\ldots,x_p) \mapsto \{x_1,\ldots,x_p\}$ là toàn ánh, và mỗi phần tử $\{x_1,\ldots,x_p\}$ của $\mathcal{C}(n, p)$ có đúng $p!$ tạo ảnh, nhận được bằng cách giao hoán $(x_1, \ldots, x_p)$.

Suy ra: $\text{Card}(\mathcal{A}(n, p)) = p!\text{Card}(\mathcal{C}(n, p))$, từ đó có Mệnh đề sau:

◆ **Mệnh đề - Định nghĩa** Cho $(n, p) \in \mathbb{N}^2$. Nếu $p \le n$, số các tổ hợp p phần tử của $\{1, \ldots, n\}$, ký hiệu là C_n^p (hoặc: $\binom{n}{p}$), là

$$\frac{n(n-1)\ldots(n-p+1)}{p!}.$$

Như vậy, với mọi (n, p) thuộc $\mathbb{N}^2$ sao cho $p \le n$: $\boxed{C_n^p = \frac{n!}{p!(n-p)!}}$.

NHẬN XÉT:

1) Theo định nghĩa C_n^p là một số tự nhiên khác không (với $0 \le p \le n$), và như vậy $p!$ chia hết A_n^p.

2) Nếu $p > n$, thì $C_n^p = 0$.

3) Ta mở rộng định nghĩa các C_n^p bằng quy ước $C_n^p = 0$ nếu $(n, p) \in \mathbb{N} \times \mathbb{Z}^*_-$.

4) $\forall_n \in \mathbb{N}$, $C_n^0 = C_n^n = 1$.

◆ **Mệnh đề 2**

1) $\forall (n, p) \in \mathbb{N} \times \mathbb{Z}$, $C_n^p = C_n^{n-p}$

2) $\forall (n, p) \in \mathbb{N} \times \mathbb{N}$, $C_n^p + C_n^{p+1} = C_{n+1}^{p+1}$ **(công thức cơ bản)**.

Chứng minh:

1) • Nếu $0 \le p \le n$: $C_n^{n-p} = \frac{n!}{(n-p)!\,p!} = C_n^p$.

• Nếu $p < 0$ hoặc $p > n$: $C_n^p = 0$ và $C_n^{n-p} = 0$.

2) • Nếu $0 \le p \le n - 1$:

$$C_n^p + C_n^{p+1} = \frac{n!}{p!(n-p)!} + \frac{n!}{(p+1)!(n-p-1)!} = \frac{n!}{(p+1)!(n-p)!}((p+1)+(n-p))$$

$$= \frac{(n+1)!}{(n+1)!\big((n+1)-(p+1)\big)!} = C_{n+1}^{p+1}.$$

- Nếu $p < -1$ hoặc $p > n$: $C_n^p = C_n^{p+1} = C_{n+1}^{p+1} = 0$.
- Nếu $p = -1$: $C_n^p + C_n^{p+1} = C_n^0 = 1$ và $C_{n+1}^{p+1} = C_{n+1}^0 = 1$.
- Nếu $p = n$: $C_n^p + C_n^{p+1} = C_n^n = 1$ và $C_{n+1}^{p+1} = C_{n+1}^{n+1} = 1$. ■

Ta sắp xếp các C_n^p thành một tam giác, gọi là **tam giác Pascal**, trong đó C_n^p ở hàng thứ n và cột thứ p (với $0 \le p \le n$).

n \ p	0	1	2	3	4	5	...	p	$p+1$	...
1	1	1								
2	1	2	1							
3	1	3	3	1			⋮			
4	1	4	6	4	1					
5	1	5	10	10	5	1				
⋮			⋯					C_n^p	C_n^{p+1}	
n									C_{n+1}^{p+1}	
$n+1$										

♦ **Định lý** **(Công thức nhị thức Newton)**

Giả sử $n \in \mathbb{N}$, A là một vành, $(x, y) \in A^2$ sao cho $xy = yx$. Ta có:

$$(x+y)^n = \sum_{k=0}^{n} C_n^k x^k y^{n-k}$$

(trong đó $x^0 = y^0 = 1$).

Chứng minh:

Quy nạp theo n, xem 2.3.2, Định lý.

Áp dụng công thức nhị thức Newton cho $(x,y) = (1,1)$ hoặc $(x,y) = (1,-1)$, ta được:

♦ **Hệ quả**

$$\forall n \in \mathbb{N}, \quad \sum_{k=0}^{n} C_n^k = 2^n$$

$$\forall n \in \mathbb{N}^*, \quad \sum_{k=0}^{n} (-1)^k C_n^k = 0.$$

Công thức nhị thức Newton sẽ được sử dụng đối với các số x,y thực, phức, cũng như đối với các ma trận vuông giao hoán (xem, chẳng hạn bài tập 8.1.9).

♦ **Mệnh đề 3** Với mọi tập hữu hạn E, $\mathfrak{P}(E)$ hữu hạn và:

$$\text{Card}(\mathfrak{P}(E)) = 2^{\text{Card}(E)}.$$

Chứng minh:

Ký hiệu $n = \text{Card}(E)$, ta có :

$$\mathfrak{P}(E) = \bigcup_{k\in\{0,\dots,n\}} \mathfrak{P}_k(E),$$

trong đó $\mathfrak{P}_k(E) = \{F \in \mathfrak{P}(E);\ \text{Card}(F) = k\}$.

Vậy $\mathfrak{P}(E)$ hữu hạn và:

$$\text{Card}(\mathfrak{P}(E)) = \sum_{k=o}^{n} \text{Card}(\mathfrak{P}_k(E)) = \sum_{k=0}^{n} C_n^k = 2^n . \qquad \blacksquare$$

Xem thêm bài tập 3.2.1.

Cuối cùng ta đi trước việc khảo sát các đa thức (chương 5) để thu được một hằng đẳng thức về các hệ tử của nhị thức.

Cho $n, p, q \in \mathbb{N}$ sao cho $n \le p + q$. Theo công thức nhị thức Newton, hệ tử của X^n trong $(X + 1)^p(X + 1)^q$ là $\sum_{k=0}^{n} C_p^k C_q^{n-k}$, thu được bằng cách khai triển tích $(X + 1)^p(X + 1)^q$. Mặt khác, cũng theo công thức nhị thức Newton, hệ tử của X^n trong $(X + 1)^{p+q}$ là C_{p+q}^n .

Vậy ta có: $\sum_{k=0}^{n} C_p^k C_q^{n-k} = C_{p+q}^n$.

Bài tập

◊ **3.3.1** Cho $n \in \mathbb{N}$ sao cho $n \ge 4$. Chứng minh :

$$C_{C_n^2}^2 = 3C_{n+1}^4 .$$

◊ **3.3.2** Cho $(n, p) \in (\mathbb{N}^*)^2$ sao cho $n > p$. Giải phương trình $C_n^p = C_{n-1}^p + C_{n-x}^{p-x}$ với ẩn $x \in \mathbb{N}^*$.

◊ **3.3.3** Tính, với $n \in \mathbb{N}^*$: $\sum_{k=0}^{n-1} (k+1)\frac{C_n^{k-1}}{C_n^k}$.

◊ **3.3.4** Ký hiệu $P_n = \prod_{k=0}^{n} C_n^k$, chứng minh, với mọi n thuộc $\mathbb{N}^*$: $\frac{P_n}{P_{n-1}} = \frac{n^{n-1}}{(n-1)!} = \frac{n^n}{n!}$.

◊ **3.3.5** Với $(p, q) \in (\mathbb{N}^*)^2$, tính : $\sum_{k=0}^{q} \frac{p}{p+q-k} \cdot \frac{C_q^k}{C_{p+q}^k}$.

◊ **3.3.6** Với mọi $(p, q) \in \mathbb{N}^2$ sao cho $1 \le p \le q$, chứng minh : $\sum_{k=1}^{p} \frac{C_p^k}{C_q^k} = \frac{p}{q-p+1}$.

◊ **3.3.7** Chứng minh : $\forall n \in \mathbb{N}^*$, $(n!)^{(n-1)!} \mid (n!)!$.

◊ **3.3.8** Chứng minh : $\forall (p, q) \in (\mathbb{N}^*)^2$, $\sum_{k=0}^{q-1} (p-2k) C_p^k = q C_p^q$.

◊ **3.3.9** Cho $(n, p, q) \in \mathbb{N}^3$ sao cho $p \ge n + q + 1$. Chứng minh: $\sum_{k=0}^{n} C_{p-k}^q = C_{p+1}^{q+1} - C_{p-n}^{q+1}$.

◊ **3.3.10** Với $(n, p) \in (\mathbb{N}^*)^2$, tính : $\sum_{i=1}^{n} \left(\prod_{j=0}^{p-1} (i+j) \right)$.

◊ **3.3.11** Với $n \in \mathbb{N}^*$, tính : $\sum_{k=0}^{E\left(\frac{n}{2}\right)} C_n^{2k}$ và $\sum_{k=0}^{E\left(\frac{n}{2}\right)} C_n^{2k+1}$.

◊ **3.3.12** Cho $(n, p) \in (\mathbb{N}^*)^2$ sao cho $n \ge 2p$. Tính $\sum_{k=0}^{p} C_n^{p-k} C_n^{p+k}$.

◊ **3.3.13** Chứng minh : $\forall (n, p, q) \in \mathbb{N}^3$, $\sum_{k=0}^{n} (n-k) C_p^{n-k} C_q^k = \frac{np}{p+q} C_{p+q}^n$.

◊ **3.3.14** a) Chứng minh rằng với mọi (n, p) thuộc $\mathbb{N}^2$ sao cho $n \ge p$:

$$\sum_{k=0}^{n} (-1)^{n-k} C_n^k C_k^p = \begin{cases} 1 & \text{nếu } n = p \\ 0 & \text{nếu } n > p \end{cases}.$$

b) Cho A là một vành, $(x_n)_{n \in \mathbb{N}}$ là một dãy trong A, $(y_n)_{n \in \mathbb{N}}$ là dãy xác định bởi:

$$\forall n \in \mathbb{N}, \quad y_n = \sum_{k=0}^{n} C_n^k x_k .$$

Chứng minh : $\forall n \in \mathbb{N}, \quad x_n = \sum_{k=0}^{n} (-1)^{n-k} C_n^k y_k$.

◊ **3.3.15** a) Với bất kỳ (n, p, q) thuộc $\mathbb{N}^3$ sao cho $n \le p + q$, chứng minh rằng:

$$\sum_{k=0}^{p} C_p^k C_q^{n-k} = C_{p+q}^n .$$

b)* Suy ra: $\forall n \in \mathbb{N}^*$, $\sum_{k=0}^{E\left(\frac{n-1}{2}\right)} \left(\frac{n-2k}{n} C_n^k \right)^2 = \frac{1}{n} C_{2n-2}^{n-1}$

◊ **3.3.16** Cho $(k, n) \in \mathbb{N}^*$ sao cho $3k \le n + 1$.

a) Chứng minh : $\forall i \in \{0, ..., k\}$, $C_n^i \le \frac{1}{2^{k-i}} C_n^k$.

b) Suy ra : $\sum_{k=0}^{k} C_n^i \le 2 C_n^k$.

◊ **3.3.17*** Cho $n \in \mathbb{N}$; xác định số các số nguyên lẻ trong các số C_n^k, $0 \le k \le n$ (sử dụng đến cách viết n trong hệ nhị phân).

◊ **3.3.18** Cho $(n, p) \in (\mathbb{N}^*)^2$ sao cho $n \ge p$. Ta ký hiệu số các toàn ánh từ $\{1, ..., n\}$ lên $\{1, ..., p\}$ là S_n^p. Chứng minh : $\sum_{k=1}^{p} C_p^k S_n^k = p^n$.

Suy ra các trị S_5^p với $p \in \{1, ..., 5\}$.

◊ **3.3.19** Với $(n, p) \in \mathbb{N}^2$, ký hiệu $S_p(n) = \sum_{k=0}^{n} k^p$.

a) Chứng minh: $\forall (n, p) \in \mathbb{N}^2$, $S_{p+1}(n+1) = \sum_{k=0}^{p+1} C_{p+1}^k S_k(n)$.

b) Suy ra: $\forall (n, p) \in \mathbb{N}^2$, $(n+1)^{p+1} = \sum_{k=0}^{p} C_{p+1}^k S_k(n)$.

c) Hãy tìm lại các giá trị của các tổng cổ điển $\sum_{k=1}^{n} k$, $\sum_{k=1}^{n} k^2$, $\sum_{k=1}^{n} k^3$.

◊ **3.3.20** Cho $(p, q) \in \mathbb{N}^2$, $E = \{0,1\}^{p+q+1}$,

$$A = \left\{ (x_1, ..., x_{p+q+1}) \in E ; \sum_{i=1}^{p+q+1} x_i \ge p+1 \right\},$$

$$B = C_E(A).$$

a) Với mỗi k thuộc $\{0, ..., q\}$, giả sử A_k là tập hợp các phần tử $(x_1, ..., x_{p+k})$ của E sao cho :

$$\sum_{i=1}^{p+k} x_i = p \quad \text{và} \quad x_{p+k+1} = 1.$$

Chứng minh : $\text{Card}(A_k) = C_{p+k}^{p} 2^{q-k}$

b) Suy ra $\text{Card}(A)$, rồi $\text{Card}(B)$.

c) Chứng minh : $\sum_{k=0}^{q} \frac{C_{p+k}^k}{2^{p+k}} + \sum_{k=0}^{p} \frac{C_{q+k}^q}{2^{q+k}} = 2$.

d) Suy ra: $\forall p \in \mathbb{N}$, $\sum_{i=0}^{n} 2^i C_{2p-i}^{p} = 2^{2p}$.

◊ **3.3.21*** Chứng minh rằng với mọi n thuộc $\mathbb{N}^*$: $\sum_{k=0}^{n} \frac{1}{C_n^k} = \frac{n+1}{2^{n+1}} \sum_{k=1}^{n+1} \frac{2^k}{k}$.

3.4 Nhóm đối xứng

Kết quả của phần này sẽ được sử dụng chủ yếu trong lý thuyết các định thức (chương 9).

Ta nhắc lại rằng (xem 3.3.1), với $n \in \mathbb{N}^*$, $\mathfrak{S}_n$ là tập hợp các hoán vị của $\{1, ..., n\}$ và $\text{Card}(\mathfrak{S}_n) = n!$.

3.4.1 Cấu trúc của $\mathfrak{S}_n$

♦ **Mệnh đề** $\mathfrak{S}_n$ là một nhóm đối với luật $\circ$, được gọi là **nhóm đối xứng**.

Chứng minh:

1) $\forall \rho, \sigma \in \mathfrak{S}_n$, $\sigma \circ \rho \in \mathfrak{S}_n$ (xem 1.3.2, Mệnh đề 1).

2) $\circ$ có tính kết hợp.

3) $\text{Id}_{\{1, ..., n\}} \in \mathfrak{S}_n$.

4) Với mọi σ thuộc $\mathfrak{S}_n$, σ là song ánh và $\sigma^{-1} \in \mathfrak{S}_n$.

Để thuận tiện, ta sẽ ký hiệu ánh xạ đồng nhất của $\{1, ..., n\}$ là e. ■

Một hoán vị σ của $\mathfrak{S}_n$ sẽ được ký hiệu là $\begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n-1) & \sigma(n) \end{pmatrix}$.

3.4.2 Chuyển vị

Ở đây ta giả thiết $n \geq 2$.

♦ **Định nghĩa 1** Với mọi (i, j) thuộc $\{1, ..., n\}^2$ sao cho $i < j$, hoán vị của $\{1, ..., n\}$ xác định bởi

$$\tau_{i,j}(i) = j,\ \tau_{i,j}(j) = i,\ \tau_{i,j}(k) = k, \text{ với mọi } k \text{ thuộc } \{1, ..., n\} - \{i, j\}$$

được gọi là **chuyển vị** đổi chỗ i và j và ký hiệu là $\tau_{i,j}$ (hoặc $\tau_{i,j}$, hoặc (i, j))

VÍ DỤ:

Với $n = 5$, $\tau_{2,4} = (2,4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$.

NHẬN XÉT:

1) $\mathfrak{S}_n$ chứa đúng C_n^2 chuyển vị.

2) Mọi chuyển vị đều đối hợp.

♦ **Định lý 1** Các chuyển vị của $\{1, ..., n\}$ sinh ra nhóm $\mathfrak{S}_n$.

Nói khác đi, mọi hoán vị của $\{1, ..., n\}$ có thể phân tích được (ít nhất bằng một cách) thành một tích (nhiều) chuyển vị.

Chứng minh :

Quy nạp theo n.

$\mathfrak{S}_2 = \{e, \tau_{1,2}\}$ và $e = \tau_{1,2}^2$, vậy $\{\tau_{1,2}\}$ sinh ra $\mathfrak{S}_2$.

Giả sử $n \in \mathbb{N}$ sao cho $n \geq 2$. Ta giả thiết rằng các chuyển vị của $\{1, ..., n\}$ sinh ra $\mathfrak{S}_n$, và giả sử $\sigma \in \mathfrak{S}_{n+1}$.

Trường hợp thứ 1: $\sigma(n+1) = n+1$.

Vì σ là song ánh, nên $\{1, ..., n\}$ ổn định đối với σ, và ánh xạ cảm sinh

$\sigma' : \{1,...,n\} \to \{1,...,n\}$ là một hoán vị của $\{1, ..., n\}$. Theo giả thiết quy nạp, tồn tại

$N \in \mathbb{N}^*$ và các chuyển vị $t_1', ..., t_N'$ của $\{1, ..., n\}$ sao cho:

$$\sigma' = t_1' \circ ... \circ t_N'.$$

Với mỗi r thuộc $\{1, ..., N\}$, ta ký hiệu ánh xạ xác định bởi: $t_r(k) = \begin{cases} t_r'(k) & \text{nếu } 1 \leq k \leq n \\ n+1 & \text{nếu } k = n+1 \end{cases}$,

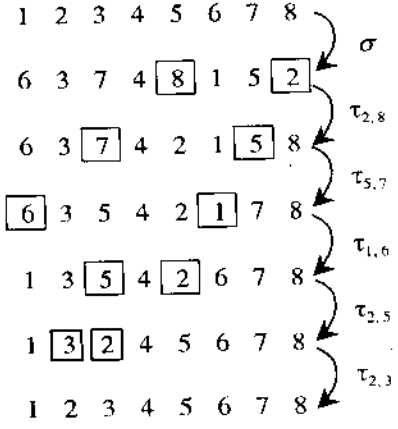
là t_r: $\{1, ..., n+1\} \to \{1, ..., n+1\}$; thì rõ ràng $t_1, ..., t_N$ là những chuyển vị của $\{1, ..., n+1\}$ và $\sigma = t_1 \circ ... \circ t_N$.

Trường hợp thứ 2 : $\sigma(n+1) \neq n+1$.

Xét $\rho = \tau_{n+1,\sigma(n+1)} \circ \sigma$. Ta có $\rho \in \mathfrak{S}_{n+1}$ và $\rho(n+1) = \tau_{n+1,\sigma(n+1)}(\sigma(n+1)) = n+1$. Theo trường hợp thứ 1, tồn tại $N \in \mathbb{N}^*$ và những chuyển vị $t_1, ... t_N$ của $\{1, ..., n+1\}$ sao cho $\rho = t_1 \circ ... \circ t_N$. Vậy $\sigma = \tau_{n+1,\sigma(n+1)} \circ t_1 \circ ... \circ t_N$ và do đó σ là một tích những chuyển vị của $\{1, ..., n+1\}$. ■

Phép chứng minh trên cung cấp một thuật toán cho phép phân tích một hoán vị bất kỳ thành một tích những chuyển vị: sắp xếp lại các phần tử 1, ..., n theo thứ tự, bằng cách (ít nhất) trong mỗi chặng đưa một phần tử về vị trí của nó.

Chẳng hạn, giả sử: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 3 & 7 & 4 & 8 & 1 & 5 & 2 \end{pmatrix}$



Trong mỗi hàng, ta đã đóng khung hai phần tử, chúng sẽ đổi chỗ cho nhau để được hàng tiếp theo.

Vậy ta có : $\tau_{2,3} \circ \tau_{2,5} \circ \tau_{1,6} \circ \tau_{5,7} \circ \tau_{2,8} \circ \sigma = e$, suy ra $\sigma = \tau_{2,8} \circ \tau_{5,7} \circ \tau_{1,6} \circ \tau_{2,5} \circ \tau_{2,3}$.

CHÚ Ý:

Thuật toán trên chứng minh rằng mọi hoán vị của $\{1, ..., n\}$ đều phân tích được, ít nhất bằng một cách, thành một tích của nhiều nhất n chuyển vị.

♦ **Định nghĩa 2** Cho $\sigma \in \mathfrak{S}_n$.

Ta nói rằng một cặp $(\sigma(i), \sigma(j))$ là **một nghịch thế đối với σ** (hoặc: **là một nghịch thế của σ**), khi và chỉ khi: $i < j$ và $\sigma(i) > \sigma(j)$.

Ta ký hiệu số các nghịch thế của σ là $I(\sigma)$, và số ký hiệu là $\varepsilon(\sigma)$ được xác định bởi : $\varepsilon(\sigma) = (-1)^{I(\sigma)}$ gọi là **ký số của σ**.

Ta nói rằng σ **chẵn** (tương ứng: **lẻ**) khi và chỉ khi $\varepsilon(\sigma) = 1$ (tương ứng : $\varepsilon(\sigma) = -1$).

Như thế: • σ chẵn $\Leftrightarrow \varepsilon(\sigma) = 1 \Leftrightarrow I(\sigma)$ chẵn.

• σ lẻ $\Leftrightarrow \varepsilon(\sigma) = -1 \Leftrightarrow I(\sigma)$ lẻ .

♦ **Mệnh đề 1** Với mọi σ thuộc $\mathfrak{S}_n$: $\sigma_n = \prod_{\{i,j\} \in \mathfrak{P}_2(n)} \frac{\sigma(j) - \sigma(i)}{j - i}$, trong đó $\mathfrak{P}_2(n)$ chỉ tập hợp các cặp thuộc $\{1,..., n\}$.

Để thuận tiện, ở đây ta đã đề cập trước đến khái niệm số hữu tỷ (xem 3.7).

Chứng minh :

1) Vì σ là một hoán vị của $\{1,..., n\}$ nên ánh xạ σ_2: $\mathfrak{P}_2(n) \to \mathfrak{P}_2(n)$, $\{i,j\} \mapsto \{\sigma(i), \sigma(j)\}$ là một hoán vị của $\mathfrak{P}_2(n)$, và như vậy:

$$\prod_{\{i,j\} \in \mathfrak{P}_2(n)} |\sigma(j) - \sigma(i)| = \prod_{\{i,j\} \in \mathfrak{P}_2(n)} |j - i| \ ,$$

điều này chứng tỏ: $\left| \prod_{\{i,j\} \in \mathfrak{P}_2(n)} \frac{\sigma(j) - \sigma(i)}{j - i} \right| = 1$.

2) Số các cặp $\{i, j\}$ thuộc $\{1,..., n\}$ sao cho $\frac{\sigma(j) - \sigma(i)}{j - i} < 0$ là $I(\sigma)$, vậy $\prod_{\{i,j\} \in \mathfrak{P}_2(n)} \frac{\sigma(j) - \sigma(i)}{j - i}$ cùng dấu với $\varepsilon(\sigma)$.

NHẬN XÉT:

Ta cũng có: $\varepsilon(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i}$.

♦ **Định lý 2** Ánh xạ ký số $\varepsilon : \mathfrak{S}_n \to \{-1, 1\}$ là một đồng cấu từ nhóm $(\mathfrak{S}_n, \circ)$ lên nhóm nhân $\{-1, 1\}$.

Chứng minh :

Giả sử ρ , $\sigma \in \mathfrak{S}_n$. Ta có :

$$\varepsilon(\sigma \circ \rho) = \prod_{\{i,j\} \in \mathfrak{P}_2(n)} \frac{(\sigma \circ \rho)(j) - (\sigma \circ \rho)(i)}{j - i}$$

$$= \prod_{\{i,j\} \in \mathfrak{P}_2(n)} \frac{\sigma(\rho(j)) - \sigma(\rho(i))}{\rho(j) - \rho(i)} \cdot \prod_{\{i,j\} \in \mathfrak{P}_2(n)} \frac{\rho(j) - \rho(i)}{j - i} .$$

Do ánh xạ $\{i,j\} \mapsto \{\rho(i), \rho(j)\}$ là một hoán vị của $\mathfrak{P}_2(n)$, nên ta có

$$\varepsilon(\sigma \circ \rho) = \prod_{\{k,l\} \in \mathfrak{P}_2(n)} \frac{\sigma(l) - \sigma(k)}{l - k} \cdot \prod_{\{i,j\} \in \mathfrak{P}_2(n)} \frac{\rho(j) - \rho(i)}{j - i} = \varepsilon(\sigma)\varepsilon(\rho) \ .$$

Mặt khác, rõ ràng $\{-1, 1\}$ là một nhóm đối với phép nhân.

♦ Mệnh đề - Định nghĩa 2

Hạt nhân của ε là một nhóm con của $\mathfrak{S}_n$, được gọi là **nhóm thay phiên**, và được ký hiệu là $\mathcal{A}_n$.

Chứng minh :

Ta biết (2.2.3, Mệnh đề 2) rằng hạt nhân của một đồng cấu nhóm là một nhóm con. ■

Như thế $\mathcal{A}_n = \varepsilon^{-1}(\{1\}) = \{\sigma \in \mathfrak{S}_n ; \varepsilon(\sigma) = 1\}$, tức là $\mathcal{A}_n$ là tập hợp các hoán vị chẵn của $\{1, ..., n\}$.

VÍ DỤ:

Với $n = 3$, thì $\mathfrak{S}_3 = \{e, \tau_{1,2}, \tau_{1,3}, \tau_{2,3}, c, c'\}$ trong đó $c = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ và $c' = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = c^2$,

và $\mathcal{A}_3 = \{e, c, c'\}$.

$\circ$	e	c	c'	$\tau_{1,2}$	$\tau_{1,3}$	$\tau_{2,3}$
e	e	c	c'	$\tau_{1,2}$	$\tau_{1,3}$	$\tau_{2,3}$
c	c	c'	e	$\tau_{1,3}$	$\tau_{2,3}$	$\tau_{1,2}$
c'	c'	e	c	$\tau_{2,3}$	$\tau_{1,2}$	$\tau_{1,3}$
$\tau_{1,2}$	$\tau_{1,2}$	$\tau_{2,3}$	$\tau_{1,3}$	e	c'	c
$\tau_{1,3}$	$\tau_{1,3}$	$\tau_{1,2}$	$\tau_{2,3}$	c	e	c'
$\tau_{2,3}$	$\tau_{2,3}$	$\tau_{1,3}$	$\tau_{1,2}$	c'	c	e

♦ Mệnh đề 3

Mọi chuyển vị của $\{1,..., n\}$ đều lẻ.

Chứng minh:

Giả sử $(i, j) \in \{1, ..., n\}^2$ sao cho $i < j$. Vì

$$\tau_{i,j} = \begin{pmatrix} 1 & \cdots & i-1 & i & i+1 & \cdots & j-1 & j & j+1 & \cdots & n \\ 1 & \cdots & i-1 & j & i+1 & \cdots & j-1 & i & j+1 & \cdots & n \end{pmatrix},$$

nên các cặp làm thành một nghịch thế (trên hàng thứ 2) là

$$(j, i+1), (j, i+2), ..., (j, j-1), (j, i), (i+1, i), (i+2, i), ..., (j-1, i),$$

số cặp như thế là $2(j - i) - 1$.

Vậy $I(\tau_{i,j})$ lẻ, $\varepsilon(\tau_{i,j}) = -1$ và $\tau_{i,j}$ lẻ.

◆ **Hệ quả** Giả sử $\sigma \in \mathfrak{S}_n$, $N \in \mathbb{N}^*$, t_1, ..., t_N là những chuyển vị của $\{1,...,n\}$ sao cho $\sigma = t_1 \circ ... \circ t_N$. Ta có $\varepsilon(\sigma) = (-1)^N$.

Như thế, một hoán vị chẵn (tương ứng: lẻ) chỉ có thể phân tích thành một tích của một số chẵn (tương ứng: lẻ) những chuyển vị.

3.4.3 Chu trình

Ở đây ta giả thiết $n \geq 2$.

◆ **Định nghĩa** Cho $p \in \mathbb{N}$ sao cho $2 \leq p \leq n$. Mọi hoán vị σ của $\{1, ..., n\}$ sao cho tồn tại $x_1, ..., x_p \in \{1, ..., n\}$, từng đôi khác nhau, thỏa mãn:

$$\begin{cases} \sigma(x_1) = x_2,\ \sigma(x_2) = x_3,\ ...,\ \sigma(x_{p-1}) = x_p,\ \sigma(x_p) = x_1 \\ \forall k \in \{1, ..., n\} - \{x_1, ..., x_p\}, \quad \sigma(k) = k \end{cases}$$

gọi là một ***p* - chu trình** (hoặc **chu trình -*p***) của $\{1, ..., n\}$.

Tập hợp $\{x_1, ..., x_p\}$ (rõ ràng là duy nhất đối với một p- chu trình đã cho) được gọi là **giá** của σ, và ký hiệu là $\sigma = (x_1, ..., x_p)$.

Một hoán vị của $\{1, ..., n\}$ được gọi là **một chu trình** khi và chỉ khi tồn tại $p \in \{2, ..., n\}$ sao cho σ là một p- chu trình.

VÍ DỤ:

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix}$ là 3- chu trình (2, 5, 3)

NHẬN XÉT:

1) $(x_1, ..., x_p) = (x_2, ..., x_p, x_1) = ... = (x_p, x_1, ..., x_{p-1})$.

2) Các 2- chu trình là các chuyển vị.

3) e không phải là một chu trình.

◆ **Định lý** Mọi hoán vị của $\{1,...,n\}$ đều có thể phân tích thành một tích những chu trình từng đôi có giá rời nhau, một cách duy nhất, sai khác về thứ tự các chu trình.

Ta có thể quy ước rằng e là phân tích được thành một tích rỗng những chu trình.

Chứng minh : (có thể gác lại khi đọc lần đầu)

1) Tồn tại

Quy nạp theo n.

Với $n = 2$ tính chất là tầm thường.

Giả sử $n \in \mathbb{N}$ sao cho $n \geq 2$, và $\sigma \in \mathfrak{S}_{n+1}$.

Trường hợp thứ 1: $\sigma(n+1) = n+1$.

Ta lập luận như trong phép chứng minh Định lý 1, 3.4.2. Vì σ là song ánh, nên $\{1, ..., n\}$ ổn định đối với σ và ánh xạ cảm sinh : $\sigma' : \{1,...,n\} \to \{1,...,n\}$ là một hoán $k \mapsto \sigma(k)$

vị của $\{1, ..., n\}$. Theo giả thiết quy nạp, tồn tại $\nu \in \mathbb{N}^*$ và những chu trình $c'_1,...,c'_\nu$ của $\{1, ..., n\}$, từng đôi có giá rời nhau, sao cho $\sigma' = c'_1 \circ \cdots \circ c'_\nu$. Với mỗi r thuộc $\{1, ..., \nu\}$, ta ký hiệu $c_r : \{1, ..., n+1\} \to \{1, ..., n+1\}$ là ánh xạ xác định bởi

$c_r(k) = \begin{cases} c'_r(k) & \text{nếu } 1 \le k \le n \\ n+1 & \text{nếu } k = n+1 \end{cases}$, thì rõ ràng $c_1, ..., c_\nu$ là những chu trình của $\{1,...,n+1\}$ từng đôi có giá rời nhau, và $\sigma = c_1 \circ ... \circ c_\nu$.

Trường hợp thứ 2: $\sigma(n+1) \neq n+1$.

Vì $n+2$ số tự nhiên $n+1$, $\sigma(n+1)$, ..., $\sigma^{n+1}(n+1)$ đều thuộc $\{1, ..., n+1\}$, nên tồn tại $(k, l) \in \{0, ..., n+1\}^2$ sao cho $k < l$ và $\sigma^k(n+1) = \sigma^l(n+1)$. Ký hiệu $m = l - k$, ta có $m \in \{1, ..., n+1\}$ và $\sigma^m(n+1) = n+1$.

Vậy, tập hợp $\{q \in \{1, ..., n+1\}; \sigma^q(n+1) = n+1\}$ là một bộ phận khác rỗng của $\mathbb{N}^*$, nên có một phần tử bé nhất, ký hiệu là p.

Như vậy ta có : $\sigma^p(n+1) = n+1$.

Mặt khác, p số tự nhiên $n+1$, $\sigma(n+1)$, ..., $\sigma^{p-1}(n+1)$ từng đôi khác nhau, vì nếu tồn tại $(k, l) \in \{0, 1, ..., p-1\}^2$ sao cho ($k < l$ và $\sigma^k(n+1) = \sigma^l(n+1)$), thì nếu ký hiệu $q = l - k$, ta sẽ có: $q \in \{1, ..., n+1\}$, $\sigma^q(n+1) = n+1$, $q \le p-1$, điều này mâu thuẫn với định nghĩa của p.

Ta ký hiệu p-chu trình $c = (n+1, \sigma(n+1), ..., \sigma^{p-1}(n+1))$là c, và $\rho = c^{-1} \circ \sigma$, do đó $\rho(n+1) = c^{-1}(\sigma(n+1)) = n+1$.

Theo kết quả khảo sát của trường hợp thứ nhất, tồn tại $\nu \in \mathbb{N}$ và các chu trình $c_1, ..., c_\nu$ của $\{1, ..., n+1\}$ từng đôi có giá rời nhau, thỏa mãn $\rho = c_1 \circ ... \circ c_\nu$.

Vì: $\rho(n+1) = n+1$, $\rho(\sigma(n+1)) = \sigma(n+1)$, ..., $\rho(\sigma^{p-1}(n+1)) = \sigma^{p-1}(n+1)$, nên các giá của các chu trình $c_1, ..., c_\nu$ không chứa một phần tử nào trong các phần tử $n+1$, $\sigma(n+1)$, ..., $\sigma^{p-1}(n+1)$. Cuối cùng, $\sigma = c \circ c_1 \circ ... \circ c_\nu$ trong đó $c, c_1, ..., c_\nu$ là những chu trình của $\{1, ..., n+1\}$ từng đôi có giá rời nhau.

2) Duy nhất

Giả sử $\sigma = c_1 \circ ... \circ c_\nu = d_1 \circ ... \circ d_{\nu'}$ là hai dạng phân tích của σ thành các chu trình từng đôi có giá rời nhau.

Ta chú ý trước tiên rằng $c_1, ..., c_\nu$ giao hoán với nhau từng đôi, và $d_1, ..., d_{\nu'}$ cũng giao hoán với nhau từng đôi.

Trường hợp $\sigma = e$, có thể thấy ngay; ta giả thiết $\sigma \neq e$.

Vậy tồn tại $i \in [1, ..., n\}$ sao cho $\sigma(i) \neq i$, và $r \in \{1, ..., \nu\}$ và $r' \in \{1, ..., \nu'\}$ sao cho i thuộc giá của c_r và thuộc giá của $d_{r'}$.

Cũng như trong 1) trên đây, tồn tại $p \in \mathbb{N}^*$ sao cho : $\begin{cases} i, \sigma(i), ..., \sigma^{p-1}(i) & \text{khác nhau từng đôi} \\ \sigma^p(i) = i \end{cases}$

Thế là ta có $c_r = d_{r'} = (i, \sigma(i), ..., \sigma^{p-1}(i))$.
Bằng cách lập lại, ta suy ra $r' = r$ và $\{c_1, ..., c_r\} = \{d_1, ..., d_{r'}\}$. ■

VÍ DỤ:

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

Bài tập

◊ **3.4.1** Chứng minh rằng $\mathfrak{S}_n$ không giao hoán khi $n \geq 3$.

◊ **3.4.2** Với $n \in \mathbb{N}^*$, xác định ký số của σ: $\{1,..., n\} \to \{1,..., n\}$, $i \mapsto n+1-i$.

◊ **3.4.3** Với $n \in \mathbb{N}^*$, xác định ký số của:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n & n+1 & n+2 & \dots & 2n \\ 2 & 4 & 6 & \dots & 2n & 1 & 3 & \dots & 2n-1 \end{pmatrix}$$

◊ **3.4.4** Cho: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 7 & 1 & 5 & 12 & 6 & 3 & 9 & 4 & 2 & 11 & 8 & 10 \end{pmatrix}$

a) Xác định số nghịch thế và tính chẵn lẻ của σ.

b) Phân tích σ (ít nhất theo một cách) thành một tích những chuyển vị.

c) Phân tích σ thành một tích những chu trình có giá rời nhau. Tìm lại trị của $\varepsilon(\sigma)$.

◊ **3.4.5** Cho $n \in \mathbb{N}$ sao cho $n \geq 3$.

a) Với mọi cặp (i, j) thuộc $\{1, ..., n\}^2$ sao cho $2 \leq i < j \leq n$, hãy kiểm chứng:

$$\tau_{ij} = \tau_{1i} \circ \tau_{1j} \circ \tau_{1i}.$$

Suy ra $\{\tau_{1i}; 2 \leq i \leq n\}$ sinh ra nhóm $\mathfrak{S}_n$.

b) Với mọi cặp (i, j) thuộc $\{2, ..., n\}^2$ sao cho $i \neq j$, kiểm chứng : $(1, i, j) = \tau_{1j} \circ \tau_{1i}$.

Suy ra rằng $\{(1, i, j); (i, j) \in \{2, ..., n\}^2, i \neq j\}$ sinh ra nhóm con $\mathcal{A}_n$.

c) Với mọi k thuộc $\{3, ..., n\}$, hãy kiểm chứng :

$$\tau_{1k} \circ \tau_{12} = \gamma_k \text{ và } \tau_{12} \circ \tau_{1k} = \gamma_k^2, \text{ trong đó } \gamma_k = (1, 2, k).$$

Suy ra: $\tau_{1i} \circ \tau_{1j} = \gamma_i \circ \gamma_j^2$ với mọi (i, j) thuộc $\{3, ..., n\}^2$.

Suy ra rằng $\{(1, 2, i) ; 3 \leq i \leq n\}$ sinh ra nhóm con $\mathcal{A}_n$.

3.5 Phép đếm

Đếm một tập hợp hữu hạn, đó là tính bản số của nó.

3.5.1 Các phép đếm cổ điển

Ta nhắc lại (xem 3.2.2, 3.3.3) rằng, nếu E, F là những tập hợp hữu hạn, thì $E \cup F$, $E \times F$, F^E, $\mathfrak{P}(E)$ đều hữu hạn và:

$$\#(E \cup F) + \#(E \cap F) = \#(E) + \#(F)$$

$$\#(E \times F) = \#(E) \cdot \#(F)$$

$$\#(F^E) = (\#(F))^{\#(E)}$$

$$\#(\mathfrak{P}(E)) = 2^{\#(E)}.$$

Ta đã thấy (xem 3.3.2) rằng, nếu E và F hữu hạn thì số các đơn ánh từ F vào E là $A_n^p = \dfrac{n!}{(n-p)!}$, trong đó $n = \#(E)$, $p = \#(F)$, $p \le n$.

Đặc biệt (xem 3.3.1) số các hoán vị của một tập hợp hữu hạn n phần tử là $n!$.

3.5.2 Ví dụ về đếm

1) Cho E, F là hai tập hữu hạn, $n = \#(E)$, $p = \#(F)$.

a) Số các quan hệ từ E đến F là 2^{np}, vì ánh xạ đặt tương ứng mỗi quan hệ từ E đến F với đồ thị của nó là một song ánh từ tập hợp các quan hệ từ E đến F, lên tập hợp các bộ phận của $E \times F$.

b) Số các luật hợp thành trong của E là n^{n^2}, vì đó là số các ánh xạ từ $E \times E$ vào E.

2) Có bao nhiêu số tự nhiên mà cách viết thập phân gồm đúng n chữ số ($n \ge 3$), trong đó có đúng 2 chữ số 8 ?

Giả sử N là một số có đúng n chữ số (vậy chữ số thứ 1 bên trái khác chữ số 0) và chứa đúng hai chữ số 8.

Trường hợp thứ 1 Một trong 2 chữ số 8 có thể là chữ số thứ 1 của N, sự kiện này cho n - 1 khả năng đặt chữ số 8 thứ 2, còn n - 2 chữ số khác là bất kỳ, khác số 8. Như thế sẽ có đúng $(n-1)9^{n-2}$ số N thuộc loại thứ 1 này. Chẳng hạn, với $n = 6$, ta có thể chọn $n = 841182$.

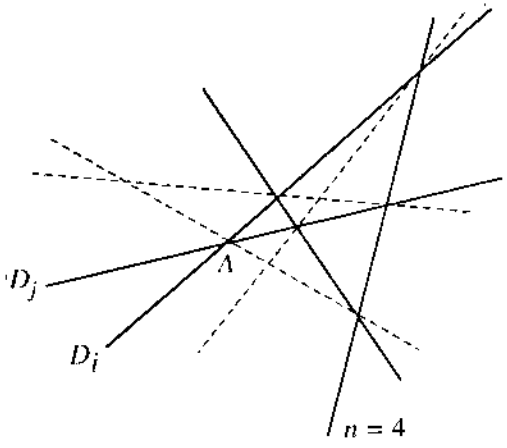
Trường hợp thứ 2 Không có chữ số 8 nào ở vị trí thứ 1 của N, sự kiện này cho C_{n-1}^2 khả năng đặt 2 chữ số 8, chữ số thứ 1 là một chữ số bất kỳ trong 1, 2, 3, 4, 5, 6, 7, 9, và n - 3 chữ số khác bất kỳ, khác 8. Như vậy có đúng $\dfrac{(n-1)(n-2)}{2} 8.9^{n-3}$ số N thuộc loại thứ hai này.

Cuối cùng số cần tìm là $(n-1)9^{n-2} + 4(n-1)(n-2)9^{n-3}$, tức là $= (4n+1)(n-1)9^{n-3}$

3) Trong một mặt phẳng cho n đường thẳng khác nhau "ở vị trí tổng quát" ($n \geq 4$).

a) Các đường thẳng này cắt nhau tại bao nhiêu điểm?

b) Có bao nhiêu đường thẳng mới được xác định bởi các giao điểm trên ?



a) Có bao nhiêu cặp đường thẳng trong $D_1, \ldots D_n$ thì có bấy nhiêu giao điểm phải tìm, vậy có C_n^2 điểm cắt nhau.

Chẳng hạn, với $n = 4$, có 6 giao điểm của từng cặp đường thẳng D_1, D_2, D_3, D_4.

b) Xét điểm A nhận được ở a). Tồn tại đúng 2 đường thẳng D_i, D_j, $(i < j)$ đi qua A (trong số $D_1, \ldots, D_n$). Trên D_i (cũng như trên D_j), ngoài A, có đúng $n - 2$ điểm nói ở a). Vậy số điểm phải nối với điểm A để được các đường thẳng mới như vậy bằng $C_n^2 - 1 - 2(n-1)$, tức là $\dfrac{(n-2)(n-3)}{2}$. Vì mỗi đường thẳng mới nối hai điểm nói ở a), nên số các đường thẳng mới là: $\dfrac{1}{2} C_n^2 \dfrac{(n-2)(n-3)}{2}$, tức là $\dfrac{1}{8} n(n-1)(n-2)(n-3)$.

Chẳng hạn, với $n = 4$, có 3 đường thẳng mới.

4) Cho E là một tập hợp hữu hạn có n phần tử, A là một bộ phận p phần tử ($0 \leq p \leq n$) của E. Đếm các cặp (X,Y) những bộ phận của E sao cho : $X \cup Y = E$ và $X \cap Y = A$.

Ta ký hiệu $B = \complement_E(A)$.

Rõ ràng ánh xạ $(X', Y') \mapsto (X' \cup A, Y' \cup A)$ là một song ánh từ

$\{(X', Y') \in (\mathfrak{P}(B))^2; X' \cup Y' = B\}$ lên $\{(X,Y) \in (\mathfrak{P}(E))^2; X \cup Y = E \text{ và } X \cap Y = A\}$.

Hơn nữa : $\forall (X', Y') \in (\mathfrak{P}(B))^2$, $(X' \cup Y' = B \Leftrightarrow \complement_B(X') \subset Y')$. Như vậy, bản số phải tính cũng là bản số của $\{(X'', Y') \in (\mathfrak{P}(B))^2; X'' \subset Y'\}$. Với $Y' \in \mathfrak{P}(B)$ cố định, có bản số ký hiệu là y', bản số của $\{X'' \in \mathfrak{P}(B); X'' \subset Y'\}$ là $2^{y'}$. Vậy bản số phải tìm là

$$\sum_{y'=0}^{n-p} 2^{y'} C_{n-p}^{y'}$$, tức là 3^{n-p}.

Bài tập

◊ **3.5.1** Có bao nhiêu hàm từ một tập hợp E có n phần tử vào một tập hợp F có p phần tử ?

◊ **3.5.2** Ta ký hiệu P_n là số các phân hoạch của $\{1, ..., n\}$, với $n \in \mathbb{N}^*$. Chứng minh :

$$\forall n \in \mathbb{N},\ P_{n+1} = \sum_{k=0}^{n} C_n^k P_k$$

(trong đó $P_0 = 1$).

Suy ra P_n với $0 \leq n \leq 5$.

◊ **3.5.3** Với $(n, p) \in (\mathbb{N}^*)^2$, ta ký hiệu $P_{n,p}$ là số các phân hoạch của $\{1, ..., n\}$ thành p tập hợp.

a) Chứng minh rằng, với mọi (n,p) thuộc $(\mathbb{N}^*)^2$:

$$P_{n+1,p+1} = P_{n,p} + (p+1)P_{n,p+1}.$$

b) Suy ra $P_{n,p}$ với $(n, p) \in \{1, ..., 5\}^2$.

c) Chứng minh rằng, với mọi n thuộc $\mathbb{N}^*$:

$$P_{n+1,n} = C_{n+1}^2, \quad P_{n+1,2} = 2^n - 1, \quad P_{n+1,3} = \frac{3^n - 2^{n+1} + 1}{2}.$$

◊ **3.5.4** Cho E là một tập hợp hữu hạn, $n = \mathrm{Card}(E)$, và, với mọi k thuộc $\mathbb{N}$:

$$A_{n,k} = \left\{ f : E \to \mathbb{N};\ \sum_{x \in E} f(x) \leq k \right\};$$

$$B_{n,k} = \left\{ f : E \to \mathbb{N};\ \sum_{x \in E} f(x) = k \right\};$$

$$a_{n,k} = \#(A_{n,k}), \quad b_{n,k} = \#(B_{n,k}).$$

a) Chứng minh rằng, với mọi (n, k) thuộc $(\mathbb{N}^*)^2$, ta có:

$$b_{n,k} = a_{n-1,k}, \quad a_{n,k} = b_{n,k} + a_{n,k-1}.$$

b) Suy ra rằng, với mọi (n, k) thuộc $\mathbb{N}^2$, ta có:

$$a_{n,k} = C_{n+k}^n, \quad b_{n,k} = C_{n+k-1}^n \text{ (nếu } n \geq 1).$$

3.6 Các tính chất của $\mathbb{Z}$

Ta nhắc lại ở đây các tính chất thông thường của tập hợp $\mathbb{Z}$ các **số nguyên,** xem như đã biết. Độc giả quan tâm sẽ tìm thấy cách xây dựng $\mathbb{Z}$ (đối xứng hóa nửa nhóm $(\mathbb{N}, +)$) trong Giáo trình của J.M.Arnaudiès và H.Fraysse, Tập 1, trang 70 - 73.

Tập hợp $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$ được trang bị một phép cộng +, một phép nhân •, và một quan hệ thứ tự toàn phần $\leq$, mở rộng các luật của $\mathbb{N}$ và thỏa mãn:

$(\mathbb{Z}, +, \bullet)$ là một vành nguyên giao hoán

$\{x \in \mathbb{Z};\ 0 \leq x\} = \mathbb{N}$

$\forall (a, b, c) \in \mathbb{Z}^3,\ (a \leq b \Leftrightarrow a + c \leq b + c)$

$$\forall (a, b, c, d) \in \mathbb{Z}^4,\ \left(\begin{cases} a \leq b \\ c \leq d \end{cases} \Rightarrow a + c \leq b + d \right)$$

$\forall (a, b, c) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{N}^*,\ (a \leq b \Leftrightarrow ac \leq bc)$

Mọi bộ phận khác rỗng và bị chặn trên (tương ứng: bị chặn dưới) của $\mathbb{Z}$ có một phần tử lớn nhất (tương ứng: bé nhất).

Ta mở rộng ra $\mathbb{Z}$ định nghĩa về tính chia hết trong $\mathbb{N}$:

♦ **Định nghĩa** Cho $(a, b) \in \mathbb{Z}^2$. Ta nói rằng a **chia hết** b (trong $\mathbb{Z}$) và ký hiệu $a \mid b$ khi và chỉ khi tồn tại $c \in \mathbb{Z}$ sao cho $b = ac$.

NHẬN XÉT:

1) $\forall a \in \mathbb{Z},\quad a \mid 0$.

2) $\forall b \in \mathbb{Z},\quad (0 \mid b \Leftrightarrow b = 0)$.

3) Trong $\mathbb{Z}$ quan hệ $\mid$ có tính phản xạ và bắc cầu, nhưng không phản đối xứng, vì, chẳng hạn, $2 \mid (-2)$, $(-2) \mid 2$, $2 \neq -2$. Nhưng ta chứng minh dễ dàng rằng :

$$\forall (a, b) \in \mathbb{Z}^2,\ \left(\begin{cases} a \mid b \\ b \mid a \end{cases} \Rightarrow (b = a \text{ hoặc } b = -a) \right).$$

♦ **Định lý - Định nghĩa (Phép chia Euclide trong $\mathbb{Z}$)**

Cho $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$. Tồn tại một cặp duy nhất (q, r) thuộc $\mathbb{Z}^2$ sao cho: $\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$. Ta nói rằng q (tương ứng : r) là **thương** (tương ứng : **dư**) của phép chia Euclide a cho b.

Chứng minh :

1) Tồn tại

Giả sử $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$. Xét $E = \{p \in \mathbb{Z};\ a \geq bp\}$.

- $E \neq \varnothing$ vì : $\begin{cases} \text{nếu } a \geq 0, \text{ thì } 0 \in E \\ \text{nếu } a < 0 \text{ , thì } a \in E \text{ .} \end{cases}$
- E bị chặn trên vì : $\begin{cases} \text{nếu } a \geq 0, \text{ thì } (\forall p \in E, p \leq a) \\ \text{nếu } a < 0, \text{ thì } (\forall p \in E, p \leq -a). \end{cases}$

Do bộ phận E của $\mathbb{Z}$ khác rỗng và bị chặn trên, nên nó có một phần tử lớn nhất, ký hiệu là q.

Đặt $r = a - bq$; ta đã có : $r \in \mathbb{Z}$.

Vì $q \in E$, nên ta có $a \geq bq$, vậy $r \geq 0$.

Vì $q + 1 \notin E$, nên ta có $a < b(q + 1)$, vậy $r < b$.

2) Duy nhất

Giả sử (q, r), (q', r') thuộc $\mathbb{Z}^2$ thỏa mãn $\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$ và $\begin{cases} a = bq' + r' \\ 0 \leq r' < b \end{cases}$

Thế thì $b(q - q') = r' - r$ và $-b < r' - r < b$, suy ra $-1 < q - q' < 1$, vậy $q' = q$, $r' = r$.

3.7 Các tính chất của $\mathbb{Q}$

Ta nhắc lại ở đây các tính chất thông thường của tập hợp $\mathbb{Q}$ các **số hữu tỷ**, xem như đã biết. Độc giả quan tâm sẽ tìm thấy cách xây dựng $\mathbb{Q}$ (thể các phân thức của vành nguyên $\mathbb{Z}$) trong Giáo trình của J.M.Arnaudiès và H.Fraysse, Tập 1, trang 78-80.

Tập hợp $\mathbb{Q}$ được trang bị một phép cộng +, một phép nhân •, và một quan hệ thứ tự toàn phần $\leq$, thỏa mãn:

$\mathbb{Z} \subset \mathbb{Q}$ (đồng nhất $\frac{a}{1}$ và a, với $a \in \mathbb{Z}$)

$(\mathbb{Q}, +, \bullet)$ là một thể giao hoán

$\forall x \in \mathbb{Q}, \exists (p, q) \in \mathbb{Z} \times \mathbb{N}^*, qx = p$ (ta ký hiệu $x = \frac{p}{q}$)

$\forall (a, b, c) \in \mathbb{Q}^3, (a \leq b \Leftrightarrow a + c \leq b + c)$

$\forall (a, b, c, d) \in \mathbb{Q}^4, \left(\begin{cases} a \leq b \\ c \leq d \end{cases} \Rightarrow a + c \leq b + d \right)$

$\forall (a, b, c) \in \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}_+^*, (a \leq b \Leftrightarrow ac \leq bc)$

nếu ký hiệu $\mathbb{Q}_+ = \{x \in \mathbb{Q};\ x \geq 0\}$, $\mathbb{Q}_- = \{x \in \mathbb{Q};\ x \leq 0\}$, $\mathbb{Q}^* = \mathbb{Q} - \{0\}$; $\mathbb{Q}_+^* = \mathbb{Q}_+ - \{0\}$, $\mathbb{Q}_-^* = \mathbb{Q}_- - \{0\}$.

Ta định nghĩa ánh xạ **trị tuyệt đối** $|\cdot| : \mathbb{Q} \to \mathbb{Q}$, $x \mapsto \begin{cases} x \text{ nếu } 0 \leq x \\ -x \text{ nếu } x \leq 0 \end{cases}$ đã được sử dụng trong phạm vi tổng quát hơn, là tập hợp các số thực, (xem Tập1, chương1) .

♦ **Mệnh đề 1** $\mathbb{Q}$ là một **thể Archimède**, tức là:

$$\forall \varepsilon \in \mathbb{Q}_+^*, \forall A \in \mathbb{Q}_+^*, \exists N \in \mathbb{N}^*, N\varepsilon > A.$$

Chứng minh :

Giả sử $(\varepsilon, A) \in (\mathbb{Q}_+^*)^2$. Tồn tại $(\alpha, \beta, a, b) \in (\mathbb{N}^*)^4$ sao cho : $\varepsilon = \frac{\alpha}{\beta}$ và $A = \frac{a}{b}$.

Ta có, với mọi N thuộc $\mathbb{N}^*$: $N\varepsilon > A \Leftrightarrow N\alpha b > a\beta$.

Vì $\alpha b \geq 1$, nên chỉ cần lấy $N = a\beta + 1$.

♦ **Mệnh đề 2** $\mathbb{Q}$ **trù mật**, tức là:

$$\forall (x, y) \in \mathbb{Q}^2, \quad (x < y \Rightarrow (\exists z \in \mathbb{Q}, x < z < y)).$$

Chứng minh :

Chỉ cần lấy $z = \frac{1}{2}(x + y)$.

♦ **Mệnh đề - Định lý 3** Với mọi x thuộc $\mathbb{Q}$, tồn tại một phần tử n của $\mathbb{Z}$ và chỉ một sao cho $n \leq x < n + 1$; phần tử n này gọi là **phần nguyên** của x, và được ký hiệu là $E(x)$.

Chứng minh :

Giả sử $x \in \mathbb{Q}$. Áp dụng Mệnh đề 1 với $\varepsilon = 1$, ta thấy rằng $\{n \in \mathbb{Z};\ n \leq x\}$ là một bộ phận bị chặn trên và khác rỗng của $\mathbb{Z}$, vậy có một phần tử lớn nhất.

Ta cũng đã định nghĩa một cách tổng quát hơn phần nguyên của một số thực (Tập1, 1.2.3, 3), Mệnh đề - Định nghĩa).

NHẬN XÉT:

Với mọi (a, b) thuộc $\mathbb{Z} \times \mathbb{H}^*$, phần nguyên của $\frac{a}{b}$ là thương của phép chia Euclide a cho b (xem 3.6, Định lý - Định nghĩa).

Chương 4

Số học trong $\mathbb{Z}$

4.1 Tính chia hết

4.1.1 Đại cương

Nhắc lại (xem 3.6):

♦ **Định nghĩa** Cho $(a, b) \in \mathbb{Z}^2$. Ta nói rằng a **chia hết** b **(trong** $\mathbb{Z}$) và ký hiệu $a \mid b$, khi và chỉ khi tồn tại $c \in \mathbb{Z}$ sao cho $b = ac$.

Thay cho a chia hết b, ta còn nói : a là **một ước của** b, hoặc: b là **một bội của** a. Ta ký hiệu tập hợp các ước của a (với $a \in \mathbb{Z}$) là $U(a)$ và tập hợp các ước chung của $a_1, ..., a_n$ (với $n \in \mathbb{N}^*$ và $(a_1, ..., a_n) \in \mathbb{Z}^n$) là:

$$UC(a_1, ..., a_n) = \{x \in \mathbb{Z};\ \forall i \in \{1,...,n\},\ x \mid a_i\}.$$

NHẬN XÉT:

1) $\forall a \in \mathbb{Z}$, $a \mid 0$.

2) $\forall b \in \mathbb{Z}$, $(0 \mid b \Leftrightarrow b = 0)$.

3) Với ký hiệu $a\mathbb{Z} = \{b \in \mathbb{Z};\ \exists c \in \mathbb{Z},\ b = ac\}$ với mọi a thuộc $\mathbb{Z}$, ta có:

$$\forall (a, b) \in \mathbb{Z}^2,\ (a \mid b \Leftrightarrow a\mathbb{Z} \supset b\mathbb{Z}).$$

♦ **Mệnh đề 1**

1) $\forall a \in \mathbb{Z}$, $a \mid a$

2) $\forall (a, b) \in \mathbb{Z}^2$, $\left(\begin{cases} a \mid b \\ b \mid a \end{cases} \Leftrightarrow |a| = |b|\right)$

3) $\forall (a, b, c) \in \mathbb{Z}^3$, $\left(\begin{cases} a \mid b \\ b \mid c \end{cases} \Rightarrow a \mid c\right)$.

Chương 4

Số học trong $\mathbb{Z}$

4.1 Tính chia hết

4.1.1 Đại cương

Nhắc lại (xem 3.6):

♦ **Định nghĩa** Cho $(a, b) \in \mathbb{Z}^2$. Ta nói rằng a **chia hết** b **(trong** $\mathbb{Z}$**)** và ký hiệu $a \mid b$, khi và chỉ khi tồn tại $c \in \mathbb{Z}$ sao cho $b = ac$.

Thay cho a chia hết b, ta còn nói : a là **một ước của** b, hoặc: b là **một bội của** a. Ta ký hiệu tập hợp các ước của a (với $a \in \mathbb{Z}$) là $U(a)$ và tập hợp các ước chung của $a_1, ..., a_n$ (với $n \in \mathbb{N}^*$ và $(a_1, ..., a_n) \in \mathbb{Z}^n$) là:

$$UC(a_1, ..., a_n) = \{x \in \mathbf{Z};\ \forall i \in \{1,...,n\},\ \ x \mid a_i\}.$$

NHẬN XÉT:

1) $\forall a \in \mathbb{Z}$, $a \mid 0$.

2) $\forall b \in \mathbb{Z}$, $(0 \mid b \Leftrightarrow b = 0)$.

3) Với ký hiệu $a\,\mathbb{Z} = \{b \in \mathbb{Z};\ \exists c \in \mathbb{Z},\ b = ac\}$ với mọi a thuộc $\mathbb{Z}$, ta có:

$$\forall (a, b) \in \mathbb{Z}^2,\ (a \mid b \Leftrightarrow a\mathbb{Z} \supset b\mathbb{Z}).$$

♦ **Mệnh đề 1**

1) $\forall a \in \mathbb{Z}$, $a \mid a$

2) $\forall (a, b) \in \mathbb{Z}^2$, $\left(\begin{cases} a \mid b \\ b \mid a \end{cases} \Leftrightarrow |a| = |b|\right)$

3) $\forall (a, b, c) \in \mathbb{Z}^3$, $\left(\begin{cases} a \mid b \\ b \mid c \end{cases} \Rightarrow a \mid c\right)$.

Chứng minh:

1) Hiển nhiên.

2) Giả sử $a \mid b$ và $b \mid a$. Tồn tại $(d, e) \in \mathbb{Z}^2$ sao cho $b = ad$ và $a = be$, suy ra $b = b(de)$.
Nếu $b = 0$, thì $a = b = 0$.
Nếu $b \neq 0$, thì $de = 1$, vậy $|d| = |e| = 1$, do đó $|b| = |a|\,|d| = |a|$.
Ngược lại, nếu $|b| = |a|$, thì tồn tại $\varepsilon \in \{-1, 1\}$ sao cho $b = \varepsilon a$ (tức là $a = \varepsilon b$), do đó $a \mid b$ và $b \mid a$.

3) Giả sử $a \mid b$ và $b \mid c$. Tồn tại $(d, e) \in \mathbb{Z}^2$ sao cho $b = ad$ và $c = be$, do đó $c = a(de)$ và $de \in \mathbb{Z}$, vậy $a \mid c$.

♦ Mệnh đề 2

1) $\forall (a, b, c) \in \mathbb{Z}^3$, $(a \mid b \Rightarrow a \mid bc)$

2) $\forall (a, b, c) \in \mathbb{Z}^3$, $\left(\begin{cases} a \mid b \\ a \mid c \end{cases} \Rightarrow a \mid b + c\right)$

3) $\forall (a, b, \alpha, \beta) \in \mathbb{Z}^4$, $\left(\begin{cases} a \mid b \\ \alpha \mid \beta \end{cases} \Rightarrow a\alpha \mid b\beta\right)$

4) $\forall (a, b, n) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{N}^*$, $(a \mid b \Rightarrow a^n \mid b^n)$.

Chứng minh:

1) Nếu $(a \mid b$ và $a \mid c)$, thì tồn tại $d \in \mathbb{Z}$ sao cho $b = ad$, do đó $bc = a(cd)$ và $cd \in \mathbb{Z}$, vậy $a \mid bc$.

2) Nếu $(a \mid b$ và $a \mid c)$, thì tồn tại $(d, e) \in \mathbb{Z}^2$ sao cho $b = ad$ và $c = ae$, do đó $b + c = a(d + e)$ và $d + e \in \mathbb{Z}$, vậy $a \mid b + c$.

3) Nếu $(a \mid b$ và $\alpha \mid \beta)$, thì tồn tại $(c, \gamma) \in \mathbb{Z}^2$ sao cho $b = ac$ và $\beta = \alpha\gamma$, do đó $b\beta = (a\alpha)(c\gamma)$ và $c\gamma \in \mathbb{Z}$, vậy $a\alpha \mid b\beta$.

4) Suy ra từ 3) bằng quy nạp theo n (hoặc bằng các quy tắc tính lũy thừa). ■

Ta nhắc lại định lý về phép chia Euclide trong $\mathbb{Z}$ (xem 3.6):

♦ Định lý - Định nghĩa

Cho $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$. Tồn tại một cặp duy nhất (q, r) thuộc $\mathbb{Z}^2$ sao cho:

$$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$$

Ta nói rằng q (tương ứng: r) là **thương** (tương ứng: **dư**) của **phép chia Euclide** a **cho** b.

NHẬN XÉT:
Với mọi (a, b) thuộc $\mathbb{Z} \times \mathbb{N}^*$, a chia hết b khi và chỉ khi dư của phép chia Euclide b cho a bằng không.

4.1.2 Đồng dư

♦ **Định nghĩa** Cho $n \in \mathbb{N}^*$, $(a, b) \in \mathbb{Z}^2$; ta nói rằng a là **đồng dư modulo** n **với** b, (hoặc: a **đồng dư với** b **theo modulo** n) và ký hiệu $a \equiv b[n]$ (hoặc: $a \underset{[n]}{\equiv} b$), khi và chỉ khi n chia hết $b - a$.

Vậy: $$a \equiv b[n] \Leftrightarrow n \mid b - a.$$

♦ **Mệnh đề 1** Với mọi n thuộc $\mathbb{N}^*$, quan hệ $\equiv [n]$ là một quan hệ tương đương trong $\mathbb{Z}$.

Chứng minh:

1) Tính phản xạ là hiển nhiên.

2) Ta có, với mọi (a, b) thuộc $\mathbb{Z}^2$:

$a \equiv b[n] \Leftrightarrow n \mid b - a \Leftrightarrow n \mid a - b \Leftrightarrow b \equiv a[n]$, điều này chứng tỏ tính đối xứng.

3) Với mọi (a, b, c) thuộc $\mathbb{Z}^3$:

$$\begin{cases} a \equiv b[n] \\ b \equiv c[n] \end{cases} \Leftrightarrow \begin{cases} n \mid b-a \\ n \mid c-b \end{cases} \Rightarrow n \mid (b-a)+(c-b) \Leftrightarrow n \mid c-a \Leftrightarrow a \equiv c[n].$$

♦ **Ký hiệu**

Với mọi n thuộc $\mathbb{N}^*$, ta ký hiệu $\mathbb{Z}/_{n\mathbb{Z}}$ thay cho $\mathbb{Z}/_{\equiv[n]}$.

Nói khác đi, $\mathbb{Z}/_{n\mathbb{Z}}$ là tập thương của $\mathbb{Z}$ theo quan hệ (tương đương) đồng dư modulo n.

Với mọi x thuộc $\mathbb{Z}$, ta ký hiệu lớp của x trong $\mathbb{Z}/_{n\mathbb{Z}}$ là $\hat{x}$ (hoặc $\overline{x}$, hoặc $\dot{x}$):

$$\hat{x} = \{y \in \mathbf{Z} \,;\, x \equiv y[n]\} = \{x + \lambda n \,;\, \lambda \in \mathbb{Z}\}.$$

Ta cũng có thể ký hiệu là lớp modulo n của x là x mod n.

Vậy rõ ràng rằng (nhờ phép chia Euclide cho n) $\mathbb{Z}/_{n\mathbb{Z}}$ là một tập hợp hữu hạn, có n phần tử, và : $\mathbb{Z}/_{n\mathbb{Z}} = \{\hat{0}, \hat{1}, \ldots, \widehat{n-1}\}$.

Chẳng hạn, $\mathbb{Z}/_{6\mathbb{Z}} = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}, \hat{5}\}$.

Để giảm bớt độ lớn của các số trong các phép tính trong $\mathbb{Z}/n\mathbb{Z}$, ta có thể chọn những đại diện phân bố quanh 0; chẳng hạn: $\mathbb{Z}/_{6\mathbb{Z}} = \{-\hat{2}, -\hat{1}, \hat{0}, \hat{1}, \hat{2}, \hat{3}\}$.

♦ **Mệnh đề 2**

Cho $n \in \mathbb{N}^*$. Với bất kỳ (a, b, c, d) thuộc $\mathbb{Z}^4$, ta có

$$\begin{cases} a \equiv b[n] \\ c \equiv d[n] \end{cases} \Rightarrow \begin{cases} a+c \equiv b+d\ [n] \\ ac \equiv bd\ [n]. \end{cases}$$

Chứng minh:

Giả sử $a \equiv b[n]$ và $c \equiv d[n]$. Tồn tại $(\lambda, \mu) \in \mathbb{Z}^2$ sao cho $b - a = \lambda n$ và $d - c = \mu n$.

Ta có:

1) $(b + d) - (a + c) = (b - a) + (d - c) = (\lambda + \mu)n$ và $\lambda + \mu \in \mathbb{Z}$, vậy $a + c \equiv b + d[n]$. ■

2) $bd - ac = (a + \lambda n)(c + \mu n) - ac = (\lambda c + a\mu + \lambda\mu n)n$ và $\lambda c + a\mu + \lambda\mu n \in \mathbb{Z}$, vậy $ac \equiv bd[n]$. ■

Như thế quan hệ tương đương $\equiv [n]$ *tương thích* với các luật + và . trong $\mathbb{Z}$.

♦ Hệ quả

$$\forall (a, b) \in \mathbb{Z}^2, \quad \forall k \in \mathbb{N}^*, \quad (a \equiv b[n] \Rightarrow a^k \equiv b^k[n]).$$ ■

Cho $n \in \mathbb{N}^*$.

Cho $(\xi, \zeta) \in (\mathbb{Z}/_{n\mathbb{Z}})^2$; tồn tại $(x, y) \in \mathbb{Z}^2$ sao cho $\xi = \hat{x}$ và $\zeta = \hat{y}$.

Nếu $(x', y') \in \mathbb{Z}^2$ là một cặp (khác) sao cho $\xi = \hat{x'}$ và $\zeta = \hat{y'}$, thì (xem Mệnh đề 2):

$$\widehat{x + y} = \widehat{x' + y'} \text{ và } \widehat{xy} = \widehat{x'y'}$$

Vậy ta có thể định nghĩa hai luật hợp thành trong trên $\mathbb{Z}/_{n\mathbb{Z}}$, ký hiệu là: $\hat{+}$ và $\hat{\bullet}$, hoặc + và . , bởi:

$$\forall (x, y) \in \mathbb{Z}^2, \begin{cases} \hat{x} + \hat{y} = \widehat{x + y} \\ \hat{x} \cdot \hat{y} = \widehat{xy} \end{cases}.$$

VÍ DỤ:

Bảng cộng và bảng nhân trong $\mathbb{Z}/4\mathbb{Z}$:

+	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$
$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{0}$
$\hat{2}$	$\hat{2}$	$\hat{3}$	$\hat{0}$	$\hat{1}$
$\hat{3}$	$\hat{3}$	$\hat{0}$	$\hat{1}$	$\hat{2}$

•	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$
$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$
$\hat{2}$	$\hat{0}$	$\hat{2}$	$\hat{0}$	$\hat{2}$
$\hat{3}$	$\hat{0}$	$\hat{3}$	$\hat{2}$	$\hat{1}$

♦ Mệnh đề 3

$(\mathbb{Z}/_{n\mathbb{Z}}, +, .)$ là một vành giao hoán.

Chứng minh:

a) 1) + là một luật hợp thành trong $\mathbb{Z}/_{n\mathbb{Z}}$.

2) $\forall(a, b, c) \in \mathbb{Z}^3$, $(\hat{a} + \hat{b}) + \hat{c} = \widehat{a+b} + \hat{c} = \widehat{(a+b)+c} = \widehat{a+(b+c)} = \hat{a}+\widehat{(b+c)} = \hat{a}+(\hat{b}+\hat{c})$, vậy + có tính kết hợp.

3) $\forall(a, b) \in \mathbb{Z}^2, \hat{a}+\hat{b} = \widehat{a+b} = \widehat{b+a} = \hat{b}+\hat{a}$, vậy + có tính giao hoán.

4) $\forall a \in \mathbb{Z}$, $\hat{a} + \hat{0} = \widehat{a+0} = \hat{a}$, vậy $\hat{0}$ là phần tử trung hòa đối với +.

5) $\forall a \in \mathbb{Z}$, $\hat{a} + (-\hat{a}) = \widehat{a+(-a)} = \hat{0}$, vậy mỗi phần tử của $\mathbb{Z}/_{n\mathbb{Z}}$ có một phần tử đối. Như thế, $(\mathbb{Z}/_{n\mathbb{Z}}, +)$ là một nhóm Abel.

b) 1) · là một luật hợp thành trong $\mathbb{Z}/_{n\mathbb{Z}}$.

2) $\forall(a, b, c) \in \mathbb{Z}^3, (\hat{a}\hat{b})\hat{c} = \widehat{(ab)}\hat{c} = \widehat{(ab)c} = \widehat{(a(bc)} = \hat{a}\widehat{(bc)} = \hat{a}(\widehat{bc})$, vậy · có tính kết hợp.

3) $\forall(a, b) \in \mathbb{Z}^2$, $\hat{a}\hat{b} = \widehat{ab} = \widehat{ba} = \hat{b}\hat{a}$, vậy . có tính giao hoán.

4) $\forall a \in \mathbb{Z}$, $\hat{a}\hat{1} = \widehat{a1} = \hat{a}$, vậy $\hat{1}$ là phần tử trung hòa đối với .

5) $\forall(a, b, c) \in \mathbb{Z}^3$, $\hat{a}(\hat{b}+\hat{c}) = \hat{a}\ \widehat{(b+c)} = a\widehat{(b+c)} = \widehat{ab+ac} = \widehat{ab}+\widehat{ac} = \hat{a}\hat{b}+\hat{a}\hat{c}$, vậy · là phân phối đối với +.

NHẬN XÉT:

Nhóm $(\mathbb{Z}/_{n\mathbb{Z}}, +)$ là nhóm xyclic, sinh bởi $\hat{1}$, vì với mọi a thuộc $\mathbb{Z}$:

$$\hat{a} = \begin{cases} \hat{1}+\ldots+\hat{1} & (a \text{ hạng tử}) \quad \text{nếu } a \geq 1 \\ \hat{0} & \text{nếu } a = 0 \\ -\hat{1}-\ldots-\hat{1} & (-a \text{ hạng tử}) \quad \text{nếu } a \leq -1. \end{cases}$$

Bài tập

◊ **4.1.1** Cho $n \in \mathbb{Z}$. Chứng minh:

$$\begin{cases} n^2 \equiv 0[8] \text{ hoặc } n^2 \equiv 4[8], \text{ nếu } n \text{ chẵn} \\ n^2 \equiv 1[8] \text{ nếu } n \text{ lẻ.} \end{cases}$$

◊ **4.1.2** Chứng minh: $\forall n \in \mathbb{N}-\{0,1\}$, $2^n \mid 5^{2^{n-2}} - 1$ và $2^{n+1} \mid 5^{2^{n-2}} - 1$

◊ **4.1.3** Chứng minh rằng với mọi n thuộc $\mathbb{N}^*$, $\sum_{k=1}^{2n} \frac{(2n)!}{k}$ là một số nguyên chia hết cho $2n + 1$.

◊ **4.1.4** Chứng minh: $\forall n \in \mathbb{N}^*$, $40^n.n! \mid (5n)!$.

◊ **4.1.5** Chứng minh rằng số n duy nhất thuộc $\mathbb{N}-\{0,1\}$ sao cho $2n - 1$ chia hết

$$(3n^2 - 3n + 1)(3n^2 - 3n + 2),$$

là $n = 3$.

◊ **4.1.6** Cho $n \in \mathbb{N}$ sao cho $n \geq 4$; chứng minh rằng tồn tại $k \in \mathbb{N}$ sao cho:

$$n! < k < (n + 1)! \text{ và } n^3 \mid k.$$

◊ **4.1.7** Cho $(a, b, c, d) \in \mathbb{Z}^4$ sao cho $ad + bc \neq 0$. Ta giả thiết rằng $ad + bc$ chia hết a, b, c, d. Chứng minh:

$$ad + bc \in \{-1, 1\}.$$

◊ **4.1.8** Chứng minh rằng, với mọi n thuộc $\mathbb{N}$, $(3+\sqrt{5})^n + (3-\sqrt{5})^n$ là một số nguyên chia hết cho 2^n.

◊ **4.1.9** Tìm các số n thuộc $\mathbb{Z}$ sao cho:

a) $3n + 4 \mid 11n + 8$ b) $n^2 + 3n - 2 \mid n^2 - 6$.

◊ **4.1.10** Chứng minh: $\forall (a, b, c) \in \mathbb{Z}^3, a + b + c \mid a^3 + b^3 + c^3 - 3abc$.

◊ **4.1.11** Ta ký hiệu ánh xạ cho tương ứng với mỗi n của $\mathbb{N}^*$ số các ước (≥ 1) của n là $d : \mathbb{N}^* \to \mathbb{N}^*$. Chứng minh: $\forall a \in \mathbb{N} - \{0, 1\}, \forall n \in \mathbb{N}^*, d(a^n - 1) \geq d(n)$.

◊ **4.1.12** Cho $n \in \mathbb{N}^*$, $1 = d_1 < d_2 < \ldots < d_k = n$ là các ước ≥ 1 của n; chứng minh:

$$\left(\prod_{i=1}^{k} d_i \right)^2 = n^k .$$

◊ **4.1.13** **Ví dụ về phương trình Diophante**

Giải các phương trình sau, trong tập hợp đã được chỉ ra :

a) $xy = 2x + 3y$, $\mathbb{Z}^2$ b) $x^2 - y^2 - x + 3y = 30$, $\mathbb{Z}^2$

c) $\frac{1}{x} + \frac{1}{y} = \frac{1}{5}$, $(\mathbb{Z}^*)^2$ d) $x^2 - 3xy + 2y^2 + x - 3y - 6 = 0$, $\mathbb{Z}^2$

e) $2x^3 + xy - 7 = 0$, $\mathbb{Z}^2$ f) $x^3 + xy + y^3 = 209$, $\mathbb{N}^2$

g) $x(x + 1)(x + 7)(x + 8) = y^2$, $\mathbb{Z}^2$ h) $x^2 = 9y^2 - 39y + 40$, $\mathbb{Z}^2$

i) $\begin{cases} x^3 - y^3 - z^3 = 3xyz \\ x^2 = 2(y + z) \end{cases}$, $\mathbb{N}^3$ j) $\begin{cases} z^2 = x^2 + y^2 \\ xy = 2(x + y + z) \end{cases}$, $(\mathbb{N}^*)^3$

k) $3^x = 8 + y^2$, $\mathbb{N}^2$.

◊ **4.1.14** Chứng minh với mọi n thuộc $\mathbb{N}$:

a) $5 \mid 2^{2n+1} + 3^{2n+1}$ b) $9 \mid 4^n - 1 - 3n$

c) $11 \mid 3^{n+3} - 4^{4n+2}$ d) $16 \mid 5^n - 1 - 4n$

e) $17 \mid 2^{6n+3} + 3^{4n+2}$ f) $17 \mid 2^{7n+1} + 3^{2n+1} + 5^{10n+1} + 7^{6n+1}$

g) $18 \mid 2^{2n+2} + 24n + 14$ h) $19 \mid 2^{3n+4} + 3^{2n+1}$

i) $19 \mid 2^{6n+2} + 3$ j) $21 \mid 2^{4^{n+1}} + 5$

k) $25 \mid 2^{n+2}3^n + 5n - 4$ l) $29 \mid 2^{5n+1} + 3^{n+3}$

m) $31 \mid 2^{4n+1} + 3^{6n+9}$ n) $32 \mid 8n^2 + 4n - 3(5^n - 1)$

o) $33 \mid 5^{2n+1} + 11^{2n+1} + 17^{2n+1}$ p) $41 \mid 5.7^{2n+2} + 2^{3n}$

q) $73 \mid 9^{2n+1} + 8^{n+2}$ r) $111 \mid 10^{6n} + 10^{3n} - 2$

s) $288 \mid 7^{2n+1} - 48n - 7$ t) $2304 \mid 7^{2n} - 2352n - 1$

u) $2^{12} \mid 3.81^{n+1} + (16n - 54)9^{n+1} - 320n^2 - 144n + 243$

◊ **4.1.15** Cho $a \in \mathbb{Z}$ là số lẻ và $n \in \mathbb{N}$ sao cho $n \geq 3$. Chứng minh: $a^{2^{n-2}} \equiv 1[2^n]$.

◊ **4.1.16** Chứng minh: $\forall (a, b, c) \in \mathbb{Z}^3$, $(7 \mid a^3 + b^3 + c^3 \Rightarrow 7 \mid abc)$.

◊ **4.1.17** Tìm tất cả các số n thuộc $\mathbb{Z}$ sao cho: $10 \mid n^2 + (n+1)^2 + (n+3)^2$.

◊ **4.1.18** Với những n nào thuộc $\mathbb{N}$ thì ta có: $8 \mid 3^n + 4n + 1$?

◊ **4.1.19** Tìm tất cả các số n thuộc $\mathbb{N}$ sao cho:

a) $21 \mid 2^{2n} + 2^n + 1$ b) $7 \mid 2^{2^n} + 2^n + 1$.

◊ **4.1.20** Chứng minh: $\forall n \in \mathbb{N} - \{0, 1\}$, $2^n \mid 3^n + 1$.

◊ **4.1.21** Chứng minh: $\forall (a, b) \in \mathbb{N}^2$, $23 \mid 2^a + 3^b$.

◊ **4.1.22** **Ví dụ về phương trình Diophante**

Chứng minh rằng các phương trình sau không có nghiệm trong tập hợp đã chỉ ra:

a) $x^2 + 5y^2 = 3$, $\mathbb{Z}^2$ b) $x^2 - 5y^2 = 3$, $\mathbb{Z}^2$

c) $15x^2 - 7y^2 = 9$, $\mathbb{Z}^2$ d) $x^2 + y^2 - 8z - 6 = 0$, $\mathbb{Z}^3$

e) $x^3 - 3y^3 + 6y^2 - 16x + 8 = 0$, $\mathbb{Z}^2$ f) $x^3 + 11^3 = y^3$, $\mathbb{N}^{*2}$.

◊ **4.1.23** Tìm tất cả các bộ ba (x, y, z) thuộc $(\mathbb{N}^*)^3$ sao cho:

$$\begin{cases} x + y \equiv 1 \ [x] \\ y + z \equiv 1 \ [x] \\ z + x \equiv 1 \ [y]. \end{cases}$$

◊ **4.1.24** Chứng minh, với mọi n lẻ thuộc $\mathbb{Z}$: $n^4 \equiv 1[16]$ (Sử dụng bài tập 4.1.1).

◊ **4.1.25** Chữ số cuối cùng của $\sum_{k=1}^{10} k^{100}$ viết trong hệ cơ sở 10 là chữ số nào?

◊ **4.1.26** Chứng minh, với mọi n thuộc $\mathbb{N}^*$: $5 \mid 1^n + 2^n + 3^n + 4^n \Leftrightarrow 4 \mid n$.

◊ **4.1.27** Cho $(a, b) \in \mathbb{N}^2$ sao cho $a \geq 4b$. Chứng minh:

$$3^a + 1 \equiv 0 \ [10] \Rightarrow \begin{cases} 3^{a+4b} + 1 \equiv 0 \ [10] \\ 3^{a-4b} + 1 \equiv 0 \ [10]. \end{cases}$$

◊ **4.1.28** Cho $(\phi_n)_{n \in \mathbb{N}}$ là **dãy Fibonacci :**

$$\phi_0 = 0, \ \phi_1 = 1, \quad \forall n \in \mathbb{N}, \quad \phi_{n+2} = \phi_{n+1} + \phi_n.$$

Chứng minh, với mọi n thuộc $\mathbb{N}$:

a) $2 \mid \phi_n \Leftrightarrow 3 \mid n$

b) $3 \mid \phi_n \Leftrightarrow 4 \mid n$

c) $4 \mid \phi_n \Leftrightarrow 6 \mid n$.

◊ **4.1.29 Các số Fermat**

Ta ký hiệu, với $n \in \mathbb{N}$, $F_n = 2^{2^n} + 1$ (được gọi **số Fermat thứ** n). Chứng minh:

$$\forall n \in \mathbb{N}^* \quad F_n \mid 2^{F_n} - 2.$$

Các bài tập từ 4.1.30 *đến* 4.1.32 *sử dụng số học để khảo sát các nhóm đơn.*

◊ **4.1.30*** Chứng minh rằng các nhóm con của $(\mathbb{Z}, +)$ là các $k\mathbb{Z}$, $k \in \mathbb{N}$.

◊ **4.1.31** Xác định các nhóm con của $(\mathbb{Z}/_{n\mathbb{Z}}, +)$, $n \in \mathbb{N}^*$ (sử dụng bài tập 4.1.30).

◊ **4.1.32** Cho $(G, \cdot)$ là một nhóm đơn. Chứng minh:

$$\begin{cases} G \cong \mathbb{Z} & \text{nếu } G \text{ là vô hạn} \\ G \cong \mathbb{Z}/_{n\mathbb{Z}} & \text{nếu } G \text{ là hữu hạn và } n = \text{Card}(G). \end{cases}$$

(Sử dụng bài tập 4.1.30)

◊ **4.1.33** Chứng minh, với mọi (x, y) thuộc $\mathbb{Z}^2$: $17 \mid 2x + \hat{3}y \Leftrightarrow 17 \mid 9x + 5y$.

◊ **4.1.34** Giải :

a) $x^2 + x + \hat{7} = \hat{0}$ trong $\mathbb{Z}/_{13\mathbb{Z}}$

b) $x^2 - \hat{4}x + \hat{3} = \hat{0}$ trong $\mathbb{Z}/_{12\mathbb{Z}}$.

◊ **4.1.35** Cho 5 số nguyên, chứng minh rằng ta có thể chọn ra ba số có tổng chia hết cho 3.

◊ **4.1.36** Cho $n \in \mathbb{N}^*$. Có bao nhiêu cách phân tích 2^n thành tổng của bốn bình phương của những số tự nhiên ?

◊ **4.1.37*** Cho $n \in \mathbb{N}^*$, và $a_0, \ldots, a_n \in \{1, \ldots, 2n\}$ từng đôi khác nhau. Chứng minh rằng tồn tại $(i, j) \in \{1, \ldots, n\}^2$ sao cho: $i \neq j$ và $a_i \mid a_j$.

◊ **4.1.38*** Với $n \in \mathbb{N}^*$, ta ký hiệu $\delta(n)$ là ước lẻ lớn nhất của n, $S(n) = \sum_{k=1}^{n} \frac{\delta(k)}{k}$,

$F(n) = S(n) - \frac{2n}{3}$.

a) Kiểm chứng : $\forall n \in \mathbb{N}^*$, $\begin{cases} \delta(2n+1) = 2n+1 \\ \delta(2n) = \delta(n) \end{cases}$

b) Suy ra: $\forall n \in \mathbb{N}^*$, $\begin{cases} S(2n+1) = S(2n) + 1 \\ S(2n) = \frac{1}{2} S(n) + n \end{cases}$

c) Chứng minh: $\forall n \in \mathbb{N}^*$, $0 < F(n) < \frac{2}{3}$.

4.2 Ước chung lớn nhất (UCLN) Bội chung nhỏ nhất (BCNN)

4.2.1 Đại cương

♦ **Mệnh đề - Định nghĩa**

Cho $n \in \mathbb{N}^*$, $(x_1, ..., x_n) \in (\mathbb{Z}^*)^n$.

1) Tập hợp các ước chung của $x_1, ..., x_n$ là hữu hạn và có một phần tử lớn nhất (đối với thứ tự ≤ thông thường), gọi là **ước chung lớn nhất** của $x_1, ..., x_n$ và ký hiệu là UCLN $(x_1, ..., x_n)$ hoặc UCLN $((x_i)_{1\le i\le n})$.

2) Tập hợp các phần tử thuộc $\mathbb{N}^*$ là bội chung của $x_1, ..., x_n$ có một phần tử nhỏ nhất (đối với thứ tự ≤ thông thường), gọi là **bội chung nhỏ nhất** của $x_1, ..., x_n$ và ký hiệu là BCNN $(x_1, ..., x_n)$ hoặc BCNN $((x_i)_{1\le i\le n})$.

Chứng minh:

1) Tập hợp UC$(x_1, ..., x_n)$ các ước chung của $x_1, ..., x_n$ là một bộ phận hữu hạn của $\mathbb{Z}$ (vì bao hàm trong $\{k \in \mathbb{Z} ; |k| \le |x_1|\}$), khác rỗng (vì nó chứa 1), vậy có một phần tử lớn nhất.

2) Tập hợp các phần tử của $\mathbb{N}^*$ là bội chung của $x_1, ..., x_n$ là một bộ phận khác rỗng của $\mathbb{N}^*$ (vì nó chứa $\left|\prod_{i=1}^{n} x_i\right|$), vậy có một phần tử nhỏ nhất. ■

Ký hiệu δ = UCLN $(x_1, ..., x_n)$, μ = BCNN $(x_1, ..., x_n)$, theo định nghĩa ta có:

$$\begin{cases} \forall k \in \mathbf{Z}, & \big((\forall i \in \{1,...,n\}, \quad k \mid x_i) \Rightarrow |k| \le \delta\big) \\ \forall k \in \mathbf{N}^*, & \big((\forall i \in \{1,...,n\}, \quad x_i \mid k) \Rightarrow \mu \le k\big). \end{cases}$$

NHẬN XÉT : Rõ ràng:

$$\forall (x_1, ..., x_n) \in (\mathbb{Z}^*)^n, \begin{cases} \text{UCLN}(x_1,...,x_n) = \text{UCLN}(|x_1|,...,|x_n|) \\ \text{BCNN}(x_1,...,x_n) = \text{BCNN}(|x_1|,...,|x_n|). \end{cases}$$

4.2.2 Tính chất

♦ **Mệnh đề 1** Cho $n \in \mathbb{N}^*$, $(x_1, ..., x_n) \in (\mathbb{Z}^*)^n$, δ = UCLN$(x_1, ..., x_n)$, μ = BCNN$(x_1, ..., x_n)$. Ta có:

$$\delta\mathbb{Z} = \sum_{i=1}^{n} x_i\mathbf{Z} \quad \text{và} \quad \mu\mathbb{Z} = \bigcap_{i=1}^{n} x_i\mathbf{Z}.$$

Chứng minh :

1) a) Giả sử $x \in \sum_{i=1}^{n} x_i\mathbf{Z}$; tồn tại $(u_1, .., u_n) \in \mathbb{Z}^n$ sao cho $x = \sum_{i=1}^{n} x_i u_i$. Vì $(\forall i \in \{1, ..., n\}, \delta \mid x_i)$, suy ra (xem 4.1.1, Mệnh đề 2) $\delta \mid x$, tức là $x \in \delta\mathbb{Z}$.

Điều này chứng tỏ: $\sum_{i=1}^{n} x_i\mathbf{Z} \subset \delta\mathbf{Z}$.

b) $\left(\sum_{i=1}^{n} x_i\mathbf{Z}\right) \cap \mathbf{N}^*$ là một bộ phận khác rỗng của $\mathbb{N}^*$ (nó chứa $|x_1|$), do đó có một phần tử nhỏ nhất, ký hiệu là d. Vì $d \in \sum_{i=1}^{n} x_i\mathbf{Z}$, nên rõ ràng $d\mathbb{Z} \subset \sum_{i=1}^{n} x_i\mathbf{Z}$.

Giả sử $x \in \sum_{i=1}^{n} x_i\mathbf{Z}$. Theo phép chia Euclide x cho d, tồn tại $(q, r) \in \mathbb{Z} \times \mathbb{N}$ sao cho:

$$x = dq + r \text{ và } 0 \le r < d.$$

Vì x và d đều thuộc $\sum_{i=1}^{n} x_i\mathbf{Z}$, và vì $\sum_{i=1}^{n} x_i\mathbf{Z}$ là một nhóm con của $(\mathbb{Z}, +)$, nên ta suy ra

$$r = x - qd \in \sum_{i=1}^{n} x_i\mathbf{Z}.$$

Nhưng $0 \le r < d$, do đó theo định nghĩa của d, $r = 0$, $x = qd \in d\mathbb{Z}$ và do vậy $\sum_{i=1}^{n} x_i\mathbf{Z} \subset d\mathbf{Z}$.

c) Như vậy ta đã chứng minh : $d\mathbb{Z} = \sum_{i=1}^{n} x_i\mathbf{Z} \subset \delta\mathbf{Z}$. Vậy tồn tại $e \in \mathbb{Z}$ sao cho $d = \delta e$, và rõ ràng $e \in \mathbb{N}^*$. Vì d và δ chia hết $x_1, ..., x_n$ và đều thuộc $\mathbb{N}^*$, nên theo định nghĩa của δ ta có: $d \le \delta$, và như vậy $e = 1$, $d = \delta$.

Cuối cùng: $\sum_{i=1}^{n} x_i\mathbf{Z} = d\mathbf{Z} = \delta\mathbf{Z}$.

2) a) $(\forall i \in \{1, ..., n\},\ x_i \mid \mu) \Rightarrow (\forall i \in \{1, ..., n\},\ x_i\mathbb{Z} \supset \mu\mathbb{Z}) \Rightarrow \bigcap_{i=1}^{n} x_i\mathbf{Z} \supset \mu\mathbf{Z}$.

b) Lập luận như 1) b) ở trên (hoặc xem bài tập 4.1.30), ta chứng minh được rằng tồn tại $m \in \mathbb{N}^*$ sao cho: $\bigcap_{i=1}^{n} x_i\mathbf{Z} = m\mathbf{Z}$. Thế thì $\mu\mathbb{Z} \subset m\mathbb{Z}$; vậy tồn tại $f \in \mathbb{N}^*$ sao cho $\mu = mf$. Vì m và μ đều là bội chung của $x_1, ..., x_n$ và đều thuộc $\mathbb{N}^*$, nên theo định nghĩa của μ ta có $\mu \le m$, và như thế $f = 1$, $m = \mu$.

Cuối cùng: $\bigcap_{i=1}^{n} x_i\mathbf{Z} = m\mathbf{Z} = \mu\mathbf{Z}$.

♦ Mệnh đề 2

$\forall n \in \mathbb{N}^*, \forall \lambda \in \mathbb{Z}^*, \forall (x_1, ..., x_n) \in (\mathbb{Z}^*)^n,$

$$\begin{cases} \text{UCLN}(\lambda x_1, ..., \lambda x_n) = |\lambda| \text{UCLN}(x_1, ..., x_n) \\ \text{BCBN}(\lambda x_1, ..., \lambda x_n) = |\lambda| \text{BCNN}(x_1, ..., x_n). \end{cases}$$

Chứng minh:

Ký hiệu $\delta = \text{UCLN}(x_1, ..., x_n)$, $\mu = \text{BCNN}(x_1, ..., x_n)$, ta có:

$$\begin{cases} \sum_{i=1}^{n} (\lambda x_i)\mathbf{Z} = \lambda \sum_{i=1}^{n} x_i\mathbf{Z} = \lambda(\delta\mathbf{Z}) = (\lambda\delta)\mathbf{Z} \\ \bigcap_{i=1}^{n} (\lambda x_i)\mathbf{Z} = \lambda \bigcap_{i=1}^{n} x_i\mathbf{Z} = \lambda(\mu\mathbf{Z}) = (\lambda\mu)\mathbf{Z}. \end{cases}$$

Suy ra:

$$\begin{cases} \text{UCLN}(\lambda x_1, ..., \lambda x_n) = |\lambda\delta| = |\lambda|\delta \\ \text{BCNN}(\lambda x_1, ..., \lambda x_n) = |\lambda\mu| = |\lambda|\mu. \end{cases}$$

♦ **Mệnh đề 3** Cho $n \in \mathbb{N}^*$, $(x_1, ..., x_n) \in (\mathbb{Z}^*)^n$, $\delta = \text{UCLN}(x_1, ..., x_n)$, $\mu = \text{BCNN}(x_1, ..., x_n)$, $(a, b) \in (\mathbb{Z}^*)^2$. Ta có:

1) $(\forall i \in \{1, ..., n\},\ a \mid x_i) \Leftrightarrow a \mid \delta$

2) $(\forall i \in \{1, ..., n\},\ x_i \mid b) \Leftrightarrow \mu \mid b.$

Chứng minh:

1) $(\forall i \in \{1, ..., n\}, a \mid x_i) \Leftrightarrow (\forall i \in \{1, ..., n\}, a\mathbb{Z} \supset x_i\mathbb{Z}) \Leftrightarrow (a\mathbb{Z} \supset \sum_{i=1}^{n} x_i\mathbf{Z})$

$\Leftrightarrow a\mathbb{Z} \supset \delta\mathbb{Z} \Leftrightarrow a \mid \delta.$

2) $(\forall i \in \{1, ..., n\}, x_i \mid b) \Leftrightarrow (\forall i \in \{1, ..., n\}, x_i\mathbb{Z} \supset b\mathbb{Z}) \Leftrightarrow (\bigcap_{i=1}^{n} x_i\mathbf{Z} \supset b\mathbf{Z})$

$\Leftrightarrow \mu\mathbb{Z} \supset b\mathbb{Z} \Leftrightarrow \mu \mid b.$

♦ **Mệnh đề 4 (Tính kết hợp của UCLN và của BCNN)**

Cho $n \in \mathbb{N}^*$, P là một phân hoạch của $\{1, ..., n\}$, $(x_1, ..., x_n) \in (\mathbb{Z}^*)^n$. Ta có:

$$\text{UCLN}(x_1, ..., x_n) = \text{UCLN}((\text{UCLN}((x_i)_{i\in I}))_{I\in P})$$

$$\text{BCNN}(x_1, ..., x_n) = \text{BCNN}((\text{BCNN}((x_i)_{i\in I}))_{I\in P}).$$

Chứng minh :

1) Do tính kết hợp và tính giao hoán của phép cộng trong $\mathbb{Z}$, ta thấy rằng:

$$\sum_{i=1}^{n} x_i\mathbf{Z} = \sum_{I\in P}\left(\sum_{i\in I} x_i\mathbf{Z}\right) = \sum_{I\in P}(\text{UCLN}(x_i)_{i\in I})\mathbf{Z}.$$

2) Tương tự, do tính kết hợp và tính giao hoán của phép giao trong $\mathfrak{P}(\mathbb{Z})$:

$$\bigcap_{i=1}^{n} x_i\mathbb{Z} = \bigcap_{i\in P}\left(\bigcap_{i\in I} x_i\mathbb{Z}\right) = \bigcap_{I\in P}(\mathrm{BCBN}(x_i)_{i\in I})\mathbb{Z}. \qquad \blacksquare$$

Mệnh đề trên chứng tỏ ta có thể biểu thị ƯCLN (tương ứng : BCNN) của nhiều số chỉ bằng các ƯCLN (tương ứng: BCNN) của hai số. Chẳng hạn:

$$\text{ƯCLN}(x_1, x_2, x_3) = \text{ƯCLN}(\text{ƯCLN}(x_1, x_2), x_3),$$

$$\text{BCNN}(x_1, x_2, x_3, x_4) = \text{BCNN}(\text{BCNN}(x_1, x_2), \text{BCNN}(x_3, x_4)).$$

♦ **Ký hiệu**

Với $(a, b) \in (\mathbb{Z}^*)^2$, ta ký hiệu $\begin{cases} a \wedge b = \text{ƯCLN}(a,b) \\ a \vee b = \text{BCNN}(a,b) \end{cases}$.

NHẬN XÉT :

1) Độc giả có thể tìm thấy trong các cuốn sách khác (giáo trình của J.M.Arnaudiès và H.Fraysse, Tập1, trang 127-128) các ký hiệu ngược lại với các ký hiệu ở đây: $\vee$ đối với ƯCLN, $\wedge$ đối với BCNN.

2) $\wedge$ và $\vee$ là những luật hợp thành trong trên $\mathbb{Z}^*$, kết hợp và giao hoán (xem Mệnh đề 4). Hơn nữa: $\forall a \in \mathbb{Z}^*$, $(a \wedge a = a \vee a = |a|, a \wedge 1 = 1, a \vee 1 = |a|)$.

Sau này ta sẽ thấy :

- $\wedge$ và $\vee$ luật này phân phối đối với luật kia (4.4.3, Hệ quả)
- $\forall (a, b) \in (\mathbb{Z}^*)^2, \forall k \in \mathbb{N}^*, a^k \wedge b^k = (a \wedge b)^k$ (4.3.3, Hệ quả).

4.2.3 Thuật toán Euclide

Cho $(a, b) \in \mathbb{N}^2$ sao cho $a \geq b$. Ta sẽ xây dựng một thuật toán cho phép tính $a \wedge b$.

Nếu $b \mid a$, thì $a \wedge b = b$.

Giả sử $b \nmid a$. Theo phép chia Euclide a cho b, tồn tại $(q_1, r_1) \in \mathbb{N}^2$ sao cho:

$$\begin{cases} a = bq_1 + r_1 \\ 0 < r_1 < b \end{cases}.$$

Ta sẽ chứng minh: $a \wedge b = b \wedge r_1$.

Với mọi c thuộc $\mathbb{Z}$:

- Nếu ($c \mid a$ và $c \mid b$) thì ($c \mid b$ và $c \mid r_1$) vì $r_1 = a - bq_1$
- Nếu ($c \mid b$ và $c \mid r_1$), thì ($c \mid b$ và $c \mid a$) vì $a = bq_1 + r_1$.

Điều này chứng tỏ ƯC(a, b) = ƯC(b, r_1), và như vậy $a \wedge b = b \wedge r_1$.

Nếu $r_1 \mid b$, thì $a \wedge b = b \wedge r_1 = r_1$.

Nếu $r_1 \nmid b$, thì ta lặp lại.

Như thế ta xây dựng các cặp (q_1, r_1), (q_2, r_2),... sao cho:

$$\begin{cases} a = bq_1 + r_1 \\ 0 < r_1 < b \end{cases}, \quad \begin{cases} b = r_1 q_2 + r_2 \\ 0 < r_2 < r_1 \end{cases}, \ldots$$

Vì $b > r_1 > r_2 > \ldots$ và $b, r_1, r_2, \ldots$ đều thuộc $\mathbb{N}^*$, nên thủ tục sẽ dừng lại sau một số hữu hạn bước. Vậy tồn tại $N \in \mathbb{N}^*$, (q_1, r_1), (q_2, r_2), ..., (q_N, r_N) thuộc $\mathbb{N}^2$ sao cho:

$$\begin{cases} a = bq_1 + r_1 \\ 0 < r_1 < b \end{cases}, \quad \begin{cases} b = r_1 q_2 + r_2 \\ 0 < r_2 < r_1 \end{cases}, \ldots \begin{cases} r_{N-2} = r_{N-1} q_N + r_N \\ 0 < r_N < r_{N-1} \end{cases}, \ r_N \mid r_{N-1}.$$

Khi đó ta có: $a \wedge b = b \wedge r_1 = r_1 \wedge r_2 = \ldots = r_{N-1} \wedge r_N = r_N$.

Trong thực hành , ta thực hiện các phép chia Euclide liên tiếp, và ƯCLN của a và b là dư cuối cùng khác không. Ta có thể áp dụng cách sắp xếp thực hành sau (khi tính "tay"):

	q_1	q_2	q_3	...	q_N	q_{N+1}
a	b	r_1	r_2	...	r_{N-1}	r_N
r_1	r_2	r_3	...		0	

VÍ DỤ

Tính $9100 \wedge 1848$

	4	1	12	5
9100	1848	1708	140	28
1708	140	28	0	

$9100 \wedge 1848 = 28$.

Bài tập

◊ **4.2.1** Chứng minh rằng, với mọi n thuộc $\mathbb{N}^*$:

a) $(n^2 + n) \wedge (2n + 1) = 1$ b) $(n^3 + 2n) \wedge (n^4 + 3n^2 + 1) = 1$

c) $(n^2 + 1) \wedge ((n + 1)^2 + 1) \in \{1, 5\}$.

◊ **4.2.2** Tính ƯCLN$\{16^n + 10^n - 1; n \in \mathbb{N}^*\}$, tức là số nguyên lớn nhất $\delta \geq 1$ sao cho:

$$\forall n \in \mathbb{N}^*, \delta \mid 16^n + 10^n - 1.$$

◊ **4.2.3** Cho $(a, b) \in (\mathbb{N}^*)^2$. Ta thực hiện thuật toán Euclide:

$$r_0 = a, \quad r_1 = b, \quad \begin{cases} r_0 = r_1 q_1 + r_2 \\ 0 < r_2 < r_1 \end{cases} \ldots\ldots \begin{cases} r_{n-2} = r_{n-1} q_{n-1} + r_n \\ 0 < r_n < r_{n-1} \end{cases}, \; r_{n-1} = r_n q_n,$$

tất cả đều là số tự nhiên.

Chứng minh: a) $\sum_{i=1}^{n} r_i q_i = a + b - (a \wedge b)$ b) $\sum_{i=1}^{n} r_i^2 q_i = ab$.

◊ **4.2.4 Phần tử có cấp hữu hạn của một nhóm**

Cho $(G, .)$ là một nhóm với phần tử trung hòa ký hiệu là e. Một phần tử x của G được gọi là **có cấp hữu hạn** khi và chỉ khi tồn tại $n \in \mathbb{N}^*$ sao cho $x^n = e$.

a) Chứng minh rằng, nếu $x \in G$ có cấp hữu hạn thì tồn tại một phần tử duy nhất thuộc $\mathbb{N}^*$, ký hiệu là $\omega(x)$, sao cho : $\begin{cases} x^{\omega(x)} = e \\ \forall k \in \mathbb{N}^*, \left(k < \omega(x) \Rightarrow x^k \neq e\right) \end{cases}$

Như thế, $\omega(x)$ là số nguyên bé nhất ≥ 1 sao cho $x^{\omega(x)} = e$.

Phần tử $\omega(x)$ thuộc $\mathbb{N}^*$ được gọi là **cấp** của x (trong G).

b) α) Chứng minh rằng, nếu G là hữu hạn thì mọi phần tử của G đều có cấp hữu hạn và: $\forall x \in G, \quad \omega(x) \mid \text{Card}(G)$. (Sử dụng định lý Lagrange, C2.1).

β) Nếu mọi phần tử của G đều có cấp hữu hạn, thì ta có thể suy ra G là hữu hạn không?

c) Chứng minh rằng, nếu $x \in G$ có cấp hữu hạn thì: $\{n \in \mathbb{N}^*, x^n = e\} = \omega(x)\mathbb{N}^*$.

d) α) Chứng minh rằng, nếu hai phần tử x, y của G có cấp hữu hạn và giao hoán, thì xy có cấp hữu hạn và: $\omega(xy) \mid \omega(x) \vee \omega(y)$.

Đẳng thức $\omega(xy) = \omega(x) \vee \omega(y)$ có nhất thiết xảy ra không?

β) Cho một ví dụ về một nhóm $(G, .)$ và hai phần tử (x, y) của G có cấp hữu hạn, sao cho xy có cấp không hữu hạn.

◊ **4.2.5** Cho $n \in \mathbb{N}^*$, $N \in \mathbb{N}$ là một số nguyên lẻ, $\sigma \in \mathfrak{S}_n$ sao cho $\sigma^N = e$. Chứng minh rằng σ chẵn. (Sử dụng dạng phân tích δ thành tích những chu trình từng đôi có giá rời nhau, xem 3.4.3. Định lý, và cấp của một phần tử của một nhóm hữu hạn, bài tập 4.2.4).

◊ **4.2.6** Cho $n \in \mathbb{N} - \{0, 1\}$, $\sigma \in \mathfrak{S}_n$, $\sigma = c_1 \circ \ldots \circ c_\nu$ là dạng phân tích σ thành tích những chu trình từng đôi có giá rời nhau (xem 3.4.3, Định lý). Chứng minh rằng cấp của σ là BCNN của các cấp các chu trình $c_1, \ldots, c_\nu$ (xem bài tập 4.2.4).

Ví dụ : Cấp của

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 7 & 8 & 1 & 6 & 5 & 12 & 3 & 10 & 9 & 11 & 2 & 4 \end{pmatrix} \text{ trong } \mathfrak{S}_{12} \text{ là bao nhiêu?}$$

4.3 Số nguyên tố cùng nhau

4.3.1 Đại cương

◆ **Định nghĩa** Cho $n \in \mathbb{N}^*$, $(x_1, ..., x_n) \in (\mathbb{Z}^*)^n$.

1) Ta nói rằng $x_1, ..., x_n$ **nguyên tố cùng nhau (trong toàn thể)** (hoặc : **xa lạ**) khi và chỉ khi : UCLN $(x_1, ..., x_n) = 1$.

2) Ta nói rằng $x_1, ..., x_n$ **nguyên tố cùng nhau từng đôi** khi và chỉ khi : $\forall (i, j) \in \{1, ..., n\}^2$, $(i \neq j \Rightarrow x_i \wedge x_j = 1)$.

NHẬN XÉT:

1) Nếu $x_1, ..., x_n$ nguyên tố cùng nhau từng đôi, thì $x_1, ..., x_n$ nguyên tố cùng nhau trong toàn thể, vì khi đó:

$$\text{UCLN}(x_1, ..., x_n) = \text{UCLN}(x_1 \wedge x_2, x_3, ..., x_n) = \text{UCLN}(1, x_3, ..., x_n) = 1.$$

2) Đảo lại là sai : nếu $n \geq 3$ $x_1, ..., x_n$ có thể nguyên tố cùng nhau (trong toàn thể) nhưng không nguyên tố cùng nhau từng đôi.

Ví dụ : $n = 3$, $x_1 = 6$, $x_2 = 10$, $x_3 = 15$.

3) Với mọi $(x_1, ..., x_n)$ thuộc $(\mathbb{Z}^*)^n$, và ký hiệu $\delta = \text{UCLN}(x_1, ..., x_n)$, tồn tại $(x'_1, ..., x'_n) \in (\mathbb{Z}^*)^n$ sao cho : $\forall i \in \{1, ..., n\}, x_i = \delta x'_i$, và $x'_1, ..., x'_n$ nguyên tố cùng nhau (trong toàn thể) vì :

$$\delta \, \text{UCLN}(x'_1, ..., x'_n) = \text{UCLN}(\delta x'_1, ..., \delta x'_n) = \delta.$$

◆ **Mệnh đề**

$$\forall (a, b, c) \in (\mathbb{Z}^*)^3, \quad \left(\begin{cases} a \wedge b = 1 \\ c \mid b \end{cases} \Rightarrow a \wedge c = 1 \right).$$

Chứng minh: Giả sử $a \wedge b = 1$ và $c \mid b$.

Với mọi d thuộc $\mathbb{N}^*$, nếu ($d \mid a$ và $d \mid c$), thì ($d \mid a$ và $d \mid b$), vậy $d = 1$. Ta kết luận : $a \wedge c = 1$.

4.3.2 Định lý Bezout

◆ **Định lý 1 (Định lý Bezout)**

Cho $n \in \mathbb{N}^*$, $(x_1, ..., x_n) \in (\mathbb{Z}^*)^n$. Để $x_1, ..., x_n$ nguyên tố cùng nhau trong toàn thể, cần và đủ là tồn tại $(u_1, ..., u_n) \in \mathbb{Z}^n$ sao cho :

$$\sum_{i=1}^{n} x_i u_i = 1.$$

Chứng minh:

1) Nếu $x_1, ..., x_n$ nguyên tố cùng nhau trong toàn thể thì

$$\sum_{i=1}^{n} x_i \mathbf{Z} = \mathrm{UCLN}(x_1, ..., x_n)\mathbf{Z} = \mathbf{Z}.$$

Vì $1 \in \mathbb{Z}$, nên tồn tại $(u_1, ..., u_n) \in \mathbb{Z}^n$ sao cho $\sum_{i=1}^{n} x_i u_i = 1$.

2) Ngược lại, nếu tồn tại $(u_1, ..., u_n)$ thuộc $\mathbb{Z}^n$ sao cho $\sum_{i=1}^{n} x_i u_i = 1$, thì

$$1 \in \sum_{i=1}^{n} x_i \mathbf{Z} = \mathrm{UCLN}(x_1, ..., x_n)\mathbf{Z},$$

do đó ƯCLN $(x_1, ..., x_n) = 1$.

NHẬN XÉT:

Định lý Bezout (hoặc Mệnh đề 4 của 4.2.2) cho phép hình thành mối liên hệ giữa một tính chất "số học" (các số nguyên tố cùng nhau trong toàn thể) và một tính chất "đại số" (đẳng thức $\sum_{i=1}^{n} x_i u_i = 1$). Chẳng hạn ta sẽ sử dụng định lý Bezout để xác định các phần tử khả nghịch của vành $(\mathbb{Z}/_{n\mathbb{Z}}, +, \cdot)$, xem 4.3.4, *1*).

♦ **Định lý 2 (Định lý Gauss)**

$$\forall (a, b, c) \in (\mathbb{Z}^*)^3, \quad \left(\begin{cases} a \mid bc \\ a \wedge b = 1 \end{cases} \Rightarrow a \mid c \right).$$

Chứng minh:

Giả sử $a \mid bc$ và $a \wedge b = 1$. Theo định lý Bezout , tồn tại $(u, v) \in \mathbb{Z}^2$ sao cho $au + bv = 1$; suy ra $c = acu + bcv$. Vì $a \mid acu$ và $a \mid bcv$, ta kết luận : $a \mid c$.

♦ **Mệnh đề** Cho $(a, b) \in (\mathbb{Z}^*)^2$ sao cho $a \wedge b = 1$. Tồn tại $(u, v) \in \mathbb{Z}^2$ sao cho:

$$au + bv = 1, \quad |u| < |b|, |v| \leq |a|.$$

Chứng minh:

Rõ ràng ta có thể giả thiết $b > 0$, nếu không chỉ cần thay (a, b) bởi $(-a, -b)$.

Theo định lý Bezout , tồn tại $(u_1, v_1) \in \mathbb{Z}^2$ sao cho $au_1 + bv_1 = 1$.

Bằng phép chia Euclide u_1 cho b, tồn tại $(q, u) \in \mathbb{Z}^2$ sao cho:

$$\begin{cases} u_1 = qb + u \\ 0 \leq u < b \end{cases}.$$

Đặt $v = qa + v_1$, ta có:

$$au + bv = a(u_1 - qb) + b(v_1 + qa) = au_1 + bv_1 = 1,$$

và $|bv| = |1 - au| \le 1 + |a||u| < 1 + |a||b|$, do đó $|bv| \le |a||b|$, vậy thì $|v| \le |a|$. ■

Bây giờ ta sẽ trình bày thuật toán tính một cặp (u,v) sao cho $au + bv = 1$, với (a, b) đã cho thỏa mãn $a \wedge b = 1$.

Giả sử $(a, b) \in \mathbb{Z}^* \times \mathbb{N}^*$ sao cho $a \wedge b = 1$. Theo thuật toán Euclide (4.2.3), tồn tại $N \in \mathbb{N}, q_1, r_1, ..., q_N, r_N, q_{N+1}$ thuộc $\mathbb{Z}$ sao cho:

$$\begin{cases} a = bq_1 + r_1 \\ 0 < r_1 < b \end{cases}, \quad \begin{cases} b = r_1 q_2 + r_2 \\ 0 < r_2 < r_1 \end{cases}, \ldots \quad \begin{cases} r_{N-2} = r_{N-1} q_N + r_N \\ 0 < r_N < r_{N-1} \end{cases}, r_{N-1} = r_N q_{N+1},$$

và $r_N = a \wedge b = 1$.

Như thế ta có các đẳng thức:

$$r_{N-2} = r_{N-1} q_N + 1, \; r_{N-3} = r_{N-2} q_{N-1} + r_{N-1},$$

$$\vdots$$

$$b = r_1 q_2 + r_2, \; a = bq_1 + r_1,$$

chúng sẽ cho phép làm xuất hiện cặp (u, v) thuộc $\mathbb{Z}^2$ thỏa mãn $1 = au + bv$.

VÍ DỤ: $a = 693$, $b = 680$

	1	52	3
693	680	13	4
13	4	1	

$$1 = \boxed{13} - 3 \cdot \boxed{4} = \boxed{13} - 3 \left(\boxed{680} - 52 \cdot \boxed{13} \right)$$

$$= 157 \cdot \boxed{13} - 3 \cdot \boxed{680} = 157 \left(\boxed{693} - 1 \cdot \boxed{680} \right) - 3 \cdot \boxed{680}$$

$$= 157 \cdot \boxed{693} - 160 \cdot \boxed{680}.$$

NHẬN XÉT:

Độc giả có thể chứng minh, bằng quy nạp mạnh theo $|a| + b$, rằng thuật toán trên sẽ cho (nếu $|a| \ge 2$) cặp (u, v) thuộc $\mathbb{Z}^2$ sao cho:

$$au + bv = 1, \quad |u| < b, \quad |v| < |a|.$$

4.3.3 Tính chất

♦ **Mệnh đề 1** Cho $n \in \mathbb{N}^*$, $a, x_1, ..., x_n \in \mathbb{Z}^*$. Ta có:

$$(\forall i \in \{1, ..., n\}, a \wedge x_i = 1) \Leftrightarrow a \wedge \left(\prod_{i=1}^{n} x_i\right) = 1.$$

Chứng minh:

1) $\Rightarrow$: Quy nạp theo n.

- Tính chất là hiển nhiên với $n = 1$.
- Trường hợp $n = 2$

Giả thiết $a \wedge x_1 = a \wedge x_2 = 1$. Theo định lý Bezout, tồn tại $u_1, v_1, u_2, v_2 \in \mathbb{Z}$ sao cho $au_1 + x_1v_1 = 1$ và $au_2 + x_2v_2 = 1$. Thế thì:

$$1 = (au_1 + x_1v_1)(au_2 + x_2v_2) = a(au_1u_2 + x_1v_1u_2 + u_1x_2v_2) + (x_1x_2)(v_1v_2),$$

và $au_1u_2 + x_1v_1u_2 + u_1x_2v_2 \in \mathbb{Z}$, $v_1v_2 \in \mathbb{Z}$, do đó $a \wedge (x_1x_2) = 1$.

- Giả thiết tính chất đúng với một n thuộc $\mathbb{N}^* - \{0, 1\}$, và giả sử $x_1, ..., x_{n+1} \in \mathbb{Z}$ sao cho: $\forall i \in \{1, ..., n+1\}$, $a \wedge x_i = 1$.

Thế thì $(\forall i \in \{1, ..., n\}, a \wedge x_i = 1)$, vậy $a \wedge \left(\prod_{i=1}^{n} x_i\right) = 1$, rồi theo kết quả khảo sát trường hợp $n = 2$:

$$a \wedge \left(\prod_{i=1}^{n+1} x_i\right) = a \wedge \left(\left(\prod_{i=1}^{n} x_i\right) x_{n+1}\right) = 1.$$

2) $\Leftarrow$:

Nếu $a \wedge \left(\prod_{i=1}^{n} x_i\right) = 1$, thì, theo 4.3.1, Mệnh đề: $\forall i \in \{1, ..., n\}$, $a \wedge x_i = 1$.

♦ **Mệnh đề 2**

$$\forall (a, b) \in (\mathbb{Z}^*)^2, \forall (k, l) \in (\mathbb{N}^*)^2, \quad (a \wedge b = 1 \Leftrightarrow a^k \wedge b^l = 1).$$

Chứng minh:

1) Giả sử $a \wedge b = 1$.

Theo Mệnh đề 1, $a \wedge b^l = 1$, và cũng theo Mệnh đề 1, $a^k \wedge b^l = 1$.

2) Ngược lại, nếu $a^k \wedge b^l = 1$, thì, theo Mệnh đề 1, $a^k \wedge b = 1$, và cũng theo Mệnh đề 1, $a \wedge b = 1$.

♦ **Hệ quả** $\forall (a, b) \in (\mathbb{Z}^*)^2$, $\forall k \in \mathbb{N}^*$, $a^k \wedge b^k = (a \wedge b)^k$.

Chứng minh:

Với ký hiệu $\delta = a \wedge b$, tồn tại $(a', b') \in (\mathbb{Z}^*)^2$ sao cho: $a = \delta a'$, $b = \delta b'$, $a' \wedge b' = 1$ (xem 4.3.1, Nhận xét 3)). Vậy ta có: $a^k \wedge b^k = (\delta^k a'^k) \wedge (\delta^k b'^k) = \delta^k (a'^k \wedge b'^k) = \delta^k$.

♦ **Mệnh đề 3** Cho $n \in \mathbb{N}^*$, $a, x_1, ..., x_n \in \mathbb{Z}^*$. Nếu $(\forall i \in \{1, ..., n\},\ x_i \mid a)$ và nếu $x_1, ..., x_n$ nguyên tố cùng nhau từng đôi , thì $\prod_{i=1}^{n} x_i \mid a$.

Chứng minh:

Quy nạp theo n.

- Tính chất là tầm thường với $n = 1$.
- Trường hợp $n = 2$

Giả sử $x_1 \mid a, x_2 \mid a, x_1 \wedge x_2 = 1$.

Tồn tại $y_1 \in \mathbb{Z}^*$ sao cho $a = x_1 y_1$. Vì $x_2 \mid x_1 y_1$ và $x_2 \wedge x_1 = 1$, nên định lý Gauss (4.3.2, Định lý 2) chứng tỏ rằng $x_2 \mid y_1$.

Vậy tồn tại $y_2 \in \mathbb{Z}$ sao cho $y_1 = x_2 y_2$, do đó : $a = x_1 y_1 = (x_1 x_2) y_2$, nên suy ra $x_1 x_2 \mid a$.

- Giả sử tính chất đúng với một n thuộc $\mathbb{N}^*$, và giả sử $x_1, ..., x_{n+1} \in \mathbb{Z}^*$, nguyên tố cùng nhau từng đôi , sao cho : $\forall i \in \{1, ..., n+1\},\ x_i \mid a$.

Thế thì $x_1, ..., x_n$ nguyên tố cùng nhau từng đôi, và $(\forall i \in \{1, ..., n\},\ x_i \mid a)$, suy ra: $\prod_{i=1}^{n} x_i \mid a$. Vì $(\forall i \in \{1, ..., n\}\ , x_{n+1} \wedge x_i = 1)$, nên theo Mệnh đề 1 ta có:

$$x_{n+1} \wedge \left(\prod_{i=1}^{n} x_i \right) = 1.$$

Tiếp theo, vì $\prod_{i=1}^{n} x_i \mid a$ và $x_{n+1} \mid a$, nên ta suy ra (trường hợp $n = 2$): $\prod_{i=1}^{n+1} x_i \mid a$.

♦ **Hệ quả** Cho $n \in \mathbb{N}^*$, $(x_1, ..., x_n) \in (\mathbb{Z}^*)^n$. Nếu $x_1, .., x_n$ nguyên tố cùng nhau từng đôi thì:

$$\text{BCNN}\ (x_1, ..., x_n) = \left| \prod_{i=1}^{n} x_i \right| .$$

♦ **Mệnh đề 4**

$$\forall (a, b) \in (\mathbb{Z}^*)^2, \quad (a \wedge b)(a \vee b) = |ab|.$$

Chứng minh:

Giả sử $(a, b) \in (\mathbb{Z}^*)^2$; ta ký hiệu $\delta = a \wedge b$, $\mu = a \vee b$. Tồn tại $(a', b') \in (\mathbb{Z}^*)^2$ sao cho: $a = \delta a'$, $b = \delta b'$, $a' \wedge b' = 1$ (xem 4.3.1, Nhận xét 3)).

Vậy theo Hệ quả trên : $\mu = (\delta a') \vee (\delta b') = \delta(a' \vee b') = \delta |a'b'|$, do đó

$$\delta\mu = \delta^2 |a'b'| = |\delta a'|\ |\delta b'| = |ab|.$$

NHẬN XÉT:

Mệnh đề trên cho phép tính các BCNN qua trung gian các UCLN.

Chẳng hạn (xem 4.2.3) : $9100 \vee 1848 = \dfrac{9100.1848}{28} = \dfrac{9100}{28}.1848 = 600600.$

4.3.4 Ứng dụng

1) Các phần tử khả nghịch của vành $\mathbb{Z}/n\mathbb{Z}$.

Cho $n \in \mathbb{N}^*$.

a) Giả sử ξ là một phần tử khả nghịch của $\mathbb{Z}/n\mathbb{Z}$. Tồn tại $\zeta \in \mathbb{Z}/n\mathbb{Z}$ sao cho $\xi\zeta = \hat{1}$ và $(x, y) \in \mathbb{Z}^2$ sao cho $\xi = \hat{x}$, $\zeta = \hat{y}$.

Ta có: $\hat{xy} = \hat{1}$, vậy $n \mid xy - 1$. Vậy tồn tại $k \in \mathbb{Z}$ sao cho $xy - 1 = kn$. Theo định lý Bezout, ta suy ra $x \wedge n = 1$.

b) Ngược lại, giả sử $x \in \mathbb{Z}^*$ sao cho $x \wedge n = 1$, và $\xi = \hat{x}$. Theo định lý Bezout tồn tại $(u, v) \in \mathbb{Z}^2$ sao cho $xu + nv = 1$. Thế thì ta có: $\hat{1} = \widehat{xu + nv} = \hat{x}\hat{u} + \hat{n}\hat{v} = \xi\hat{u}$, điều này chứng tỏ ξ khả nghịch trong $\mathbb{Z}/n\mathbb{Z}$(và có phần tử nghịch đảo là $\hat{u}$).

Ta kết luận:

♦ **Mệnh đề** Với $n \in \mathbb{N}^*$, các phần tử khả nghịch của $\mathbb{Z}/n\mathbb{Z}$ là các $\hat{x}$, trong đó $x \in \mathbb{Z}$ và $x \wedge n = 1$.

VÍ DỤ: Các phần tử khả nghịch của $\mathbb{Z}/9\mathbb{Z}$ là: $\hat{1}, \hat{2}, \hat{4}, \hat{5}, \hat{7}, \hat{8}$.

2) Dạng bất khả quy của một số hữu tỷ khác không

Mọi cặp (α, β) thuộc $(\mathbb{Z}^*)^2$ sao cho: $r = \dfrac{\alpha}{\beta}$ và $\alpha \wedge \beta = 1$, được gọi là một **đại diện bất khả quy** của một số hữu tỷ r khác không.

a) Giả sử $r \in \mathbb{Q}^*$; tồn tại $(a, b) \in (\mathbb{Z}^*)^2$ sao cho $r = \dfrac{a}{b}$.

Với ký hiệu $\delta = a \wedge b$, tồn tại $(\alpha, \beta) \in (\mathbb{Z}^*)^2$ sao cho: $a = \delta\alpha$, $b = \delta\beta$, $\alpha \wedge \beta = 1$ (xem 4.3.1, Nhận xét 3)). Thế thì $r = \dfrac{\alpha}{\beta}$ và $\alpha \wedge \beta = 1$, vậy (α, β) là một đại diện bất khả quy của r. Như thế:

Mỗi số hữu tỷ khác không có ít nhất một đại diện bất khả quy.

b) Giả sử $r \in \mathbb{Q}^*$, (α, β) là một đại diện bất khả quy của r, (c, d) là một đại diện khác của r (tức là: $(c, d) \in (\mathbb{Z}^*)^2$ và $r = \dfrac{c}{d}$).

Vì $c\beta = d\alpha$ và $\alpha \wedge \beta = 1$, nên định lý Gauss chứng tỏ rằng $\alpha \mid c$. Vậy tồn tại $k \in \mathbb{Z}$ sao cho $c = k\alpha$, do đó $d = k\beta$. Như thế:

Cho $r \in \mathbb{Q}^*$ và (α, β) là một đại diện bất khả quy của r; mọi đại diện của r đều có dạng $(k\alpha, k\beta)$, $k \in \mathbb{Z}^*$.

c) Giả sử $r \in \mathbb{Q}^*$, (α, β), (γ, δ) là hai đại diện bất khả quy của r. Theo *b)*, ta có: $\alpha \mid \gamma$, $\beta \mid \delta$, $\gamma \mid \alpha$, $\delta \mid \beta$. Suy ra tồn tại $\varepsilon \in \{-1, 1\}$ sao cho $\gamma = \varepsilon\alpha$ và $\delta = \varepsilon\beta$.

Vậy:

Mọi số hữu tỷ khác không có đúng hai đại diện bất khả quy $(\alpha, \beta), (-\alpha, -\beta)$.

Kết quả là mỗi số hữu tỷ khác không có đúng một và chỉ một đại diện bất khả quy (α, β) sao cho $\beta \in \mathbb{N}^*$.

Bài tập

◊ **4.3.1** Cho $n \in \mathbb{Z}$ lẻ sao cho $3 \mid n$; chứng minh : $n^2 \equiv 1[24]$.

◊ **4.3.2** Giải trong $(\mathbb{N}^*)^2$:

a) $\begin{cases} x \wedge y = 18 \\ x \vee y = 540 \end{cases}$ b) $\begin{cases} x \vee y - x \wedge y = 534 \\ x \vee y - 5(x \wedge y) = 510 \end{cases}$

c) $x \vee y - 3(x \wedge y) = 135$

d) $\begin{cases} x + y = 1008 \\ x \wedge y = 24 \end{cases}$ e) $\begin{cases} x^2 + y^2 = 19476 \\ x \vee y = 126 \end{cases}$

f) $x \wedge y + x \vee y = y + 9$.

◊ **4.3.3** a) Chứng minh rằng 442 và 495 nguyên tố cùng nhau.

b) Tìm tất cả các (u, v) thuộc $\mathbb{Z}^2$ sao cho: $442u + 495v = 1$.

c) Giải phương trình $\widehat{442}x = \widehat{314}$ với ẩn $x \in \mathbb{Z}/_{495\mathbb{Z}}$.

◊ **4.3.4** Bản số của $\{(x, y) \in \mathbb{N}^2;\ 2x + 3y = n\}$ là bao nhiêu, với $n \in \mathbb{N}$ đã cho?

◊ **4.3.5** Với $(a, b, c) \in \mathbb{Z}^* \times \mathbb{Z}^* \times \mathbb{Z}$, giải phương trình $ax + by = c$ với ẩn $(x, y) \in \mathbb{Z}^2$.

Ví dụ: Giải trong $\mathbb{Z}^2$: a) $9x + 15y = 11$ b) $9x + 15y = 18$.

◊ **4.3.6*** Cho $(a, b) \in (\mathbb{N}^*)^2$ sao cho: $a \wedge b = 1$, $a \geq 3$, $b \geq 3$.

Chứng minh rằng tồn tại $(x, y) \in \mathbb{Z}^2$ duy nhất sao cho: $ax + by = 1, |x| < \frac{1}{2}b$, $|y| < \frac{1}{2}a$.

◊ **4.3.7*** Cho $(a, b) \in (\mathbb{Z}^*)^2$ sao cho $a \wedge b = 1$. Chứng minh rằng mọi c thuộc $\mathbb{Z}$ sao cho $|c| < |ab|$ đều có thể biểu diễn theo ít nhất một cách và nhiều nhất hai cách, dưới dạng $c = ua + vb$ với : $(u, v) \in \mathbb{Z}^2, |u| < |b|$, $|v| < |a|$.

◊ **4.3.8** Chứng minh :

$$n \wedge 2 = n \wedge 5 = 1 \Rightarrow 23040 \mid (n^2 - 1)(n^2 - 9)(n^2 - 49).$$

với mọi n thuộc $\mathbb{Z}$.

◊ **4.3.9** Chứng minh : $\begin{cases} x^2 + 10y^2 = z^2 \\ 10x^2 + y^2 = t^2 \end{cases} \Rightarrow x = y = z = t = 0$

với mọi (x, y, z, t) thuộc $\mathbb{Z}^4$.

◊ **4.3.10** Chứng minh: $\forall n \in \mathbb{N}^*$, $(n + 1) \mid C_{2n}^n$.

◊ **4.3.11***

a) Chứng minh: $\forall (a, b) \in (\mathbb{Z}^*)^2$, $(a^2 \mid b^2 \Rightarrow a \mid b)$.

b) Suy ra : $\forall \alpha \in \mathbb{Q}^*$, $(\alpha^2 \in \mathbb{Z} \Rightarrow \alpha \in \mathbb{Z})$

c)* Giải trong $\mathbb{Z}^2$: $(x^2 + y)(x + y^2) = (x - y)^3$.

◊ **4.3.12** Chứng minh : $c \mid ab \Rightarrow c \mid (a \wedge c)(b \wedge c)$ với mọi (a, b, c) thuộc $(\mathbb{Z}^*)^3$.

◊ **4.3.13** Cho $n \in \mathbb{N} - \{0, 1\}$, $(a, b) \in (\mathbb{N}^*)^2$ sao cho $a \neq b$.

Chứng minh: $\left(\dfrac{a^n - b^n}{a - b}\right) \wedge (a - b) = (n(a \wedge b)^{n-1}) \wedge (a - b)$.

◊ **4.3.14*** Chứng minh rằng phương trình $6x^2 + 5x + 1 = 0$ không có nghiệm trong $\mathbb{Z}$, nhưng với mọi n thuộc $\mathbb{N}^*$, đồng dư thức $6x^2 + 5x + 1 \equiv 0[n]$ có ít nhất một nghiệm trong $\mathbb{Z}$.

◊ **4.3.15** Cho $n \in \mathbb{N} - \{0, 1\}$, $a_1, ..., a_n \in \mathbb{Z}^*$ nguyên tố cùng nhau từng đôi; Với mỗi i thuộc $\{1, ..., n\}$, ta ký hiệu $A_i = \prod_{\substack{1 \le k \le n \\ k \neq i}} a_k$.

Chứng minh rằng $A_1, ..., A_n$ nguyên tố cùng nhau trong toàn thể.

◊ **4.3.16*** **Định lý Trung Hoa**

Cho $n \in \mathbb{N}^*$, $a_1, ..., a_n \in \mathbb{N}^*$ nguyên tố cùng nhau từng đôi, $a = \prod_{i=1}^{n} a_i$.

a) Chứng minh rằng, với mọi $(b_1, ..., b_n)$ thuộc $\mathbb{Z}^n$, tồn tại $\beta \in \mathbb{Z}$ sao cho:

$$\forall x \in \mathbb{Z}, \quad ((\forall i \in \{1, ..., n\}, x \equiv b_i[a_i]) \Leftrightarrow (x \equiv \beta[a])).$$

Ví dụ : Giải trong $\mathbb{Z}$: $\begin{cases} x \equiv 4[5] \\ x \equiv 3[6] \\ x \equiv 2[7] \end{cases}$.

b) Với bất kỳ m thuộc $\mathbb{N}^*$ và bất kỳ x thuộc $\mathbb{Z}$, ta ký hiệu lớp của x modulo m là $\mathrm{cl}_m(x)$:

$$\mathrm{cl}_m(x) = \{y \in \mathbb{Z};\ m \mid y - x\} = x + m\,\mathbb{Z}.$$

Suy ra rằng (từ *a*) tồn tại một đẳng cấu nhóm $\theta : \mathbb{Z}/_{a\mathbb{Z}} \to \mathbb{Z}/_{a_1\mathbb{Z}} \times ... \times \mathbb{Z}/_{a_n\mathbb{Z}}$ sao cho

$$\forall x \in \mathbb{Z},\ \theta(\mathrm{cl}_a(x)) = \left(\mathrm{cl}_{a_1}(x), ..., \mathrm{cl}_{a_n}(x)\right).$$

◊ **4.3.17** Cho $(a, b, x, y) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Q} \times \mathbb{Q}$ sao cho : $\begin{cases} y - 2x - a = 0 \\ y^2 - xy + x^2 - b = 0 \end{cases}$. Chứng minh : $(x, y) \in \mathbb{Z}^2$. (Sử dụng bài tập 4.3.11, b)).

◊ **4.3.18** Cho $n \in \mathbb{N}^*$, $(a, b, c, d) \in \mathbb{Z}^4$ sao cho n chia hết ac, $bc + ad$, bd. Chứng minh: $n \mid bc$ và $n \mid ad$. (Sử dụng bài tập 4.3.11, a)).

◊ **4.3.19*** Tìm tất cả các $(x, y, z) \in \mathbb{N}^3$ sao cho:

$$2 \le x \le y \le z \text{ và } xy \equiv 1[z] \text{ và } xz \equiv 1[y] \text{ và } yz \equiv 1[x].$$

◊ **4.3.20*** Chứng minh:

$$x^3 + 3y^3 + 9z^3 - 9xyz = 0 \Rightarrow x = y = z = 0,$$

với mọi (x, y, z) thuộc $\mathbb{Z}^3$.

◊ **4.3.21** Xác định các phần tử sinh của nhóm xyclic $(\mathbb{Z}/_{n\mathbb{Z}}, +)$, $n \in \mathbb{N}^*$.

◊ **4.3.22** Với $n \in \mathbb{N} - \{0, 1\}$, xác định các ước của không của vành $(\mathbb{Z}/_{n\mathbb{Z}}, +, \cdot)$.

4.4 Số nguyên tố

4.4.1 Đại cương

Ta đã thấy (3.1.3, Định nghĩa 2):

♦ **Định nghĩa** Một phần tử p của $\mathbb{N}$ được gọi là **nguyên tố** khi và chỉ khi $p \geq 2$ và:

$$\forall a \in \mathbb{N}^*,\ (a \mid p \Rightarrow (a = 1 \text{ hoặc } a = p)).$$

Một số nguyên $n \geq 2$ được gọi là **hợp số** khi và chỉ khi nó không phải là nguyên tố.

Ta có thể nói một số nguyên n là **nguyên tố** khi và chỉ khi $|n|$ là nguyên tố.

NHẬN XÉT : Để cho một phần tử p của $\mathbb{N} - \{0, 1\}$ là nguyên tố, cần và đủ là :

$$U(p) = \{-p, -1, 1, p\}.$$

♦ **Mệnh đề 1** Cho p nguyên tố, $a \in \mathbb{Z}^*$. Ta có:

$$p \mid a \quad \text{hoặc} \quad p \wedge a = 1.$$

Chứng minh:

Vì $p \wedge a \mid p$, ta có: $p \wedge a = p$ hoặc $p \wedge a = 1$, vậy $p \mid a$ hoặc $p \wedge a = 1$.

♦ **Hệ quả**

Nếu p, q là hai số nguyên tố khác nhau (và dương), thì $p \wedge q = 1$.

♦ **Mệnh đề 2** Cho p nguyên tố , $n \in \mathbb{N}^*$, $x_1, ..., x_n \in \mathbb{Z}^*$. Ta có:

$$p \mid \prod_{i=1}^{n} x_i \Leftrightarrow (\exists i \in \{1, ..., n\},\quad p \mid x_i).$$

Chứng minh:

1) $\Rightarrow$:

Giả sử $p \mid \prod_{i=1}^{n} x_i$.

Ta lập luận phản chứng ; giả sử :

$$\forall i \in \{1, ..., n\}, p \nmid x_i.$$

Theo Mệnh đề 1, ta có:

$$\forall i \in \{1, ..., n\}, p \wedge x_i = 1.$$

Ta suy ra (xem 4.3.3, Mệnh đề 1): $p \wedge \left(\prod_{i=1}^{n} x_i \right) = 1$.

Nhưng, vì $p \mid \sum_{i=1}^{n} x_i$, nên ta sẽ có $p = 1$, mâu thuẫn.

Điều này chứng tỏ rằng: $\exists i \in \{1, ..., n\}$, $p \mid x_i$.

2) $\Leftarrow$:

Suy ra từ 4.3.1, Mệnh đề, sự kiện p nguyên tố không tham gia trong lập luận.

NHẬN XÉT:

Nếu một hợp số chia hết một tích, thì ta không thể suy ra rằng nó chia hết một trong các thừa số của tích, chẳng hạn như trong ví dụ sau: $6 \mid 3.4$, $6 \nmid 3$, $6 \nmid 4$.

4.4.2 Thể $\mathbb{Z}/_{p\mathbb{Z}}$, p nguyên tố

◆ **Mệnh đề** Cho $n \in \mathbb{N}^*$. Ba tính chất sau là tương đương:

(i) n nguyên tố

(ii) $\mathbb{Z}/_{n\mathbb{Z}}$ là một thể (giao hoán)

(iii) $\mathbb{Z}/_{n\mathbb{Z}}$ là một vành nguyên.

Chứng minh:

(i) $\Rightarrow$ (ii)

Giả sử n nguyên tố.

Giả sử $\xi \in \mathbb{Z}/_{n\mathbb{Z}} - \{ \hat{0} \}$; tồn tại $x \in \mathbb{Z}$ sao cho $\xi = \hat{x}$. Vì $\hat{x} \neq \hat{0}$, nên ta có: $n \nmid x$.

Vì n là nguyên tố , ta suy ra (xem 4.4.1, Mệnh đề 1)): $n \wedge x = 1$, và như vậy (xem 4.3.4, 1)), $\hat{x}$ khả nghịch trong $\mathbb{Z}/_{n\mathbb{Z}}$.

Điều này chứng tỏ $\mathbb{Z}/_{n\mathbb{Z}}$ là một thể.

(ii) $\Rightarrow$ (iii)

Tổng quát hơn, mọi thể giao hoán là một vành nguyên. Thật vậy, nếu K là một thể giao hoán và nếu $(a, b) \in K^2$ sao cho $ab = 0$ và $a \neq 0$, thì $b = a^{-1}(ab) = 0$.

(iii) $\Rightarrow$ (i)

Bằng lập luận phản đảo, ta chứng minh rằng, nếu n là hợp số thì vành $\mathbb{Z}/_{n\mathbb{Z}}$ không phải là vành nguyên. Thật vậy, nếu n là hợp số, tồn tại $(a, b) \in (\mathbb{N}^*)^2$ sao cho $n = ab$, $1 < a < n$, $1 < b < n$, do đó: $\hat{a}\hat{b} = \hat{0}$, $\hat{a} \neq \hat{0}$, $\hat{b} \neq \hat{0}$.

4.4.3 Phân tích nguyên tố

♦ **Định lý 1** Mọi phần tử của $\mathbb{N} - \{0, 1\}$ có một dạng phân tích thành tích những số nguyên tố, duy nhất sai khác về thứ tự các nhân tử.

Chứng minh:

1) **Tồn tại**

Quy nạp mạnh theo n.

Tính chất đúng với $n = 2$ (2 nguyên tố).

Giả sử rằng mọi số nguyên thuộc $\{2,...,n\}$ đều phân tích được thành một tích những số nguyên tố.

- Nếu $n + 1$ là hợp số, thì tồn tại $(a, b) \in (\mathbb{N}^*)^2$ sao cho:

$$n + 1 = ab, \quad 2 \le a \le n, \quad 2 \le b \le n.$$

Theo giả thiết quy nạp, a và b phân tích được thành tích những số nguyên tố, vậy $n + 1 = ab$ phân tích được thành một tích những số nguyên tố.

- Nếu $n + 1$ nguyên tố, thì $n + 1$ phân tích được thành một tích chỉ có một thừa số, là chính nó.

2) **Duy nhất**

Quy nạp mạnh theo n.

Tính chất hiển nhiên với $n = 2$.

Giả sử dạng phân tích mọi số nguyên thuộc $\{2, ..., n\}$ thành một tích những số nguyên tố là duy nhất, sai khác về thứ tự các nhân tử.

Giả sử $N, N' \in \mathbb{N}^*$, $p_1, ..., p_N, q_1, ..., q_{N'}$ là những số nguyên tố sao cho:

$$n + 1 = p_1 ... p_N = q_1 ... q_{N'}.$$

Vì p_1 nguyên tố và chia hết $q_1 ... q_{N'}$, nên tồn tại $i_1 \in \{1, ..., N'\}$ sao cho $p_1 \mid q_{i_1}$ (xem 4.4.1, Mệnh đề 2); nhưng hơn nữa q_{i_1} nguyên tố, vậy $p_1 = q_{i_1}$.

Vậy khi sắp xếp lại $q_1, ..., q_{N'}$, ta có, chẳng hạn: $p_1 = q_1$.

Khi đó $p_2 ... p_N = q_2 ... q_{N'} \le n$, vậy theo giả thiết quy nạp, $N = N'$, $p_2 = q_2, ..., p_N = q_N$ sai khác về thứ tự. ■

Cho $n \in \mathbb{N} - \{0, 1\}$. Theo định lý trên, tồn tại $N \in \mathbb{N}^*$, $p_1, ..., p_N$ là những số nguyên tố và từng đôi khác nhau, $r_1, ..., r_N \in \mathbb{N}^*$ sao cho $n = \prod_{i=1}^{N} p_i^{r_i}$. Đẳng thức này được gọi là dạng **phân tích nguyên tố** của n.

Với mọi số nguyên tố p (≥ 2), ta gọi số tự nhiên sao cho: $p^{v_p(n)} \mid n$ và $p^{v_p(n)+1} \not\mid n$ là p **- định giá** của n, và ký hiệu là $v_p(n)$.

Với các ký hiệu trên, ta có: $\forall i \in \{1, ..., N\}$, $v_{p_i}(n) = r_i$, và, với mọi số nguyên tố p khác với $p_1, ..., p_N$: $v_p(n) = 0$.

Rõ ràng rằng, với mọi (m, n) thuộc $(\mathbb{N} - \{0, 1\})^2$:

$$m \mid n \Leftrightarrow (\forall p \in \mathcal{P},\ v_p(m) \le v_p(n)).$$

Để thuận tiện trong cách biểu diễn $n = \prod_{i=1}^{N} p_i^{r_i}$ một số r_i có thể bằng không (xem dưới đây).

VÍ DỤ: $9100 = 2^2 . 5^2 . 7 . 13 = 2^2 . 3^0 . 5^2 . 7^1 . 11^0 . 13^1$

$1848 = 2^3 . 3 . 7 . 11 = 2^3 . 3^1 . 5^0 . 7^1 . 11^1 . 13^0$. ■

♦ **Hệ quả**

Mọi số nguyên a thuộc $\mathbb{Z}$ - {-1,0,1} có ít nhất một ước nguyên tố.

♦ **Định lý 2**

Tập hợp $\mathcal{P}$ các số nguyên tố là vô hạn.

Chứng minh:

Ta chứng minh bằng phản chứng: Giả sử $\mathcal{P}$ là hữu hạn và ký hiệu $k = \text{Card}(\mathcal{P})$, $p_1, ..., p_k$ là những phần tử của $\mathcal{P}$.

Số nguyên $M = 1 + \prod_{i=1}^{k} p_i$ có ít nhất một nhân tử nguyên tố p. Như thế tồn tại $j \in \{1, ..., k\}$ sao cho $p = p_j$, do đó $p \mid \prod_{i=1}^{k} p_i$ và như vậy $p \mid M - \prod_{i=1}^{k} p_i$, $p \mid 1$, mâu thuẫn. ■

♦ **Mệnh đề** Cho $(a, b) \in (\mathbb{N} - \{0, 1\})^2$, $a = \prod_{i=1}^{N} p_i^{r_i}$, $b = \prod_{i=1}^{N} p_i^{s_i}$, trong đó $N \in \mathbb{N}^*$, $p_1, ..., p_N$ là các số nguyên tố từng đôi khác nhau, $r_1, ..., r_N$, $s_1, ..., s_N \in \mathbb{N}$. Ta có: $a \wedge b = \prod_{i=1}^{N} p_i^{\text{Min}(r_i, s_i)}$ và $a \vee b = \prod_{i=1}^{N} p_i^{\text{Max}(r_i, s_i)}$.

Chứng minh:

1) Ký hiệu $d = \prod_{i=1}^{N} p_i^{\text{Min}(r_i, s_i)}$ và $\delta = a \wedge b$.

- Vì $(\forall i \in \{1, ..., n\}, \begin{cases} \text{Min}(r_i, s_i) \le r_i \\ \text{Min}(r_i, s_i) \le s_i \end{cases})$, nên ta có ($d \mid a$ và $d \mid b$), vậy $d \mid \delta$.
- Mặt khác, vì $\delta \mid a$ và $\delta \mid b$, nên ta có:

$$\forall i \in \{1, ..., n\}, \begin{cases} v_{p_i}(\delta) \le v_{p_i}(a) = r_i \\ v_{p_i}(\delta) \le v_{p_i}(b) = s_i \end{cases},$$

do đó: $\forall i \in \{1, ..., n\}$, $v_{p_i}(\delta) \le \text{Min}(r_i, s_i)$. Kết quả là $\delta \mid d$, và cuối cùng $\delta = d$.

2) Vì $(a \wedge b)(a \vee b) = |ab|$ (xem 4.3.3, Mệnh đề 4), ta có :

$$a \vee b = \prod_{i=1}^{N} p_i^{r_i+s_i-\mathrm{Min}(r_i,s_i)} = \prod_{i=1}^{N} p_i^{\mathrm{Max}(r_i,s_i)}.$$

VÍ DỤ:

$$9100 = 2^2 . 3^0 . 5^2 . 7^1 . 11^0 . 13^1 \text{ và } 1848 = 2^3 . 3^1 . 5^0 . 7^1 . 11^1 . 13^0,$$

do đó:

$$\begin{cases} 9100 \wedge 1848 = 2^2.3^0.5^0.7^1.11^0.13^0 = 28 \\ 9100 \vee 1848 = 2^3.3^1.5^2.7^1.11^1.13^1 = 600600 \end{cases}$$

♦ Hệ quả

Trong $\mathbb{Z}^*$, các luật $\wedge$ và $\vee$ luật này có tính phân phối đối với luật kia.

Chứng minh:

Giả sử $(a, b, c) \in (\mathbb{Z}_i^*)^3$.

Xét các dạng phân tích nguyên tố:

$$|a| = \prod_{i=1}^{N} p_i^{\alpha_i}, \quad |b| = \prod_{i=1}^{N} p_i^{\beta_i}, \quad |c| = \prod_{i=1}^{N} p_i^{\gamma_i},$$

trong đó $N \in \mathbb{N}^*$, $p_1, ..., p_N$ là những số nguyên tố từng đôi khác nhau, $\alpha_1, ..., \alpha_N$, $\beta_1, ..., \beta_N, \gamma_1, ..., \gamma_N \in \mathbb{N}$.

Ta có:

$$a \wedge (b \vee c) = \prod_{i=1}^{N} p_i^{u_i} \text{ và } (a \wedge b) \vee (a \wedge c) = \prod_{i=1}^{N} p_i^{v_i},$$

trong đó, với mọi i thuộc $\{1, ..., N\}$:

$$u_i = \mathrm{Min}(\alpha_i, \mathrm{Max}(\beta_i, \gamma_i)) \text{ và } v_i = \mathrm{Max}(\mathrm{Min}(\alpha_i, \beta_i), \mathrm{Min}(\alpha_i, \gamma_i)).$$

Giả sử $i \in \{1, ..., N\}$; vì β_i và γ_i giữ các vai trò đối xứng, nên ta có thể giả thiết, chẳng hạn, $\beta_i \leq \gamma_i$.

Vì thứ tự $\leq$ thông thường trong $\mathbb{N}$ là toàn phần, nên ta có thể tách ra ba trường hợp:

	$\alpha_i \leq \beta_i \leq \gamma_i$	$\beta_i \leq \alpha_i \leq \gamma_i$	$\beta_i \leq \gamma_i \leq \alpha_i$
trị của u_i	α_i	α_i	γ_i
trị của v_i	α_i	α_i	γ_i

Vậy ta có: $(\forall i \in \{1, ..., n\}, u_i = v_i)$, do đó $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

Chứng minh tương tự đối với $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$. ■

Bài tập

◊ **4.4.1** Chứng minh rằng các số nguyên sau là những hợp số :

a) $n^4 - n^2 + 16$ với $n \in \mathbb{Z}$

b) $4n^3 + 6n^2 + 4n + 1$ với $n \in \mathbb{N}^*$

c) $2^{4n+2} + 1$ với $n \in \mathbb{N}^*$.

◊ **4.4.2** Cho $n \in \mathbb{N} - \{0, 1\}$; chứng minh $5^n - 3^n$ là hợp số.

◊ **4.4.3** Cho $(a, b, c, d) \in (\mathbb{N}^*)^4$ sao cho $ab = cd$. Chứng minh rằng, với mọi n thuộc $\mathbb{N}^*$, $a^n + b^n + c^n + d^n$ là hợp số.

◊ **4.4.4** Tìm tất cả các số p thuộc $\mathbb{N} - \{0, 1\}$ sao cho p và $p^3 + p^2 + 11p + 2$ là những số nguyên tố.

◊ **4.4.5** Cho $n \in \mathbb{N}^*$, $x_1, ..., x_n \in \mathbb{N}^*$ từng đôi khác nhau và không có một ước nguyên tố nào ≥ 5. Chứng minh : $\sum_{k=1}^{n} \frac{1}{x_k} < 3$.

◊ **4.4.6** Cho p là số nguyên tố và ≥ 3, $n \in \mathbb{N}$. Chứng minh: $(1+p)^{p^n} \equiv 1 + p^{n+1} [p^{n+2}]$.

◊ **4.4.7** Chứng minh rằng dãy $(u_n)_{n\geq 0}$ xác định bởi : $\forall n \in \mathbb{N}$, $u_n = E(n + \sqrt{n} + 5)$ chứa tất cả các số nguyên tố ≥ 5.

◊ **4.4.8** Cho $(a, b) \in \mathbb{N}^2$ sao cho $\frac{1}{2}(a^3 + b^3)$ là một số nguyên tố. Chứng minh: $a = b = 1$.

◊ **4.4.9** Cho $n \in \mathbb{N}$ sao cho $n \geq 11$. Chứng minh rằng, nếu $n - 10$, $n + 10$, $n + 60$ là những số nguyên tố, thì $n + 90$ cũng là số nguyên tố.

◊ **4.4.10** Cho $n \in \mathbb{N}$. Chứng minh rằng, nếu n và $n^2 + 8$ là những số nguyên tố, thì $n^3 + 4$ cũng là số nguyên tố (chứng minh $n = 3$).

◊ **4.4.11** Tìm tất cả các số n thuộc $\mathbb{Z}$ sao cho $n^4 + 4n^3 + 6n^2 + 4n + 5$ nguyên tố.

◊ **4.4.12** Tìm tất cả các số p thuộc $\mathbb{N} - \{0, 1\}$ sao cho p và $2^p + p^2$ là những số nguyên tố.

◊ **4.4.13** Cho số nguyên tố $p \geq 5$, $n \in \mathbb{N}$. Chứng minh p chia hết $\sum_{k=0}^{p-1} (n+k)^2$.

◊ **4.4.14** Cho $(a, b, m, n) \in (\mathbb{N}^*)^4$ sao cho $a^m + b^n$ là số nguyên tố và $m \geq 2$, $n \geq 2$. Chứng minh tồn tại $\alpha \in \mathbb{N}$ sao cho $m \wedge n = 2^\alpha$.

◊ **4.4.15** Cho $p \in \mathbb{N}$ sao cho $p \geq 4$. Chứng minh rằng, nếu p và $p + 2$ là những số nguyên tố, thì $p \equiv -1 [6]$.

◊ **4.4.16** Cho $(p, q, r) \in (\mathbb{N} - \{0, 1\})^3$. Chứng minh rằng, nếu $p, q, r, p^2 + q^2 + r^2$ là những số nguyên tố, thì một trong ba số p, q, r là 3.

◊ **4.4.17** Tìm tất cả các số nguyên tố có dạng $2^{2^n} + 5$, $n \in \mathbb{N}$.

◊ **4.4.18** Cho $n \in \mathbb{N} - \{0, 1\}$ và p là ước nguyên tố nhỏ nhất của n; ta giả thiết $\sqrt[3]{n} < p < n$. Chứng minh rằng $\frac{n}{p}$ là số nguyên tố.

◊ **4.4.19** Những số nguyên tố nào là tổng của hai hợp số?

◊ **4.4.20** Chứng minh rằng, nếu p là số nguyên tố ≥ 5, thì $4p^2 + 1$ có thể phân tích thành tổng của ba bình phương của những số nguyên ≥ 1.

◊ **4.4.21** a) Cho p là một số nguyên tố ; chứng minh: $\forall k \in \{1, ..., p\text{-}1\}, p \mid C_p^k$.

b)* *Tổng quát hóa.* Cho p là một số nguyên tố, $n \in \mathbb{N} - \{0, 1\}$, $(i_1, ..., i_n) \in \{0, ..., p - 1\}$ sao cho $i_1 + ... + i_n = p$. Chứng minh rằng $\dfrac{p!}{i_1!...i_n!}$ là một số nguyên chia hết cho p.

◊ **4.4.22*** Cho số nguyên tố p. Chứng minh rằng không tồn tại một cặp (a, n) nào thuộc $(\mathbb{N} - \{0, 1\})^2$ thỏa mãn: $2^p + 3^p = a^n$.

◊ **4.4.23** Chứng minh: $\forall n \in \mathbb{Z}$, $49 \not| n^3 - n^2 - 2n + 1$.

◊ **4.4.24** Xác định các số n thuộc $\mathbb{N}^*$ sao cho: $(2n^7 + 1) \wedge (3n^2 + 2) \neq 1$.

◊ **4.4.25** a) Cho $k \in \mathbb{N}^*$; chứng minh rằng, nếu $2^k + 1$ nguyên tố, thì k là một lũy thừa của 2.

Các số $F_n = 2^{2^n} + 1$ ($n \in \mathbb{N}$) được gọi là **các số Fermat**. Chúng không phải đều là số nguyên tố; chẳng hạn F_5 là hợp số, chia hết cho 641.

b) Chứng minh rằng với mọi (m, n) thuộc $\mathbb{N}^2$: $m \neq n \Rightarrow F_m \wedge F_n = 1$.

Trong các bài tập 4.4.26 *và* 4.4.27, *ta có thể sử dụng lý thuyết các đa thức (chương 5).*

◊ **4.4.26*** Cho $n \in \mathbb{N}^*$ sao cho tồn tại số nguyên tố p thỏa mãn: $p \geq 5$ và $p \mid n$. Chứng minh rằng $4^n - 2^n + 1$ là hợp số.

◊ **4.4.27*** Chứng minh rằng, nếu $n \in \mathbb{N}^*$ sao cho $4^n + 2^n + 1$ nguyên tố, thì n là một lũy thừa của 3.

◊ **4.4.28** Cho $n \in \mathbb{N} - \{0, 1\}$. Chứng minh rằng n là hợp số khi và chỉ khi $\sigma(n) > n + \sqrt{n}$, trong đó $\sigma(n)$ là tổng các ước ≥ 1 của n.

◊ **4.4.29** Chứng minh: $\forall (a, b) \in (\mathbb{N} - \{0,1\})^2$, $\dfrac{\sigma(a)}{a} \leq \dfrac{\sigma(ab)}{ab} \leq \dfrac{\sigma(a)\sigma(b)}{ab}$, trong đó, $\sigma(n)$ là tổng các ước ≥ 1 của n, với mọi n thuộc $\mathbb{N} - \{0, 1\}$.

◊ **4.4.30** Chứng minh: $\forall (a, b) \in (\mathbb{N}^*)^2$, $(a^2 + ab + b^2) \wedge ab = (a \vee b)^2$.

◊ **4.4.31** Khẳng định sau đây có đúng không: $\forall (a, b) \in (\mathbb{N}^*)^2$, $(a^a \mid b^b \Rightarrow a \mid b)$?

◊ **4.4.32** Cho $(a, b) \in (\mathbb{N}^*)^2$; chứng minh rằng tồn tại $(x, y) \in (\mathbb{N}^*)^2$ sao cho:

$$x \mid a \ , \ y \mid b, \ x \wedge y = 1 \ , \ xy = a \vee b.$$

◊ **4.4.33** Cho $a, b, c, k \in \mathbb{N}^*$ sao cho: $ab = c^k$ và $a \wedge b = 1$. Chứng minh rằng tồn tại $(\alpha, \beta) \in (\mathbb{N}^*)^2$ sao cho : $a = \alpha^k$ và $b = \beta^k$.

◊ **4.4.34** Cho $(a, b) \in (\mathbb{Z}^*)^2$, $(f, g) \in (\mathbb{N}^*)^2$ sao cho $a^f \mid b^g$. Chứng minh rằng $a \mid b^\alpha$, trong đó α là số nguyên nhỏ nhất thỏa mãn $\dfrac{g}{f} \leq \alpha$.

◊ **4.4.35** Chứng minh: $\forall (a, b, c) \in (\mathbb{Z}^*)^3$, $(a \vee b)(a \vee c)(b \vee c)(a \wedge b \wedge c) = (a \vee b \vee c)\,|\,abc\,|$.

◊ **4.4.36** Cho $n \in \mathbb{N}^*$, $a_1, ..., a_n \in \mathbb{Z}^*$, $a = \prod_{i=1}^{n} a_i$.

Chứng minh: $\left(\bigwedge_{i=1}^{n} a_i\right)\left(\bigvee_{i=1}^{n} \frac{a}{a_i}\right) = \left(\bigvee_{i=1}^{n} a_i\right)\left(\bigwedge_{i=1}^{n} \frac{a}{a_i}\right) = a.$

◊ **4.4.37** Với $n \in \mathbb{N} - \{0, 1\}$, ta ký hiệu $d(n)$ là số các ước ≥ 1 của n, và $\sigma(n)$ là tổng các ước ≥ 1 của n. Chứng minh rằng, nếu dạng phân tích nguyên tố của n là $n = \prod_{i=1}^{N} p_i^{r_i}$, thì:

$$d(n) = \prod_{i=1}^{N} (r_i + 1) \quad \text{và} \quad \sigma(n) = \prod_{i=1}^{N} \frac{p_i^{r_i+1} - 1}{p_i - 1}.$$

◊ **4.4.38** Với $n \in \mathbb{N} - \{0, 1\}$, tính tích các ước của n (sử dụng dạng phân tích nguyên tố của n).

◊ **4.4.39** Cho $n \in \mathbb{N} - \{0, 1\}$. Chứng minh rằng, để cho n là tích của các ước khác với n của nó (tức là: $n = \prod_{\substack{1 \leq d < n \\ d|n}} d$), điều kiện cần và đủ là n là lập phương của một số nguyên tố, hoặc là tích của hai số nguyên tố khác nhau.

◊ **4.4.40** Cho $k \in \mathbb{N}^*$. Với mọi n thuộc $\mathbb{N}^*$, ta ký hiệu $\sigma_k(n)$ là tổng các lũy thừa bậc k của các ước ≥ 1 của n : $\sigma_k(n) = \sum_{\substack{1 \leq d \leq n \\ d|n}} d^k$.

a) Chứng minh rằng, nếu dạng phân tích nguyên tố của n là $n = \prod_{i=1}^{N} p_i^{r_i}$, thì

$\sigma_k(n) = \prod_{i=1}^{N} \frac{p_i^{k(r_i+1)} - 1}{p_i^k - 1}$ (xem bài tập 4.4.37).

b) Suy ra rằng σ_k là một **hàm số học nhân tính**, tức là:

$$\forall (a, b) \in (\mathbb{N}^*)^2,\ (a \wedge b = 1 \Rightarrow \sigma_k(ab) = \sigma_k(a)\sigma_k(b)).$$

◊ **4.4.41** Xác định tất cả các cặp (n,p) thuộc $(\mathbb{N}^*)^2$ sao cho p là số nguyêntố ≥ 5, và nếu ký hiệu $N = 2^n 3p$, thì ta có $\sigma(N) = 3N$, trong đó $\sigma(N)$ là tổng các ước của N.

◊ **4.4.42** Giải :

a) $x^2 + \hat{4}x + \hat{1} = \hat{0}$ trong $\mathbb{Z}/_{11\mathbb{Z}}$ b) $\begin{cases} \hat{5}x + \hat{2}y = \hat{3} \\ \hat{2}x + \hat{4}y = \hat{6} \end{cases}$ trong $(\mathbb{Z}/_{12\mathbb{Z}})^2$.

◊ **4.4.43** Cho p là một số nguyên tố.

a) Chứng minh: $\forall k \in \{1, ..., p - 1\}, p \mid C_p^k$.

b)* Suy ra : $\forall N \in \mathbb{N}^*, \forall f \in \mathbb{N}^*, \forall (x_1, ..., x_N) \in \mathbb{Z}^N, \left(\sum_{i=1}^{N} x_i\right)^{p^f} \equiv \sum_{i=1}^{N} x_i^{p^f}\ [p]$

◊ **4.4.44** Cho $(a, b, c, d) \in \mathbb{Z}^4$ sao cho $5 \nmid d$. Chứng minh:

$(\exists x \in \mathbb{Z}, 5 \mid ax^3 + bx^2 + cx + d) \Rightarrow (\exists y \in \mathbb{Z}, 5 \mid dy^3 + cy^2 + by + a)$.

◊ **4.4.45** Cho p nguyên tố. Chứng minh : $C_{np-1}^{p-1} \equiv 1[p]$ và $C_{np}^{p} \equiv n[p]$ với mọi n thuộc $\mathbb{N}^*$.

◊ **4.4.46** Tìm tất cả các cặp (x, y) thuộc $(\mathbb{N}^*)^2$ sao cho : $\dfrac{x+y}{x^2 - xy + y^2} = \dfrac{2}{7}$.

◊ **4.4.47*** Chứng minh rằng phương trình $15x^2 - 4y^2 = 7^z$ không có nghiệm trong $\mathbb{N}^3$.

◊ **4.4.48* Định lý Wolstenhome**

Cho p là số nguyên tố ≥ 5, $H_{p-1} = \sum_{k=1}^{p-1} \frac{1}{k}$. Chứng minh rằng tử số của H_{p-1} chia hết cho p^2.

◊ **4.4.49** Cho p là số nguyên tố , $p \geq 5$.

a) Chứng minh : $p \mid \sum_{k=1}^{p-1} k$ và $p \mid \sum_{k=1}^{p-1} k^2$.

b) Suy ra rằng, với ký hiệu $a = \sum_{i=1}^{p-1} \frac{(p-1)!}{i}$ và $b = \sum_{1 \leq i < j \leq p-1} \frac{(p-1)!}{ij}$, thì ta có: $p^2 \mid a$ và $p \mid b$.

c) Chứng minh: $p^3 \mid C_{2p-1}^{p-1} - 1$.

◊ **4.4.50 Định lý nhỏ Fermat**

Cho p là số nguyên tố.

a) Chứng minh: $\forall n \in \mathbb{Z}$, $n^p \equiv n\ [p]$.

b) Suy ra : $\forall n \in \mathbb{Z}$, $(p \mid n \Rightarrow n^{p-1} \equiv 1[p])$.

Khi giải các bài tập từ 4.4.51 *đến* 4.4.64 *có thể sử dụng định lý nhỏ Fermat.*

◊ **4.4.51** Chứng minh : $\forall n \in \mathbb{Z}$, $\dfrac{n^7}{7} + \dfrac{n^5}{5} + \dfrac{23n}{35} \in \mathbb{Z}$.

◊ **4.4.52** Chứng minh, với mọi n thuộc $\mathbb{Z}$:

a) $42 \mid n^7 - n$

b) $2730 \mid n^{13} - n$

c) $2^{15} - 2^3 \mid n^{15} - n^3$.

◊ **4.4.53** Chứng minh:

a) Với mọi số nguyên n lẻ sao cho $n \geq 15$: $21840 \mid n^{12} - 1$

b) Với mọi số nguyên tố $p \geq 19$: $16320 \mid p^{16} - 1$.

◊ **4.4.54** Chứng minh: $\forall (a, b, c, d) \in (\mathbb{N}^*)^4$, $30 \mid a^{4b+d} - a^{4c+d}$.

◊ **4.4.55** Chứng minh rằng số 1729 thỏa mãn :

$$\forall n \in \mathbb{Z},\ (n \wedge 1729 = 1 \Rightarrow n^{1728} \equiv 1[1729]),$$

nhưng 1729 lại không phải là số nguyên tố.

Nói khác đi, đảo của định lý nhỏ Fermat là sai.

◊ **4.4.56** Cho p là số nguyên tố và $n \in \mathbb{N}^*$ sao cho $n \wedge p = 1$. Chứng minh:

a) Nếu p lẻ, thì $p \mid n^{\frac{p-1}{2}} - 1$ hoặc $p \mid n^{\frac{p-1}{2}} + 1$.

b) $p^2 \mid n^{\frac{p(p-1)}{2}} - 1$ hoặc $p^2 \mid n^{\frac{p(p-1)}{2}} + 1$.

◊ **4.4.57** Cho p là một số nguyên tố lẻ. Chứng minh: $\forall n \in \mathbb{Z}, (n+1)^p - (n^p + 1) \equiv 0[2p]$.

◊ **4.4.58** Cho p là số nguyên tố. Chứng minh:

$$(n^{p-1})^{p^k} \equiv 1[p^{k+1}],$$

Với mọi k thuộc $\mathbb{N}$ và mọi n thuộc $\mathbb{Z}^*$ sao cho $n \wedge p = 1$.

◊ **4.4.59*** a) cho p là một số nguyên tố, $(a, \alpha) \in \mathbb{Z}^2$, $(b, \beta) \in \mathbb{N}^2$ sao cho: $p \nmid a$, $\alpha \equiv a[p]$, $\beta \equiv b[p-1]$. Chứng minh: $\alpha^\beta \equiv a^b[p]$.

b) Giải trong $(\mathbb{N}^*)^2$: $\begin{cases} x^y \equiv 2[5] \\ y^x \equiv 3[7] \end{cases}$.

◊ **4.4.60** Cho p nguyên tố, $(a, b) \in \mathbb{Z}^2$ sao cho $a^p \equiv b^p[p]$. Chứng minh: $a^p \equiv b^p[p^2]$.

◊ **4.4.61** Cho p, q là hai số nguyên tố khác nhau.

Chứng minh: $p^{q-1} + q^{p-1} \equiv 1[pq]$.

◊ **4.4.62** Cho p là số nguyên tố. Với mọi a thuộc $\mathbb{Z}$ sao cho $p \nmid a$, ta ký hiệu $F_p(a) = \dfrac{a^{p-1} - 1}{p}$ (đó là một số nguyên theo định lý nhỏ Fermat). Chứng minh rằng, với mọi (a, b) thuộc $(\mathbb{N}^*)^2$ sao cho $p \nmid a$ và $p \nmid b$, ta có: $F_p(ab) \equiv F_p(a) + F_p(b)[p]$.

◊ **4.4.63** Chứng minh rằng phương trình $x^3 + 781 = 3y^3$ không có nghiệm trong $\mathbb{Z}^2$.

◊ **4.4.64** Giải trong $(\mathbb{N}^*)^2$: $x^3 - y^3 = 999$.

◊ **4.4.65** a) Cho p là số nguyên tố. Chứng minh rằng, trong vành $\mathbb{Z}/p\mathbb{Z}[X]$ thì:

$X^{p-1} - \hat{1} = \prod_{k=1}^{p-1} (X - \hat{k})$. (Ta có thể sử dụng định lý nhỏ Fermat, bài tập 4.4.50).

Suy ra **định lý Wilson** : Nếu p nguyên tố, thì $(p-1)! \equiv -1[p]$.

b) Ngược lại, chứng minh rằng nếu $(n-1)! \equiv -1[n]$, thì n là nguyên tố, với mọi n.

Khi giải các bài tập từ 4.4.66 *đến* 4.4.74 *có thể sử dụng định lý Wilson.*

◊ **4.4.66** Cho $n \in \mathbb{N}$, $n \geq 5$. Chứng minh rằng nếu $n+2$ nguyên tố, thì $n! - 1$ là hợp số.

◊ **4.4.67** Cho n là một số nguyên chẵn sao cho $p = 2n + 1$ nguyên tố. Chứng minh: $p \mid (n!)^2 + 1$.

◊ **4.4.68** Cho p là số nguyên tố lẻ. Chứng minh: $2((p-3)!) \equiv -1[p]$.

◊ **4.4.69** Cho p là một số nguyên tố sao cho $p \equiv 3[4]$. Chứng minh:

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv 1[p].$$

◊ **4.4.70** Cho p là một số nguyên tố lẻ. Chứng minh: $\left(\prod_{k=1}^{\frac{p-1}{2}}(2k-1)\right)^2 \equiv (-1)^{\frac{p+1}{2}}[p]$.

◊ **4.4.71** Cho $n \in \mathbb{N} - \{0, 1\}$, lẻ. Chứng minh rằng n và $n + 2$ là những số nguyên tố khi và chỉ khi : $4((n-1)! + 1) + n) \equiv 0[n(n+2)]$.

◊ **4.4.72** Cho p nguyên tố. Chứng minh:

$$\forall n \in \mathbb{N}^*\left(\begin{cases} n < p \\ (-1)^n n! \equiv 1[p] \end{cases} \Rightarrow (p-n-1)! \equiv -1[p]\right).$$

Áp dụng: Chứng minh $61! \equiv 63! \equiv -1[71]$.

◊ **4.4.73** Cho p là số nguyên tố và $n \in \mathbb{N}$ thỏa mãn $1 \le n \le p-1$. Chứng minh:

$$(p-n)!(n-1)! \equiv (-1)^n[p].$$

◊ **4.4.74** Cho p là số nguyên tố. Chứng minh: $\forall n \in \mathbb{Z}, \quad p \mid n^p + (p-1)!n$.

(Sử dụng các định lý Fermat và Wilson).

Hàm chỉ Euler, các bài tập từ 4.4.75 *đến* 4.4.89.

◊ **4.4.75 Hàm chỉ Euler**

Với mọi n thuộc $\mathbb{N}^*$, ta ký hiệu $\varphi(n)$ là số các số nguyên gồm giữa 1 và n và nguyên tố với n :

$$\varphi(n) = \text{Card}\{k \in \{1, \ldots, n\}, k \wedge n = 1\}.$$

Ánh xạ $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ được gọi là **hàm chỉ Euler**.

a) Cho $(a, b) \in (\mathbb{N}^*)$ sao cho $a \wedge b = 1$.Chứng minh rằng các vành $\mathbb{Z}/_{ab\mathbb{Z}}$ và $\mathbb{Z}/_{a\mathbb{Z}} \times \mathbb{Z}/_{b\mathbb{Z}}$ (vành tích, xem 2.1, Định nghĩa 14) là đẳng cấu (xem bài tập 4.3.16).

b) Suy ra: $\forall (a, b) \in (\mathbb{N}^*), \ (a \wedge b = 1 \Rightarrow \varphi(ab) = \varphi(a)\varphi(b))$.

Ta nói rằng φ là một **hàm số học nhân tính**.

c) Cho p nguyên tố. Chứng minh: $\forall r \in \mathbb{N}^*, \varphi(p^r) = p^r - p^{r-1}$.

d) Suy ra rằng, nếu $n \in \mathbb{N}^*$ có dạng phân tích nguyên tố $n = \prod_{i=1}^{N} p_i^{r_i}$, thì:

$$\varphi(n) = \prod_{i=1}^{N}\left(p_i^{r_i} - p_i^{r_i-1}\right) = n\prod_{i=1}^{N}\left(1 - \frac{1}{p_i}\right).$$

◊ **4.4.76* Định lý Euler**

Chứng minh: $\forall n \in \mathbb{N}^*, \ \forall a \in \mathbb{Z}^*, (a \wedge n = 1 \Rightarrow a^{\varphi(n)} \equiv 1[n])$.

(Sử dụng định lý Lagrange C 2.1).

Định lý Euler là một dạng khái quát của định lý nhỏ Fermat (bài tập 4.4.50).

◊ **4.4.77** Chứng minh: $\forall (n, k) \in (\mathbb{N}^*)^2, \varphi(n^k) = n^{k-1}\varphi(n)$.

◊ **4.4.78** Chứng minh: $\forall n \in \mathbb{Z}^*, \left(\begin{cases} n \wedge 2 = 1 \\ n \wedge 5 = 1 \end{cases} \Rightarrow 13200 \middle| n^{21} - n \right)$.

◊ **4.4.79*** a) Chứng minh: $\forall n \in \mathbb{N}^*, \quad \sum_{d|n} \phi(d) = n$.

b) Suy ra: $\forall n \in \mathbb{N}^*, \sum_{k=1}^{n} E\left(\frac{n}{k}\right) \varphi(k) = \frac{n(n+1)}{2}$.

◊ **4.4.80** Chứng minh: $\forall n \in \mathbb{N} - \{0, 1\}, \sum_{\substack{1 \le k \le n \\ k \wedge n = 1}} k = \frac{n\varphi(n)}{2}$.

◊ **4.4.81** Cho $n \in \mathbb{N}^*$, chẵn. Chứng minh: $\sum_{\substack{d_1 | n \\ d_1 \text{ lẻ}}} \varphi\left(\frac{n}{d_1}\right) = \sum_{\substack{d_2 | n \\ d_2 \text{ chẵn}}} \varphi\left(\frac{n}{d_2}\right) = \frac{n}{2}$.

(Sử dụng bài tập 4.4.79 a)).

◊ **4.4.82** Cho $n \in \mathbb{N} - \{0, 1\}$, hợp số; chứng minh: $\varphi(n) \le n - \sqrt{n}$.

◊ **4.4.83** Chứng minh: $\forall (a, b) \in (\mathbb{N}^*)^2, (a \wedge b = 1 \Rightarrow a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 [ab]$.

(Sử dụng định lý Euler, bài tập 4.4.76).

◊ **4.4.84** Cho $(a, n) \in \mathbb{Z} \times \mathbb{N}^*$ sao cho: $a \wedge n = (a - 1) \wedge n = 1$. Chứng minh:

$$\sum_{k=0}^{\varphi(n)-1} a^k \equiv 0 [n].$$

(Sử dụng định lý Euler, bài tập 4.4.76).

◊ **4.4.85** Chứng minh: $\forall (a, b) \in (\mathbb{N}^*)^2, (a | b \Rightarrow a\varphi(b) = b\varphi(a))$.

◊ **4.4.86** Chứng minh: $\forall (a, b) \in (\mathbb{N}^*)^2, \varphi(ab) = \frac{(a \wedge b)\varphi(a)\varphi(b)}{(a \wedge b)}$.

(Sử dụng bài tập 4.4.85).

◊ **4.4.87** Cho $(a, b) \in (\mathbb{N}^*)^2$, c là tích các ước nguyên tố của $a \wedge b$. Chứng minh:

$$\varphi(ab) = \frac{c\varphi(a)\varphi(b)}{\varphi(c)}.$$

(Sử dụng bài tập 4.4.85).

◊ **4.4.88*** Chứng minh: $\forall a \in \mathbb{N} - \{0, 1\}$, $\forall k \in \mathbb{N}^*, k | \varphi(a^k - 1)$. (Sử dụng định lý Euler, bài tập 4.4.76).

◊ **4.4.89** Cho $n \in \mathbb{N}^*$ và $(u_k)_{k \in \mathbb{N}}$ là dãy xác định bởi $u_0 = n$ và : $\forall k \in \mathbb{N}, u_{k+1} = \varphi(u_k)$.

Chứng minh: $\exists r \in \mathbb{N}, \quad u_r = 1$.

Bổ sung

◊ C 4.1 Định lý bốn bình phương của Lagrange và tổng các trùng phương

I - Vấn đề là chứng minh rằng mọi số tự nhiên đều có thể phân tích thành tổng các bình phương của bốn số tự nhiên.

1) a) **Hằng đẳng thức Lagrange**

Với a, b, c, d, x, y, z, t bất kỳ thuộc $\mathbb{R}$, hãy kiểm chứng:

$(ax + by + cz + dt)^2 + (ay - bx + ct - dz)^2 + (az - bt - cx + dy)^2 + (at + bz - cy - dx)^2 =$

$= (a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + t^2)$.

b) Suy ra rằng, nếu hai số nguyên đều phân tích được thành tổng của các bình phương của bốn số nguyên, thì tích của chúng cũng như thế.

2) a) Cho p là một số nguyên tố lẻ. Chứng minh rằng tồn tại $(x, y) \in \{0, \ldots, \frac{p-1}{2}\}^2$ sao cho : $x^2 + y^2 + 1 \equiv 0[p]$.

(Có thể xét $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, $X \mapsto X^2$ và $g : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, $Y \mapsto -Y^2 - 1$)

b) Suy ra rằng với số nguyên tố p bất kỳ, tồn tại $(k, x, y, z, t) \in \mathbb{N}^5$ sao cho :

$$x^2 + y^2 + z^2 + t^2 = kp \text{ và } 1 \leq k \leq p - 1.$$

3) Cho p là số nguyên tố nguyên lẻ. Ta ký hiệu m là số nguyên nhỏ nhất ≥ 1 sao cho tồn tại $(x, y, z, t) \in \mathbb{N}^4$ thỏa mãn $x^2 + y^2 + z^2 + t^2 = mp$.

a) Chứng minh rằng, nếu m là chẵn thì có thể hoán vị x, y, z, t để cho $\frac{x-y}{2}$, $\frac{x+y}{2}$, $\frac{z-t}{2}$, $\frac{z+t}{2}$ là những số nguyên, và suy ra mâu thuẫn.

b) Ta giả sử m lẻ và $m > 1$. Ta ký hiệu a, b, c, d là các phần tử của $\left\{-\frac{m-1}{2}, \ldots, \frac{m-1}{2}\right\}$ tương ứng đồng dư modulo m với x, y, z, t.

Chứng minh rằng tồn tại $q \in \mathbb{N}$ sao cho $a^2 + b^2 + c^2 + d^2 = qm$ và $q < m$, rồi suy ra một mâu thuẫn (có thể tách các trường hợp $q = 0$, $q > 0$).

Như thế ta đã chứng minh rằng tồn tại $(x, y, z, t) \in \mathbb{N}^4$ sao cho $x^2 + y^2 + z^2 + t^2 = p$.

4) Kết luận bằng **định lý bốn bình phương của Lagrange** : Mọi số tự nhiên đều phân tích được, ít nhất theo một cách, thành tổng của các bình phương của bốn số tự nhiên.

II - 1) a) Kiểm chứng : $\sum_{1 \leq i < j \leq 4} \left((x_i + x_j)^4 + (x_i - x_j)^4\right) = 6\left(\sum_{k=1}^{4} x_k^2\right)^2$ với mọi (x_1, x_2, x_3, x_4) thuộc $\mathbb{N}^4$.

b) Suy ra rằng mọi số nguyên có dạng $6n^2$ ($n \in \mathbb{N}$) đều phân tích được thành tổng của 12 trùng phương, *một trùng phương* theo định nghĩa là lũy thừa bậc 4 của một số nguyên.

(Áp dụng định lý bốn bình phương).

2) Chứng minh rằng mọi số nguyên có dạng $6m$ ($m \in \mathbb{N}$) đều phân tích được thành tổng của 48 trùng phương. (Sử dụng định lý bốn bình phương).

3) a) Kiểm chứng rằng 0, 1, 2, 81, 16, 17 phân tích được thành tổng của nhiều nhất hai trùng phương.

b) Suy ra mọi số nguyên ≥ 81 có thể phân tích thành tổng của nhiều nhất 50 trùng phương.

4) Kết luận bằng định lý:

Mọi số tự nhiên đều phân tích được thành tổng của nhiều nhất 50 trùng phương.

Nhận xét: Kết quả có thể cải tiến thêm (19 thay cho 50).

Tham khảo: K.H.Rosen, *Elementary Number Theory*, trang 407-413, Addison-Wesley Reading, 1988.

◊ **C 4.2 Giải** $x^2+y^2+2=xyz$ **trong** $\mathbb{Z}^3$

Ta ký hiệu $E=\{(x, y, z)\in\mathbb{Z}^3;\ x^2+y^2+2=xyz\}$.

1) a) Chứng minh rằng với mọi (x, y, z) thuộc E, các phần tử sau cũng thuộc E:

$$(-x, -y, z),\ (-x, y, -z),\ (x, -y, -z),\ (y, x, z).$$

b) Suy ra rằng chỉ cần xác định tập hợp:

$$F=\{(x, y, z)\in(\mathbb{N}^*)^3;\ x^2+y^2+2=xyz \text{ và } x\le y\}.$$

2) Ta ký hiệu $G=\{(x, y, z)\in(\mathbb{N}^*)^3;\ x^2+y^2+2=xyz \text{ và } x<y\}$ và

$$f:\mathbb{Z}^3\to\mathbb{Z}^3,\quad (x, y, z)\mapsto(zx-y, x, z)$$

a) Chứng minh: $\forall(x, y, z)\in G,\quad f(x, y, z)\in F$.

b) Chứng minh: $\complement_F(G)=\{(1, 1, 4)\}$

3) Suy ra $F=\{g^n(1, 1, 4);\ n\in\mathbb{N}\}$, trong đó $g:\ \mathbb{Z}^3\to\mathbb{Z}^3,\ (X,Y,Z)\mapsto(Y,YZ-X,Z)$, $g^0=\mathrm{Id}_{\mathbb{Z}^3}$, $g^1=g$, $g^2=g\circ g$ ...

◊ **C 4.3* Thặng dư bậc hai**

Cho p là một số nguyên tố lẻ (vậy $p\ge 3$).

Với $a\in\mathbb{N}$ sao cho $p\nmid a$, ta nói rằng a là một **thặng dư bậc hai modulo** p (ký hiệu : RQ mod p)khi và chỉ khi tồn tại $x\in\mathbb{Z}$ sao cho $x^2\equiv a[p]$. Trong trường hợp trái lại, ta nói rằng a là **không thặng dư modulo** p (ký hiệu : NRQ mod p).

Với $\alpha\in\mathbb{Z}/_{p\mathbb{Z}}-\{0\}$, ta nói rằng α là một **thặng dư bậc hai** trong $\mathbb{Z}/_{p\mathbb{Z}}$ khi và chỉ khi tồn tại $\xi\in\mathbb{Z}/_{p\mathbb{Z}}$ sao cho $\xi^2=\alpha$.

Rõ ràng là, với a bất kỳ thuộc $\mathbb{Z}$ sao cho $p\nmid a$, a là RQ mod p khi và chỉ khi $\hat{a}$ (lớp modulo p của a) là thặng dư bậc hai trong $\mathbb{Z}/_{p\mathbb{Z}}$. Nói khác đi, với mọi (a, b) thuộc $\mathbb{Z}^2$ sao cho $p\nmid a$, $p\nmid b$ và $\hat{a}=\hat{b}$, a là RQ mod p khi và chỉ khi b cũng là RQ mod p.

Như thế ta thường có thể đưa về giả thiết $a\in\{1, ..., p-1\}$.

Ví dụ: $p=11$

x	1	2	3	4	5
x^2	1	4	9	5	3

Các thặng dư bậc hai modulo 11 là: 1, 3, 4, 5, 9.

I - 1) a) Cho $a\in\mathbb{Z}$ sao cho $p\nmid a$. Chứng minh rằng phương trình $\xi^2=\hat{a}$, với ẩn $\xi\in\mathbb{Z}/_{p\mathbb{Z}}$ vô nghiệm hoặc có đúng hai nghiệm.

b) Suy ra rằng trong $\{1, ..., p-1\}$ có đúng $\frac{p-1}{2}$ thặng dư bậc hai modulo p, và $\frac{p-1}{2}$ không thặng dư bậc hai modulo p.

Ví dụ: Với $p=11$, có 5 RQ mod 11, đó là 1, 3, 4, 5, 9 và 5 NRQ mod 11, đó là 2, 6, 7, 8 , 10.

Với $a\in\mathbb{Z}$ sao cho $p\nmid a$, ta định nghĩa **ký hiệu Legendre**:

$$\left(\frac{a}{p}\right)=\begin{cases}1 & \text{nếu } a \text{ là RQ mod } p\\ -1 & \text{nếu } a \text{ là NRQ mod } p\end{cases}.$$

Ví dụ:

$$\begin{cases}\left(\frac{3}{11}\right)=1 & \text{vì 3 là RQ mod 11}\\ \left(\frac{6}{11}\right)=-1 & \text{vì 6 không phải là RQ mod 11}\end{cases}$$

c) α) Chứng minh, với bất kỳ a thuộc $\mathbb{Z}$ sao cho $p \nmid a$: $\sum_{k=1}^{p-1}\left(\frac{ka}{p}\right) = 0$

β) 1) Cho $k \in \{1, ..., p-2\}$, $k' \in \{1, ..., p-1\}$ sao cho $kk' \equiv 1[p]$.

Chứng minh rằng $k' \neq p-1$ và $\left(\frac{k(k+1)}{p}\right) = \left(\frac{k'+1}{p}\right)$.

2) Suy ra : $\sum_{k=1}^{p-2}\left(\frac{k(k+1)}{p}\right) = -1$.

2) a) **Định lý Euler**

Chứng minh, với mọi a thuộc $\mathbb{Z}$ sao cho $p \nmid a$: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}[p]$.

(Áp dụng định lý nhỏ Fermat, bài tập 4.4.50 và định lý Wilson, bài tập 4.4.65. a)).

Ví dụ: Tính $\left(\frac{10}{31}\right)$.

b) Suy ra : $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{nếu } p \equiv 1[4] \\ -1 & \text{nếu } p \equiv 3[4] \end{cases}$.

c) α) Cho $n \in \mathbb{N}^*$ sao cho $n \equiv 3[4]$. Chứng minh rằng tồn tại ít nhất một ước nguyên tố q của n sao cho $q \equiv 3[4]$.

β) Suy ra rằng phương trình $x^2 + y^3 - 8(2z+1)^3 + 1 = 0$, với ẩn $(x, y, z) \in \mathbb{Z}^3$, không có nghiệm.

Đặc biệt, **phương trình Lebesgue** $x^2 + y^3 = 7$ vô nghiệm trong $\mathbb{Z}^2$.

3) a) Cho $a, b \in \mathbb{Z}$ sao cho $p \nmid a$ và $p \nmid b$. Chứng minh:

1) $\left(\frac{1}{p}\right) = 1$ 2) $a \equiv b[p] \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

3) $\left(\frac{a^2}{p}\right) = 1$ 4) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

Tính chất 4 có thể diễn tả dưới dạng của một "quy tắc về dấu" đối với tích (ký hiệu R thay vì RQ mod p, và N thay vì NRQ mod p):

b \ a	R	N
R	R	N
N	N	R

b) Cho $a \in \mathbb{N}^*$ sao cho $p \nmid a$; ta ký hiệu $a = \prod_{i=1}^{N} p_i^{r_i}$ là dạng phân tích nguyên tố của a, I là tập hợp các i thuộc $\{1, ..., N\}$ sao cho r_i lẻ, $a' = \prod_{i \in I} p_i$. Chứng minh:

$$\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right).$$

4) **Bổ đề Gauss**

Cho $a \in \mathbb{Z}$ sao cho $p \nmid a$.

Với j bất kỳ thuộc $\left\{1,...,\frac{p-1}{2}\right\}$, ta ký hiệu r_j là dư của phép chia Euclide ja cho p.

a) Chứng minh rằng $r_1, ..., r_{\frac{p-1}{2}}$ khác nhau từng đôi.

Ta ký hiệu $u_1, ..., u_s$ là các phần tử $\le \frac{p-1}{2}$ thuộc $\left\{r_1,...,r_{\frac{p-1}{2}}\right\}$ và $v_1, ..., v_t$ là các phần tử $\ge \frac{p+1}{2}$ thuộc $\left\{r_1,...,r_{\frac{p-1}{2}}\right\}$

b) Chứng minh: 1) $u_1, ..., u_s, v_1, ..., v_t$ khác nhau từng đôi và tạo thành $\left\{r_1,...,r_{\frac{p-1}{2}}\right\}$.

2) $u_1, ..., u_s, p - v_1, ..., p - v_t$ từng đôi khác nhau và tạo thành $\left\{1,...,\frac{p-1}{2}\right\}$.

c) Suy ra: $\left(\frac{a}{p}\right) = (-1)^t$.

Như thế ta đã chứng minh **bổ đề Gauss**: $\left(\frac{a}{p}\right) = (-1)^t$, trong đó t là số các dư của các phép chia Euclide $a, 2a, ..., \frac{p-1}{2}a$ cho p có dư lớn hơn $\frac{p}{2}$.

Ví dụ: Tính $\left(\frac{8}{29}\right)$ bằng cách áp dụng bổ đề Gauss.

d) Chứng minh: $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

(Ta có thể chứng minh: $\frac{p-1}{2} - E\left(\frac{p}{4}\right) \equiv \frac{p^2-1}{8} [2]$).

Chẳng hạn: $\begin{cases} \left(\frac{2}{3}\right), \left(\frac{2}{5}\right), \left(\frac{2}{11}\right), \left(\frac{2}{13}\right), \left(\frac{2}{19}\right) & \text{đều bằng } -1 \\ \left(\frac{2}{7}\right), \left(\frac{2}{17}\right), \left(\frac{2}{23}\right) & \text{đều bằng } 1 \end{cases}$

Ví dụ: Tính $\left(\frac{8}{31}\right)$.

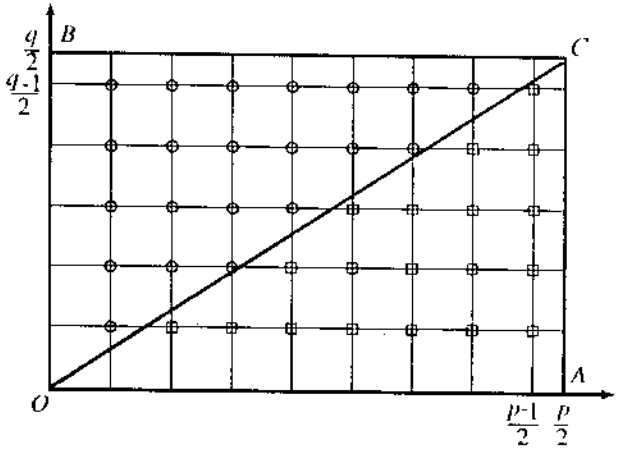
e) Cho $n \in \mathbb{N}$. Chứng minh rằng nếu $8n + 7$ nguyên tố thì : $8n + 7 \mid 2^{4n+3} - 1$ và (nếu $n \ge 1$) $2^{4n+3} - 1$ là hợp số.

Ví dụ: $23 \mid 2^{11} - 1$, $31 \mid 2^{15} - 1$, $47 \mid 2^{23} - 1$, $71 \mid 2^{35} - 1$, $79 \mid 2^{39} - 1$.

II - Luật tương hỗ thặng dư bậc hai của Gauss

1) Cho p, q là hai số nguyên tố lẻ khác nhau.

Trong mặt phẳng thông thường, ta ký hiệu $A\left(\frac{p}{2},0\right)$, $B\left(0,\frac{q}{2}\right)$, $C\left(\frac{p}{2},\frac{q}{2}\right)$.



Ví dụ: $p = 17$, $q = 11$

a) Chứng minh rằng số các điểm của $(\mathbb{N}^*)^2$ nằm (hẳn) trong hình chữ nhật $OAC'B$ là $\frac{p-1}{2}\cdot\frac{q-1}{2}$.

b) Chứng minh rằng không có một điểm nào của $(\mathbb{N}^*)^2$ nằm trên đoạn OC.

c) Chứng minh rằng số các điểm của $(\mathbb{N}^*)^2$ nằm trong tam giác OAC là $\sum_{j=1}^{\frac{p-1}{2}} \mathrm{E}\left(\frac{jq}{p}\right)$, và số các điểm của $(\mathbb{N}^*)^2$ nằm trong tam giác OBC là $\sum_{k=1}^{\frac{q-1}{2}} \mathrm{E}\left(\frac{kp}{q}\right)$.

d) Bằng cách sử dụng các ký hiệu trong bổ đề Gauss (I 4), với q thay chỗ của a), chứng minh

$$t \equiv \sum_{j=1}^{\frac{p-1}{2}} \mathrm{E}\left(\frac{jq}{p}\right) [2].$$

e) Suy ra: $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

Như vậy ta đã chứng minh **luật tương hỗ bậc hai của Gauss**:

Với mọi số nguyên tố lẻ khác nhau p và q: $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

2) a) Suy ra từ luật tương hỗ bậc hai rằng, với mọi số nguyên tố lẻ p và q khác nhau :

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{nếu } \left(p \equiv 1[4] \text{ hoặc } q \equiv 1[4]\right) \\ -\left(\frac{p}{q}\right) & \text{nếu } \left(p \equiv 3[4] \text{ và } q \equiv 3[4]\right) \end{cases}$$

b) *Ví dụ:* Tính $\left(\frac{6417}{6607}\right)$ (6607 là số nguyên tố).

3)* **Trắc nghiệm Pépin**

Với mọi n thuộc $\mathbb{N}^*$, ta ký hiệu $F_n = 2^{2^n} + 1$ (**các số Fermat**).

Chứng minh rằng F_n nguyên tố khi và chỉ khi $3^{\frac{F_n-1}{2}} \equiv -1[F_n]$.

(Đối với khẳng định đảo, ta sẽ cần đến một ước nguyên tố bất kỳ p của F_n và số nguyên bé nhất $\alpha \geq 1$ sao cho $3^\alpha \equiv 1[p]$, và ta sẽ chứng minh $\alpha \mid F_n - 1$ và $\alpha \nmid \frac{F_n - 1}{2}$).

Ví dụ: Chứng minh rằng $F_5 = 2^{2^5} + 1$ là hợp số.

4) Trong câu hỏi này ta giả thiết $p \geq 5$. Chứng minh:

a) $\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{nếu } p \equiv \pm 1[12] \\ -1 & \text{nếu } p \equiv \pm 5[12] \end{cases}$

b) $\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{nếu } p \equiv 1[6] \\ -1 & \text{nếu } p \equiv -1[6] \end{cases}$.

Chương 5

Đa thức, phân thức hữu tỷ

Độc giả đã biết đến các hàm đa thức $f: \mathbb{R} \to \mathbb{R}$, $x \mapsto a_0+a_1x+\ldots+a_nx^n$ ở Trung học phổ thông.

Các tính chất của f được suy ra từ các hệ tử $a_0, \ldots, a_n$; do đó ta sẽ xét và nghiên cứu các đa thức "hình thức".

Dẫu rằng $a_0, \ldots, a_n$ là thực, các tính chất của f có thể liên quan đến các thể phức, đó là lý do tại sao ta xét và nghiên cứu các đa thức với hệ tử phức và, tổng quát hơn, với hệ tử trong một thể giao hoán.

Trong suốt chương 5 này, K chỉ một thể giao hoán.

Trong thực tế thì thông thường là $K = \mathbb{R}$ hoặc $\mathbb{C}$.

5.1 Đại số $K[X]$

5.1.1 Định nghĩa

♦ Định nghĩa 1

1) Với mọi dãy $(a_n)_{n\in\mathbb{N}}$ thuộc $K^{\mathbb{N}}$, ta gọi tập hợp các n thuộc $\mathbb{N}$ sao cho $a_n \neq 0$ là **giá** của $(a_n)_{n\in\mathbb{N}}$.

2) **Đa thức (một ẩn và lấy hệ tử trong K)** là dãy $(a_n)_{n\in\mathbb{N}}$ bất kỳ thuộc $K^{\mathbb{N}}$ có giá hữu hạn.

Tập hợp các đa thức một ẩn và lấy hệ tử trong K được ký hiệu là $K[X]$ (hoặc $K^{(\mathbb{N})}$).

Như thế, $K[X] \subset K^{\mathbb{N}}$ và, với mọi dãy $(a_n)_{n\in\mathbb{N}}$ thuộc $K^{\mathbb{N}}$:

$$(a_n)_{n\in\mathbb{N}} \in K[X] \Leftrightarrow (\exists N \in \mathbb{N}, \forall n \in \mathbb{N}, (n > N \Rightarrow a_n = 0)).$$

Dưới đây (5.1.4) ký hiệu $K[X]$ sẽ được lý giải.

Các phần tử của $K[X]$ cũng được gọi là **đa thức hình thức**.

Ta ký hiệu 0 là dãy hằng không thuộc $K^{\mathbb{N}}$ (xác định bởi : $\forall n \in \mathbb{N}$, $a_n = 0$), được gọi là **đa thức không**.

Đa thức hằng là các đa thức $(a_n)_{n\in\mathbb{N}}$ thuộc $K[X]$ sao cho :

$$\forall n \geq 1,\ a_n = 0.$$

Đơn thức là đa thức $(a_n)_{n\in\mathbb{N}}$ thuộc $K[X]$ bất kỳ sao cho tồn tại $n_0 \in \mathbb{N}$ thỏa mãn :

$$\forall n \in \mathbb{N},\quad (n \neq n_0 \Rightarrow a_n = 0).$$

NHẬN XÉT :

1) Theo Định nghĩa, hai đa thức $(a_n)_{n\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}}$ bằng nhau khi và chỉ khi :

$$\forall n \in \mathbb{N},\quad a_n = b_n.$$

2) $K[X] \neq K^{\mathbb{N}}$ vì dãy hằng (1) (xác định bởi : $\forall n \in \mathbb{N}$, $a_n = 1$) thuộc $K^{\mathbb{N}}$, không thuộc $K[X]$.

♦ **Định nghĩa 2** Cho $P = (a_n)_{n\in\mathbb{N}} \in K[X]$.

1) • Nếu $P \neq 0$, số tự nhiên n lớn nhất sao cho $a_n \neq 0$ gọi là **bậc của** P, và kí hiệu là $\deg(P)$. Phần tử $a_{\deg(P)}$ được gọi là **hệ tử của hạng tử có bậc cao nhất** (hoặc : **hệ tử cao nhất**) của P. Ta nói rằng P là **chuẩn tắc** khi và chỉ khi $P \neq 0$ và $a_{\deg(P)} = 1$.

• Ta ký hiệu $\deg(0) = -\infty$.

2) • Nếu $P \neq 0$, **định giá của** P, ký hiệu là $\mathrm{val}(P)$, là số tự nhiên n bé nhất sao cho $a_n \neq 0$.

• Ta ký hiệu $\mathrm{val}(0) = +\infty$.

NHẬN XÉT :

$$\forall P \in K[X] - \{0\},\quad \mathrm{val}(P) \leq \deg(P).$$

♦ **Định nghĩa 3** Cho $P = (a_n)_{n\in\mathbb{N}} \in K[X]$.

1) Ta nói rằng P là **chẵn** khi và chỉ khi :

$$\forall p \in \mathbb{N},\quad a_{2p+1} = 0.$$

2) Ta nói rằng P là **lẻ** khi và chỉ khi :

$$\forall p \in \mathbb{N},\quad a_{2p} = 0.$$

5.1.2 Phép cộng

Mệnh đề 1

Cho $P = (a_n)_{n\in\mathbb{N}}$, $Q = (b_n)_{n\in\mathbb{N}} \in K[X]$.

Thế thì $P + Q = (a_n + b_n)_{n\in\mathbb{N}} \in K[X]$.

Chứng minh :

Vì P, Q là những đa thức, nên tồn tại N_1, $N_2 \in \mathbb{N}$ sao cho :

$$\begin{cases} \forall n \in \mathbf{N} & (n > N_1 \Rightarrow a_n = 0) \\ \forall n \in \mathbf{N} & (n > N_2 \Rightarrow b_n = 0) \end{cases}$$

Kí hiệu $N = \text{Max}(N_1, N_2) \in \mathbb{N}$, ta có :

$$\forall n \in \mathbb{N}, \quad (n > N \Rightarrow a_n = b_n = 0 \Rightarrow a_n + b_n = 0),$$

và như vậy : $P + Q \in K[X]$. ■

Điều này chứng tỏ rằng $K[X]$ là một bộ phận của $K^{\mathbb{N}}$ ổn định đối với +.

Mệnh đề 2 Ta có, với P, Q bất kỳ thuộc $K[X]$:

1) • $\deg(P + Q) \le \text{Max}(\deg(P), \deg(Q))$.
   • $\deg(P) \ne \deg(Q) \Rightarrow \deg(P + Q) = \text{Max}(\deg(P), \deg(Q))$

2) • $\text{val}(P + Q) \ge \text{Min}(\text{val}(P), \text{val}(Q))$
   • $\text{val}(P) \ne \text{val}(Q) \Rightarrow \text{val}(P + Q) = \text{Min}(\text{val}(P), \text{val}(Q))$.

Chứng minh :

Các tính chất trên là hiển nhiên nếu $P = 0$ hoặc $Q = 0$.

• Giả sử $P \ne 0$ và $Q \ne 0$, và ta ký hiệu

$$P = (a_n)_{n\in\mathbb{N}},\ Q = (b_n)_{n\in\mathbb{N}},\ \nu_1 = \text{val}(P),\ \nu_2 = \text{val}(Q),$$
$$N_1 = \deg(P),\ N_2 = \deg(Q),\ \nu = \text{Min}(\nu_1, \nu_2),\ N = \text{Max}(N_1, N_2).$$

Thế thì $P + Q = (a_n + b_n)_{n\in\mathbb{N}}$ và, với mọi n thuộc $\mathbb{N}$:

$$n < \nu \Rightarrow \begin{cases} n < \nu_1 \\ n < \nu_2 \end{cases} \Rightarrow \begin{cases} a_n = 0 \\ b_n = 0 \end{cases} \Rightarrow a_n + b_n = 0$$

$$n > N \Rightarrow \begin{cases} n > N_1 \\ n > N_2 \end{cases} \Rightarrow \begin{cases} a_n = 0 \\ b_n = 0 \end{cases} \Rightarrow a_n + b_n = 0.$$

Điều này chứng tỏ : $\text{val}(P + Q) \ge \nu$ và $\deg(P + Q) \le N$.

• Giả sử $\deg(P) \ne \deg(Q)$; chẳng hạn : $N_1 = \deg(P) < \deg(Q) = N_2$.

Thế thì $a_N + b_N = a_{N_2} + b_{N_2} = b_{N_2} \ne 0$, vậy $\deg(P + Q) = N_2 = N$.

Tương tự, nếu, chẳng hạn, $\nu_1 = \text{val}(P) > \text{val}(Q) = \nu_2$, thì $a_\nu + b_\nu = a_{\nu_2} + b_{\nu_2} = b_{\nu_2} \ne 0$, vậy $\text{val}(P + Q) = \nu_2 = \nu$.

NHẬN XÉT :

Theo Mệnh đề trên, nếu $\deg(P) < \deg(Q)$, thì hạng tử có bậc cao nhất của $P + Q$ cũng là hạng tử có bậc cao nhất của Q.

♦ **Mệnh đề 3**

$(K[X], +)$ là một nhóm Abel.

Chứng minh :

1) Phép + là luật hợp thành trong trong $K[X]$ (xem Mệnh đề 1).

2) Vì phép + có tính kết hợp và tính giao hoán trong $K^{\mathbb{N}}$ (xem bài tập 2.1.13) nên dĩ nhiên cũng kết hợp và giao hoán trong $K[X]$.

3) 0 là phần tử trung hòa đối với + trong $K[X]$.

4) Mọi $P = (a_n)_{n\in\mathbb{N}}$ thuộc $K[X]$ có một đối xứng đối với + trong $K[X]$, đó là $(-a_n)_{n\in\mathbb{N}}$, và được ký hiệu là $-P$.

5.1.3 Phép nhân

♦ **Mệnh đề - Định nghĩa 1** Cho $P = (a_n)_{n\in\mathbb{N}}$, $Q = (b_n)_{n\in\mathbb{N}} \in K[X]$.
Tích của P với Q, kí hiệu là PQ, là dãy $(c_n)_{n\in\mathbb{N}}$ thuộc $K^{\mathbb{N}}$ xác định bởi :

$$\forall n \in \mathbb{N}, \quad c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{i+j=n} a_i b_j \ .$$

Vậy ta có : $PQ \in K[X]$.

Chứng minh :

Nếu $P = 0$ hoặc $Q = 0$, thì $PQ = 0$.

Giả sử $P \neq 0$ và $Q \neq 0$. Kí hiệu $N_1 = \deg(P)$, $N_2 = \deg(Q)$.

Giả sử $n \in \mathbb{N}$ sao cho $n > N_1 + N_2$. Thế thì : $\forall k \in \{0, ..., n\}$, ($k > N_1$ hoặc $n - k > N_2$), vậy : $\forall k \in \{0, ..., n\}$, $a_k b_{n-k} = 0$, và suy ra $c_n = 0$.

Điều này chứng tỏ : $PQ \in K[X]$.

♦ **Mệnh đề 2**

$$\forall (P, Q) \in (K[X])^2, \begin{cases} \deg(PQ) = \deg(P) + \deg(Q) \\ \mathrm{val}(PQ) = \mathrm{val}(P) + \mathrm{val}(Q). \end{cases}$$

Ta quy ước ở đây :

- $\forall N \in \mathbb{N}$, $((-\infty) + N = -\infty, \quad (+\infty) + N = +\infty)$
- $(-\infty) + (-\infty) = -\infty, \quad (+\infty) + (+\infty) = +\infty$.

Chứng minh :

Tính chất cần chứng minh là hiển nhiên khi $P = 0$ hoặc $Q = 0$. Giả sử $P \neq 0$ và $Q \neq 0$, và ký hiệu :

$$P = (a_n)_{n\in\mathbb{N}}, \quad Q = (b_n)_{n\in\mathbb{N}}, \quad N_1 = \deg(P), \ N_2 = \deg(Q), \ PQ = (c_n)_{n\in\mathbb{N}}.$$

Theo phép chứng minh của Mệnh đề - Định nghĩa trên đây :

$$\forall n \in \mathbb{N}, (n > N_1 + N_2 \Rightarrow c_n = 0).$$

Ngoài ra :

$$c_{N_1+N_2} = \sum_{k=0}^{N_1+N_2} a_k b_{N_1+N_2-k} = a_{N_1} b_{N_2} ,$$

vì, với mọi k thuộc $\mathbb{N}$:

$$\begin{cases} k < N_1 \Rightarrow N_1 + N_2 - k > N_2 \Rightarrow b_{N_1+N_2-k} = 0 \\ k > N_1 \Rightarrow a_k = 0. \end{cases}$$

Điều này chứng tỏ : $\deg(PQ) = \deg(P) + \deg(Q)$.

Công thức về các định giá được chứng minh tương tự.

♦ Mệnh đề 3

$(K[X], +, \cdot)$ là một vành nguyên.

Chứng minh (có thể để lại khi đọc lần đầu) :

1) Theo 5.1.2, Mệnh đề 3, $(K[X], +)$ là một nhóm Abel.

2) Phép nhân là một luật hợp thành trong trong $K[X]$ (xem Mệnh đề - Định nghĩa 1).

3) Ta sẽ chứng minh $\cdot$ có tính kết hợp trong $K[X]$.

Giả sử $P = (a_n)_{n\in\mathbb{N}}$, $Q = (b_n)_{n\in\mathbb{N}}$, $R = (c_n)_{n\in\mathbb{N}} \in K[X]$.

Thế thì : $PQ = (d_n)_{n\in\mathbb{N}}$ trong đó : $\forall n \in \mathbb{N}, d_n = \sum_{k=0}^{n} a_k b_{n-k}$,

suy ra $(PQ)R = (e_n)_{n\in\mathbb{N}}$ trong đó : $\forall n \in \mathbb{N}, e_n = \sum_{k=0}^{n} d_k c_{n-k}$.

Và $QR = (f_n)_{n\in\mathbb{N}}$ trong đó : $\forall n \in \mathbb{N}, \ f_n = \sum_{k=0}^{n} b_k c_{n-k}$,

suy ra $P(QR) = (g_n)_{n\in\mathbb{N}}$ trong đó : $\forall n \in \mathbb{N}, g_n = \sum_{k=0}^{n} a_k f_{n-k}$.

Ta có, với mọi n thuộc $\mathbb{N}$:

$$\begin{aligned} g_n &= \sum_{i+p=n} a_i f_p = \sum_{i+p=n} a_i \left(\sum_{j+k=p} b_j c_k \right) \\ &= \sum_{i+(j+k)=n} a_i (b_j c_k) = \sum_{(i+j)+k=n} (a_i b_j) c_k \\ &= \sum_{q+k=n} \left(\sum_{i+j=q} a_i b_j \right) c_k \\ &= \sum_{q+k=n} d_q c_k = e_n . \end{aligned}$$

Điều này chứng tỏ : $(PQ)R = P(QR)$.

4) Theo cách tương tự, ta chứng minh được rằng • có tính giao hoán, và phân phối đối với +.

5) Rõ ràng là đa thức (1, 0, ..., 0, ...) là phần tử trung hòa đối với phép nhân. Ta ký hiệu 1 thay cho (1, 0, ..., 0...).

6) Theo Mệnh đề 2, nếu $P \neq 0$ và $Q \neq 0$, thì $\deg(PQ) = \deg(P) + \deg(Q) \neq -\infty$, vậy $PQ \neq 0$.

♦ **Mệnh đề 4** Các phần tử khả nghịch của vành $K[X]$ là các dãy $(\alpha, 0, ..., 0, ...)$ với $\alpha \in K - \{0\}$.

Chứng minh :

1) Giả sử P là một phần tử khả nghịch của $K[X]$; vậy tồn tại $Q \in K[X]$ sao cho $PQ = 1$. Thế thì $P \neq 0$, $Q \neq 0$ và $\deg(P) + \deg(Q) = \deg(PQ) = 0$, suy ra $\deg(P) = \deg(Q) = 0$. Vậy tồn tại $\alpha \in K - \{0\}$ sao cho $P = (\alpha, 0, ..., 0, ...) = \alpha$.

2) Ngược lại, rõ ràng rằng, với mọi α thuộc $K - \{0\}$, đa thức $(\alpha, 0, ..., 0, ...)$ khả nghịch và có phần tử nghịch đảo là $(\alpha^{-1}, 0, ..., 0, ...)$.

5.1.4 Luật ngoài

Các mệnh đề sau đây có thể chứng minh dễ dàng.

♦ **Mệnh đề - Định nghĩa 1**

Cho $\lambda \in K$, $P = (a_n)_{n \in \mathbb{N}} \in K[X]$.

Ta ký hiệu $\lambda P = (\lambda a_n)_{n \in \mathbb{N}}$, và ta có : $\lambda P \in K[X]$.

♦ **Mệnh đề 2**

$$\forall \lambda \in K - \{0\}, \forall P \in K[X], \begin{cases} \deg(\lambda P) = \deg(P) \\ \text{val}(\lambda P) = \text{val}(P) \end{cases}.$$

♦ **Mệnh đề 3** $K[X]$, được trang bị các luật +, · (ngoài), . (trong) là một K - đại số kết hợp, giao hoán, có đơn vị.

Về định nghĩa một K - đại số, xem 6.1, Định nghĩa 2.

Chứng minh :

1) $(K[X], +)$ là một nhóm Abel (xem 5.1.2, Mệnh đề 3).

2) Có thể thấy ngay các tính chất sau, với mọi λ, μ thuộc K và P, Q thuộc $K[X]$:

$$(\lambda + \mu)P = \lambda P + \mu P,\ \lambda(P + Q) = \lambda P + \lambda Q,\ 1P = P,\ \lambda(\mu P) = (\lambda\mu)P.$$

Như thế, $(K[X], +, .$ (ngoài)) là một K - không gian vectơ.

3) Ta đã thấy (5.1.3, Mệnh đề), rằng phép nhân trong $K[X]$ có các tính chất kết hợp, giao hoán, phân phối đối với +, và có phần tử trung hòa (đó là 1).

4) Cuối cùng, tính chất $\forall \lambda \in K, \forall P, Q \in K[X]$, $\lambda(PQ) = (\lambda P)Q$ có thể chứng minh dễ dàng.

♦ Mệnh đề 4

Ánh xạ $\theta : K \to K[X]$, $\lambda \mapsto \lambda 1$ là một đồng cấu đơn ánh các K - đại số.

Về định nghĩa đồng cấu K - đại số, xem 7.1.1, Định nghĩa 4.

Chứng minh :

Các tính chất sau là hiển nhiên :

1) $\forall(\lambda, \mu) \in K^2, \quad \theta(\lambda + \mu) = \theta(\lambda) + \theta(\mu)$
2) $\forall(\lambda, \mu) \in K^2, \quad \theta(\lambda\mu) = \theta(\lambda)\theta(\mu)$
3) $\theta(1) = 1$
4) $\forall \lambda \in K, \quad (\theta(\lambda) = 0 \Rightarrow \lambda = 0)$.

Mệnh đề trên cho phép "đồng nhất" một phần tử λ thuộc K với một đa thức $\lambda 1$ thuộc $K[X]$, tức là "nhúng" K vào $K[X]$.

♦ Ký hiệu

Ta ký hiệu $X = (0, 1, 0, ..., 0, ...)$, gọi là **ẩn**.

Theo 2.1, Ký hiệu, ta sẽ ký hiệu $X^0 = 1$ và, với mọi n thuộc $\mathbb{N}$, $X^{n+1} = X^n X$; đặc biệt : $X^1 = X$.

Một phép quy nạp đơn giản chứng tỏ rằng :

$$\forall n \in \mathbb{N}^*, \quad X^n = (0, ..., 0, 1, 0, ..., 0, ...)$$

trong đó 1 ở vị trí thứ n (số 0 đầu tiên ở vị trí thứ 0).

Cho $P = (a_n)_{n\in\mathbb{N}} \in K[X]$, $N \in \mathbb{N}$ sao cho $N \geq \deg(P)$; ta có :

$$\begin{aligned} P &= (a_0, a_1, ..., a_N, 0, ..., 0, ...) \\ &= a_0(1, 0, ..., 0, ...) + a_1(0, 1, 0, ..., 0, ...) + ... + a_N(0, ..., 0, 1, 0, ..., 0, ...) \\ &= a_0 + a_1 X + ... + a_N X^N = \sum_{n=0}^{N} a_n X^n . \end{aligned}$$

Bây giờ ta từ bỏ ký hiệu $(a_n)_{n\in\mathbb{N}}$ đối với một đa thức, và ta thay nó bằng ký hiệu $\sum_{n=0}^{N} a_n X^n$ (trong đó $N \geq \deg(P)$), hoặc $\sum_{n\in\mathbb{N}} a_n X^n$, hoặc $\sum_{n=0}^{+\infty} a_n X^n$ (để tránh chỉ rõ bậc của đa thức).

Đối với $P = \sum_{n\in\mathbb{N}} a_n X^n \in K[X]$ và $n \in \mathbb{N}$, phần tử a_n của K được gọi là **hệ tử của X^n trong P**, và đơn thức $a_n X^n$ **là hạng tử bậc n của P**.

Mệnh đề sau đây là hiển nhiên.

♦ **Mệnh đề - Định nghĩa**

Họ vô hạn $(X^n)_{n\in\mathbb{N}}$, tức là $(1, X, X^2, ..., X^n, ...)$ là một cơ sở của K-kgv $K[X]$, gọi là **cơ sở chính tắc** của $K[X]$.

Với $n \in \mathbb{N}$ cố định, tập hợp $\{P \in K[X] ; \deg(P) \leq n\}$ rõ ràng là một K-không gian vectơ con của $K[X]$, thường được kí hiệu $K_n[X]$. Họ hữu hạn $(1, X, ..., X^n)$ là một cơ sở của $K_n[X]$, gọi **cơ sở chính tắc** của $K_n[X]$. Vậy ta có : $\dim(K_n[X]) = n + 1$.

♦ **Mệnh đề 6** Cho I là một bộ phận của $\mathbb{N}$, $(P_i)_{i\in I}$ là một họ những đa thức thuộc $K[X] - \{0\}$ sao cho :

$$\forall (i, j) \in I^2, \quad (i \neq j \Rightarrow \deg(P_i) \neq \deg(P_j)).$$

Thế thì $(P_i)_{i\in I}$ độc lập trong K-kgv $K[X]$.

Chứng minh :

Giả sử J là một bộ phận hữu hạn khác rỗng của I, i_1, ..., i_k là các phần tử của J, mà ta có thể giả thiết được sắp xếp sao cho :

$$\deg(P_{i_1}) < ... < \deg(P_{i_k})$$

Giả sử $\lambda_1, ..., \lambda_k \in K$ thỏa mãn $\sum_{j=1}^{k} \lambda_j P_{ij} = 0$.

Hệ tử của $X^{\deg(P_{i_k})}$ trong $\sum_{j=1}^{k} \lambda_j P_{i_j}$ là $\lambda_k \alpha_{i_k}$ (trong đó α_{i_k} là hệ tử cao nhất của P_{i_k}), do đó $\lambda_k = 0$.

Bằng cách lập lại, ta suy ra : $\lambda_k = 0, \lambda_{k+1} = 0, ..., \lambda_1 = 0$, và như vậy $(P_i)_{i\in J}$ độc lập.

Vì mọi họ con hữu hạn của $(P_i)_{i\in I}$ đều độc lập, nên $(P_i)_{i\in I}$ độc lập (xem 6.3.1, 2)).

NHẬN XÉT :

Một trường hợp đặc biệt thường gặp là trường hợp $I = \mathbb{N}$ và $(\forall i \in \mathbb{N}, \deg(P_i) = i)$.

Khi đó ta nói rằng $(P_i)_{i\in\mathbb{N}}$ là một họ các đa thức **có bậc kế tiếp**.

Trong trường hợp này, $(P_i)_{i\in\mathbb{N}}$ là một cơ sở của $K[X]$ và, với mọi n thuộc $\mathbb{N}$, $(P_i)_{0\leq i\leq n}$ là một cơ sở của $K_n[X]$.

Với mọi n thuộc $\mathbb{N}$, ma trận chuyển từ cơ sở chính tắc $(1, X, ..., X^n)$ của $K_n[X]$ sang cơ sở $(P_i)_{0\leq i\leq n}$ (xem 8.2.1, Định nghĩa) là ma trận tam giác trên có tất cả các hạng tử chéo khác không. Như vậy có thể tính nghịch đảo của nó theo "bậc thang".

5.1.5 Phép hợp đa thức

♦ **Định nghĩa** Cho $P = \sum_{n=0}^{N} a_n X^n \in K[X]$ và $Q \in K[X]$. Ta định nghĩa **đa thức hợp** $P \circ Q$ (hoặc : $P(Q)$) là : $P \circ Q = P(Q) = \sum_{n=0}^{N} a_n Q^n$.

Như vậy, ta được $P(Q)$ bằng cách thế Q vào chỗ X trong P. Độc giả có thể chứng minh các mệnh đề sau :

♦ **Mệnh đề 1**

$$\forall (P, Q) \in (K[X] - \{0\})^2, \quad \deg(P \circ Q) = \deg(P).\deg(Q).$$

♦ **Mệnh đề 2** Với mọi α thuộc K và P, Q, R thuộc $K[X]$:

1) $(P + \alpha Q) \circ R = P \circ R + \alpha Q \circ R$

2) $(PQ) \circ R = (P \circ R) \cdot (Q \circ R)$

3) $(P \circ Q) \circ R = P \circ (Q \circ R)$

4) $X \circ P = P \circ X = P$.

Theo 4) ta sẽ ký hiệu một đa thức là P hoặc $P(X)$.

NHẬN XÉT :

1) Luật $\circ$ không giao hoán trong $K[X]$.

Ví dụ : $K = \mathbb{R}$, $\begin{cases} X^2 \circ (X+1) = (X+1)^2 = X^2 + 2X + 1 \\ (X+1) \circ X^2 = X^2 + 1. \end{cases}$

2) Luật $\circ$ không phân phối trái đối với + trong $K[X]$.

Ví dụ : $K = \mathbb{R}$, $P = X^2$, $Q = 1$, $R = 1$; ta có : $P \circ (Q + R) = X^2 \circ 2 = 4$ và $(P \circ Q) + (P \circ R) = (X^2 \circ 1) + (X^2 \circ 1) = 1 + 1 = 2$.

5.1.6 Phép đạo hàm

♦ **Định nghĩa** Với mọi $P = \sum_{n=0}^{N} a_n X^n$ thuộc $K[X]$, **đa thức đạo hàm của** P, và ký hiệu là P', là đa thức định nghĩa bởi :

$$P' = \sum_{n=1}^{N} n a_n X^{n-1} = \sum_{n=0}^{N-1} (n+1) a_{n+1} X^n .$$

Ta ký hiệu $P^{(0)} = P$, $P^{(1)} = P'$, $P^{(2)} = P'' = (P')'$, và, với k bất kỳ thuộc $\mathbb{N}^*$, $P^{(k)} = (P^{(k-1)})'$.

Với những ký hiệu trên, nếu $N = 0$ thì $P' = 0$.

Ba Mệnh đề sau là hiển nhiên.

♦ **Mệnh đề 1**

$$\forall P \in K[X],\quad \deg(P') = \begin{cases} \deg(P)-1 & \text{nếu } \deg(P) \geq 1 \\ -\infty & \text{nếu } \deg(P) \leq 0 \end{cases}$$

♦ **Mệnh đề 2**

$$\forall P \in K[X],\ \forall n \in \mathbb{N},\quad (\deg(P) \leq n \Leftrightarrow P^{(n+1)} = 0).$$

♦ **Mệnh đề 3** Với mọi α thuộc K và mọi P, Q thuộc $K[X]$:

1) $(P + \alpha Q)' = P' + \alpha Q'$

2) $(PQ)' = P'Q + PQ'$.

Như vậy, theo Mệnh đề 3, 1), phép đạo hàm các đa thức $K[X] \to K[X]$, $P \mapsto P'$ là K-tuyến tính.

♦ **Mệnh đề 4 (Công thức Leibniz)**

$$\forall (P, Q) \in (K[X])^2,\ \forall k \in \mathbb{N},\quad (PQ)^{(k)} = \sum_{i=0}^{k} C_k^i P^{(i)} Q^{(k-i)}.$$

Chứng minh :

Quy nạp theo k, tương tự như phép chứng minh công thức nhị thức Newton (2.3.2, Định lí) hoặc công thức Leibniz về đạo hàm các hàm một biến thực (Tập 1, 5.1.4).

5.1.7 Hàm đa thức

♦ **Định nghĩa** Với mọi $P = \sum_{n=0}^{N} a_n X^n$ thuộc $K[X]$, ta ký hiệu $\widetilde{P} : K \to K,\ x \mapsto \sum_{n=0}^{N} a_n x^n$

hàm này gọi là **hàm đa thức liên kết với** P.

Lược đồ Hörner

Ta chú ý, chẳng hạn : $a_3x^3 + a_2x^2 + a_1x + a_0 = a_0 + (a_1 + (a_2 + a_3x)x)x$.

Trong thực hành tính toán $\widetilde{P}(x)$ khi biết P và x, ta có thể sử dụng thuật toán sau đây, được gọi là **lược đồ Hörner**.

Đặt $b_N = a_N$, và với n đi từ N - 1 đến 0 : $b_n = a_n + b_{n+1}x$.

Khi đó ta được : $P(x) = b_0$.

Ví dụ : $K = \mathbb{R}$, $P = X^3 - 2X^2 + 4X + 5$, $x = 4$:

$$b_3 = a_3 = 1,\quad b_2 = a_2 + b_3x = 2,\quad b_1 = a_1 + b_2x = 12,\quad b_0 = a_0 + b_1x = 53,$$

suy ra $\widetilde{P}(4) = 53$.

NHẬN XÉT :

Ta có thể tổng quát hóa Định nghĩa trên. Cho A là một K-đại số kết hợp và giao hoán, $P = \sum_{n=0}^{N} a_n X^n \in K[X]$; ta ký hiệu $\widetilde{P} : A \to A$, $x \mapsto \sum_{n=0}^{N} a_n x^n$ (trong đó $x^0 = 1_A$, $x^n = x(x^{n-1})$, với $n \in \mathbb{N}^*$, xem 2.1, Ký hiệu).

- Chẳng hạn, nếu E là một K - kgv, với mọi $P = \sum_{n=0}^{N} a_n X^n$ thuộc $K[X]$ và f bất kỳ thuộc $\mathcal{L}_K(E)$, đa thức $\widetilde{P}(f) = \sum_{n=0}^{N} a_n f^n$ (cũng ký hiệu là $P(f)$), được gọi là **đa thức tự đồng cấu**.

- Tương tự, với mọi $P = \sum_{n=0}^{N} a_n X^n$ thuộc $K[X]$ và mọi A thuộc $\mathbf{M}_p(K)$ ($p \in \mathbb{N}^*$), đa thức $\widetilde{P}(A) = \sum_{n=0}^{N} a_n A^n$ (cũng kí hiệu là $P(A)$), được gọi là **đa thức ma trận**.

Ta sẽ sử dụng các ký hiệu này trong Tập 6 (2.4).

- Phép hợp đa thức (xem 5.1.5) cũng là một dạng tổng quát hóa :

$$\forall P, Q \in K[X], \quad P \circ Q = \widetilde{P}(Q).$$

♦ **Mệnh đề 1** Với mọi α thuộc K và mọi P, Q thuộc $K[X]$:

1) $\widetilde{P + \alpha Q} = \widetilde{P} + \alpha \widetilde{Q}$ 2) $\widetilde{PQ} = \widetilde{P}\widetilde{Q}$ 3) $\widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}$.

Chứng minh

Ta ký hiệu $P = \sum_{n=0}^{N} a_n X^n$, $Q = \sum_{n=0}^{N} b_n x^n$, trong đó $N \geq \text{Max}(\deg(P), \deg(Q))$.

1) $\forall x \in K$,

$$\widetilde{P+\alpha Q}(x) = \sum_{n=0}^{N} (a_n + \alpha b_n) x^n = \sum_{n=0}^{N} a_n x^n + \alpha \sum_{n=0}^{N} b_n x^n = \widetilde{P}(x) + \alpha \widetilde{Q}(x),$$

do đó : $\widetilde{P+\alpha Q} = \widetilde{P} + \alpha \widetilde{Q}$.

2) $\forall x \in K$, $\widetilde{PQ}(x) = \sum_{n \in \mathbb{N}} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) x^n = \sum_{n \in \mathbb{N}} \sum_{k=0}^{n} a_k x^k b_{n-k} x^{n-k}$

$$= \left(\sum_{k=0}^{N} a_k x^k \right) \left(\sum_{l=0}^{N} b_l x^l \right) = \widetilde{P}(x)\widetilde{Q}(x),$$

do đó : $\widetilde{PQ} = \widetilde{P}\widetilde{Q}$.

3) $\forall x \in K$, $\widetilde{P \circ Q}(x) = \left(\widetilde{\sum_{n=0}^{N} a_n Q^n}\right)(x) = \sum_{n=0}^{N} a_n (\tilde{Q}(x))^n$ (xem 1) và 2))

$= \tilde{P}(\tilde{Q}(x)) = (\tilde{P} \circ \tilde{Q})(x)$,

do đó $\widetilde{P \circ Q} = \tilde{P} \circ \tilde{Q}$.

NHẬN XÉT : Với mọi P thuộc $\mathbb{R}[X]$ ta có $\widetilde{P'} = \tilde{P}'$, trong đó :

- $\widetilde{P'}$ là hàm đa thức liên kết với P'
- $\tilde{P}'$ là đạo hàm (theo nghĩa của Tập 1, 5.1.3) của hàm đa thức liên kết với P. ■

Xét ánh xạ $\phi : K[X] \to K^K$.
$P \mapsto \tilde{P}$

Theo 1) và 2) của Mệnh đề trên (và $\phi(1) = 1$), ϕ là một đồng cấu những K - đại số có đơn vị. Ta sẽ nghiên cứu tính đơn ánh của ϕ.

1) Giả sử K hữu hạn ; ký hiệu $\{x_1, ..., x_N\} = K$ và xét $P = \prod_{k=1}^{N} (X - x_k)$. Ta có :

- $P \neq 0$, vì $\deg(P) = N \geq 1$
- $\tilde{P} = 0$, vì : $\forall k \in \{1, ..., N\}$, $\tilde{P}(x_k) = 0$.

Điều này chứng tỏ ϕ không phải là đơn ánh.

2) Giả sử K vô hạn và giả sử $P \in K[X]$ sao cho $\tilde{P} = 0$. Giả sử $P \neq 0$, và ký hiệu $N = \deg(P)$. Vì K vô hạn, nên tồn tại $x_1, ..., x_{N+1} \in K$ từng đôi khác nhau. Vậy ta có : $\forall k \in \{1, ..., N+1\}$, $\tilde{P}(x_k) = 0$.

Theo 5.3.1, Hệ quả 1 mà ta sẽ thấy sau đây, ta suy ra $P = 0$, mâu thuẫn.

Điều này chứng tỏ rằng nếu K vô hạn thì ϕ là đơn ánh.

Cuối cùng :

♦ **Mệnh đề 2** Ánh xạ $K[X] \to K^K$, $P \mapsto \tilde{P}$ là đơn ánh khi và chỉ khi K vô hạn.

NHẬN XÉT : Vậy khi K là vô hạn, ta có thể đồng nhất P và $\tilde{P}$, tức là kí hiệu P thay cho $\tilde{P}$. Trong thực hành, thường thường $K = \mathbb{R}$ hoặc $\mathbb{C}$, điều đó cho phép ta đồng nhất P và $\tilde{P}$; trong trường hợp này, ta sẽ ký hiệu $\tilde{P}$ hoặc P miễn là thuận tiện.

♦ **Định lí (Định lí Taylor đối với đa thức)**

Cho $P \in \mathbb{C}[X]$, $N \in \mathbb{N}$ thỏa mãn $\deg(P) \leq N$, $a \in \mathbb{C}$. Ta có :

$$P(a + X) = \sum_{n=0}^{N} \widetilde{\frac{P^{(n)}(a)}{n!}} X^n .$$

Chứng minh :

1) Với mọi i thuộc $\mathbb{N}$, ta ký hiệu $e_i = X^i$, và ta chứng minh công thức với e_i.

Một phép quy nạp đơn giản chứng tỏ rằng :

$$\forall n \in \mathbb{N}\ ;\ e_i^{(n)} = \begin{cases} i(i-1)\ldots(i-n+1)e_{i-n} & \text{nếu } n \le i \\ 0 & \text{nếu } n > i \end{cases}$$

do đó :

$$\forall n \in \mathbb{N},\ e_i^{(n)}(a) = \begin{cases} \dfrac{i!}{(i-n)!}a^{i-n} & \text{nếu } n \le i \\ 0 & \text{nếu } n > i \end{cases}$$

Theo công thức nhị thức Newton ta được :

$$e_i(a+X) = (a+X)^i = \sum_{n=0}^{i} C_i^n a^{i-n}X^n = \sum_{n=0}^{i} \frac{i!}{(i-n)!\,n!}a^{i-n}X^n = \sum_{n=0}^{i} \frac{e_i^{(n)}(a)}{n!}X^n .$$

2) Với mọi đa thức $P = \sum_{i=0}^{N} \alpha_i X^i$:

$$\begin{aligned} P(a+X) &= \sum_{i=0}^{N} \alpha_i e_i(a+X) = \sum_{i=0}^{N} \alpha_i \left(\sum_{n=0}^{i} \frac{e_n^{(n)}(a)}{n!}X^n \right) \\ &= \sum_{n=0}^{N} \alpha_i \left(\sum_{n=0}^{N} \frac{e_i^{(n)}(a)}{n!}X^n \right) \quad (\text{vì } e_i^{(n)}(a) = 0 \text{ nếu } n > i) \\ &= \sum_{n=0}^{N} \frac{1}{n!}\left(\sum_{i=0}^{N} \alpha_i e_i^{(n)}(a) \right) X^n = \sum_{n=0}^{N} \frac{1}{n!}\widetilde{P^{(n)}}(a)X^n \end{aligned}$$

NHẬN XÉT :

1) Trong định lý trên, thể được sử dụng là $\mathbb{C}$, vì ta cần chia (trong K) cho các số nguyên (các $n!$). Một cách tổng quát hơn, có thể áp dụng định lý Taylor cho các đa thức khi K là một thể có đặc số 0 (xem bài tập 2.3.4), tức là một thể thỏa mãn : $\forall n \in \mathbb{N}^*,\ n1_K \neq 0_K$.

2) Định lý Taylor đối với đa thức cho ta dạng phân tích của $P(a+X)$ theo cơ sở chính tắc $(1, X, \ldots, X^n, \ldots)$ của $K[X]$.

3) Trong đại số $\mathbb{C}[X, Y]$ các đa thức của hai ẩn trên $\mathbb{C}$ (xem dưới đây, 5.1.8), ta sẽ chứng minh một cách tổng quát hơn rằng với mọi P thuộc $\mathbb{C}[X]$ và N thuộc $\mathbb{N}$ sao cho $\deg(P) \le N$, thì :

$$P(X+Y) = \sum_{n=0}^{N} \frac{P^{(n)}(X)}{n!}Y^n .$$

Thay Y bởi a, ta suy ra :

$$P(X+a) = \sum_{n=0}^{N} \frac{a^n}{n!}P^{(n)}(X)$$

đó chính là dạng phân tích $P(X+a)$ theo cơ sở $(P^{(n)}(X))_{0 \le n \le N}$ của $\mathbb{C}_N[X]$ (nếu $N = \deg(P)$).

4) Thay X bởi X - a, ta được (với giả thiết $\deg(P) \leq N$) :

$$P(X) = \sum_{n=0}^{N} \frac{\widetilde{P^{(n)}}}{n!}(X-a)^n .$$

5) Trong thực hành, để tính các hệ tử của dạng phân tích của $P(X + a)$ theo cơ sở chính tắc của $K[X]$, ta có thể sử dụng một thuật toán xuất phát từ sơ đồ Horner.

Giả sử $n \in \mathbb{N}^*$, $P = \alpha_0 + \alpha_1 X + ... + \alpha_n X^n \in K[X]$, $a \in K$.

Đặt $\beta_{n-1} = \alpha_n$, rồi với k từ $n - 1$ đến 0 : $\beta_{k+1} = \beta_k a + \alpha_k$ và cuối cùng $\gamma_0 = \beta_0$.

Ta chứng minh dễ dàng rằng với ký hiệu $P_1 = \beta_0 + \beta_1 X + ... + \beta_{n-1} X^{n-1}$, ta có :

$$\begin{cases} P = (X-a)P_1 + \gamma_0 \\ \gamma_0 = \widetilde{P}(a) \end{cases}$$

Bằng cách lặp lại cách xây dựng tương tự với P_1, ... ta sẽ suy ra dạng phân tích của P theo họ $(1, X - a, (X - a)^2, ..., (X - a)^n)$.

VÍ DỤ : $K = \mathbb{R}$, $P = X^3 + 4X^2 - 6X + 2$, $a = 3$:

Các hệ tử của P :	1	4	-6	2	
Các hệ tử của P_1 :		1	7	15	47 (= γ_0)
			1	10	45
				1	13
					1

Mỗi hạng tử (trừ các hạng tử ở hàng thứ 1) bằng tích của a với hạng tử ở bên trái nó, cộng với hạng tử ở trên hạng tử này.

Ta suy ra : $P = 47 + 45(X - 3) + 13(X - 3)^2 + (X - 3)^3$

5.1.8 Khái niệm về đa thức nhiều ẩn

Lý thuyết trên (từ 5.1.1 đến 5.1.7) có thể lặp lại một cách tổng quát hơn, với một vài sửa đổi, bằng cách thay thế K bởi một vành giao hoán A. Như vậy ta sẽ xây dựng **vành $A[X]$ các đa thức của một ẩn và lấy hệ tử trong A.**

Đặc biệt, lấy $A = K[Y]$, ta sẽ xây dựng **đại số $K[X, Y] = (K[Y])[X]$ các đa thức của hai ẩn và lấy hệ tử trong K.** Bằng cách lặp lại, với $n \in \mathbb{N}^*$ ta sẽ xây dựng **đại số $K[X_2, ..., X_n])[X_1]$ các đa thức n ẩn và lấy hệ tử trong K.**

Độc giả có thể chứng minh rằng K - không gian vectơ $K[X_1, ..., X_n]$ nhận $(X_1^{i_1}, ..., X_n^{i_n})_{(i_1,...,i_n)\in\mathbb{N}^n}$ làm cơ sở.

Bài tập

◊ **5.1.1** Tìm điều kiện cần và đủ đối với $(\lambda, \mu) \in \mathbb{R}^2$ để cho $X^4 + \lambda X^3 + \mu X^2 + 12X + 4$ là bình phương của một đa thức thuộc $\mathbb{R}[X]$.

◊ **5.1.2** Cho $n \in \mathbb{N}$. Áp dụng $(1 + X)^{2n}(1 - X)^{2n} = (1 - X^2)^{2n}$, chứng minh :

$$\sum_{k=0}^{2n} (-1)^k (C_{2n}^k)^2 = (-1)^n C_{2n}^n .$$

◊ **5.1.3** Cho $n \in \mathbb{N}$, $(a_0, ..., a_n) \in \mathbb{Z}^{n+1}$ sao cho $(\forall k \in \{1, ..., n\}, 0 \le a_k \le a_0)$, $P = \sum_{k=0}^{n} a_k X^k$.

Cho $(b_0, ..., b_{2n}) \in \mathbb{Z}^{2n+1}$ sao cho $P^2 = \sum_{l=0}^{2n} b_l X^l$. Chứng minh:

$$b_{n+1} \le \frac{1}{2}\left(P(1)\right)^2.$$

◊ **5.1.4** Cho $n \in \mathbb{N}$ với $k = \{0, ..., n\}$, ta ký hiệu $P_k = (X + k)^k$.

Chứng minh $(P_k)_{0 \le k \le n}$ là một cơ sở của $\mathbb{R}_n[X]$.

◊ **5.1.5** Cho $n \in \mathbb{N}^*$.

a) Chứng minh: $\forall P \in \mathbb{R}_n[X]$, $\exists! \hat{P} \in \mathbb{R}_n[X]$, $\hat{P}(X^2) = P(X)P(-X)$.

b) Chứng minh rằng ánh xạ $\varphi : \mathbb{R}_n[X] \to \mathbb{R}_n[X]$ (xác định ở a) thỏa mãn:

$$P \mapsto \hat{P}$$
$$\forall P, Q \in \mathbb{R}_n[X], \quad \varphi(PQ) = \varphi(P)\varphi(Q).$$

c) φ có tuyến tính không?

◊ **5.1.6** Cho $n \in \mathbb{N}^*$, $P \in \mathbb{C}[X]$ sao cho $\deg(P) < n$.

Chứng minh: $\sum_{k=0}^{n} P(k)(-1)^k C_n^k = 0$. (Ta có thể xét $\Delta : \underset{A \mapsto A(X+1) - A(X)}{\mathbb{C}[X] \to \mathbb{C}[X]}$).

◊ **5.1.7** Cho $(\alpha, \beta) \in \mathbb{C}^2$ sao cho $\alpha \ne \beta$, $A \in \mathbb{C}[X]$.

Chứng minh: $\exists! P \in \mathbb{C}[X]$, $P(X - \alpha) + P(X - \beta) = A$.

◊ **5.1.8*** Tìm tất cả các tự đẳng cấu của K-đại số $K[X]$.

◊ **5.19** Giải các phương trình sau:

a) $X(X - 1)P'' + (X + 2)P' - P = 0$, với ẩn $P \in \mathbb{R}[X]$

b) $P(2X) = P'(X)P''(X)$, với ẩn $P \in \mathbb{C}[X]$.

◊ **5.1.10** Chứng minh rằng, với mọi n thuộc $\mathbb{N}$, tồn tại $P_n \in \mathbb{Z}[X]$ duy nhất sao cho $P_n - P_n' = X^n$, và tính P_n.

◊ **5.1.11*** Cho $(P_n)_{n \ge 0}$ là một dãy trong $\mathbb{R}[X]$ xác định bởi $P_0 = 1$ và:

$$\forall n \in \mathbb{N}^*, P_n = \frac{1}{n!} X(X + n)^{n-1}.$$

a) Chứng minh: $\forall n \in \mathbb{N}^*$, $P_n' = P_{n-1}(X + 1)$,

(trong đó $P_{n-1}(X + 1)$ chỉ đa thức hợp thành của P_{n-1} và của $X + 1$).

b) Suy ra: $\forall n \in \mathbb{N}$, $\forall (x, y) \in \mathbb{R}^2$, $P_n(x + y) = \sum_{i+j=n} P_i(x)P_j(y)$.

c) Suy ra: $\forall n \in \mathbb{N}$, $\sum_{i+j=n} C_n^i (i + 1)^{i-1}(j + 1)^{j-1} = 2(n + 2)^{n-1}$.

◊ **5.1.12** *Nhân tử hóa:

a) $-X^4 - Y^4 - Z^4 + 2X^2Y^2 + 2X^2Z^2 + 2Y^2Z^2$ trong $\mathbb{C}[X, Y, Z]$

b) $(X + Y + Z)^5 - (X^5 + Y^5 + Z^5)$ trong $\mathbb{R}[X, Y, Z]$.

◊ **5.1.13*** Cho $A = K[X_1, X_2, X_3, X_4]$, $I = \{P_1X_1 + P_2X_2 ; (P_1, P_2) \in A^2\}$,

$J = \{P_3X_3 + P_4X_4 ; (P_3, P_4) \in A^2\}$, $E = \{PQ ; (P, Q) \in I \times J\}$.

Kiểm chứng rằng I, J là những iđêan của A (xem sau đây, 5.2.3, *1)*, Định nghĩa), nhưng E không phải là một iđêan của A.

5.2 Số học trong $K[X]$

Độc giả nên so sánh mục 5.2 này với chương 4 về số học trong $\mathbb{Z}$.

5.2.1 Tính chia hết

♦ **Định nghĩa** Cho $(A,P) \in (K[X])^2$. Ta nói rằng A **chia hết** P (trong $K[X]$) và ký hiệu $A \mid P$, khi và chỉ khi tồn tại $Q \in K[X]$ sao cho $P = AQ$.

Thay cho A chia hết P, ta cũng nói: A là một **ước** của P, hoặc: P là một **bội** của A.

NHẬN XÉT:

1) $\forall A \in K[X], \quad A \mid 0.$

2) $\forall P \in K[X], \quad (0 \mid P \Leftrightarrow P = 0).$

3) Nếu ký hiệu: $AK[X] = \{P \in K[X];\ \exists Q \in K[X],\ P = AQ\}$ với mọi A thuộc $K[X]$, thì ta có với mọi (A, P) thuộc $(K[X])^2$: $A \mid P \Leftrightarrow AK[X] \supset PK[X]$.

♦ **Mệnh đề 1**

1) $\forall A \in K[X], \quad A \mid A.$

2) $\forall (A, P) \in (K[X])^2, \quad \left(\begin{cases} A \mid P \\ P \mid A \end{cases} \Leftrightarrow (\exists \alpha \in K - \{0\},\ P = \alpha A) \right)$

3) $\forall (A, B, C) \in (K[X])^3, \quad \left(\begin{cases} A \mid B \\ B \mid C \end{cases} \Rightarrow A \mid C \right).$

Chứng minh:

1) Hiển nhiên.

2) • Giả sử $A \mid P$ và $P \mid A$. Tồn tại $B, Q \in K[X]$ sao cho $P = AQ$ và $A = PB$, do đó $P = P(BQ)$.

Nếu $P = 0$, thì $A = P = 0$.

Nếu $P \neq 0$, thì vì vành $K[X]$ là vành nguyên nên ta suy ra $BQ = 1$, rồi (xem 5.1.3 Mệnh đề 2) $\deg(B) = \deg(Q) = 0$. Vậy tồn tại $\alpha \in K - \{0\}$ sao cho $Q = \alpha$, do đó $P = \alpha A$.

• Ngược lại, nếu tồn tại $\alpha \in K - \{0\}$ sao cho $P = \alpha A$, thì rõ ràng rằng $A \mid P$ và $P \mid A$ (vì $\alpha^{-1} \in K$ và $A = \alpha^{-1}P$).

3) Giả sử $A \mid B$ và $B \mid C$. Tồn tại $(D, E) \in (K[X])^2$ sao cho $B = AD$ và $C = BE$, do đó $C = A(DE)$ và $DE \in K[X]$, vậy $A \mid C$. ■

NHẬN XÉT:

Các điểm 1) và 3) trên đây chứng tỏ rằng tính chia hết là một **tiền thứ tự** trong $K[X]$, tức là có các tính chất phản xạ và bắc cầu.

Ta chứng minh Mệnh đề sau tương tự như trong 4.1.1:

♦ **Mệnh đề 2**

1) $\forall (A, B, C) \in (K[X])^3,\ (A \mid B \Rightarrow A \mid BC)$.

2) $\forall (A, B, C) \in (K[X])^3,\ \left(\begin{cases} A \mid B \\ A \mid C \end{cases} \Rightarrow A \mid B + C\right)$

3) $\forall (A, B, P, Q) \in (K[X])^4,\ \left(\begin{cases} A \mid B \\ P \mid Q \end{cases} \Rightarrow AP \mid BQ\right)$

4) $\forall (A, B, n) \in (K[X])^2 \times \mathbb{N}^*,\ (A \mid B \Rightarrow A^n \mid B^n)$.

Bài tập

◊ **5.2.1** Chứng minh: $\forall n \in \mathbb{N},\ X^2 \mid (X+1)^n - nX - 1$ trong $K[X]$.

◊ **5.2.2** Chứng minh: $\forall (n, p) \in (\mathbb{N}^*)^2,\ \sum_{i=0}^{n-1} X^i \left| \left(\sum_{i=0}^{n} X^i\right)^p - X^n \right.$ trong $K[X]$.

◊ **5.2.3** Cho $\theta \in \mathbb{R},\ n \in \mathbb{N}^*,\ A = X^2 - 2X\cos\theta + 1,\ B_n = X^n \sin\theta - X\sin n\theta + \sin(n-1)\theta$. Chứng minh $A \mid B_n$ và xây dựng đa thức C_n thỏa mãn $B_n = AC_n$.

(Có thể nhận xét rằng: $B_n = XB_{n-1} + A\sin(n-1)\theta$).

5.2.2 Phép chia Euclide

♦ **Định lý - Định nghĩa** Cho $(A, B) \in K[X] \times (K[X] - \{0\})$. Tồn tại một cặp duy nhất (Q, R) thuộc $(K[X])^2$ sao cho:

$$\begin{cases} A = BQ + R \\ \deg(R) < \deg(B). \end{cases}$$

Đa thức Q (tương ứng : R) gọi là **thương** (tương ứng: **dư**) **của phép chia Euclide** A **cho** B.

Chứng minh:

1) **Tồn tại**

Ta ký hiệu $p = \deg(B) \geq 0,\ B = \sum_{j=0}^{p} b_j X^j$ (vậy $b_p \neq 0$). Ta sẽ tiến hành phép quy nạp theo bậc của A. Xét tính chất $\mathcal{P}_n$ sau:

Với mọi A thuộc $K[X]$ sao cho $\deg(A) \leq n$, tồn tại $(Q, R) \in (K[X])^2$ sao cho:

$$A = BQ + R \quad \text{và } \deg(R) < \deg(B).$$

- $\mathcal{P}_0$ đúng. Thật vậy, nếu A là một hằng thì chỉ cần lấy:

$$\begin{cases} Q = 0 \text{ và } R = A. & \text{nếu } \deg(B) \geq 1. \\ Q = A\, b_p^{-1} \text{ và } R = 0, & \text{nếu } \deg(B) = 0. \end{cases}$$

- Giả sử $\mathcal{P}_n$ đúng với một n thuộc $\mathbb{N}$, và giả sử $A \in K[X]$ sao cho $\deg(A) = n + 1$.

Ta ký hiệu: $A = \sum_{i=0}^{n+1} a_i X^i$, và xét:

$$Q_{n+1} = a_{n+1} b_p^{-1} X^{n+1-p} \quad \text{và } R_{n+1} = A - BQ_{n+1}.$$

Do cách chọn Q_{n+1}, các hạng tử bậc $n + 1$ của A và của BQ_{n+1} là như nhau, vậy $\deg(R_{n+1}) \leq n$.

Theo $\mathcal{P}_n$, tồn tại $(Q_n, R_n) \in (K[X])^2$ sao cho: $R_{n+1} = BQ_n + R_n$ và $\deg(R_n) < \deg(B)$.

Đặt $Q = Q_{n+1} + Q_n$ và $R = R_n$, ta có:

$$A = BQ_{n+1} + (BQ_n + R_n) = BQ + R \text{ và } \deg(R) < \deg(B).$$

2) **Duy nhất**

Giả sử tồn tại (Q_1, R_1), (Q_2, R_2) thích hợp. Thế thì ta có $R_1 - R_2 = B(Q_2 - Q_1)$. Nếu $Q_1 \neq Q_2$, thì $Q_2 - Q_1 \neq 0$ và $\deg(R_1 - R_2) = \deg(B) + \deg(Q_2 - Q_1) \geq \deg(B)$ điều này mâu thuẫn với:

$$\deg(R_1 - R_2) \leq \text{Max}\,(\deg(R_1), \deg(R_2)) < \deg(B).$$

Do đó $Q_1 = Q_2$ và $R_1 = R_2$.

VÍ DỤ:

1) Thực hiện phép chia Euclide $A = X^4 + 2X^3 - X + 6$ cho $B = X^3 - 6X^2 + X + 4$ trong $R[X]$.

$$\begin{array}{l|l} X^4 + 2X^3 - X + 6 & X^3 - 6X^2 + X + 4 \\ \hline 8X^3 - X^2 - 5X + 6 & X + 8 \\ 47X^2 - 13X - 26 & \end{array}$$

$$Q = X + 8, \quad R = 47X^2 - 13X - 26.$$

2) Thực hiện phép chia Euclide $A = iX^3 - X^2 + (1 - i)$ cho $B = (1 + i)X^2 - iX + 3$ trong $\mathbb{C}[X]$.

$$\begin{array}{l|l} iX^3 - X^2 + (1-i) & (1+i)X^2 - iX + 3 \\ \hline \frac{-3+i}{2} X^2 - \frac{3+3i}{2} X + 1 - i & \frac{1+i}{2} X + \frac{-1+2i}{2} \\ \frac{-5-4i}{2} X + \frac{5-8i}{2} & \end{array}$$

$$Q = \frac{1+i}{2}X + \frac{-1+2i}{2}, \qquad R = \frac{-5-4i}{2}X + \frac{5-8i}{2}.$$

NHẬN XÉT:

Rõ ràng ràng với mọi (A, B) thuộc $K[X] \times (K[X] \setminus \{0\})$, B chia hết A khi và chỉ khi dư của phép chia Euclide A cho B là đa thức không. ■

Cho $P \in K[X]$, $a \in K$.

Do phép chia Euclide P cho $X - a$, tồn tại $(Q, R) \in (K[X])^2$ sao cho:

$$P = (X - a)Q + R \text{ và } \deg(R) < 1.$$

Vậy R là hằng.

Hơn nữa: $\widetilde{P}(a) = \widetilde{R}(a)$, do đó $R = \widetilde{R}(a) = \widetilde{P}(a)$. Điều này chứng tỏ dư của phép chia Euclide P cho $X - a$ là $\widetilde{P}(a)$. Đặc biệt:

◆ **Mệnh đề**

$$\forall P \in K[X],\ \forall a \in K,\quad (X - a \mid P \Leftrightarrow \widetilde{P}(a) = 0)$$ ■

CHÚ Ý: **Phép đổi thể**

Cho L là một thể, K là một thể con của L (trong thực hành: $K = \mathbb{R}$, $L = \mathbb{C}$), $(A, B) \in (K[X])^2$, Q, R là thương và dư của phép chia Euclide A cho B trong $K[X]$. Vì Q, R cũng thuộc $L[X]$, nên rõ ràng ràng Q, R cũng là thương và dư của phép chia Euclide A cho B trong $L[X]$. Đặc biệt, B chia hết A trong $K[X]$ khi và chỉ khi B chia hết A trong $L[X]$.

Bài tập

◊ **5.2.4** Tìm các $a \in \mathbb{R}$ sao cho $X^2 - aX + 1 \mid X^4 - X + a$ trong $\mathbb{R}[X]$.

◊ **5.2.5** Với $(n, \theta) \in \mathbb{N}^* \times \mathbb{R}$ cố định, tìm dư của phép chia Euclide $(X \sin\theta + \cos\theta)^n$ cho $X^2 + 1$ trong $\mathbb{C}[X]$.

◊ **5.2.6** Cho $(k, n) \in (\mathbb{N}^*)^2$, r là dư của phép chia Euclide k cho n. Chứng minh rằng dư của phép chia Euclide X^k cho $X^n - 1$ là X^r.

◊ **5.2.7** Cho $P \in \mathbb{C}[X]$, $a \in \mathbb{C}$. Tính thương của phép chia Euclide P cho $X - a$. Biểu diễn kết quả trong cơ sở $((X - a)^k)_{0 \le k \le n-1}$.

◊ **5.2.8** Cho $P \in K[X]$ sao cho $\deg(P) \ge 1$.

a) Cho Q và R là thương và dư của phép chia Euclide A cho B. Chứng minh rằng thương và dư của phép chia Euclide $A \circ P$ cho $B \circ P$ là $Q \circ P$ và $R \circ P$.

b) Suy ra: $\forall (A, B) \in (K[X])^2$, $(B \mid A \Leftrightarrow B \circ P \mid A \circ P)$.

5.2.3 UCLN, BCNN

1) Idêan của K[X]

♦ **Định nghĩa** Mọi bộ phận bất kỳ $\Im$ của $K[X]$ thỏa mãn:

- $\Im \neq \varnothing$
- $\forall (P, Q) \in \Im^2, \quad P + Q \in \Im$
- $\forall A \in K[X], \forall P \in \Im, \quad AP \in \Im$

được gọi là **idêan** của $K[X]$.

Tổng quát hơn người ta đã định nghĩa khái niệm **idêan của một vành giao hoán** hoặc thậm chí cả **idêan trái, idêan phải của một vành**.

NHẬN XÉT:

Nếu $\Im$ là một idêan của $K[X]$, thì ta có:

$$\begin{cases} \Im \neq \varnothing \\ \forall (P,Q) \in \Im^2, \quad P+Q \in \Im \\ \forall P \in \Im, \quad -P \in \Im \end{cases}$$

và do đó $\Im$ là một nhóm con của $(K[X], +)$.

2) Cho $P_0 \in K[X]$ và $P_0K[X]$ là tập hợp các bội của P_0 trong $K[X]$, tức là:

$$P_0K[X] = \{P_0A;\ A \in K[X]\}.$$

Rõ ràng rằng $P_0K[X]$ là một idêan của $K[X]$.

♦ **Định lý** Với bất kỳ idêan $\Im$ của $K[X]$, tồn tại $P_0 \in K[X]$ sao cho:

$$\Im = P_0K[X] = \{P \in K[X];\ \exists A \in K[X],\ P = P_0A\}.$$

Ta phát biểu kết quả này là: Mọi idêan của $K[X]$ là **idêan chính**, hoặc là: $K[X]$ là một **vành chính**.

Chứng minh:

Giả sử $\Im$ là một idêan của $K[X]$.

Nếu $\Im = \{0\}$, thì $\Im = 0K[X]$.

Giả sử $\Im \neq \{0\}$. Tập hợp $\{\deg(P);\ P \in \Im - \{0\}\}$ là một bộ phận khác rỗng của $\mathbb{N}$. Vậy nó có phần tử bé nhất, ký hiệu là n_0, và tồn tại $P_0 \in \Im - \{0\}$ sao cho $\deg(P_0) = n_0$.

Ta sẽ chứng minh rằng : $\Im = P_0K[X]$.

1) Vì $P_0 \in \Im$ và vì $\Im$ là một idêan của $K[X]$, nên ta có: $\forall A \in K[X], P_0A \in \Im$, tức là: $P_0K[X] \subset \Im$.

2) Ngược lại, giả sử $P \in \Im$. Bằng phép chia Euclide P cho P_0, tồn tại $(Q, R) \in (K[X])^2$ sao cho: $P = P_0Q + R$ và $\deg(R) < \deg(P_0)$.

Do $R = P - P_0Q$, mà P, P_0 đều thuộc $\Im$, và vì $\Im$ là một idêan của $K[X]$, nên ta suy ra: $R \in \Im$. Hơn nữa, theo định nghĩa của P_0, vì $\deg(R) < \deg(P_0)$, nên ta được $R = 0$, do đó: $P = P_0Q \in P_0K[X]$. ■

NHẬN XÉT:
Chứng minh ở trên đã chứng tỏ một cách khá tổng quát rằng mọi vành được gọi là vành Euclide đều là vành chính.

2) UCLN, BCNN

Cho $n \in \mathbb{N}^*$, $(P_1, ..., P_n) \in (K[X] - \{0\})^n$.

Tập hợp các bậc của các đa thức P thuộc $K[X] - \{0\}$ sao cho $(\forall i \in \{1, ..., n\}, P|P_i)$ là một bộ phận khác rỗng của $\mathbb{N}$ (vì: $\forall i \in \{1, ..., n\}$, $1 | P_i$), bị chặn trên bởi $\deg(P_i)$.

Vậy tồn tại một đa thức chuẩn tắc Δ, khác không, là ước chung của $P_1, ..., P_n$, và có bậc cao nhất trong các ước chung của $P_1, ..., P_n$. Tương tự, tồn tại một đa thức chuẩn tắc M khác không, là bội chung của $P_1, ..., P_n$ và có bậc thấp nhất trong các bội chung của $P_1, ..., P_n$.

Ta sẽ chứng minh rằng:

$$\sum_{i=1}^{n} P_i K[X] = \Delta K[X], \quad \bigcap_{i=1}^{n} P_i K[X] = MK[X],$$

và đẳng thức này theo 5.2.1, Mệnh đề 1, 2), sẽ chứng minh tính duy nhất của Δ và của M.

1) • Vì mỗi $P_iK[X]$ $(1 \le i \le n)$ là một iđêan của $K[X]$, nên rõ ràng rằng $\sum_{i=1}^{n} P_i K[X]$ là một iđêan của $K[X]$.

Do $K[X]$ là một vành chính, nên tồn tại $D \in K[X]$ sao cho:

$$\sum_{i=1}^{n} P_i K[X] = DK[X].$$

• Theo định nghĩa của Δ: $\forall i \in \{1, ..., n\}$, $\Delta | P_i$, do đó: $\forall i \in \{1, ..., n\}$, $P_iK[X] \subset \Delta K[X]$, và: $\sum_{i=1}^{n} P_i K[X] \subset \Delta K[X]$.

Vậy tồn tại $D_1 \in K[X]$ sao cho $D = \Delta D_1$.

• Mặt khác: $\forall i \in \{1, ..., n\}$: $P_iK[X] \subset \sum_{i=1}^{n} P_i K[X] = DK[X]$,

suy ra: $\forall i \in \{1, ..., n\}$, $D | P_i$.

Hơn nữa, rõ ràng rằng $D \neq 0$ (vì $P_1 \in DK[X]$).

Theo định nghĩa của Δ ta có: $\deg(D) \le \deg(\Delta)$.

• Vì $D = \Delta D_1$ và $\deg(D) \le \deg(\Delta)$, ta suy ra $D_1 \in K - \{0\}$, do đó:

$$\sum_{i=1}^{n} P_i K[X] = DK[X] = \Delta K[X].$$

• Cuối cùng, nếu Δ_1, Δ_2 là hai đa thức chuẩn tắc, khác không, đều là ước chung của $P_1, ..., P_n$ và có bậc cao nhất, thì

$$\Delta_1 K[X] = \sum_{i=1}^{n} P_i K[X] = \Delta_2 K[X],$$

nên ta suy ra $\Delta_1 = \Delta_2$, điều này chứng tỏ tính duy nhất của Δ đã định nghĩa trên đây.

2) • Vì mỗi $P_iK[X]$ $(1 \le i \le n)$ là một iđêan của $K[X]$, nên rõ ràng rằng $\bigcap_{i=1}^{n} P_iK[X]$ cũng là một iđêan của $K[X]$. Vì $K[X]$ là một vành chính, nên tồn tại $P \in K[X]$ sao cho:

$$\bigcap_{i=1}^{n} P_iK[X] = PK[X].$$

• Theo định nghĩa của M: $\forall i \in \{1, ..., n\}$, $P_i \mid M$, do đó: $\forall i \in \{1, ..., n\}$, $MK[X] \subset P_iK[X]$, rồi: $MK[X] \subset \bigcap_{i=1}^{n} P_iK[X]$.

Vậy tồn tại $Q_1 \in K[X]$ sao cho $M = Q_1P$.

• Mặt khác:

$$\forall i \in \{1, ..., n\},\ P_iK[X] \supset \bigcap_{i=1}^{n} P_iK[X] = PK[X],$$

do đó: $\forall i \in \{1, ..., n\}$, $P_i \mid P$.

Hơn nữa, rõ ràng là $P \neq 0$ (bởi vì $\prod_{i=1}^{n} P_i \in PK[X]$).

Theo định nghĩa của M, ta có: $\deg(M) \le \deg(P)$.

• Vì $M = Q_1P$ và $\deg(M) \le \deg(P)$, ta suy ra $Q_1 \in K - \{0\}$, từ đây:

$$\bigcap_{i=1}^{n} P_iK[X] = PK[X] = MK[X].$$

• Cuối cùng, nếu M_1, M_2 là hai đa thức chuẩn tắc, khác không, đều là bội chung của $P_1, ..., P_n$ và có bậc thấp nhất thì vì

$$M_1K[X] = \bigcap_{i=1}^{n} P_iK[X] = M_2K[X],$$

nên ta suy ra $M_1 = M_2$, điều này chứng tỏ tính duy nhất của M đã định nghĩa trên đây.

Ta tóm tắt kết quả khảo sát trên đây bằng:

♦ Mệnh đề - Định nghĩa 1

Cho $n \in \mathbb{N}^*$, $(P_1, ..., P_n) \in (K[X] - \{0\})^n$.

1) Tồn tại một và chỉ một đa thức Δ, chuẩn tắc, khác không, là ước chung của $P_1, ..., P_n$ và có bậc cao nhất trong các ước chung của $P_1, ..., P_n$; Δ được gọi là **ước chung lớn nhất** (viết tắt: **ƯCLN**) của $P_1, ..., P_n$ và được ký hiệu $\text{ƯCLN}(P_1, ..., P_n)$ (hoặc: $\text{ƯCLN}((P_i)_{1 \le i \le n})$).

2) Tồn tại một và chỉ một đa thức M, chuẩn tắc, khác không, là bội chung của $P_1, ..., P_n$ và có bậc thấp nhất trong các bội chung của $P_1, ..., P_n$; M được gọi là **bội chung nhỏ nhất** (viết tắt: **BCNN**) của $P_1, ..., P_n$ và được ký hiệu $\text{BCNN}(P_1, ..., P_n)$ (hoặc: $\text{BCNN}((P_i)_{1 \le i \le n})$).

♦ **Mệnh đề 2** Cho $n \in \mathbb{N}^*$, $(P_1, ... P_n) \in (K[X] - \{0\})^n$,
$\Delta = \text{ƯCLN}(P_1, ..., P_n)$, $M = \text{BCNN}(P_1, ..., P_n)$. Ta có:

$$\sum_{i=1}^{n} P_i K[X] = \Delta K[X] \quad \text{và} \quad \bigcap_{i=1}^{n} P_i K[X] = MK[X]. \qquad \blacksquare$$

Độc giả có thể chứng minh các Mệnh đề sau đây, phỏng theo việc khảo sát số học trong $\mathbb{Z}$ (4.2):

♦ **Mệnh đề 3** Cho $n \in \mathbb{N}^*$, $(P_1, ..., P_n) \in (K[X] - \{0\})^n$,
$(\alpha_1, ..., \alpha_n) \in (K - \{0\})^n$. Ta có:

$$\begin{cases} \text{UCLN}((\alpha_i P_i)_{1 \le i \le n}) = \text{UCLN}((P_i)_{1 \le i \le n}) \\ \text{BCNN}((\alpha_i P_i)_{1 \le i \le n}) = \text{BCNN}((P_i)_{1 \le i \le n}) \end{cases}$$

♦ **Mệnh đề 4** Cho $n \in \mathbb{N}^*$, $(P_1, ..., P_n) \in (K[X] - \{0\})^n$, $A \in K[X] - \{0\}$ là chuẩn tắc. Ta có:

$$\begin{cases} \text{UCLN}((AP_i)_{1 \le i \le n}) = A\,\text{UCLN}((P_i)_{1 \le i \le n}) \\ \text{BCNN}((AP_i)_{1 \le i \le n}) = A\,\text{BCNN}((P_i)_{1 \le i \le n}). \end{cases}$$

♦ **Mệnh đề 5** Cho $n \in \mathbb{N}^*$, $(P_1, ..., P_n) \in (K[X] - \{0\})^n$,
$\Delta = \text{ƯCLN}(P_1, ..., P_n)$, $M = \text{BCNN}(P_1, ..., P_n)$, $(A, B) \in (K[X] - \{0\})^2$.
Ta có:
1) $(\forall_i \in \{1, ..., n\}, \quad A \mid P_i) \Leftrightarrow A \mid \Delta$.
2) $(\forall_i \in \{1, ..., n\}, \quad P_i \mid B) \Leftrightarrow M \mid B$.

♦ **Mệnh đề 6 (Tính kết hợp của UCLN và của BCNN)**
Cho $n \in \mathbb{N}^*$, H là một phân hoạch của $\{1, ..., n\}$, $(P_1, ..., P_n) \in (K[X] - \{0\})^n$.
Ta có:

$$\begin{cases} \text{UCLN}((P_i)_{1 \le i \le n}) = \text{UCLN}((\text{UCLN}((P_i)_{i \in I}))_{I \in H}) \\ \text{BCNN}((P_i)_{1 \le i \le n}) = \text{BCNN}((\text{BCNN}((P_i)_{i \in I}))_{I \in H}) \end{cases}$$

Mệnh đề trên chứng tỏ rằng ta có thể biểu thị UCLN (tương ứng : BCNN) của nhiều đa thức mà chỉ dùng đến các UCLN (tương ứng : BCNN) của hai đa thức.

♦ **Ký hiệu**
Với $(P,Q) \in (K[X] - \{0\})^2$, ta ký hiệu: $\begin{cases} P \wedge Q = \text{UCLN}(P,Q) \\ P \vee Q = \text{BCNN}(P,Q) \end{cases}$

NHẬN XÉT:

$\wedge$ và $\vee$ là những luật hợp thành trong trong $K[X]-\{0\}$, kết hợp và giao hoán. Hơn nữa, với mọi đa thức chuẩn tắc và khác không P thì:

$$P \wedge P = P, \quad P \vee P = P, \quad P \wedge 1 = 1, \quad P \vee 1 = P.$$

Dưới đây ta sẽ thấy rằng:

- $\wedge$ và $\vee$ phân phối luật này đối với luật kia (5.2.5, Hệ quả).
- $\forall (P,Q) \in (K[X]-\{0\})^2, \forall k \in \mathbb{N}^*, P^k \wedge Q^k = (P \wedge Q)^k$ (5.2.4, *3*), Hệ quả).

3) Thuật toán Euclide

Lập luận như trong khi khảo sát thuật toán Euclide trong $\mathbb{Z}$ (4.2.3), ta thấy rằng, với mọi (P, Q) thuộc $(K[X]-\{0\})^2$, ƯCLN của P và Q là dư cuối cùng khác không chuẩn tắc hóa trong dãy các phép chia Euclide liên tiếp.

VÍ DỤ:

Tính ƯCLN của $P = X^5 + X + 1$ và $Q = X^4 - 2X^3 - X + 2$ trong $\mathbb{R}[X]$.

	$X+2$	$\frac{1}{4}X - \frac{9}{16}$	$4X-3$
$P = X^5 + X + 1$	$Q = X^4 - 2X^3 - X - 2$	$R_1 = 4X^3 + X^2 + X - 3$	$R_2 = X^2 + X + 1$
$2X^4 + X^2 - X + 1$	$-\frac{9}{4}X^3 - \frac{1}{4}X^2 - \frac{1}{4}X + 2$	$-3X^2 - 3X - 3$	
$R_1 = 4X^3 + X^2 + X - 3$	$R_2 = \frac{5}{16}X^2 + \frac{5}{16}X + \frac{5}{16}$	0	

Ta được: $P \wedge Q = X^2 + X + 1$.

Trong ví dụ này, trong một pha tính toán ta đã thay $\frac{5}{16}(X^2 + X + 1)$ bởi $X^2 + X + 1$ (xem 2), Mệnh đề 3.

Bài tập

◊ **5.2.9** Cho L là một thể, K là một thể con của L, $P, Q \in K[X]$. Chứng minh rằng ƯCLN của P, Q trong $K[X]$ cũng là ƯCLN của P, Q trong $L[X]$.

5.2.4 Đa thức nguyên tố cùng nhau

1) Đại cương

◆ **Định nghĩa** Cho $n \in \mathbb{N}^*$, $(P_1, ..., P_n) \in (K[X]-\{0\})^n$.

1) Ta nói rằng $P_1, ..., P_n$ **nguyên tố cùng** nhau trong toàn thể (hoặc: **xa lạ**) khi và chỉ khi: $\text{ƯCLN}(P_1, ..., P_n) = 1$.

2) Ta nói rằng $P_1, ..., P_n$ **nguyên tố cùng nhau từng đôi** khi và chỉ khi:

$$\forall (i, j) \in \{1, ..., n\}^2, (i \neq j \Rightarrow P_i \wedge P_j = 1).$$

NHẬN XÉT:

1) Nếu $P_1, ..., P_n$ nguyên tố cùng nhau từng đôi thì $P_1, ..., P_n$ nguyên tố cùng nhau trong toàn thể.

2) Khẳng định đảo là sai: Nếu $n \geq 3$, $P_1, ..., P_n$ có thể nguyên tố cùng nhau trong toàn thể nhưng không nguyên tố cùng nhau từng đôi.

Ví dụ: $n = 3$, $K = \mathbb{Z}$, $P_1 = (X - 1)X$, $P_2 = (X - 1)(X + 1)$, $P_3 = X(X + 1)$.

3) Với mọi n thuộc $\mathbb{N}^*$ và mọi $(P_1, ..., P_n)$ thuộc $(K[X] - \{0\})^n$, với ký hiệu: $\Delta = \text{UCLN}(P_1, ..., P_n)$, thì tồn tại $(Q_1, ..., Q_n) \in (K[X] - \{0\})^n$ sao cho $(\forall i \in \{1, ..., n\}, P_i = \Delta Q_i)$ và $Q_1, ..., Q_n$ nguyên tố cùng nhau trong toàn thể. ■

Độc giả có thể chứng minh Mệnh đề sau tương tự như trong 4.3.1 :

♦ **Mệnh đề**

$$\forall (A, B, C) \in (K[X] - \{0\})^3, \left(\begin{cases} A \wedge B = 1 \\ C | B \end{cases} \Rightarrow A \wedge C = 1 \right).$$

2) Định lý Bezout

♦ **Định lý 1 (Định lý Bezout)**

Cho $n \in \mathbb{N}^*$, $(P_1, ..., P_n) \in (K[X] - \{0\})^n$. Để $(P_1, ..., P_n)$ nguyên tố cùng nhau trong toàn thể, cần và đủ là tồn tại $(U_1, ..., U_n) \in (K[X])^n$ sao cho:

$$\sum_{i=1}^{n} P_i U_i = 1 .$$

Chứng minh: Tương tự như phép chứng minh định lý Bezout trong $\mathbb{Z}$, 4.3.2, Định lý 1.

♦ **Định lý 2 (Định lý Gauss)**

$$\forall (A, B, C) \in (K[X] - \{0\})^3, \left\{ \begin{matrix} A | BC \\ A \wedge B = 1 \end{matrix} \Rightarrow A | C \right\}$$

Chứng minh: Tương tự như phép chứng minh định lý Gauss trong $\mathbb{Z}$, 4.3.2, Định lý 2.

♦ **Mệnh đề**

Cho $A, B \in K[X] - \{0\}$ nguyên tố cùng nhau và không đều là hằng. Tồn tại $(U, V) \in (K[X])^2$ duy nhất sao cho:

$$AU + BV = 1, \quad \deg(U) < \deg(B), \quad \deg(V) < \deg(A).$$

Chứng minh:

1) Tồn tại

Nếu, chẳng hạn A là hằng, chỉ cần lấy $U = A^{-1}$, $V = 0$.

Vậy ta giả thiết: $\deg(A) \geq 1$ và $\deg(B) \geq 1$.

Theo định lý Bezout, tồn tại $(U_1, V_1) \in (K[X])^2$ sao cho $AU_1 + BV_1 = 1$. Bằng phép chia Euclide U_1 cho B, tồn tại $(Q, U) \in (K[X])^2$ sao cho:

$$U_1 = BQ + U \text{ và } \deg(U) < \deg(B).$$

Đặt $V = AQ + V_1$.

Ta có: $AU + BV = A(U_1 - BQ) + B(AQ + V_1) = AU_1 + BV_1 = 1$.

Vì A và B đều khác hằng, rõ ràng là U và V đều khác không và: $\deg(AU) = \deg(BV) \geq 1$. Thế thì:

$\deg(V) + \deg(B) = \deg(BV) = \deg(AU) = \deg(A) + \deg(U) < \deg(A) + \deg(B)$,

do đó $\deg(V) < \deg(A)$.

2) Duy nhất

Giả sử (U_1, V_1), (U_2, V_2) thích hợp. Thế thì ta có $A(U_1 - U_2) = B(V_2 - V_1)$. Vì $A \wedge B = 1$, nên định lý Gauss chứng tỏ rằng: $A \mid V_2 - V_1$.

Nhưng $\deg(V_2 - V_1) \leq \text{Max}(\deg(V_1), \deg(V_2)) < \deg(A)$.

Do đó $V_2 - V_1 = 0$, $V_2 = V_1$, $U_2 = U_1$.

Tương tự như ở 4.3.2, ta có một thuật toán để tính cặp (U, V) thuộc $(K[X])^2$ sao cho $AU + BV = 1$ (nếu $A \wedge B = 1$), và cặp (U, V) thu được như thế thỏa mãn: $\deg(U) < \deg(B)$ và $\deg(V) < \deg(A)$ (Nếu $\deg(A) \geq 1$ và $\deg(B) \geq 1$).

VÍ DỤ:

Chứng minh rằng (trong $\mathbb{R}[X]$) các đa thức $A = X^4 + 1$ và $B = X^3 - 1$ nguyên tố cùng nhau và tính một cặp (U, V) thuộc $(K[X])^2$ thỏa mãn $AU + BV = 1$.

Ta thực hiện các phép chia Euclide liên tiếp:

			X		$X^2 - X + 1$
X^4	$+1$	X^3	-1		$X + 1$
	$X + 1$		$-X^2 - 1$		
			$X - 1$		
			-2		

Ta được: $-2 = (X^3 - 1) - (X + 1)(X^2 - X + 1)$

$= (X^3 - 1) - ((X^4 + 1) - X(X^3 - 1))(X^2 - X + 1)$

$= (X^3 - X^2 + X + 1)(X^3 - 1) - (X^2 - X + 1)(X^4 + 1)$.

Một cặp (U, V) thích hợp là:

$$U = -\frac{1}{2}(X^2 - X + 1), \quad V = -\frac{1}{2}(X^3 - X^2 + X + 1).$$

3) Tính chất

♦ **Mệnh đề 1** Cho $n \in \mathbb{N}^*$, $A, P_1, ..., P_n \in K[X] - \{0\}$. Ta có:

$$(\forall i \in \{1, ..., n\}, \quad A \wedge P_i = 1) \Rightarrow A \wedge \left(\prod_{i=1}^{n} P_i\right) = 1$$

♦ **Mệnh đề 2** $\forall (A, B) \in (K[X] - \{0\})^2, \forall (k, l) \in (\mathbb{N}^*)^2,$

$$(A \wedge B = 1 \Leftrightarrow A^k \wedge B^k = 1).$$

♦ **Hệ quả**

$$\forall (A, B) \in (K[X] - \{0\})^2, \forall k \in \mathbb{N}^*, A^k \wedge B^k = (A \wedge B)^k.$$

♦ **Mệnh đề 3** Cho $n \in \mathbb{N}^*$, $A, P_1, ..., P_n \in K[X] - \{0\}$.

Nếu $(\forall i \in \{1, ..., n\}, P_i \mid A)$ và nếu $P_1, ..., P_n$ nguyên tố cùng nhau từng đôi, thì: $\prod_{i=1}^{n} P_i \mid A$.

♦ **Hệ quả** Cho $n \in \mathbb{N}^*$, $(P_1, ..., P_n) \in (K[X] - \{0\})^n$. Nếu $P_1, ..., P_n$ nguyên tố cùng nhau từng đôi thì BCNN của $P_1, ..., P_n$ là đa thức chuẩn tắc của $\prod_{i=1}^{n} P_i$ (tức là $\frac{1}{\alpha}\prod_{i=1}^{n} P_i$ trong đó α là hệ tử cao nhất của $\prod_{i=1}^{n} P_i$).

♦ **Mệnh đề 4** Với mọi (A, B) thuộc $(K[X] - \{0\})^2$, $(A \wedge B)(A \vee B)$ là đa thức chuẩn tắc của AB.

5.2.5 Đa thức bất khả quy

♦ **Định nghĩa** Một đa thức P thuộc $K[X]$ được gọi là **đa thức bất khả quy** (hoặc: **đa thức nguyên tố**) khi và chỉ khi $\deg(P) \geq 1$ và P chỉ có ước (trong $K[X]$) là các α ($\alpha \in K - \{0\}$) và các βP ($\beta \in K - \{0\}$).

NHẬN XÉT: **Phép đổi thể**

Cho L là một thể, K là một thể con của L (trong thực hành: $K = \mathbb{R}$ và $L = \mathbb{C}$), $P \in K[X]$.

• Nếu P bất khả quy trong $L[X]$, thì P bất khả quy trong $K[X]$.

• Khẳng định đảo là sai: P có thể bất khả quy trong $K[X]$, nhưng không bất khả quy trong $L[X]$.

VÍ DỤ: $X^2 + 1$ bất khả quy trong $\mathbb{R}[X]$, nhưng không bất khả quy trong $\mathbb{C}[X]$:

$$X^2 + 1 = (X + i)(X - i).$$

♦ **Mệnh đề 1** Cho $P \in K[X]$ bất khả quy, $A \in K[X] - \{0\}$. Ta có: $P \mid A$ hoặc $P \wedge A = 1$.

♦ **Mệnh đề 2** Cho $P \in K[X]$ bất khả quy, $n \in \mathbb{N}^*$, $A_1, ..., A_n \in K[X] - \{0\}$.

Ta có: $P \left| \prod_{i=1}^{n} A_i \Leftrightarrow (\exists i \in \{1,...,n\},\ P \mid A_i) \right.$.

♦ **Định lý** Mọi đa thức thuộc $K[X]$ có bậc ≥ 1 đều có một dạng phân tích thành tích những đa thức bất khả quy, duy nhất sai khác thứ tự các nhân tử và sai khác về các nhân tử bậc không thuộc $K - \{0\}$.

Chứng minh: Tương tự như trong 4.4.3, Định lý 1.

Cho $A \in K[X]$ sao cho $\deg(A) \geq 1$. Theo định lý trên, tồn tại $N \in \mathbb{N}^*$, $P_1, ..., P_N$ bất khả quy và nguyên tố cùng nhau từng đôi, $r_1, ..., r_N \in \mathbb{N}^*$ sao cho: $A = \prod_{i=1}^{n} P_i^{r_i}$. Đẳng thức này được gọi là **dạng phân tích nguyên tố** (viết tắt: PTNT) **của A trong $K[X]$.**

VÍ DỤ:

- PTNT của $X^4 + X^3 + X + 1$ trong $\mathbb{R}[X]$ là:
$$X^4 + X^3 + X + 1 = (X + 1)^2(X^2 - X + 1).$$
- PTNT của $X^4 + X^3 + X + 1$ trong $\mathbb{C}[X]$ là:
$$X^4 + X^3 + X + 1 = (X + 1)^2(X + j)(X + j^2).$$

NHẬN XÉT:

Để thuận lợi trong PTNT của A, $A = \prod_{i=1}^{n} P_i^{r_i}$, một số các r_i có thể bằng không.

♦ **Hệ quả** Mọi đa thức thuộc $K[X]$ có bậc ≥ 1 có ít nhất một ước bất khả quy.

♦ **Mệnh đề 3** Cho $A, B \in K[X]$ đều có bậc ≥ 1, chuẩn tắc, $A = \prod_{i=1}^{N} A_i^{r_i}$, $B = \prod_{i=1}^{N} P_i^{s_i}$ là các PTNT của A và B (trong đó $N \in \mathbb{N}^*$, $P_1, ..., P_N$ đều bất khả quy, chuẩn tắc và nguyên tố cùng nhau từng đôi, $r_1, ..., r_N$, $s_1, ..., s_N \in \mathbb{N}$).

Ta có:
$$\begin{cases} A \wedge B = \prod_{i=1}^{n} P_i^{\mathrm{Min}(r_i, s_i)} \\ A \vee B = \prod_{i=1}^{n} P_i^{\mathrm{Max}(r_i, s_i)} \end{cases}$$

♦ **Hệ quả** Trong $K[X] - \{0\}$, các luật $\wedge$ và $\vee$ có tính phân phối luật này đối với luật kia.

Bài tập

◊ **5.2.10** Cho $(P_n)_{n\in\mathbb{N}}$ là một dãy trong $K[X]$ xác định bởi: $\begin{cases} P_0 = 1, P_1 = X \\ \forall n \in N, P_{n+2} = XP_{n+1} - P_n \end{cases}$

a) Chứng minh: $\forall n \in \mathbb{N}$, $P_{n+1}^2 - P_nP_{n+2} = 1$.

b) Suy ra: $\forall n \in \mathbb{N}$, $P_n \wedge P_{n+1} = 1$.

◊ **5.2.11** Cho $A, B, C \in K[X]$. Chứng minh rằng, nếu A, B, C nguyên tố cùng nhau từng đôi, thì $AB + BC + CA$ và ABC nguyên tố cùng nhau.

◊ **5.2.12** Cho $(A, B) \in (K[X] - \{0\})^2$. Chứng minh hai tính chất sau là tương đương:

(i) A và B không nguyên tố cùng nhau

(ii) $\exists (U, V) \in (K[X] - \{0\})^2$. $\begin{cases} \deg(U) < \deg(B) \\ \deg(V) < \deg(A) \\ AU + BV = 0 \end{cases}$

◊ **5.2.13** Cho $n \in \mathbb{N}^*$, $(a,b) \in \mathbb{K}^2$ sao cho $a \neq b$. Tìm một cặp (U, V) thuộc $(\mathbb{K}[X])^2$ sao cho:

$$\begin{cases} (X-a)^n U + (X-b)^n V = 1 \\ \deg(U) \leq n-1, \ \deg(V) \leq n-1 \end{cases}$$

(Có thể khai triển $((X - a) + (X - b))^{2n-1}$ bằng cách áp dụng công thức nhị thức Newton).

5.2.6 Phép chia theo lũy thừa tăng

♦ **Mệnh đề - Định nghĩa** Cho $n \in \mathbb{N}$, $A \in K[X]$, $B \in K[X]$ sao cho $\text{val}(B) = 0$ (tức là: $\tilde{B}(0) \neq 0$). Tồn tại một cặp duy nhất (Q, R) thuộc $(K[X])^2$ sao cho:

$$A = BQ + X^{n+1}R \quad \text{và} \quad \deg(Q) \leq n.$$

Đa thức Q (tương ứng: R) gọi là **thương** (tương ứng: **dư**) **của phép chia** A **cho** B **theo lũy thừa tăng đến cấp** n.

Chứng minh: 1) **Tồn tại**

Quy nạp theo n

- Trường hợp $n = 0$

Ta ký hiệu a_0, b_0 là các hạng tử hằng tương ứng của A, B (tức là : $a_0 = \tilde{A}(0)$, $b_0 = \tilde{B}(0) \neq 0$), $Q = a_0 b_0^{-1}$. Hạng tử hằng của $A - BQ$ là không, vậy tồn tại $R \in K[X]$ sao cho $A - BQ = XR$. Vậy: $A = BQ + XR$ và $\deg(Q) \leq 0$.

• Giả sử $n \in \mathbb{N}$ và giả sử tồn tại $(Q, R) \in (K[X])^2$ sao cho: $A = BQ + X^{n+1}R$ và $\deg(Q) \leq n$. Theo sự khảo sát trường hợp $n = 0$, áp dụng cho R thay vì A, tồn tại $(q, R_1) \in (K[X])^2$ sao cho: $R = Bq + XR_1$ và $\deg(q) \leq 0$.

Đặt $Q_1 = Q + X^{n+1}q$ ta suy ra:

$$\begin{cases} A = BQ + X^{n+1}(Bq + XR_1) = BQ_1 + X^{n+2}R_1 \\ \deg(Q_1) \leq n+1 \end{cases}$$

2) Duy nhất

Giả sử (Q_1, R_1), (Q_2, R_2) thích hợp. Suy ra $B(Q_1 - Q_2) = X^{n+1}(R_2 - R_1)$, do đó bằng cách chuyển sang các định giá:

$$\text{val}(Q_1 - Q_2) = n + 1 + \text{val}(R_2 - R_1) \geq n + 1.$$

Nếu $Q_1 - Q_2 \neq 0$, thì: $n \geq \deg(Q_1 - Q_2) \geq \text{val}(Q_1 - Q_2) \geq n + 1$, mâu thuẫn.

Vậy $Q_1 = Q_2$, nên $R_1 = R_2$.

VÍ DỤ:

Thực hiện phép chia $A = 2 + X - 3X^2 + X^3$ cho $B = 1 + 4X - X^2 + X^3$ (trong $\mathbb{R}[X]$) theo lũy thừa tang đến cấp 2

$$\begin{array}{l|l} 2 + X - 3X^2 + X^3 & 1 + 4X - X^2 + X^3 \\ \hline -7X - X^2 - X^3 & 2 - 7X + 27X^2 \\ \quad 27X^2 - 8X^3 + 7X^4 & \\ \quad\quad -116X^3 + 34X^4 - 27X^5 & \end{array}$$

Suy ra thương $Q = 2 - 7X + 27X^2$ và dư $R = -116 + 34X - 27X^2$. ■

Phép chia theo lũy thừa tang được dùng chủ yếu để :

- Phân tích một phân thức hữu tỷ thành những phần tử đơn giản (xem 5.4.2, 2) *b)* *I)*).
- Tính các khai triển hữu hạn của một thương (xem Tập 2, 8.3.4, Nhận xét).

Bài tập

◊ **5.2.14** Cho $n \in \mathbb{N}^*$, $(a, b) \in K^2$, $A = 1 - abX^2$, $B = 1 - (a + b)X + abX^2$. Tìm thương và dư của phép chia A cho B theo lũy thừa tang đến cấp n.

◊ **5.2.15** Cho $n \in \mathbb{N}^*$, $A = \sum_{k=0}^{n} X^k$, $B = \sum_{k=0}^{n} (-1)^k X^k$. Tìm thương và dư của phép chia A cho B theo lũy thừa tang đến cấp n.

5.3 Không điểm của đa thức

5.3.1 Đại cương

◆ **Định nghĩa 1** Cho $P \in K[X]$, $a \in K$. Ta nói rằng a là một **không điểm** (hoặc: **một nghiệm**) của P khi và chỉ khi: $\tilde{P}(a) = 0$.

Ta nhắc lại rằng $\tilde{P}$ là ánh xạ đa thức liên kết với P, và nếu K vô hạn (trường hợp thường gặp nhất trong thực hành) thì có thể đồng nhất P và $\tilde{P}$ (xem 5.1.7, Mệnh đề 2).

Mọi phương trình $\tilde{P}(x) = 0$, có ẩn $x \in K$, trong đó $P \in K[X]$ cố định, gọi là **phương trình đại số.**

Ta đã thấy (5.2.2, Mệnh đề) rằng a là một không điểm của P khi và chỉ khi $X - a$ chia hết P.

◆ **Mệnh đề 1** Cho $P \in K[X]$, $n \in \mathbb{N}^*$, $x_1, \ldots, x_n \in K$ từng đôi khác nhau.
Nếu $x_1, \ldots, x_n$ là các không điểm của P thì: $\prod_{i=1}^{n} (X - x_i) \mid P$.

Chứng minh:

Theo 5.2.2, Mệnh đề: $\forall i \in \{1, \ldots, n\}$, $X - x_i \mid P$. Vì $x_1, \ldots, x_n$ từng đôi khác nhau, nên các đa thức $X - x_1, \ldots, X - x_n$ nguyên tố cùng nhau từng đôi, vậy (xem 5.2.4, 3), Mệnh đề 3):

$$\prod_{i=1}^{n} (X - x_i) \mid P .$$

◆ **Hệ quả 1** Cho $P \in K[X]$, $n \in \mathbb{N}^*$. Nếu $\deg(P) < n$ và nếu P có ít nhất n không điểm từng đôi khác nhau, thì $P = 0$. ■

◆ **Hệ quả 2** Nếu một đa thức P thuộc $K[X]$ triệt tiêu tại một số vô hạn các phần tử thuộc K, thì $P = 0$. ■

VÍ DỤ:

Đa thức nội suy Lagrange

Cho $n \in \mathbb{N}$, $x_0, \ldots, x_n \in K$ từng đôi khác nhau.

- Với mỗi i thuộc $\{0, \ldots, n\}$, tồn tại một đa thức L_i thuộc $K[X]$ và chỉ một sao cho:

$$\begin{cases} \deg(L_i) \le n \\ \forall j \in \{0, \ldots n\} \quad (j \neq i \Rightarrow \tilde{L}_i(x_j) = 0) \\ \tilde{L}_i(x_i) = 1 \end{cases}$$

và ta có: $L_i = \dfrac{1}{\prod_{\substack{0 \le j \le n \\ j \neq i}} (x_i - x_j)} \prod_{\substack{0 \le j \le n \\ j \neq i}} (X - x_j)$.

Các đa thức $L_i\ (0 \le i \le n)$ được gọi là các **đa thức nội suy Lagrange** tại các điểm $x_0, ..., x_n$.

- Với mọi $(b_0, ..., b_n)$ thuộc K^{n+1}, tồn tại một đa thức P thuộc $K[X]$ và chỉ một sao cho:

$$\begin{cases} \deg(P) \le n \\ \forall i \in \{0,...,n\},\ \widetilde{P}(x_i) = b_i \end{cases}$$

và ta có: $P = \sum_{i=0}^{n} b_i L_i$.

◆ **Định nghĩa 2** Cho $P \in K[X]$, $a \in K$, $\alpha \in \mathbb{N}^*$.

1) Ta nói rằng a là một **không điểm cấp bội không thấp hơn** α **của** P khi và chỉ khi:

$$(X - a)^{\alpha} \mid P.$$

2) Ta nói rằng a là một **không điểm cấp bội đúng bằng** α **của** P khi và chỉ khi :

$$(X - a)^{\alpha} \mid P \quad \text{và} \quad (X - a)^{\alpha+1} \nmid P.$$

Nếu $\alpha = 1$ (tương ứng: 2, tương ứng: 3), ta nói a là **không điểm đơn** (tương ứng: **kép**, tương ứng: **bội ba**).

Ta chứng minh dễ dàng mệnh đề sau:

◆ **Mệnh đề - Định nghĩa 2**

Cho $P \in K[X] - \{0\}$, $a \in K$. Nếu a là không điểm của P, thì tồn tại $\alpha \in \mathbb{N}^*$ duy nhất sao cho a là không điểm cấp bội đúng bằng α của P, và ta nói rằng α **là cấp bội của không điểm** a **trong** (hoặc: **của**) P.

◆ **Mệnh đề 3** Cho $n \in \mathbb{N}^*$, $x_1, ..., x_n \in K$ từng đôi khác nhau, $A = \prod_{k=1}^{n} (X - x_k)$, $B \in K[X]$. Thế thì ta có:

$$A \mid B \Leftrightarrow (\forall k \in \{1, ..., n\},\ \widetilde{B}(x_k) = 0).$$

Chứng minh:

1) Nếu $A \mid B$, thì tồn tại $Q \in K[X]$ sao cho $B = AQ$, do đó:

$$\forall k \in \{1, ..., n\},\quad \widetilde{B}(x_k) = \widetilde{A}(x_k)\,\widetilde{Q}(x_k) = 0.$$

2) Ngược lại, nếu $(\forall k \in \{1, ..., n\},\ \widetilde{B}(x_k) = 0)$, thì: $\forall k \in \{1, ..., n\}$, $X - x_k \mid B$, vậy, do $X - x_1, ..., X - x_n$ nguyên tố cùng nhau từng đôi, nên ta kết luận (theo 5.2.4, *3*), Mệnh đề 3): $A \mid B$.

Bài tập

◊ **5.3.1** Cho $n \in \mathbb{N}$, $x_0, \ldots, x_n \in K$ từng đôi khác nhau, $P = \prod_{i=0}^{n} (X - x_i)$. Với mọi i thuộc $\{0, \ldots, n\}$ ta ký hiệu $L_i = \frac{1}{\prod_{\substack{0 \le j \le n \\ j \ne i}} (x_i - x_j)} \prod_{\substack{0 \le j \le n \\ j \ne i}} (X - x_j)$ (đa thức nội suy Lagrange tại các điểm $x_0, \ldots, x_n$, xem 5.3.1, Ví dụ). Chứng minh rằng, với mọi A thuộc $K[X]$, dư của phép chia Euclide A cho P là: $\sum_{i=0}^{n} \tilde{A}(x_i) L_i$.

◊ **5.3.2** Cho $n \in \mathbb{N}^*$, $a_1, \ldots, a_n \in \mathbb{R}$, $P_n = \prod_{k=1}^{n} (X \sin a_k + \cos a_k)$. Tìm dư của phép chia Euclide P_n cho $X^2 + 1$.

◊ **5.3.3** Cho $P \in K[X]$, $n \in \mathbb{N}^*$. Chứng minh:

a) $X - 1 \mid P(X^n) \Rightarrow \sum_{k=0}^{2n-1} X^k \mid P(X^{2n})$

b) $X - 1 \mid P(X^n) \Rightarrow (\forall k \in \mathbb{N}^*, X^k - 1 \mid P(X^k))$.

◊ **5.3.4** Với $n \in \mathbb{N}$, tính dư của phép chia Euclide $X^{2n+1} + (X + 1)^{n+2}$ cho $X^2 + X + 1$ trong $\mathbb{Z}[X]$.

◊ **5.3.5** Cho $n \in \mathbb{N}^*$, $A = X^5 + 1$,

$$P_n = (X^4 - 1)(X^3 - X^2 + X - 1)^n + (X + 1)X^{4n-1} \in \mathbb{Z}[X].$$

Chứng minh: $A \mid P_n$.

5.3.2 Đa thức tách

♦ **Định nghĩa 1** Một đa thức P của $K[X]$ được gọi là đa thức **tách** (hay: **tách được**) trên K khi và chỉ khi tồn tại $\lambda \in K - \{0\}$, $n \in \mathbb{N}^*$, $x_1, \ldots, x_n \in K$ sao cho:

$$P = \lambda \prod_{i=1}^{n} (X - x_i).$$

Ở đây, $x_1, \ldots, x_n$ không nhất thiết khác nhau từng đôi.

Dưới đây sẽ thấy rằng (định lý d'Alembert, 5.3.4) mọi đa thức khác hằng thuộc $\mathbb{C}[X]$ đều tách được trên $\mathbb{C}$.

NHẬN XÉT:

Phép đổi thể

Cho L là một thể, K là một thể con của L, $P \in K[X]$. P có thể tách được trên L nhưng không tách được trên K. Ví dụ: $K = \mathbb{R}$, $L = \mathbb{C}$, $P = X^2 + 1$. ■

Với $x_1, x_2, x_3 \in K$, ta khai triển:

- $\prod_{i=1}^{2}(X - x_i) = (X - x_1)(X - x_2) = X^2 - (x_1 + x_2)X + x_1x_2$

- $\prod_{i=1}^{3}(X - x_i) = (X - x_1)(X - x_2)(X - x_3)$

$$= X^3 - (x_1 + x_2 + x_3)X^2 + (x_1x_2 + x_1x_3 + x_2x_3)X - x_1x_2x_3.$$

Kết quả này dẫn đến Định nghĩa sau.

♦ Định nghĩa 2

Cho $n \in \mathbb{N}^*$, $x_1, ..., x_n \in K$. Các "biểu thức" sau:

$$\sigma_1 = \sum_{i=1}^{n} x_i = x_1 + x_2 + ... + x_n$$

$$\sigma_2 = \sum_{1 \le i_1 < i_2 \le n} x_{i_1}x_{i_2} = (x_1x_2 + x_1x_3 + ... + x_1x_n) + (x_2x_3 + ... + x_2x_n) + ...$$

$$... + (x_{n-2}x_{n-1} + x_{n-2}x_n) + x_{n-1}x_n.$$

$$\vdots$$

$$\sigma_k = \sum_{1 \le i_1 < i_2 < ... < i_k \le n} x_{i_1}x_{i_2}...x_{i_k} \quad (1 \le k \le n)$$

$$\vdots$$

$$\sigma_n = x_1x_2 ... x_n$$

gọi là các **hàm đối xứng cơ bản** của $x_1, ..., x_n$.

Chẳng hạn các hàm đối xứng cơ bản của x_1, x_2, x_3, x_4 là:

$$\begin{cases} \sigma_1 = x_1 + x_2 + x_3 + x_4 \\ \sigma_2 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \\ \sigma_3 = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 \\ \sigma_4 = x_1x_2x_3x_4 \end{cases}$$

NHẬN XÉT:

1) Tổng quát hơn, xét các ẩn $X_1, ..., X_n$ thay cho các phần tử $x_1, ..., x_n$ của K, ta có thể định nghĩa các **đa thức đối xứng cơ bản** $\sigma_1, ... \sigma_n$ của $K[X_1, ..., X_n]$:

$$\forall k \in \{1, ..., n\}, \quad \sigma_k = \sum_{1 \le i_1 < ... < i_k \le n} X_{i_1}X_{i_2}...X_{i_k}$$

2) Hàm đối xứng cơ bản σ_k của $x_1, ..., x_n$ gồm C_n^k "hạng tử".

♦ **Mệnh đề (Hệ thức giữa hệ tử và không điểm)**

Cho $n \in \mathbb{N}^*$, $(a_0, ..., a_n) \in K^{n+1}$ sao cho $a_n \neq 0$ và $P = \sum_{i=0}^{n} a_i X^i$.

Giả thiết P tách được trên K và ký hiệu $x_1, ..., x_n$ là các không điểm của P (không nhất thiết từng đôi khác nhau), sao cho:

$$P = a_n \prod_{i=1}^{n} (X - x_i).$$

Thế thì ta có:

$$\sigma_1 = -\frac{a_{n-1}}{a_n}, ..., \sigma_k = (-1)^k \frac{a_{n-k}}{a_n}, ..., \sigma_n = (-1)^n \frac{a_0}{a_n}$$

trong đó $\sigma_1, ..., \sigma_n$ chỉ các hàm đối xứng cơ bản của $x_1, ..., x_n$.

Chứng minh:

Chỉ cần khai triển và đồng nhất hệ số của các hạng tử cùng bậc trong:

$$a_n \prod_{i=1}^{n} (X - x_i) = a_n X^n + a_{n-1} X^{n-1} + ... + a_0$$

VÍ DỤ:

Tính $\sum_{i=1}^{4} x_i^2$ trong đó $x_1, ..., x_4$ là các không điểm của $X^4 + X^3 + X^2 + 1$ trong $\mathbb{C}$.

Ta có: $\sum_{i=1}^{4} x_i^2 = \sigma_1^2 - 2\sigma_2, \sigma_1 = -1, \sigma_2 = 1$, do đó $\sum_{i=1}^{4} x_i^2 = -1$. Đặc biệt $x_1, ..., x_4$ không phải tất cả đều là những số thực.

Bài tập

◊ **5.3.6** Cho a, b là hai không điểm khác nhau của $z^3 + 3z^2 + z + 1 = 0$ (ẩn $z \in \mathbb{C}$). Trị của $a^2b + ab^2 + 3ab$ là bao nhiêu?

◊ **5.3.7** *Ví dụ về cách tính hàm đối xứng của các không điểm của một phương trình đại số*
Ký hiệu $x_1, x_2, x_3, ...$ là các không điểm của phương trình được chỉ ra (trong $\mathbb{C}$), hãy tính biểu thức E, trong đó Σ chỉ tổng của tất cả các hạng tử nhận được do hoán vị các chỉ số:

a) $x^3 + px + q = 0$, $(p, q) \in \mathbb{C} \times \mathbb{C}^*$, $E = \Sigma \frac{1}{x_1^2}$ (ba hạng tử)

b) $x^3 - 3x^2 + x - 1 = 0$, $E = \Sigma x_1^3 x_2^2$ (sáu hạng tử)

c) $x^3 + px^2 + qx + r = 0$, $(p, q, r) \in \mathbb{C}^3$, $E = \Sigma (x_1 + x_2)^3$ (ba hạng tử)

d) $x^3 + px + q = 0$, $(p, q) \in \mathbb{C}^2$, $E = \Sigma x_1^5 x_2^2$ (sáu hạng tử)

e) $x^5 + 4x^4 + 3x^3 + x + 1 = 0$, $E = \Sigma x_1^4 x_2$ (hai mươi hạng tử).

◊ **5.3.8** Cho $z_1, ..., z_4 \in \mathbb{C}$, $u_1 = z_1z_2 + z_3z_4$, $u_2 = z_1z_3 + z_2z_4$, $u_3 = z_1z_4 + z_2z_3$.

Tính các hàm đối xứng cơ bản $\sigma_1, \sigma_2, \sigma_3$ của u_1, u_2, u_3 theo các hàm đối xứng cơ bản $\tau_1, ..., \tau_4$ của $z_1, ..., z_4$.

◊ **5.3.9** Xác định tập hợp các số thực p sao cho hệ phương trình: $\begin{cases} x + y + z = 2 \\ xy + xz + xz = 1 \\ xyz = p \end{cases}$

có ít nhất một nghiệm (x, y, z) trong $\mathbb{R}^3$.

◊ **5.3.10** Giải các hệ phương trình sau với ẩn $(x, y, z) \in \mathbb{C}^3$:

a) $\begin{cases} x + y + z = 3 \\ xy + yz + zx = 2 \\ x^3 + y^3 + z^3 = 9 \end{cases}$ b) $\begin{cases} x + y + z = 0 \\ x^3 + y^3 + z^3 = 6 \\ x^5 + y^5 + z^5 = 30 \end{cases}$

c) $\begin{cases} x + y + z = 1 \\ \frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1 \\ x^2 + y^2 + z^2 = -1 \end{cases}$ d) $\begin{cases} x + y + z = -2 \\ \frac{1}{x} + \frac{1}{y} + \frac{1}{z} = -2 \\ \frac{xy}{z} + \frac{yz}{x} + \frac{zx}{y} = 0. \end{cases}$

◊ **5.3.11** *Ví dụ điều kiện cần và đủ (viết tắt:* **ĐKCĐ***) đối với các hệ tử của một phương trình đại số để các không điểm thoả mãn một hệ thức đã cho (trong* $\mathbb{C}$*)*

a) ĐKCĐ đối với $\lambda \in \mathbb{C}$ để hai trong các không điểm z_1, z_2, z_3 của $z^3 + 5z^2 - 8z + \lambda = 0$ (chẳng hạn z_1 và z_2) thỏa mãn $z_1 + z_2 = -1$; giải phương trình trong trường hợp đó.

b) ĐKCĐ đối với $(p, q) \in \mathbb{C}^2$ để $z^3 + pz + q = 0$ có hai không điểm mà hiệu bằng 1.

c) ĐKCĐ đối với $(p, q, r) \in \mathbb{C}^3$ để các không điểm của $z^3 + pz^2 + qz + r = 0$ là các tọa vị của các đỉnh của một tam giác đều trong mặt phẳng phức (sử dụng bài tập 2.3.3, Tập 1).

d) ĐKCĐ đối với $\lambda \in \mathbb{C}$ để hai trong các không điểm z_1, z_2, z_3 của $z^3 - 7z + 1 = 0$ (chẳng hạn z_1 và z_2) thỏa mãn $z_2 = 2z_1$.

e) ĐKCĐ đối với $(a, b, c, d) \in \mathbb{C}^4$ để đa thức $X^4 + aX^3 + bX^2 + cX + d$ có hai không điểm kép.

f) ĐKCĐ đối với $(a, b) \in \mathbb{C}^2$ để $z^4 + az + b = 0$ có hai nghiệm z_1, z_2 sao cho $z_1z_2 = 1$.
Áp dụng: Giải $z^4 - 21z + 8 = 0$ trong $\mathbb{C}$.

g) ĐKCĐ đối với $(\lambda, \mu) \in \mathbb{C}^2$ để các không điểm z_1, z_2, z_3, z_4 của $z^4 - 4z^3 + \lambda z^2 + \mu z + 5 = 0$ thỏa mãn $z_1 + z_2 = z_3 + z_4$.

h) ĐKCĐ đối với $\lambda \in \mathbb{C}$ để các không điểm z_1, z_2, z_3, z_4 của $z^4 - z^3 + \lambda z^2 + 23z - 20 = 0$ thỏa mãn $z_1z_2 = -5$. Giải phương trình trong trường hợp này.

i) ĐKCĐ đối với $\lambda \in \mathbb{R}$ để đa thức $X^5 - 209X + \lambda$ có hai không điểm thực và có tích bằng 1.

◊ **5.3.12** *Ví dụ về phương trình thuận nghịch*

Giải trong $\mathbb{C}$ các phương trình (ẩn x):

a) $x^5 + 3x^4 + x^3 + x^2 + 3x + 1 = 0$

b) $x^6 - 4x^5 + 7x^4 - 9x^3 + 7x^2 - 4x + 1 = 0$.

(Sau khi khử các nghiệm 1, -1 có thể có, chia cho một lũy thừa thích hợp của x và đặt $y = x + \frac{1}{x}$).

◊ **5.3.13** Giải $z^6 - z^5 - 4z^4 + 5z^3 - 41z^2 + 36z - 36 = 0$ (ẩn $z \in \mathbb{C}$) cho biết nó có hai nghiệm đối nhau.

◊ **5.3.14** *Một phương pháp giải phương trình bậc ba (trong* $\mathbb{C}$*)*

a) Bằng phép đổi biến $z = x + \dfrac{a}{3}$, chứng minh rằng phương trình $x^3 + ax^2 + bx + c = 0$ (ẩn $x \in \mathbb{C}$; $(a, b, c) \in \mathbb{C}^3$ cố định) quy về phương trình $z^3 + pz + q = 0$ (ẩn $z \in \mathbb{C}$; $(p, q) \in \mathbb{C}^2$ cố định).

b) Bằng phép đổi biến $y = \dfrac{\alpha - z}{\beta - z}$ ($(\alpha, \beta) \in \mathbb{C}^2$ phải tìm), chứng minh rằng phương trình $z^3 + pz + q$ quy về phương trình $y^3 + A = 0$, $A \in \mathbb{C}$.

◊ **5.3.15** Với $P \in K[X]$ và $a \in K$, ta ký hiệu $\omega_P(a)$ là bậc của a trong P, với các quy ước:

$$\begin{cases} \omega_P(a) = 0 & \text{nếu } a \text{ không phải là không điểm của } P \\ \omega_0(a) = +\infty. \end{cases}$$

Chứng minh rằng với mọi P, Q thuộc $K[X]$:

a) $\omega_{P+Q}(a) \geq \text{Min}(\omega_P(a), \omega_Q(a))$

b) $\omega_{PQ}(a) = \omega_P(a) + \omega_Q(a)$

c) $\displaystyle\sum_{a \in Z(P)} \omega_P(a) \leq \deg(P)$, nếu $P \neq 0$, trong đó $Z(P)$ là tập hợp các không điểm của P trong K.

d) $\displaystyle\sum_{a \in Z(P)} \omega_P(a) = \deg(P)$, nếu và chỉ nếu P ($\neq 0$) tách được.

◊ **5.3.16** Cho $P \in \mathbb{C}[X] - \{0\}$, $n = \deg(P)$; chứng minh rằng các tổng các không điểm của $P, P', \ldots, P^{(n-1)}$ tạo thành một cấp số cộng.

◊ **5.3.17** Cho $(a, b) \in \mathbb{R}^2$, $A = X^4 + (2a + 1)X^3 + (a - 1)^2X^2 + bX + 4$.

Tìm tất cả các cặp (a, b) sao cho tồn tại $P, Q \in \mathbb{R}[X]$ thỏa mãn:

$$\begin{cases} A = PQ. \\ \deg(P) = \deg(Q) = 2. \\ P \text{ và } Q \text{ đều chuẩn tắc} \\ Q \text{ có hai không điểm khác nhau } \alpha, \beta \text{ thuộc } \mathbb{R}. \\ P(\alpha) = \beta \text{ và } P(\beta) = \alpha. \end{cases}$$

◊ **5.3.18** Cho $(p, q, r) \in \mathbb{C}^3$, a, b, c, là các nghiệm của $x^3 + px^2 + qx + r = 0$ trong $\mathbb{C}$; thành lập phương trình bậc ba mà các nghiệm là $a^2 - bc$, $b^2 - ca$, $c^2 - ab$.

◊ **5.3.19** ĐKCĐ đối với $(p, q) \in \mathbb{C}^2$ để hai phương trình $z^4 + 2z^2 + p = 0$, $z^3 + z + q = 0$ (ẩn $z \in \mathbb{C}$) có hai nghiệm chung khác nhau.

◊ **5.3.20** Cho $n \in \mathbb{N}^*$, $x_1, \ldots, x_n \in \mathbb{R}$, $\sigma_1, \ldots, \sigma_n$ là các hàm đối xứng cơ bản của $x_1, \ldots, x_n$.

Chứng minh: $(\forall i \in \{1, \ldots, n\}, x_i \in \mathbb{R}_+) \Leftrightarrow (\forall i \in \{1, \ldots, n\}, \sigma_i \in \mathbb{R}_+)$.

◊ **5.3.21** Cho $P, Q \in K[X]$ sao cho $P \mid Q$. Chứng minh rằng, nếu Q tách được, thì P cũng tách được.

◊ **5.3.22** Cho $A, B \in K[X]$ sao cho B tách được và có tất cả không điểm đơn. Chứng minh tồn tại $P \in K[X]$ sao cho: $B \mid P^2 - A$.

5.3.3 Sử dụng phép đạo hàm

Trong tiết 5.3.3 này, ta giả thiết rằng K là một thể con của $\mathbb{C}$; trong thực hành thông thường là $K = \mathbb{R}$ hoặc $\mathbb{C}$. Vậy ta có thể đồng nhất P và hàm đa thức liên kết $\widetilde{P}$ (xem 5.1.7, Nhận xét).

♦ **Định lý** Cho $P \in K[X]$, $a \in K$, $\alpha \in \mathbb{N}^*$.

1) Để a là không điểm bội không thấp hơn α của P, cần và đủ là:

$$\forall k \in \{0, ..., \alpha - 1\}, \quad P^{(k)}(a) = 0.$$

2) Để a là không điểm bội đúng bằng α của P, cần và đủ là:

$$\begin{cases} \forall k \in \{0, ..., \alpha - 1\}, & P^{(k)}(a) = 0 \\ P^{(\alpha)}(a) \neq 0 \end{cases}$$

Chứng minh:

Theo công thức Taylor đối với đa thức, ta có, nếu ký hiệu $N = \text{Max}(\alpha, \deg(P))$:

$$P(X) = \sum_{k=0}^{N} \frac{P^k(a)}{k!}(X - a)^k.$$

Suy ra:

- $(X - a)^\alpha \mid P \Leftrightarrow P(a) = P'(a) = ... = P^{(\alpha - 1)}(a) = 0$
- $\begin{cases} (X-a)^\alpha \mid P \\ (X-a)^{\alpha+1} \nmid P \end{cases} \Leftrightarrow \begin{cases} P(a) = P'(a) = ... = P^{(\alpha-1)}(a) = 0 \\ P^\alpha(a) \neq 0. \end{cases}$

Bài tập

◊ **5.3.23** Tìm tất cả các P thuộc $\mathbb{R}[X]$ sao cho:

$$P(0) = 1, \quad P(1) = 0, \quad P'(0) = 0, \quad P'(1) = 1.$$

◊ **5.3.24** Chứng minh: a) $\forall n \in \mathbb{N}^*$, $(X-1)^2 \left| \left(\sum_{k=0}^{n-1} X^k \right)^2 - n^2 X^{n-1} \right.$

b) $\forall n \in \mathbb{N}^*$, $(X-1)^3 \left| nX^2 - (n+2)X^{n+1} + (n+2)X - n \right.$.

◊ **5.3.25** Cho $n \in \mathbb{N}^*$, $(a, b) \in \mathbb{C}^2$ sao cho $a \neq b$, $A = (X - a)^{2n} + (X - b)^{2n}$, $B = (X - a)^2(X - b)^2$.

Xác định dư của phép chia Euclide A cho B.

◊ **5.3.26** ĐKCĐ đối với $(a, b) \in \mathbb{C}^2$ để cho $X^4 + aX^3 + bX + 1$ (thuộc $\mathbb{C}[X]$) có ít nhất một không điểm bậc không thấp hơn 3.

◊ **5.3.27** Cho $n \in \mathbb{N} - \{0, 1\}$, $P_n = X^{2n} - n^2X^{n+1} + 2(n^2 - 1)X^n - n^2X^{n-1} + 1 \in \mathbb{C}[X]$. Chứng minh rằng 1 là không điểm của P_n và xác định cấp bội của nó.

◊ **5.3.28** Cho $(p, q) \in (\mathbb{N}^*)^2$, $A = X^{p+q} - X^p - X^q + 1$. Xác định $A \wedge A'$.

◊ **5.3.29** Cho $\lambda \in \mathbb{R}^*$, $P, Q \in \mathbb{R}[X]$, $a \in \mathbb{R}$. Ta giả thiết rằng a là một không điểm kép của $P^2 + \lambda Q^2$; chứng minh rằng $PQ' - P'Q$ triệt tiêu tại a.

◊ **5.3.30** Cho $A, B \in \mathbb{C}[X]$ sao cho: $A \wedge B = 1$, $\deg(A) \geq 1$, $\deg(B) \geq 1$. Ta giả thiết rằng mọi không điểm của B đều đơn ; chứng minh:

$$(A'B - AB') \wedge B^2 = 1.$$

5.3.4 Trường hợp $\mathbb{C}[X]$

Do thể $\mathbb{C}$ là vô hạn, ở đây ta đồng nhất đa thức P thuộc $\mathbb{C}[X]$ và hàm đa thức $\widetilde{P}$.

◆ **Định lý (Định lý d'Alembert)**

Mọi đa thức khác hằng thuộc $\mathbb{C}[X]$ có ít nhất một không điểm trong $\mathbb{C}$. Ta nói rằng thể $\mathbb{C}$ là đóng đại số.

Chứng minh (có thể gác lại ở lần đọc đầu tiên):

Có nhiều phép chứng minh định lý d'Alembert (cũng được gọi: Định lý cơ bản của Đại số), đều sử dụng đến Giải tích. Sau đây là một.

Ta chứng minh bằng phản chứng: Giả sử tồn tại $P \in \mathbb{C}[X]$, khác hằng và không có một không điểm nào trong $\mathbb{C}$. Ta ký hiệu $n = \deg(P) \geq 1$, $P = \sum_{i=0}^{n} a_i X^i$, và $\varphi : \begin{matrix} \mathbb{C} \to \mathbb{C} \\ z \mapsto |P(z)| \end{matrix}$

1) Vì $\varphi(z) \underset{|z| \to +\infty}{\longrightarrow} +\infty$, ta có:

$$\forall A > 0, \exists B > 0, \forall z \in \mathbb{C}, \quad (|z| > B \Rightarrow \varphi(z) > A).$$

Đặc biệt, tồn tại $B \in \mathbb{R}_+^*$ sao cho:

$$\forall z \in \mathbb{C}, \quad (|z| > B \Rightarrow \varphi(z) > \varphi(0)).$$

Mặt khác, φ liên tục trên tập compac $\{z \in \mathbb{C}; |z| \leq B\}$, nên φ bị chặn và đạt các biên trên tập compac này; vậy tồn tại $z_0 \in \mathbb{C}$ sao cho:

$$\varphi(z_0) = \inf_{|z| \leq B} \varphi(z).$$

Vì hơn nữa:

$$\forall z \in \mathbb{C}, \quad (|z| > B \Rightarrow \varphi(z) > \varphi(0) \geq \varphi(z_0)),$$

nên ta kết luận:

$$\varphi(z_0) = \inf_{z \in \mathbb{C}} \varphi(z).$$

Ta có thể so sánh kết quả này với bài tập 4.3.16 của Tập 1, về trường hợp một ánh xạ từ $\mathbb{R}$ vào $\mathbb{R}$.

2) Theo công thức Taylor đối với đa thức (5.1.7, Định lý), ta có:

$$\forall h \in \mathbb{C},\ P(z_0 + h) = P(z_0) + hP'(z_0) + \ldots + \frac{h^n}{n!} P^{(n)}(z_0).$$

Ta sẽ chứng minh rằng có thể chọn h sao cho $|P(z_0 + h)| < |P(z_0)|$, tức là $\varphi(z_0 + h) < \varphi(z_0)$, điều này sẽ cho một mâu thuẫn.

Vì $P^{(n)}(z_0) = n!\, a_n \neq 0$, nên tồn tại $k \in \mathbb{N}^*$ sao cho:

$$\begin{cases} P^{(k)}(z_0) \neq 0 \\ \forall l \in \{1, \ldots, k\}, \quad (l < k \Rightarrow P^{(l)}(z_0) = 0) \end{cases}$$

Nói khác đi, k là số nguyên bé nhất ≥ 1 sao cho $P^{(k)}(z_0) \neq 0$.

Vậy ta có: $\forall h \in \mathbb{C},\ \dfrac{P(z_0 + h)}{P(z_0)} = 1 + h^k \dfrac{P^{(k)}(z_0)}{k!\,P(z_0)} + \cdots + h^n \dfrac{P^{(n)}(z_0)}{n!\,P(z_0)}$.

Theo sự khảo sát các căn bậc k trong $\mathbb{C}$, Tập 1, 2.4.3 (vốn không sử dụng đến định lý d'Alambert), tồn tại $\omega \in \mathbb{C}^*$ sao cho: $\omega^k = -\dfrac{P^{(k)}(z_0)}{k!\,P(z_0)}$.

Vậy ta có (với $t \in \mathbb{R}$) KTHH$_1$(0) sau:

$$\frac{P\left(z_0 + \begin{matrix} t \\ \omega \end{matrix}\right)}{P(z_0)} = 1 - t^k + \underset{t \to 0}{o}(t^k)$$

Vậy tồn tại $\eta > 0$ sao cho: $\forall t \in]0, \eta[,\ \left|\dfrac{P\left(z_0 + \begin{matrix} t \\ \omega \end{matrix}\right)}{P(z_0)}\right| < 1$,

điều này mâu thuẫn với định nghĩa của z_0.

♦ Hệ quả 1

Mọi đa thức khác hằng thuộc $\mathbb{C}[X]$ đều tách được trên $\mathbb{C}$.

♦ Hệ quả 2

Các đa thức bất khả quy thuộc $\mathbb{C}[X]$ là các đa thức bậc 1.

Như vậy, dạng phân tích nguyên tố của một đa thức bất kỳ P thuộc $\mathbb{C}[X]$ (có bậc ≥ 1), có dạng: $P = \lambda \prod_{i=1}^{N} (X - x_i)^{r_i}$, trong đó $\lambda \in \mathbb{C}^*$, $N \in \mathbb{N}^*$, $x_1, \ldots, x_N \in \mathbb{C}$ từng đôi khác nhau, $r_1, \ldots, r_N \in \mathbb{N}^*$.

Bài tập

◊ **5.3.31** Nhân tử hóa $2X^3 - X^2 - X - 3$ trong $\mathbb{C}[X]$.

◊ **5.3.32** Cho $a \in \mathbb{C}^*$, $n \in \mathbb{N}^*$. Chứng minh rằng, để các không điểm của phương trình $\left(\frac{1+iz}{1-iz}\right)^n = a^n$ (ẩn $z \in \mathbb{C}$) đều là thực, cần và đủ là $|a| = 1$. Giải phương trình trong trường hợp này.

◊ **5.3.33** a) Cho $n \in \mathbb{N}$, $P_n = (X + i)^{2n+1} - (X - i)^{2n+1}$. Lập dạng phân tích nguyên tố của P_n trong $\mathbb{C}[X]$.

b) Suy ra trị của $\prod_{k=1}^{n}\left(a^2 + \operatorname{cotan}^2 \frac{k\pi}{2n+1}\right)$ với $(n, a) \in \mathbb{N}^* \times \mathbb{R}$.

◊ **5.3.34** a) Cho $n \in \mathbb{N}^*$, $P_n = \sum_{k=0}^{n} X^k$. Lập dạng phân tích nguyên tố của P_n trong $\mathbb{C}[X]$.

b) Suy ra trị của $\prod_{k=1}^{n} \sin \frac{k\pi}{n+1}$ với $(n \in \mathbb{N}^*)$.

◊ **5.3.35** a) ĐKCĐ đối với $n \in \mathbb{N}^*$ để: $X^2 + X + 1 \mid (X^n + 1)^n - X^n$.

b) ĐKCĐ đối với $n \in \mathbb{N}$ để: $X^3 - X^2 + X - 1 \mid (X^2 - X + 1)^n - X^{2n} + X^n - 1$.

c) ĐKCĐ đối với $(n, p, q) \in \mathbb{N}^* \times \mathbb{R} \times \mathbb{R}$ để $X^8 + X^4 + 1 \mid X^{8n} + pX^{4n} + q$.

◊ **5.3.36** Cho $n, p \in \mathbb{N}^*$, $A = \sum_{k=0}^{p} X^k$. ĐKCĐ để: $A \mid A(X^n)$.

◊ **5.3.37** Cho $(p, q, r) \in (\mathbb{N}^*)^3$ thỏa mãn $p \wedge q = p \wedge r = q \wedge r = 1$. Chứng minh:

$$(X^p - 1)(X^q - 1)(X^r - 1) \mid (X - 1)^2(X^{pqr} - 1) \text{ trong } \mathbb{C}[X].$$

◊ **5.3.38** Cho $(n, p) \in (\mathbb{N} - \{0, 1\})^2$; chứng minh: $(X^n - 1)(X^p - 1) \mid (X^{n \wedge p} - 1)(X^{n \vee p} - 1)$ trong $\mathbb{C}[X]$.

◊ **5.3.39** Cho $n \in \mathbb{N} - \{0, 1\}$, $M \in \mathbb{R}_+^*$, $(a_1, \ldots, a_n) \in \mathbb{C}^n$, sao cho: $(\forall k \in \{1, \ldots, n\}, |a_k| < M)$,

$P = 1 + \sum_{k=1}^{n} a_k X^k$. Chứng minh rằng P không có không điểm nào trong đĩa mở tâm 0 và có bán kính $\frac{1}{M+1}$.

◊ **5.3.40** a) Cho $n \in \mathbb{N}$, sao cho $n \geq 3$, $a_0, \ldots, a_{n-3} \in \mathbb{R}$, $P = X^n + X^{n-1} + X^{n-2} + \sum_{k=0}^{n-3} a_k X^k$.

Chứng minh rằng các không điểm của P không phải đều là số thực.

b) Câu hỏi tương tự đối với $Q = 1 + X + X^2 + \sum_{k=3}^{n} b_k X^k$, trong đó $b_3, \ldots, b_n \in \mathbb{R}$.

◊ **5.3.41** Cho $n \in \mathbb{N}^*$, $a_0, ..., a_n \in \mathbb{R}$, $P = \sum_{k=0}^{n} a_k X^k$. Ta giả thiết $a_n > 0$ và:

$$\{k \in \{0, ..., n-1\} : \ a_k \le 0\} \neq \varnothing.$$

Ta ký hiệu $p = \text{Max}\{k \in \{0, ..., n-1\}, a_k \le 0\}$ và $M = \text{Max}\{|a_i|; a_i \le 0\}$.

a) Chứng minh: $\forall x \in]1; +\infty[$, $P(x) \ge a_n x^n - M\dfrac{x^{p+1}-1}{x-1}$.

b) Suy ra: $x \le 1 + \left(\dfrac{M}{a_n}\right)^{\frac{1}{n-p}}$ với mọi không điểm thực x của P.

c) *Ví dụ:* Chứng minh rằng mọi không điểm thực của $6X^{10} + 4X^9 - 7X^2 - X - 1$ đều $< 2{,}02$.

◊ **5.3.42*** Cho $n \in \mathbb{N}^*$, $n_0, n_1, ..., n_N$ là các số nguyên sao cho $0 = n_0 < n_1 < ... < n_N$.

$P = \sum_{k=0}^{N} X^{n_k}$. Chứng minh: $|z| \ge \dfrac{\sqrt{5}-1}{2}$ với mọi không điểm z của P trong $\mathbb{C}$.

◊ **5.3.43** Cho $n \in \mathbb{N}^*$, $(a_0, ..., a_{n-1}) \in (\mathbb{R}_+)^n - \{(0,...,0)\}$, $P = X^n - \sum_{k=0}^{n-1} a_k X^k$. Chứng minh rằng, trong $\mathbb{R}_+^*$, P có một và chỉ một không điểm.

◊ **5.3.44** Chứng minh rằng, với mọi n thuộc $\mathbb{N}$, đa thức $P_n = \sum_{k=0}^{2n} (-1)^k (k+1) X^{2n-k}$ không có không điểm thực.

◊ **5.3.45*** Tìm tất cả các P thuộc $\mathbb{R}[X]$ sao cho: $P(X)\,P(X+1) = P(X^2 + X + 1)$.

◊ **5.3.46*** Tìm tất cả các P thuộc $\mathbb{C}[X]$ sao cho: $P(X)\,P(X+3) = P(X+1)P(X+2)$.

◊ **5.3.47** Cho $A = X^3 + X - 2$, α, β là các không điểm khác 1 của A trong $\mathbb{C}$.

a) Chứng minh tồn tại $B \in \mathbb{Q}[X]$ duy nhất sao cho: $B(1) = 1$, $B(\alpha) = \beta$, $B(\beta) = \alpha$ và tính B.

b) Chứng minh: $A \mid B \circ B - X$.

◊ **5.3.48** Cho $P \in \mathbb{Q}[X]$, $a \in \mathbb{Q}$, $b \in \mathbb{Q}_+$ sao cho: $\forall r \in \mathbb{Q}$, $b \neq r^2$. Chứng minh:

a) Nếu $a + \sqrt{b}$ là không điểm của P trong $\mathbb{R}$, thì $a - \sqrt{b}$ cũng thế.

b) Nếu $a + \sqrt{b}$ là một không điểm ít nhất bội hai của P trong $\mathbb{R}$, thì tồn tại $P_1, P_2 \in \mathbb{Q}[X]$ sao cho $P = P_1 P_2^2$.

◊ **5.3.49** Cho $P, Q, R \in \mathbb{C}[X]$ sao cho: $P(X^3) + XQ(X^3) = (1 + X + X^2)R(X)$. Chứng minh rằng $X - 1$ chia hết P, Q, R.

◊ **5.3.50** a) Cho n là số nguyên tố ≥ 5. Chứng minh tồn tại $A \in \mathbb{R}[X]$ với các hệ tử nguyên sao cho: $X^{2n} - X^n + 1 = (X^2 - X + 1)A$.

b) Cho $n \in \mathbb{N}^*$ có ít nhất một ước nguyên tố ≥ 5; chứng minh rằng $2^{2n} - 2^n + 1$ là hợp số.

Trong các bài tập sau, $\mathbb{Z}[X]$ chỉ vành các đa thức với hệ tử trong $\mathbb{Z}$; độc giả có thể thấy rằng khi thay thế K bởi một vành giao hoán A, thì việc khảo sát $K[X]$ bị sửa đổi rất ít.

◊ **5.3.51** Cho $a, b, c \in \mathbb{Z}$ từng đôi khác nhau, $P \in \mathbb{Z}[X]$ sao cho $P(a) = P(b) = P(c) = 2$. Chứng minh: $\forall x \in \mathbb{Z},\ P(x) \neq 3$.

◊ **5.3.52** Cho $a, b, c \in \mathbb{Z}$ từng đôi khác nhau, $P \in \mathbb{Z}[X]$. Chứng minh rằng ta không thể có:

$$P(a) = P(b),\quad P(b) = c,\quad P(c) = a.$$

◊ **5.3.53** Chứng minh rằng $X^3 + X + 3$ bất khả quy trong $\mathbb{Z}[X]$.

◊ **5.3.54*** Cho $P \in \mathbb{Z}[X] - \{0\}$, $n = \deg(P)$. Chứng minh:

$$\forall a \in \mathbb{Z},\quad \forall (P(k))_{0 \le k \le n}) \mid P(a).$$

◊ **5.3.55*** Cho $n \in \mathbb{N}^*$, $a_1, \ldots, a_n \in \mathbb{Z}$, $P = \left(\prod_{k=1}^{n} (X - a_k)\right)^2 - 1$.

Chứng minh rằng P bất khả quy trong $\mathbb{Z}[X]$.

5.3.5 Trường hợp $\mathbb{R}[X]$

Do thể $\mathbb{R}$ là vô hạn, ở đây ta đồng nhất P thuộc $\mathbb{R}[X]$ và hàm đa thức $\tilde{P}$.

◆ **Mệnh đề 1** Cho $P \in \mathbb{C}[X]$. Ta có:

$$P \in \mathbb{R}[X] \Leftrightarrow (\forall z \in \mathbb{C},\quad \overline{P(z)} = P(\bar{z})).$$

Chứng minh:

Ta ký hiệu $P = \sum_{k=0}^{n} a_k X^k, (a_0,\ldots,a_n) \in \mathbb{C}^{n+1}$. Ta có:

$$\overline{P(z) - P(\bar{z})} = \sum_{k=0}^{n} (a_k - \overline{a_k}) z^k$$

với mọi z thuộc $\mathbb{C}$.

Do đó: $\left(\forall z \in \mathbb{C},\ \overline{P(z)} = P(\bar{z})\right) \Leftrightarrow \left(\forall z \in \mathbb{C}, \sum_{k=0}^{n} (a_k - \overline{a_k}) z^k = 0\right)$

$\Leftrightarrow (\forall k \in \{0,\ldots,n\},\ a_k - \overline{a_k} = 0) \Leftrightarrow P \in \mathbb{R}[X]$.

◆ **Mệnh đề 2** Cho $P \in \mathbb{K}[X]$, $a \in \mathbb{C}$, $\alpha \in \mathbb{N}^*$. Để cho a là không điểm cấp bội không thấp hơn α (tương ứng: đúng bằng α) của P, cần và đủ là $\bar{a}$ là không điểm cấp bội không thấp hơn α (tương ứng: đúng bằng α) của P.

Chứng minh:

1) Giả sử a là không điểm cấp không thấp hơn α của P. Theo 5.3.3, Định lý, ta có:

$$\forall k \in \{0,\ldots,\alpha-1\},\ P^{(k)}(a) = 0.$$

Vì $P, P', \ldots, P^{(\alpha-1)}$ đều thuộc $\mathbb{R}[X]$, nên theo Mệnh đề 1, ta có:

$$\forall k \in \{0,\ldots,\alpha-1\},\ P^{(k)}(\bar{a}) = \overline{P^{(k)}(a)} = 0,$$

vậy (xem 5.3.3, Định lý) $\bar{a}$ là không điểm cấp bội không thấp hơn α của P.

Ta suy ra phần đảo từ phần thuận bằng cách thay a bởi $\bar{a}$.

2) Cách lập luận tương tự cho phép kết luận trong trường hợp cấp bội đúng bằng α.

◆ **Mệnh đề 3** Các đa thức bất khả quy của $\mathbb{R}[X]$ là:

- Các đa thức bậc nhất
- Các đa thức bậc hai có biệt thức < 0.

Chứng minh:

1) Giả sử $P \in \mathbb{R}[X]$ bất khả quy và $\deg(P) \geq 2$.

Vì $P \in \mathbb{C}[X]$, định lý d'Alambert chứng tỏ P có ít nhất một không điểm z trong $\mathbb{C}$. Nếu $z \in \mathbb{R}$, thì $X - z$ chia hết P trong $\mathbb{R}[X]$, điều này mâu thuẫn với tính bất khả quy của P trong $\mathbb{R}[X]$; vậy $z \in \mathbb{C} - \mathbb{R}$.

Theo Mệnh đề 2, $\bar{z}$ cũng là một không điểm của P. Đặt $T = (X - z)(X - \bar{z})$, thì T chia hết P trong $\mathbb{C}[X]$.

Nhưng $T = X^2 - 2\mathrm{Re}(z)X + |z|^2 \in \mathbb{R}[X]$ và $P \in \mathbb{R}[X]$. Suy ra rằng (xem 5.2.2, Nhận xét) T chia hết P trong $\mathbb{R}[X]$.

Vì P bất khả quy, nên tồn tại $\lambda \in \mathbb{C}^*$ sao cho $P = \lambda T$, và như vậy P là một tam thức bậc hai có biệt thức < 0: $\Delta' = (\mathrm{Re}(z))^2 - |z|^2 = -(\mathrm{Im}(z))^2 < 0$.

2) Đảo

• Rõ ràng rằng các đa thức bậc nhất là bất khả quy trong $\mathbb{K}[X]$ (tổng quát hơn điều này cũng đúng với bất kỳ thể K nào thay vì $\mathbb{R}$).

• Giả sử $(a, b, c) \in \mathbb{R}^3$ sao cho $b^2 - 4ac < 0$ và $T = aX^2 + bX + c$.

Nếu tồn tại $(\alpha, \beta) \in \mathbb{R}^* \times \mathbb{R}$ sao cho $\alpha X + \beta \mid T$, thì $T\left(-\dfrac{\beta}{\alpha}\right) = 0$, mâu thuẫn vì

$T = a\left(\left(X + \dfrac{b}{2a}\right)^2 + \dfrac{-\Delta}{4a^2}\right)$, vốn không triệt tiêu tại một số thực nào.

Vậy T không có (trong $\mathbb{R}[X]$) một ước nào bậc nhất. Vì T là bậc hai, ta kết luận T là bất khả quy. ■

Như vậy, *phân tích nguyên tố* (PTNT) một đa thức bất kỳ P của $\mathbb{R}[X]$ (có bậc ≥ 1) có dạng:

$$P = \lambda \prod_{i=1}^{N} (X - x_i)^{r_i} \prod_{j=1}^{N'} \left(X^2 + p_j X + q_j\right)^{s_j},$$

trong đó:

$\lambda \in \mathbb{R}^*$
$N, N' \in \mathbb{N}^*$
$x_1, \ldots, x_N \in \mathbb{R}$, từng đôi khác nhau
$(p_1, q_1), \ldots, (p_{N'}, q_{N'}) \in \mathbb{R}^2$, từng cặp khác nhau
$\forall j \in \{1, \ldots, N'\}, p_j^2 - 4q_j < 0$
$r_1, \ldots, r_N, s_1, \ldots, s_{N'} \in \mathbb{N}^*$.

NHẬN XÉT:

1) Với $P \in \mathbb{R}[X]$, không có mối liên hệ lôgic giữa sự tồn tại ít nhất một không điểm thực của P và tính bất khả quy của P trong $\mathbb{R}[X]$. Thật vậy:

• Mọi đa thức bậc nhất thuộc $\mathbb{R}[X]$ đều bất khả quy và có một không điểm thực. Ví dụ: $X - 1$.

• $X^4 + 2X^2 + 1$ không có không điểm thực (vì: $\forall x \in \mathbb{R}, x^4 + 2x^2 + 1 \geq 1 > 0$) và $X^4 + 2X^2 + 1$ không bất khả quy, vì $X^4 + 2X^2 + 1 = (X^2 + 1)^2$.

2) Mọi đa thức P thuộc $\mathbb{R}[X]$ với bậc lẻ có ít nhất một không điểm thực, vì ánh xạ $P : \mathbb{R} \to \mathbb{R}$, $x \mapsto P(x)$ liên tục trên khoảng $\mathbb{R}$ và có giới hạn vô cùng với dấu trái nhau ở $-\infty$ và $+\infty$ (định lý về trị trung gian, Tập 1, 4.3.3).

3) Mọi đa thức thuộc $\mathbb{R}[X]$ với bậc ≥ 3 đều không bất khả quy.

Nhân tử hóa các tam thức trùng phương thực

Các đa thức $aX^4 + bX^2 + c$, $(a, b, c) \in \mathbb{R}^* \times \mathbb{R} \times \mathbb{R}$ được gọi là **tam thức trùng phương thực**. Bằng cách nhân tử hóa bởi a, ta quy về việc nghiên cứu $X^4 + pX^2 + q$, $(p, q) \in \mathbb{R}^2$. Đặt $\Delta = p^2 - 4q$.

1) Nếu $\Delta > 0$, phân tích chính tắc một tam thức thực (Tập 1, 1.2.3, 2)) cho ta:

$$X^4 + pX^2 + q = \left(X^2 + \frac{p}{2}\right)^2 - \frac{\Delta}{4} = \left(X^2 + \frac{p-\sqrt{\Delta}}{2}\right)\left(X^2 + \frac{p+\sqrt{\Delta}}{2}\right)$$

và ta sẽ có thể dễ dàng suy ra PTNT của $X^4 + pX^2 + q$ trong $\mathbb{R}[X]$.

VÍ DỤ: • $X^4 - 5X^2 + 4 = (X^2 - 4)(X^2 - 1) = (X - 2)(X - 1)(X + 1)(X + 2)$

• $X^4 - 2X^2 - 3 = (X^2 - 3)(X^2 + 1) = (X - \sqrt{3})(X + \sqrt{3})(X^2 + 1)$

• $X^4 + 5X^2 + 6 = (X^2 + 2)(X^2 + 3)$.

2) Nếu $\Delta < 0$, ta gộp X^4 và hạng tử hằng ($q > 0$ vì $p^2 - 4q < 0$):

$$X^4 + pX^2 + q = (X^2 + \sqrt{p})^2 - (2\sqrt{q} - p)X^2$$

Hơn nữa: $p^2 - 4q < 0 \Rightarrow 2\sqrt{q} > p$.

từ đó: $X^4 + pX^2 + q = (X^2 - \sqrt{2\sqrt{q} - p}\,X + \sqrt{q})(X^2 \sqrt{2\sqrt{q} - p}\,X + \sqrt{q})$.

Hai tam thức thu được rõ ràng là bất khả quy trong $\mathbb{R}[X]$.

VÍ DỤ: • $X^4 + 1 = (X^2 + 1)^2 - 2X^2 = (X^2 - \sqrt{2}\,X + 1)(X^2 + \sqrt{2}\,X + 1)$.

• $X^4 + X^2 + 1 = (X^2 + 1)^2 - X^2 = (X^2 - X + 1)(X^2 + X + 1)$.

NHẬN XÉT:

Để nhân tử hóa một đa thức thuộc $\mathbb{R}[X]$, đôi khi ta có thể "đi qua" $\mathbb{C}[X]$.

VÍ DỤ:

Với $n \in \mathbb{N} - \{0,1\}$, nhân tử hóa $X^n - 1$ trong $\mathbb{R}[X]$.

PTNT của $X^n - 1$ trong $\mathbb{C}[X]$ là: $X^n - 1 = \prod_{k=0}^{n} (X - \omega_k)$, trong đó $\omega_k = \exp\left(\frac{2ik\pi}{n}\right)$.

• Nếu n chẵn, $n = 2p$ ($p \in \mathbb{N}^*$), -1 và 1 là các không điểm đơn của $X^n - 1$ và các không điểm khác là phức và từng đôi liên hợp với nhau: $\forall k \in \{1, \ldots, p-1\}, \omega_{2p-k} = \overline{\omega}_k$.

Từ đó:
$$X^{2p} - 1 = (X-1)(X+1)\prod_{k=1}^{p-1}(X - \omega_k)(X - \overline{\omega}_k)$$
$$= (X-1)(X+1)\prod_{k=1}^{p-1}\left(X^2 - 2\cos\frac{2k\pi}{2p}X + 1\right),$$

đây chính là PTNT của $X^{2p} - 1$ trong $\mathbb{R}[X]$.

• Tương tự, nếu n lẻ, $n = 2p + 1$ ($p \in \mathbb{N}$), ta được:

$$X^{2p+1} - 1 = (X-1)\prod_{k=1}^{p}\left(X^2 - 2\cos\frac{2k\pi}{2p+1}X + 1\right).$$

Bài tập

◊ **5.3.56** Nhân tử hóa trong $\mathbb{R}[X]$:

a) $X^3 - 5X^2 + 3X + 9$ b) $(X^2 - X + 2)^2 + (X - 2)^2$

c) $6X^5 + 15X^4 + 20X^3 + 15X^2 + 6X + 1$

d) $X^5 - 7X^3 - 2X^2 + 12X + 8$, cho biết nó có các không điểm bội.

e) $X^5 + 1$ f) $X^6 + 4X^4 + 6X^2 + 9$

g) $X^6 + 3X^5 + 4X^4 + 4X^3 + 4X^2 + 3X + 1$ h) $X^8 + X^4 + 1$

i) $X^{12} + 1$

j) $X^{2n} - 2\cos aX^n + 1$, $(n, a) \in \mathbb{N}^* \times (\mathbb{R} \setminus \pi\mathbb{Z})$.

◊ **5.3.57** Cho $P \in \mathbb{R}[X]$, $z_1, \ldots, z_n$ là các không điểm của P trong $\mathbb{C}$.

Ta giả thiết: $\forall k \in \{1, \ldots, n\}$, $\mathrm{Re}(z_k) \leq 0$.

Chứng minh rằng tất cả các hệ tử của P đều cùng một dấu.

◊ **5.3.58** Tìm tất cả các $(k, P) \in \mathbb{N} \times \mathbb{R}[X]$ sao cho: $P \circ P = P^k$.

◊ **5.3.59*** Cho $n \in \mathbb{N}^*$, $P \in \mathbb{R}[X]$ sao cho $\deg(P) = n$ và: $\forall k \in \{0, \ldots, n\}$, $P(k) = 2^k$. Tính $P(n + 1)$.

◊ **5.3.60*** Cho $n \in \mathbb{N}^*$, $P \in \mathbb{R}[X]$ sao cho $\deg(P) = n$ và: $\forall k \in \{0, \ldots, n\}$, $P(k) = \dfrac{1}{k}$. Tính $P(n + 2)$.

◊ **5.3.61** Cho $n \in \mathbb{N}^*$, $P \in \mathbb{R}[X]$ sao cho $\deg(P) = n$ và: $\forall k \in \{0, \ldots, n\}$, $P(k) = \dfrac{1}{C_{n+1}^k}$. Tính $P(n + 1)$.

◊ **5.3.62** Cho $(p, q) \in (\mathbb{R}[X])^2$ sao cho:

$$\begin{cases} P \circ Q = Q \circ P \\ \text{phương trình } P(x) = Q(x) \text{ (ẩn } x \in \mathbb{R}) \text{ vô nghiệm.} \end{cases}$$

Chứng minh rằng phương trình $P \circ P(x) = Q \circ Q(x)$ (ẩn $x \in \mathbb{R}$) vô nghiệm.

◊ **5.3.63** Cho $A, B, C \in \mathbb{C}[X] \setminus \{0\}$ sao cho: $A^2 + B^2 = C^2$ và $\mathrm{UCLN}(A, B, C) = 1$.

Chứng minh rằng các không điểm của $C + A$, $C - A$, $C - B$ tất cả đều có bội chẵn.

◊ **5.3.64** Cho $P \in \mathbb{R}[X]$ tách được trên $\mathbb{R}$, $n = \deg(P) \in \mathbb{N}^*$, $x_1, \ldots, x_n$ là các không điểm của P, $x \in \mathbb{R}$ sao cho: $\forall k \in \{2, \ldots, n\}$, $|x - x_1| \leq |x - x_k|$.

Chứng minh: $|P(x)| \geq 2^{-n+1} |P'(x_1)(x - x_1)|$.

◊ **5.3.65** Cho $P \in \mathbb{C}[X]$ sao cho $\deg(P) \geq 2$. Chứng minh rằng $P : \underset{x \mapsto P(x)}{\mathbb{C} \to \mathbb{C}}$ không phải là đơn ánh.

◊ **5.3.66*** Cho $P \in \mathbb{R}[X]$ tách được trên $\mathbb{R}$, $A \in \mathbb{R}[X]$ tách được trên $\mathbb{R}$, $n = \deg(A)$, $(a_0, \ldots, a_n) \in \mathbb{R}^{n+1}$ sao cho $A = \sum_{k=0}^{n} a_k X^k$.

Chứng minh rằng $\sum_{k=0}^{n} a_k P^{(k)}$ tách được trên $\mathbb{R}$.

5.4 Phân thức hữu tỷ

5.4.1 Thể $K(X)$

1) Tập hợp $K(X)$

Ta ký hiệu $E = K[X] \times (K[X] - \{0\})$ và xét quan hệ $\mathcal{R}$ xác định trong E bởi:

$$(A, S)\ \mathcal{R}\ (B, T) \Leftrightarrow AT = BS.$$

Quan hệ $\mathcal{R}$ là một quan hệ tương đương trong E.

Thật vậy, tính phản xạ và tính đối xứng là hiển nhiên, còn về tính bắc cầu thì với mọi (A, S), (B, T), (C, U) thuộc E:

$$\begin{cases}(A,S)\,\mathcal{R}\,(B,T)\\(B,T)\,\mathcal{R}\,(C,U)\end{cases} \Leftrightarrow \begin{cases}AT = BS\\BU = CT\end{cases}$$

$\Rightarrow (AU)T = (AT)U = (BS)U = (BU)S = (CT)S = (CS)T \Rightarrow AU = CS$, vì $T \neq 0$ và $K[X]$ là vành nguyên. ■

Tập thương $E/\mathcal{R}$ được ký hiệu là $K(X)$ và các phần tử của nó được gọi là các **phân thức hữu tỷ một ẩn và lấy hệ tử trong** K. Với $(A, S) \in E$, ta ký hiệu $\dfrac{A}{S}$ là lớp modulo $\mathcal{R}$ của (A, S). Như thế, với mọi (A, S), (B, T) thuộc E, ta có:

$$\frac{A}{S} = \frac{B}{T} \Leftrightarrow AT = BS\,.$$

2) Phép cộng trong $K(X)$

Ta định nghĩa một luật trong, ký hiệu +, trong E bởi:

$$(A, S) + (B, T) = (AT + BS, ST)$$

(ta có $ST \neq 0$, vì $S \neq 0$ và $T \neq 0$).

Luật + này tương thích với $\mathcal{R}$ (C.1.1), tức là:

$\forall (A, S), (B, T), (C, U) \in E,\ (A, S)\ \mathcal{R}\ (B, T) \Rightarrow ((A, S) + (C, U))\ \mathcal{R}\ ((B, T) + (C, U))$.

Thật vậy, nếu $(A, S)\ \mathcal{R}\ (B, T)$, thì $AT = BS$, từ đây:

$$(AU + CS)TU = ATU^2 + CSTU = BSU^2 + CSTU = (BU + CT)SU,$$

vậy $(AU + CS, SU)\ \mathcal{R}\ (BU + CT, TU)$, ■

tức là: $((A, S) + (C, U))\ \mathcal{R}\ ((B, T) + (C, U))$.

Vậy ta có thể định nghĩa một luật, vẫn ký hiệu là +, trong $K(X)$ bởi:

$$\forall (A,S),(B,T) \in E,\quad \frac{A}{S} + \frac{B}{T} = \frac{AT + BS}{ST}\,.$$

3) Phép nhân trong $K(X)$

Tương tự như ở 2), ta chứng minh rằng ta có thể định nghĩa một luật trong trong $K(X)$, ký hiệu $\cdot$ (hoặc bằng cách không viết dấu nào cả) bởi:

$$\forall (A,S),(B,T) \in E, \quad \frac{A}{S} \cdot \frac{B}{T} = \frac{AB}{ST}.$$

♦ **Định lý - Định nghĩa**

$(K(X), +, \cdot)$ là một thể giao hoán, gọi là **thể các phân thức hữu tỷ một ẩn và lấy hệ tử trong** K.

Chứng minh:

Độc giả có thể chứng minh dễ dàng các tính chất sau:

a) + kết hợp, giao hoán, có $\frac{0}{1}$ (ký hiệu 0) là phần tử trung hòa, và mọi phần tử $\frac{A}{S}$ thuộc $K(X)$ đều có một phần tử đối là $\frac{-A}{S}$, ký hiệu là $-\frac{A}{S}$.

b) $\cdot$ kết hợp, giao hoán, phân phối đối với +, có $\frac{1}{1}$ (ký hiệu 1) là phần tử trung hòa, và với mọi phần tử $\frac{A}{S}$ thuộc $K(X) - \{0\}$, ta có $A \neq 0$ và $\frac{A}{S}$ có một phần tử nghịch đảo, đó là $\frac{S}{A}$.

4) Luật ngoài trong $K(X)$

Tương tự như ở 2) ta chứng minh rằng ta có thể định nghĩa một luật ngoài trong $K(X)$ (lấy hệ tử trong K), được ký hiệu bằng cách không viết dấu nào cả:

$$\forall \lambda \in K, \forall (A,S) \in E, \quad \lambda \frac{A}{S} = \frac{\lambda A}{S}.$$

♦ **Mệnh đề**

$(K(X), +, \ , \cdot)$ là một K-đại số kết hợp, giao hoán, có đơn vị.

Chứng minh:

Độc giả có thể chứng minh dễ dàng các tính chất sau (trong đó một số đã thu được ở 3)):

a) $(K(X), +)$ là một nhóm Abel.

b) $(K(X), +, \ )$ là một K- không gian vectơ.

c) $\forall \lambda \in K, \forall F, G \in K(X), (\lambda F)G = \lambda (FG)$.

d) $\cdot$ kết hợp, giao hoán, có phần tử trung hòa (1).

5) Nhúng $K[X]$ vào $K(X)$

Ánh xạ $\Psi : K[X] \to K(X)$ là một đồng cấu đơn ánh (đơn cấu) đại số, tức là:

$$P \mapsto \frac{P}{1}$$

- $\forall P, Q \in K[X], \quad \Psi(P + Q) = \Psi(P) + \Psi(Q)$
- $\forall P, Q \in K[X], \quad \Psi(PQ) = \Psi(P)\Psi(Q)$
- $\forall \lambda \in K, \forall P \in K[X], \quad \Psi(\lambda P) = \lambda \Psi(P)$
- $\Psi(1) = 1$
- $\forall P \in K[X], \quad (\Psi(P) = 0 \Rightarrow P = 0)$.

Vậy ta có thể đồng nhất một đa thức P với phân thức hữu tỷ $\frac{P}{1}$. Như thế, $K[X]$ được xem như là một đại số con có đơn vị của $K(X)$; đặc biệt, $K[X]$ là một vành con của thể $K(X)$, và $K[X]$ là là một không gian vectơ con của K- không gian vectơ $K(X)$.

6) Bậc của một phân thức hữu tỷ

Với mọi (A,S), (B,T) thuộc E sao cho $\frac{A}{S} = \frac{B}{T}$, ta có:

$$\deg(A) - \deg(S) = \deg(AT) - \deg(ST) = \deg(BS) - \deg(ST) = \deg(B) - \deg(T).$$

Điều này cho phép ta định nghĩa **bậc của một phân thức hữu tỷ** bởi:

$$\forall (A,S) \in E, \quad \deg\left(\frac{A}{S}\right) = \deg(A) - \deg(S) \in \{-\infty\} \cup \mathbb{Z}.$$

Ta chú ý rằng ánh xạ deg: $K(X) \to \{-\infty\} \cup \mathbb{Z}$ thác triển ánh xạ:

deg: $K[X] \to \{-\infty\} \cup \mathbb{N}$ (định nghĩa ở 5.1.1, Định nghĩa 2) vì:

$$\forall P \in K[X], \quad \deg\left(\frac{P}{1}\right) = \deg(P) - \deg(1) = \deg(P).$$

Độc giả có thể chứng minh, xem như bài tập, các công thức sau, với mọi k thuộc K^* và mọi F,G thuộc $K(X)$:

1) $\deg(F + G) \leq \text{Max}(\deg(F), \deg(G))$.

2) $\deg(kF) = \deg(F)$

3) $\deg(FG) = \deg(F) + \deg(G)$.

7) Dạng bất khả quy của một phân thức hữu tỷ khác không

Phương pháp tiến hành tương tự như trong 4.3.4. 2).

Đại diện bất khả quy của một phân thức hữu tỷ khác không F thuộc $K(X)$ là cặp (A,S) bất kỳ thuộc $(K[X] - \{0\})^2$ sao cho:

$$F = \frac{A}{S} \quad \text{và} \quad A \wedge S = 1.$$

Lập luận tương tự như trong 4.3.4, 2) ta chứng minh được:

a) Mọi phân thức hữu tỷ khác không có ít nhất một đại diện bất khả quy.

b) Cho $F \in K(X)$ và (A,S) là một đại diện bất khả quy của F; mọi đại diện của F đều có dạng (QA,QS), $Q \in K[X] - \{0\}$.

c) Cho $F \in K(X)$ và (A,S) là một đại diện bất khả quy của F; các đại diện bất khả quy của F là các (kA, kS), $k \in K - \{0\}$.

8) Không điểm và cực điểm của một phân thức hữu tỷ

♦ **Định nghĩa** Cho $F \in K(X) - \{0\}$, (A, S) là một đại diện bất khả quy của F.

1) Các không điểm của A được gọi là **không điểm** của F. Nếu a là một không điểm của F, cấp bội của a với tư cách là không điểm của A gọi là **cấp bội của không điểm a của F**.

2) Các không điểm của S được gọi là **cực điểm** của F. Nếu a là một cực điểm của F, cấp bội của a với tư cách là không điểm của S gọi là **cấp bội của cực điểm a của F**.

VÍ DỤ:

Với $F = \dfrac{X^4 - X^2}{X^2 - 3X + 2} \in \mathbb{R}(X)$, dạng bất khả quy của F là $F = \dfrac{X^2(X+1)}{X-2}$, các không điểm của F là -1 (đơn), 0 (kép), và F chỉ có một cực điểm: 2 (đơn).

9) Đạo hàm một phân thức hữu tỷ

Cho $F \in K(X)$, $(A,S) \in E$ sao cho $F = \dfrac{A}{S}$.

Ta định nghĩa **phân thức hữu tỷ đạo hàm** của F, ký hiệu F' bởi: $F' = \dfrac{A'S - AS'}{S^2}$.

Định nghĩa này hợp lệ vì nếu (A,S), (B,T) là hai phần tử của E sao cho $F = \dfrac{A}{S} = \dfrac{B}{T}$, thì $AT = BS$, do đó $A'T + AT' = B'S + BS'$, vậy:

$$\begin{aligned}(A'S - AS')T^2 - (B'T - BT')S^2 &= (A'T - B'S)ST - AS'T^2 + BT'S^2\\ &= (BS' - AT')ST - AS'T^2 + BT'S^2\\ &= (BS - AT)(S'T + ST') = 0.\end{aligned}$$ ■

Ánh xạ $K(X) \to K(X)$ thác triển ánh xạ $K[X] \to K[X]$ vì:

$$F \mapsto F' \qquad\qquad P \mapsto P'$$

$$\forall P \in K[X], \quad \left(\frac{P}{1}\right)' = \frac{P'1 - P.0}{1^2} = P'.$$

Độc giả có thể chứng minh dễ dàng các công thức sau, với mọi λ thuộc K và mọi F, G thuộc $K(X)$:

$$(F+G)' = F' + G', \quad (\lambda F)' = \lambda F',$$
$$(FG)' = F'G + FG', \quad \left(\frac{F}{G}\right)' = \frac{F'G - FG'}{G^2} \text{ (nếu } G \neq 0). \quad \blacksquare$$

Có thể xảy ra là $\deg(F') \neq \deg(F)-1$, như trong các ví dụ sau:

- $F = 1, F' = 0$: $\deg(F) = 0, \deg(F') = -\infty$.
- $F = \dfrac{X+1}{X}, F' = -\dfrac{1}{X^2}$: $\deg(F) = 0, \deg(F') = -2$

Tuy nhiên ta có thể chú ý rằng: $\forall F \in K(X) - \{0\}$, $\deg(F') < \deg(F)$. $\blacksquare$

Ta định nghĩa bằng quy nạp các **đạo hàm kế tiếp của một phân thức hữu tỷ** F:

$$\begin{cases} F^{(0)} = F, \quad F^{(1)} = F' \\ \forall n \in \mathbb{N}^*, \ F^{(n)} = (F^{(n-1)})'. \end{cases}$$

Độc giả có thể chứng minh các công thức sau:

- $\forall F \in K(X), \forall (i,j) \in \mathbb{N}^2, \quad (F^{(i)})^{(j)} = F^{(i+j)}$.
- $\forall n \in \mathbb{N}, \forall (F,G) \in (K(X))^2, \ (FG)^{(n)} = \sum_{k=0}^{n} C_n^k F^{(k)} G^{(n-k)}$ **(công thức Leibniz).**

♦ **Mệnh đề** Cho $P \in K[X]$, tách được: $P = \lambda \prod_{i=1}^{n} (X - x_i), \lambda \in K - \{0\}$, $n \in \mathbb{N}^*, x_1, \ldots, x_n \in K$. Ta có:

$$\frac{P'}{P} = \sum_{i=1}^{n} \frac{1}{X - x_i}.$$

Chứng minh:

Suy ra từ $P' = \lambda \sum_{i=1}^{n} \left(\prod_{\substack{1 \leq j \leq n \\ j \neq i}} (X - x_j) \right)$ bằng cách chia cho P.

10) Hàm hữu tỷ

♦ **Định nghĩa** Cho $F \in K(X)$, (A,S) là một đại diện bất khả quy của F. Hàm từ K vào K, ký hiệu $\tilde{F}$, được xác định bởi: $\tilde{F}(x) = \dfrac{\tilde{A}(x)}{\tilde{S}(x)}$, với mọi x thuộc K sao cho $\tilde{S}(x) \neq 0$, được gọi là **hàm hữu tỷ liên kết với** F.

Định nghĩa này hợp lệ, vì các đại diện bất khả quy của F là các (kA, kS), $k \in K$-$\{0\}$ (xem 7)).

Với các ký hiệu trên, tập xác định của $\tilde{F}$ là K bớt đi các cực điểm của F.

VÍ DỤ: $K = \mathbb{R}$, $F = \dfrac{X^3 - 2X^2 + X}{X^2 + X}$.

Dưới dạng bất khả quy: $F = \dfrac{X^2 - 2X + 1}{X + 1}$, vậy $\tilde{F} : \mathbb{R} - \{1\} \to \mathbb{R}$, $x \mapsto \dfrac{(x-1)^2}{x+1}$.

Mọi hàm f từ K vào K sao cho tồn tại một phân thức hữu tỷ F của $K(X)$ mà $f = \tilde{F}$ được gọi là **hàm hữu tỷ** (trong K).

VÍ DỤ:

$f : \mathbb{C}^* \to \mathbb{C}$, $z \mapsto \dfrac{1}{z^2}$ là một hàm hữu tỷ, đó là hàm hữu tỷ liên kết với phân thức hữu tỷ $\dfrac{1}{X^2}$.

Bài tập

◊ **5.4.1** Cho $n \in \mathbb{N} - \{0, 1\}$, $P_n = \sum_{k=0}^{n-1} (k+1)X^k$.

Chứng minh rằng phương trình $P_n(x) = n^n$, ẩn $x \in \mathbb{C}$, có ít nhất một nghiệm trong $]1 ; 2[\cap \mathbb{R}$.

◊ **5.4.2** Chứng minh rằng không tồn tại F thuộc $K(X)$ sao cho $F^2 = X$.

◊ **5.4.3** Cho $P \in \mathbb{R}[X]$, có bậc $n \in \mathbb{N}^*$, sao cho: $P(-1) \neq 0$ và $-\dfrac{P'(-1)}{P(-1)} \leq \dfrac{n}{2}$. Chứng minh rằng P có ít nhất một không điểm với modun ≥ 1.

5.4.2 Phân tích thành phân thức đơn giản

1) Khảo sát lý thuyết

Độc giả có thể bỏ qua phần khảo sát lý thuyết này và thừa nhận kết quả về sự tồn tại và tính duy nhất của phép phân tích một phân tích hữu tỷ (Định lý) thành phân thức đơn giản.

Mục đích của §1 này là phân tích một phân thức hữu tỷ thành một tổng các phân thức hữu tỷ "đơn giản hơn", nhằm cùng với các phép tính khác, tính các nguyên hàm của phân thức hữu tỷ này (Tập 2, 9.5) và để tìm phân tích thành chuỗi nguyên của phân thức hữu tỷ này (khi nó không có cực điểm là số 0; xem Tập 4, 5.5.2, Mệnh đề 4).

♦ **Bổ đề 1** Cho $F \in K(X)$, $(A,S) \in K[X] \times (K[X] - \{0\})$ sao cho : $F = \dfrac{A}{S}$.

Tồn tại một cặp duy nhất (E,R) thuộc $(K[X])^2$ sao cho:

$$F = E + \frac{R}{S} \quad \text{và} \quad \deg(R) < \deg(S).$$

Hơn nữa, nếu $A \wedge S = 1$, thì $R \wedge S = 1$.

Đa thức E được gọi là **phần nguyên** của F; phân thức hữu tỷ $\dfrac{R}{S}$ đôi khi được gọi là **phần phân thức** của F.

Chứng minh:

1) Tồn tại

Theo phép chia Euclide A cho S, tồn tại $(E,R) \in (K[X])^2$ sao cho:

$A = SE + R$ và $\deg(R) < \deg(S)$, từ đó thu được kết quả cần chứng minh.

Hơn nữa, theo thuật toán Euclide, nếu $A \wedge S = 1$ thì $R \wedge S = 1$.

2) Duy nhất

Giả sử (E_1,R_1), (E_2,R_2) thích hợp. Thế thì $E_1 - E_2 = \dfrac{R_2 - R_1}{S}$, vậy:

$$\deg(E_1 - E_2) = (R_1 - R_2) - \deg(S) < 0,$$

do đó $E_1 - E_2 = 0$, $E_1 = E_2$, $R_1 = R_2$.

VÍ DỤ:

Với $K = \mathbb{R}$, $F = \dfrac{X^4 + X^3 - 2X^2 + X - 1}{X^3 - 3X^2 + 1}$, nhờ phép chia Euclide $X^4 + X^3 - 2X^2 + X - 1$ cho $X^3 - 3X^2 + 1$, ta được: $F = X + 4 + \dfrac{10X^2 - 5}{X^3 - 3X^2 + 1}$.

♦ **Bổ đề 2** Cho $A \in K[X]$, $n \in \mathbb{N}^*$, $S_1, ..., S_n \in K[X] - \{0\}$ sao cho $S_1, ..., S_n$ nguyên tố cùng nhau từng đôi.

Thế thì tồn tại $A_1, ..., A_n \in K[X]$ sao cho: $\dfrac{A}{S_1 ... S_n} = \dfrac{A_1}{S_1} + \cdots + \dfrac{A_n}{S_n}$.

Chứng minh:

Quy nạp theo n.

- Tính chất là tầm thường với $n = 1$.
- Trường hợp $n = 2$

Theo định lý Bezout, vì $S_1 \wedge S_2 = 1$, nên tồn tại $(U_1,U_2) \in (K[X])^2$ sao cho $S_1U_1 + S_2U_2 = 1$. Vậy ta có: $\dfrac{A}{S_1S_2} = \dfrac{A(S_1U_1 + S_2U_2)}{S_1S_2} = \dfrac{AU_2}{S_1} + \dfrac{AU_1}{S_2}$.

- Giả sử tính chất đúng với một n thuộc $\mathbb{N}^*$, và giả sử $S_1, ..., S_{n+1} \in K[X] - \{0\}$ nguyên tố cùng nhau từng đôi. Theo 5.2.4, 3), Mệnh đề 1, lúc đó ta có:

$$(S_1 ... S_n) \wedge S_{n+1} = 1.$$

Theo khảo sát trường hợp $n = 2$, tồn tại $C_1, A_{n+1} \in K[X]$ sao cho:

$$\frac{A}{S_1 ... S_n S_{n+1}} = \frac{C_1}{S_1 ... S_n} + \frac{A_{n+1}}{S_{n+1}}.$$

Rồi theo giả thiết quy nạp, tồn tại $A_1, ..., A_n \in K[X]$ sao cho:

$$\frac{C_1}{S_1 ... S_n} = \frac{A_1}{S_1} + \cdots + \frac{A_n}{S_n},$$

cuối cùng ta được: $\dfrac{A}{S_1 ... S_{n+1}} = \dfrac{A_1}{S_1} + \cdots + \dfrac{A_{n+1}}{S_{n+1}}$. ■

Bây giờ ta sẽ kết hợp các bổ đề 1 và 2 để thu được kết quả sau đây.

♦ **Bổ đề 3** Cho $A \in K[X]$, $n \in \mathbb{N}^*$, $S_1, ..., S_n \in K[X] - \{0\}$ sao cho $S_1, ..., S_{n+1}$ nguyên tố cùng nhau từng đôi. Tồn tại $(E, R_1, ..., R_n) \in (K[X])^{n+1}$ duy nhất sao cho:

$$\begin{cases} \dfrac{A}{S_1...S_n} = E + \dfrac{R_1}{S_1} + \cdots + \dfrac{R_n}{S_n}. \\ \forall i \in \{1,...,n\},\ \deg(R_i) < \deg(S_i) \end{cases}$$

Hơn nữa, E là phần nguyên của $\dfrac{A}{S_1...S_n}$.

Chứng minh:

1) Tồn tại

Theo Bổ đề 2, tồn tại $A_1, ..., A_n \in K[X]$ sao cho:

$$\frac{A}{S_1 \ldots S_n} = \frac{A_1}{S_1} + \ldots + \frac{A_n}{S_n}.$$

Rồi theo Bổ đề 1, tồn tại $E_1, ..., E_n, R_1, ...R_n \in K[X]$ sao cho:

$$\forall i \in \{1, ..., n\},\ \begin{cases} \dfrac{A_i}{S_i} = E_i + \dfrac{R_i}{S_i} \\ \deg(R_i) < \deg(S_i) \end{cases}$$

Ký hiệu $E = E_1 + ... + E_n$, ta được kết quả mong muốn.

2) Duy nhất

Quy nạp theo n

- Trường hợp $n = 1$ thì ta đã thấy (Bổ đề 1).
- Trường hợp $n = 2$

Giả sử (E, R_1, R_2), (D, P_1, P_2) thích hợp, tức là:

$$\begin{cases} \dfrac{A}{S_1S_2} = E + \dfrac{R_1}{S_1} + \dfrac{R_2}{S_2} = D + \dfrac{P_1}{S_1} + \dfrac{P_2}{S_2} \\ \forall i \in \{1, 2\},\ \begin{cases} \deg(R_i) < \deg(S_i) \\ \deg(P_i) < \deg(S_i) \end{cases} \end{cases}$$

Vậy ta có: $S_1(R_2 - P_2) = S_1S_2(D - E) + S_2(P_1 - R_1)$, nên: $S_1 \mid S_2(P_1 - R_1)$.

Vì $S_1 \wedge S_2 = 1$, định lý Gauss chứng tỏ rằng $S_1 \mid P_1 - R_1$.

Nhưng mặt khác: $\deg(P_1 - R_1) < \deg(S_1)$.

Ta suy ra $P_1 - R_1 = 0$, $P_1 = R_1$, rồi cũng tương tự $P_2 = R_2$ và cuối cùng $D = E$.

- Giả thiết tính chất đúng với một n thuộc $\mathbb{N}^*$.

Giả sử $E, R_1,...,R_{n+1}, D, P_1,..., P_{n+1} \in K[X]$ thỏa mãn:

$$\begin{cases} \dfrac{A}{S_1...S_{n+1}} = E + \displaystyle\sum_{i=1}^{n+1} \frac{R_i}{S_i} = D + \sum_{i=1}^{n+1} \frac{P_i}{S_i} \\ \forall i \in \{1,...,n+1\},\ \begin{cases} \deg(R_i) < \deg(S_i) \\ \deg(P_i) < \deg(S_i) \end{cases} \end{cases}.$$

Ký hiệu $T = S_1 \ldots S_n$, $B = \sum_{i=1}^{n} \left(R_i \left(\prod_{\substack{i \le j \le n \\ j \ne i}} S_j \right) \right)$, $C = \sum_{i=1}^{n} \left(P_i \left(\prod_{\substack{i \le j \le n \\ j \ne i}} S_j \right) \right)$,

ta có: $\begin{cases} T \wedge S_{n+1} = 1 \\ \dfrac{A}{TS_{n+1}} = E + \dfrac{B}{T} + \dfrac{R_{n+1}}{S_{n+1}} = D + \dfrac{C}{T} + \dfrac{P_{n+1}}{S_{n+1}} \end{cases}$.

Từ sự khảo sát trường hợp $n = 2$, ta suy ra:

$$D = E,\ C = B,\ P_{n+1} = R_{n+1}.$$

Như vậy: $\begin{cases} \sum_{i=1}^{n} \dfrac{R_i}{S_i} = \sum_{i=1}^{n} \dfrac{P_i}{S_i} \\ \forall i \in \{1,\ldots,n\},\ \begin{cases} \deg(R_i) < \deg(S_i) \\ \deg(P_i) < \deg(S_i) \end{cases} \end{cases}$

do đó, theo giả thiết quy nạp: $P_1 = R_1, \ldots, P_n = R_n$.

3) Với các ký hiệu của Bổ đề, vì:

$$\deg\left(\frac{R_1}{S_1} + \cdots + \frac{R_n}{S_n} \right) \le \operatorname{Max}\left(\left(\deg\left(\frac{R_i}{S_i} \right) \right)_{1 \le i \le n} \right) < 0,$$

nên theo Bổ đề 1, E là phần nguyên của $\dfrac{A}{S_1 \ldots S_n}$.

♦ **Bổ đề 4** Cho $A \in K[X]$, $S \in K[X]$ sao cho $\deg(S) \ge 1$, $\alpha \in \mathbb{N}^*$.

Tồn tại $(E, C_1, \ldots, C_\alpha) \in K[X]^{\alpha+1}$ duy nhất sao cho:

$$\begin{cases} \dfrac{A}{S^\alpha} = E + \dfrac{C_\alpha}{S^\alpha} + \dfrac{C_{\alpha-1}}{S^{\alpha-1}} + \cdots + \dfrac{C_1}{S} \\ \forall j \in \{1,\ldots,\alpha\},\ \deg(C_j) < \deg(S). \end{cases}$$

Hơn nữa, E là phần nguyên của $\dfrac{A}{S^\alpha}$.

Chứng minh:

1) **Tồn tại**

Quy nạp theo α

- Trường hợp $\alpha = 1$ thì ta thấy (Bổ đề 1).
- Giả sử tính chất đúng với một α thuộc $\mathbb{N}^*$; vậy tồn tại $E_1, C_2, \ldots, C_{\alpha+1} \in K[X]$ sao cho:

$$\begin{cases} \dfrac{A}{S^\alpha} = E_1 + \dfrac{C_{\alpha+1}}{S^\alpha} + \cdots + \dfrac{C_2}{S} \\ \forall j \in \{1,\ldots,\alpha\},\ \deg(C_{j+1}) < \deg(S) \end{cases}$$

Theo Bổ đề 1, tồn tại $E, C_1 \in K[X]$ sao cho:

$$\frac{E_1}{S} = E + \frac{C_1}{S} \quad \text{và} \quad \deg(C_1) < \deg(S).$$

Vậy ta có:

$$\begin{cases} \dfrac{A}{S^{\alpha+1}} = \dfrac{A}{S^{\alpha}.S} = E_1 + \dfrac{C_{\alpha+1}}{S^{\alpha+1}} + \cdots + \dfrac{C_1}{S} \\ \forall j \in \{1,\ldots,\alpha+1\}, \quad \deg(C_j) < \deg(S). \end{cases}$$

2) Duy nhất

Quy nạp theo α

- Trường hợp $\alpha = 1$ thì ta đã thấy (xem Bổ đề 1).
- Giả thiết tính chất đúng với một α thuộc $\mathbb{N}^*$.

Giả sử $E_1, C_1, \ldots, C_{\alpha+1}, E_2, D_1, \ldots, D_{\alpha+1} \in K[X]$ sao cho:

$$\begin{cases} \dfrac{A}{S^{\alpha+1}} = E_1 + \dfrac{C_{\alpha+1}}{S^{\alpha+1}} + \cdots + \dfrac{C_1}{S} = E_2 + \dfrac{D_{\alpha+1}}{S^{\alpha+1}} + \cdots + \dfrac{D_1}{S} \\ \forall j \in \{1,\ldots,\alpha+1\}, \begin{cases} \deg(C_j) < \deg(S) \\ \deg(D_j) < \deg(S) \end{cases} \end{cases}$$

Nhân với S^{α}, ta được:

$$\begin{aligned} \frac{A}{S} &= \left(E_1 S^{\alpha} + C_{\alpha} + C_{\alpha-1} S + \cdots + C_1 S^{\alpha-1}\right) + \frac{C_{\alpha+1}}{S} \\ &= \left(E_2 S^{\alpha} + D_{\alpha} + D_{\alpha-1} S + \cdots + D_1 S^{\alpha-1}\right) + \frac{D_{\alpha+1}}{S}. \end{aligned}$$

Theo Bổ đề 1, ta suy ra $D_{\alpha+1} = C_{\alpha+1}$, rồi áp dụng giả thiết quy nạp:

$$D_{\alpha} = C_{\alpha}, \ldots, \quad D_1 = C_1, \quad E_2 = E_1.$$

3) Với các ký hiệu của Bổ đề, vì

$$\deg\left(\frac{C_{\alpha}}{S^{\alpha}} + \cdots + \frac{C_1}{S}\right) \le \operatorname{Max}\left(\left(\deg\left(\frac{C_j}{S_j}\right)\right)_{1 \le j \le \alpha}\right) < 0,$$

nên theo Bổ đề 1, E là phần nguyên của $\dfrac{A}{S^{\alpha}}$.

♦ **Định nghĩa** Các **phân thức đơn giản** của $K(X)$ là :

- Các đơn thức của $K[X]$
- Các phần tử của $K(X)$ có dạng $\dfrac{C}{S^{\alpha}}$ trong đó:

$$\begin{cases} S \in K[X], \deg(S) \ge 1, S \text{ là bất khả quy} \\ \alpha \in \mathbb{N}^* \\ C \in K[X] - \{0\} \\ \deg(C) < \deg(S) \end{cases}$$

Các phần tử đơn giản có dạng $\dfrac{c}{S^{\alpha}}$ trong đó ($S \in K[X]$, $\deg(S) = 1$, $\alpha \in \mathbb{N}^*$, $c \in K - \{0\}$) được gọi là các **phân thức đơn giản loại 1**.

Từ các bổ đề trên, ta suy ra định lý sau.

♦ **Định lý (Sự tồn tại và tính duy nhất của phép phân tích một phân thức hữu tỷ thành phân thức đơn giản)**

Cho $F = \dfrac{A}{S_1^{\alpha_1} ... S_n^{\alpha_n}}$ trong đó:

$n \in \mathbb{N}^*$

$S_1, ..., S_n \in K[X] - \{0\}$ bất khả quy và nguyên tố cùng nhau từng đôi một

$\alpha_1, ..., \alpha_n \in \mathbb{N}^*$

$A \in K[X]$.

Tồn tại một họ duy nhất các đa thức $(E, C_{\alpha 1,1},...,C_{\alpha 1,\alpha 1}, C_{\alpha 2,1},...,C_{\alpha 2,\alpha 2},..., C_{\alpha n,1},...,C_{\alpha n,\alpha n})$ thuộc $K[X]$ sao cho:

$$\begin{cases} F = E + \sum_{i=1}^{n} \sum_{j=1}^{\alpha_i} \dfrac{C_{\alpha_{i,j}}}{S_i^j} \\ \forall i \in \{1,...,n\},\ \forall j \in \{1,.....\alpha_i\},\ \deg(C_{\alpha_{i,j}}) < \deg(S_i). \end{cases}$$

Công thức trên được gọi là **phân tích thành phân thức đơn giản** (viết tắt: **PTĐG**) **của phân thức hữu tỷ** F.

2) Thực hành phép phân tích thành phân thức đơn giản (PTĐG)

a) Trường hợp cực điểm đơn

Cho $(A,S) \in K[X] \times (K[X] - \{0\})$, $F = \dfrac{A}{S}$, a là một không điểm của S.

Giả sử rằng a là một không điểm đơn của S. Thế thì tồn tại $S_1 \in K[X]$ sao cho:

$$S = (X - a)S_1 \quad \text{và} \quad \tilde{S}_1(a) \neq 0.$$

PTĐG của F chứa hạng tử $\dfrac{\lambda}{X - a}$ ($\lambda \in K$), trong đó ta tìm cách tính λ.

Theo Bổ đề 2, tồn tại $A_1 \in K[X]$ sao cho: $F = \dfrac{A}{S} = \dfrac{\lambda}{X - a} + \dfrac{A_1}{S_1}$.

Vậy ta có: $A = \lambda S_1 - (X - a)A_1$, từ đây, thay X bởi a: $\tilde{A}(a) = \lambda \tilde{S}_1(a)$.

Vậy: $\lambda = \dfrac{\tilde{A}(a)}{\tilde{S}_1(a)} = \widetilde{((X - a)F)}(a)$

Tóm lại:

♦ **Mệnh đề 1** Cho $(A,S) \in K[X] \times (K[X] - \{0\})$, $F = \dfrac{A}{S}$, a là một không điểm đơn của S. Hệ tử λ của hạng tử $\dfrac{\lambda}{X - a}$ trong PTĐG của F là $\widetilde{((X - a)F)}(a)$.

Nói khác đi, ta được λ bằng cách *nhân hai vế của đẳng thức* $F = \dfrac{A}{S}$ *với* $A - a$, rồi *thay* X bởi a.

VÍ DỤ:

PTĐG của $F = \dfrac{X}{(X-1)(X-2)}$ trong $\mathbb{R}(X)$.

Phần nguyên bằng 0, vậy PTĐG có dạng $F = \dfrac{\lambda}{X-1} + \dfrac{\mu}{X-2}$, $(\lambda, \mu) \in \mathbb{R}^2$

Theo Mệnh đề 1: $\lambda = \widetilde{((X-1)F)}(1) = \left(\widetilde{\dfrac{X}{X-2}}\right)(1) = -1$

$$\mu = \widetilde{((X-2)F)}(2) = \left(\widetilde{\frac{X}{X-1}}\right)(2) = 2.$$

Vậy: $F = \dfrac{-1}{X-1} + \dfrac{2}{X-2}$, mà ta có thể kiểm tra lại dễ dàng bằng cách quy đồng về mẫu số chung. ■

Trong một số trường hợp, với các ký hiệu của Mệnh đề 1 việc tính $\widetilde{((X-a)F)}(a)$ có thể cho những kết quả xem ra phức tạp hoặc không thể sử dụng được.

Vì $S = (X-a)S_1$, nên khi đạo hàm hai vế , ta được:

$$S' = (X-a)S'_1 + S_1, \quad \text{từ đây } \tilde{S}'(a) = \tilde{S}_1(a)$$

Vậy ta đã chứng minh Mệnh đề sau:

♦ **Mệnh đề** Cho $(A,S) \in K[X] \times (K[X] - \{0\})$, $F = \dfrac{A}{S}$, a là một không điểm đơn của S. Hệ tử λ của hạng tử $\dfrac{\lambda}{X-a}$ trong PTĐG của $\dfrac{A}{S}$ là $\dfrac{\tilde{A}(a)}{\tilde{S}(a)}$.

VÍ DỤ:

Với $n \in \mathbb{N}^*$ tìm PTĐG của $F = \dfrac{1}{X^n - 1}$ trong $\mathbb{C}(X)$.

Ta có phân tích nguyên tố của $X^n - 1$ (trong $\mathbb{C}[X]$) là: $X^n - 1 = \prod_{K=0}^{n-1} (X - \omega_k)$, trong đó: $\omega_k = \exp\left(\dfrac{2ik\pi}{n}\right)$, $0 \le k \le n-1$.

Các không điểm của $X^n - 1$ đều toàn đơn, vậy PTĐG của F có dạng:

$$F = \sum_{k=0}^{n-1} \frac{\lambda_k}{X - \omega_k}, \text{ trong đó } \lambda_k \in \mathbb{C},\ 0 \le k \le n-1.$$

Theo Mệnh đề 2, với mọi k thuộc $\{0, ..., n-1\}$:

$$\lambda_k = \left(\widetilde{\frac{1}{nX^{n-1}}}\right)(\omega_k) = \frac{1}{n\omega_k^{n-1}} = \frac{\omega_k}{n}.$$

Do có PTĐG: $\dfrac{1}{X^n - 1} = \sum_{k=0}^{n-1} \dfrac{\frac{\omega_k}{n}}{X - \omega_k}$.

Ở đây nếu áp dụng Mệnh đề 1 sẽ được: $\lambda_k = \dfrac{1}{\prod\limits_{\substack{0\le j\le n-1\\ j\ne k}} (\omega_k - \omega_j)}$.

kết quả này đúng, nhưng thoáng nhìn thì thấy là không sử dụng được.

b) Trường hợp cực điểm bội

1) Trường hợp cực điểm 0

Ta hãy quan tâm đến một phân thức hữu tỷ $F = \dfrac{A}{X^n T}$, trong đó $A, T \in K[X]$, $\tilde{T}(0) \neq 0$.

Theo định lý về phép phân tích thành phân thức đơn giản, tồn tại $\alpha_1, ..., \alpha_n \in K$, $B \in K[X]$ sao cho: $F = \dfrac{\alpha_n}{X^n} + ... + \dfrac{\alpha_1}{X} + \dfrac{B}{T}$.

Vậy ta có: $A = (\alpha_n + \alpha_{n-1}X + ... + \alpha_1 X^{n-1})T + X^n B$.

Theo định lý về phép chia theo lũy thừa tăng (xem 5.2.6), $\alpha_n + \alpha_{n-1}X + ... + \alpha_1 X^{n-1}$ là **thương của phép chia A cho T theo lũy thừa tăng đến cấp n - 1** (và B là dư của phép chia).

VÍ DỤ:

Lập PTĐG của $F = \dfrac{X^5 + 1}{X^3(X-2)}$ trong $\mathbb{R}(X)$.

PTĐG của F có dạng: $F = E + \dfrac{\alpha_3}{X^3} + \dfrac{\alpha_2}{X^2} + \dfrac{\alpha_1}{X} + \dfrac{\lambda}{X-2}$,

trong đó E là phần nguyên của F và $\alpha_3, \alpha_2, \alpha_1, \lambda \in \mathbb{R}$.

- Ta tính E xem như thương của phép chia Euclide X^5+1 cho $X^4 - 2X^3$; ta được: $E = X + 2$.
- Ta tính λ bằng cách nhân và thay thế:

$$\lambda = ((X - 2)F)(2) = \left(\frac{X^5 - 1}{X^3}\right)(2) = \frac{33}{8}.$$

- Ta tính $\alpha_3, \alpha_2, \alpha_1$ bằng phép chia $1 + X^5$ cho $-2 + X$ theo lũy thừa tăng đến cấp 2:

$$\begin{array}{rl|l} 1 & +X^5 & -2+X \\ \hline \frac{1}{2}X & +X^5 & -\frac{1}{2}-\frac{1}{4}X-\frac{1}{8}X^2 \\ \frac{1}{4}X^2 & +X^5 & \\ \frac{1}{8}X^3 & +X^5 & \end{array}$$

Ta được: $\alpha_3 = \dfrac{1}{2}$, $\alpha_2 = -\dfrac{1}{4}$, $\alpha_1 = -\dfrac{1}{8}$.

Ta có thể chú ý rằng trong phép chia này, không có các hạng tử có bậc ≥ 3 tham gia vào. Vậy trong thực hành ta có thể sử dụng một phép chia "chặt cụt":

$$\begin{array}{l|l} 1 & -2+X \\ \hline \frac{1}{2}X & -\frac{1}{2}-\frac{1}{4}X-\frac{1}{8}X^2 \\ \frac{1}{4}X^2 & \\ \hline 0 & \end{array}$$

Cuối cùng: $\dfrac{X^5+1}{X^3(X-2)} = X+2+\dfrac{-\frac{1}{2}}{X^3}+\dfrac{-\frac{1}{4}}{X^2}+\dfrac{-\frac{1}{8}}{X}+\dfrac{\frac{33}{8}}{X-2}$.

2) Trường hợp cực điểm khác 0

Nếu a là một không điểm bội của S, để nhận được các hệ tử tương ứng với cực điểm a trong PTĐG của $\dfrac{A}{S}$, ta sẽ thực hiện một "phép đổi ẩn" $Y = X - a$, và ta sẽ quy về trường hợp trên (đối với ẩn Y).

VÍ DỤ:

PTĐG của $F = \dfrac{1}{(X-1)^4(X+2)^3}$ trong $\mathbb{R}(X)$.

Rõ ràng rằng phần nguyên bằng không. PTĐG của F có dạng:

$$F = \frac{\alpha_4}{(X-1)^4}+\frac{\alpha_3}{(X-1)^3}+\frac{\alpha_2}{(X-1)^2}+\frac{\alpha_1}{X-1}+\frac{\beta_3}{(X+2)^3}+\frac{\beta_2}{(X+2)^2}+\frac{\beta_1}{X+2},$$

trong đó $\alpha_4, ..., \alpha_1, \beta_3, ..., \beta_1$ đều là những số thực phải tính.

• *Tính* $\alpha_4, ..., \alpha_1$

Đổi ẩn $Y = X - 1$ (vậy $X = 1 + Y$), $F = \dfrac{1}{(X-1)^4(X+2)^3} = \dfrac{1}{Y^4(3+Y)^3}$, rồi chia theo lũy thừa tăng đến cấp 3 (= 4 - 1) 1 cho $(3 + Y)^3$:

$$\begin{array}{l|l} 1 & 27+27Y+9Y^2+Y^3 \\ \hline -Y-\frac{1}{3}Y^2-\frac{1}{27}Y^3 & \frac{1}{27}-\frac{1}{27}Y+\frac{2}{81}Y^2-\frac{10}{729}Y^3 \\ \frac{2}{3}Y^2+\frac{8}{27}Y^3 & \\ -\frac{10}{27}Y^3 & \\ \hline 0 & \end{array}$$

Ta được: $\alpha_4 = \dfrac{1}{27}$, $\alpha_3 = -\dfrac{1}{27}$, $\alpha_2 = \dfrac{2}{81}$, $\alpha_1 = -\dfrac{10}{729}$.

• *Tính* $\beta_3, ..., \beta_1$

Đổi ẩn $Z = X + 2$ (vậy $X = -2 + Z$),

$$F = \frac{1}{(X-1)^4(X+2)^3} = \frac{1}{(-3+Z)^4 Z^3},$$

rồi chia theo lũy thừa tăng đến cấp 2 (= 3 - 1) 1 cho $(3 + Z)^4$:

$$\begin{array}{l|l} 1 & 81 - 108Z + 54Z^2 \\ \hline \frac{4}{3}Z - \frac{2}{3}Z^2 & \frac{1}{81} + \frac{4}{243}Z + \frac{10}{729}Z^2 \\ \frac{10}{9}Z^2 & \\ 0 & \end{array}$$

Ta được: $\beta_3 = \frac{1}{81}$, $\beta_2 = \frac{4}{243}$, $\beta_1 = \frac{10}{729}$.

Cuối cùng:

$$\frac{1}{(X-1)^4(X+2)^3} = \frac{\frac{1}{27}}{(X-1)^4} + \frac{\frac{1}{27}}{(X-1)^3} + \frac{\frac{2}{81}}{(X-1)^2} + \frac{\frac{10}{729}}{X-1} + \frac{\frac{1}{81}}{(X+2)^3} + \frac{\frac{4}{243}}{(X+2)^2} + \frac{\frac{10}{729}}{X+2}.$$

c) Nhận xét về tính chẵn lẻ

Khi sử dụng tính duy nhất của PTĐG của một phân thức hữu tỷ, ta thấy rằng nếu phân thức hữu tỷ F chẵn (tương ứng : lẻ) và nếu phân thức đơn giản $\frac{C(X)}{(S(-X))^k}$ có mặt trong PTĐG của F, thì phân thức đơn giản $\frac{C(X)}{(S(-X))^k}$ (tương ứng: $-\frac{C(-X)}{(S(-X))^k}$) cũng có mặt trong PTĐG của F.

VÍ DỤ:

PTĐG của $F = \frac{2X^2+5}{(X^2-1)^3}$ trong $\mathbb{R}(X)$.

Dạng của PTĐG của F là:

$$F = \frac{a}{(X-1)^3} + \frac{b}{(X-1)^2} + \frac{c}{X-1} + \frac{\alpha}{(X-1)^3} + \frac{\beta}{(X+1)^2} + \frac{\gamma}{X+1}$$

trong đó $a, ..., \gamma$ đều là các số thực phải tìm.

Thay X bởi -X:

$$F(-X) = \frac{-a}{(X+1)^3} + \frac{b}{(X+1)^2} + \frac{-c}{X+1} + \frac{-\alpha}{(X-1)^3} + \frac{\beta}{(X-1)^2} + \frac{-\gamma}{X-1}.$$

Vì F chẵn, tính duy nhất của PTĐG của F chứng tỏ rằng: $a = -\alpha$, $b = \beta$, $c = -\gamma$.

Tính a, b, c

Đổi ẩn: $Y = X - 1$ (vậy $X = 1 + Y$),

$$F = \frac{2X^2+5}{(X-1)^3(X+1)^3} = \frac{2(1+Y)^2+5}{Y^3(2+Y)^3},$$

rồi chia $2(1+Y)^2+5$ cho $(2+Y)^3$ theo lũy thừa tăng đến cấp 2:

$$\begin{array}{r|l} 7+4Y+2Y^2 & 8+12Y+6Y^2 \\ \hline -\frac{13}{2}Y-\frac{13}{4}Y^2 & \frac{7}{8}-\frac{13}{16}Y+\frac{13}{16}Y^2 \\ \frac{13}{2}Y^2 & \\ 0 & \end{array}$$

Ta được: $a=\frac{7}{8}$, $b=-\frac{13}{16}$, $c=\frac{13}{16}$.

Cuối cùng: $\frac{2X^2+5}{(X^2-1)^3}=\frac{\frac{7}{8}}{(X-1)^3}+\frac{-\frac{13}{6}}{(X-1)^2}+\frac{\frac{13}{6}}{(X-1)}+\frac{-\frac{7}{8}}{(X+1)^3}+\frac{-\frac{13}{16}}{(X+1)^2}+\frac{-\frac{13}{16}}{X+1}$.

d) Khi chỉ còn một hoặc hai hệ tử cần xác định trong một PTĐG, ta có thể xét đến việc thay X bởi một trị đặc biệt, hoặc cho X tiến ra vô tận (một cách chặt chẽ: sử dụng phép đổi biến $Y=\frac{1}{X}$, rồi thay Y bởi 0) sau khi đã nhân nếu cần thiết hai vế của đẳng thức với một lũy thừa của X.

VÍ DỤ:

PTĐG của $F=\frac{X}{(X-1)^2(X-2)}$ trong $\mathbb{R}(X)$.

Dạng của PTĐG là: $F=\frac{a}{(X-1)^2}+\frac{b}{X-1}+\frac{\lambda}{X-2}$, trong đó $a, b, \lambda \in \mathbb{R}$.

Bằng cách nhân với X - 2, rồi thay X bởi 2, ta được: $\lambda = 2$.

Bằng cách nhân với $(X-2)^2$ rồi thay X bởi 1, ta được: $a = -1$.

Bằng cách nhân với X rồi cho X tiến ra vô tận, ta được: $b + \lambda = 0$, từ đây $b = -2$.

Cuối cùng: $\frac{X}{(X-1)^2(X-2)}=\frac{-1}{(X-1)^2}+\frac{-2}{X-1}+\frac{+2}{X-2}$.

e) ***Trường hợp*** $\mathbb{C}(X)$

Cho $A \in \mathbb{C}[X]$, $S \in \mathbb{C}[X]$ chuẩn tắc sao cho $\deg(S) \geq 1$, $F=\frac{A}{S}$. Theo định lý d'Alambert (5.3.4, Định lý), S tách được trên $\mathbb{C}$; vậy tồn tại $n \in \mathbb{N}^*$, $z_1, \ldots, z_n \in \mathbb{C}$ từng đôi khác nhau, $\alpha_1, \ldots, \alpha_n \in \mathbb{N}^*$ sao cho:

$$F=\frac{A}{\prod_{i=1}^{n}(X-z_i)^{\alpha_i}}$$

PTĐG của F có dạng :

$$F=E+\sum_{i=1}^{n}\sum_{j=1}^{\alpha_i}\frac{\lambda_{\alpha_{i,j}}}{(X-z_i)^j},$$

trong đó E là phần nguyên của F và các $\lambda_{\alpha_{i,j}}$ là những số phức.

Trong thực hành, để tính các $\lambda_{\alpha_{i,j}}$, ta sẽ sử dụng:

• phương pháp nhân và thay thế, hoặc công thức sử dụng đạo hàm (5.4.2, 2) *a*)) khi $\alpha_i = 1$

• một phép đổi ẩn tiếp theo là một phép chia theo lũy thừa tang (xem 5.4.2, 2) *b*)) khi $\alpha_i > 1$.

f) Trường hợp $\mathbb{R}(X)$

Giả sử $A \in \mathbb{R}[X], S \in \mathbb{R}[X]$ chuẩn tắc sao cho $\deg(S) \geq 1$, $F = \dfrac{A}{S}$.

Theo 5.3.5, phân tích nguyên tố của S có dạng:

$$S = \prod_{i=1}^{N} (X - x_i)^{r_i} \prod_{k=1}^{N'} (X^2 + p_k X + q_k)^{s_k}$$

Trong đó:
- $N, N' \in \mathbb{N}$
- $x_1, ..., x_N \in \mathbb{R}$, từng đôi khác nhau
- $(p_1, q_1), ..., (p_{N'}, q_{N'}) \in \mathbb{R}^2$ từng cặp khác nhau
- $\forall k \in \{1, ..., N'\}$, $p_k^2 - 4q_k < 0$
- $r_1, ..., r_N, s_1, ..., s_{N'} \in \mathbb{N}^*$.

Vậy PTĐG của F có dạng:

$$F = E + \sum_{i=1}^{N} \sum_{j=1}^{r_i} \frac{\lambda_{i,j}}{(X - x_i)^j} + \sum_{k=1}^{N'} \sum_{l=1}^{s_k} \frac{\mu_{k,l} X + \nu_{k,l}}{(X^2 + p_k X + q_k)^l},$$

trong đó E là phần nguyên của F, và các $\lambda_{i,j}, \mu_{k,l}, \nu_{k,l}$ là những số thực.

• Các phần tử đơn giản $\dfrac{\lambda_{i,j}}{(X - x_i)^j}$ được gọi là các **phân thức đơn giản loại 1** (xem 5.4.2, *1*)).

• Các phần tử đơn giản $\dfrac{\mu_{k,l} X + \nu_{k,l}}{(X^2 + p_k X + q_k)^l}$ được gọi là các **phân thức đơn giản loại 2**.

Một trường hợp riêng

Giả sử F có dạng $F = \dfrac{A}{T^s}$, trong đó $A \in K[X]$, T là một tam thức bất khả quy, $s \in \mathbb{N}^*$. PTĐG của F có dạng:

$$F = \frac{A}{T^s} = E + \frac{C_s}{T^s} + \frac{C_{s-1}}{T^{s-1}} + ... + \frac{C_1}{T}$$

trong đó E là phần nguyên của F và $C_1, ..., C_s$ là những đa thức thuộc $\mathbb{R}[X]$ đều có bậc ≤ 1.

Ta có thể tính $C_s, C_{s-1}, ..., C_1, E$ bằng những **phép chia Euclide liên tiếp**. Thật vậy, tồn tại các đa thức $Q_1, ..., Q_s, R_1, ..., R_s$ thuộc $\mathbb{R}[X]$ sao cho:

$$\begin{cases} A = Q_1 T + R_1, \ Q_1 = Q_2 T + R_2, \ ... \ Q_{s-1} = Q_s T + R_s \\ \forall j \in \{1, ..., s\}, \ \deg(R_j) < 2 \end{cases}$$

và khi đó ta có:

$$\frac{A}{T^s} = \frac{R_1}{T^s} + \frac{Q_1}{T^{s-1}} = \ldots = \frac{R_1}{T^s} + \frac{R_2}{T^{s-1}} + \ldots + \frac{R_s}{T} + Q_s$$

từ đó, do tính duy nhất của PTĐG của F:

$$C_s = R_1, \quad C_{s-1} = R_2, \ldots, \quad C_1 = R_s, \quad E = Q_s.$$

VÍ DỤ:

PTĐG của $F = \dfrac{X^8 - X^4 + 2}{(X^2 + X + 1)^3}$ trong $\mathbb{R}(X)$.

$$\begin{array}{l|l}
X^8 - X^4 + 2 & X^2 + X + 1 \\
\hline
-X^7 - X^6 & X^6 - X^5 + X^3 - 2X^2 + X + 1 \\
\quad X^5 & \\
\quad -2X^4 - X^3 & \\
\quad\quad X^3 + 2X^2 & \\
\quad\quad\quad X^2 - X + 2 & \\
\quad\quad\quad -2X + 1 &
\end{array}$$

$$\begin{array}{l|l}
X^6 - X^5 + X^3 - 2X^2 + X + 1 & X^2 + X + 1 \\
\hline
-2X^5 - X^4 & X^4 - 2X^3 + X^2 + 2X - 5 \\
\quad X^4 + 3X^3 & \\
\quad\quad 2X^3 - 3X^2 & \\
\quad\quad\quad -5X^2 - X & \\
\quad\quad\quad\quad 4X + 6 &
\end{array}$$

$$\begin{array}{l|l}
X^4 - 2X^3 + X^2 - 2X - 5 & X^2 + X + 1 \\
\hline
-3X^3 & X^2 - 3X + 3 \\
\quad 3X^2 + 5X & \\
\quad\quad 2X - 8 &
\end{array}$$

Ta kết luận:

$$\frac{X^8 - X^4 + 2}{(X^2 + X + 1)^3} = X^2 - 3X + 3 + \frac{-2X + 1}{(X^2 + X + 1)^3} + \frac{4X + 6}{(X^2 + X + 1)^2} + \frac{2X - 8}{X^2 + X + 1}.$$

■

Trong trường hợp tổng quát, ta sẽ thử kết hợp các phương pháp đã nói trên đây. Nhưng việc tính một PTĐG trong $\mathbb{R}(X)$ có thể dài, khi mẫu chứa nhiều tam thức bất khả quy, có lũy thừa cao. Việc chuyển qua số phức thường dẫn đến những phép tính phức tạp.

Ngày nay, đã có những phần mềm tính toán hình thức cho phép tính được PTĐG của các phân thức hữu tỷ trong $\mathbb{C}(X)$ và $\mathbb{R}(X)$.

VÍ DỤ:

1) PTĐG của $F = \dfrac{X}{(X-1)^2(X^2+1)^2}$ trong $\mathbb{R}(X)$.

PTĐG có dạng:

$$F = \frac{\lambda}{(X-1)^2} + \frac{\mu}{X-1} + \frac{\alpha X+\beta}{(X^2+1)^2} + \frac{\gamma X+\delta}{X^2+1},$$

trong đó λ, ..., δ là các số thực phải tính.

• *Tính λ, μ*

Đổi ẩn Y = X - 1 (Vậy X = 1 + Y), $F = \dfrac{1+Y}{Y^2((1+Y)^2+1)^2}$, rồi chia 1 + Y cho $((1 + Y)^2 + 1)^2$, hoặc cho 4 + 8Y, theo lũy thừa tăng đến cấp 1:

1 + Y	4 + 8Y
- Y	$\frac{1}{4} - \frac{1}{4}Y$
0	

Do đó: $\lambda = \dfrac{1}{4}$, $\mu = \dfrac{1}{4}$.

• *Tính α, β*

Nhân với $(X^2 + 1)^2$ rồi thay X bởi i: $\alpha_i + \beta = \dfrac{i}{(i-1)^2} = -\dfrac{1}{2}$, suy ra $\alpha = 0$, $\beta = -\dfrac{1}{2}$.

• *Tính γ, δ*

Thay X bởi 0: $0 = \lambda - \mu + \beta + \delta$, suy ra $\delta = 0$.

Nhân với X rồi cho X tiến ra vô cùng: $0 = \mu + \gamma$, từ đây $\gamma = \dfrac{1}{4}$.

Cuối cùng: $\dfrac{X}{(X-1)^2(X^2+1)^2} = \dfrac{\frac{1}{4}}{(X-1)^2} + \dfrac{-\frac{1}{4}}{(X-1)} + \dfrac{-\frac{1}{2}}{(X^2+1)^2} + \dfrac{\frac{1}{4}X}{X^2+1}$.

2) PTĐG của $F = \dfrac{X^2+2}{(X^2+1)^3(X^2+X+1)}$ trong $\mathbb{R}(X)$.

PTĐG của F có dạng: $F = \dfrac{aX+b}{(X^2+1)^3} + \dfrac{cX+d}{(X^2+1)^2} + \dfrac{eX+f}{(X^2+1)} + \dfrac{\lambda X+\mu}{(X^2+X+1)}$,

trong đó a, ..., μ là những số thực phải tính.

• *Tính λ, μ*

Nhân với $X^2 + X + 1$ rồi thay X bởi j:

$$\lambda_j + \mu = \frac{j^2+2}{(j^2+1)^3} = \frac{-j+1}{(-j)^3} = j-1,$$

do đó $\lambda = 1$, $\mu = -1$, vì (1, j) là một cơ sở của $\mathbb{R}$ - không gian vectơ $\mathbb{C}$.

• *Tính a, ..., f*

Xét $G = F - \dfrac{X-1}{X^2+X+1} = \dfrac{X^2+2-(X-1)(X^2+1)^3}{(X^2+1)^3(X^2+X+1)}$.

Ta có: $(X^2+2) - (X-1)(X^2+1)^3 = -X^7 + X^6 - 3X^5 + 3X^4 - 3X^3 + 4X^2 - X + 3$

$= (X^2+X+1)(-X^5 + 2X^4 - 4X^3 + 5X^2 - 4X + 3)$.

Do đó: $G = \dfrac{-X^5+2X^4-4X^3+5X^2-4X+3}{(X^2+1)^3}$.

Ta dùng phương pháp chia Euclide liên tiếp:

$$\begin{array}{l|l} -X^5+2X^4-4X^3+5X^2-4X+3 & X^2+1 \\ \hline 2X^4-3X^3 & -X^3+2X^2-3X+3 \quad \big| \quad X^2+1 \\ -3X^3+3X^2 & 2X^2-2X \quad \big| \quad -X+2 \\ 3X^2-X & -2X+1 \\ -X & \end{array}$$

Do đó: $G = \dfrac{-X}{(X^2+1)^3} + \dfrac{-2X+1}{(X^2+1)^2} + \dfrac{-X+2}{X^2+1}$, và cuối cùng:

$$\frac{X^2+2}{(X^2+1)^3(X^2+X+1)} = \frac{-X}{(X^2+1)^3} + \frac{-2X+1}{(X^2+1)^2} + \frac{-X+2}{(X^2+1)} + \frac{X-1}{X^2+X+1}.$$

Bài tập

◊ **5.4.4** *Ví dụ về phân tích thành phân thức đơn giản loại 1 trong* $\mathbb{R}(X)$

a) $\dfrac{-X^3+5X^2-4X+1}{X^3(X-1)^4}$ b) $\dfrac{8X^4+8}{(X-1)^3(X+1)^3}$ c) $\dfrac{2X^4+5X^3+21X^2-X+5}{(X+1)^4(X-1)^3}$

◊ **5.4.5** *Ví dụ về phân tích thành phân thức đơn giản loại 1 và loại 2 trong* $\mathbb{R}(X)$

a) $\dfrac{X^8-1}{(X^2+2X+1)^3}$ b) $\dfrac{X^2+1}{X^4+1}$ c) $\dfrac{X^3}{X^4+1}$

d) $\dfrac{1}{X^4+X^2+1}$ e) $\dfrac{X}{(X^4+1)(X^4-X^2+1)}$ f) $\dfrac{1}{(X^2+2X+3)(2X^2+3X+4)}$

g) $\dfrac{X^6-X^5+2X^4+X^2+1}{X^3(X^2+1)^2}$ h) $\dfrac{X^5+6X^4+17X^3+25X^2+19X+7}{(X+1)^2(X^2+X+1)}$

i) $\dfrac{3X^5+3X^4+5X^3+2X^2+X}{(X^2+1)^2(X^2+X+1)^2}$ j) $\dfrac{X^{2n}}{(X^2+1)^n}$, $n \in \mathbb{N}^*$.

◊ **5.4.6** Tính: $\displaystyle\sum_{n=2}^{N} = \frac{3n^2-1}{(n-1)^2n^2(n+1)^2}$, với $N \in \mathbb{N} - \{0, 1\}$.

◊ **5.4.7** Tính $\sum_{k=1}^{4} = \frac{z_k^3 + 2}{(z_k^2 - 1)^2}$, trong đó $z_1, ..., z_4$ là các không điểm trong $\mathbb{C}$ của $X^4 - X^3 + 1$.

◊ **5.4.8** a) Phân tích $\frac{1}{(X-1)^3(X+1)^3}$ thành những phân thức đơn giản trong $\mathbb{C}(X)$.

b) Suy ra một cặp (U, V) thuộc $(\mathbb{C}[X])^2$ sao cho: $(X+1)^3U + (X-1)^3V = 1$.

◊ **5.4.9** Cho $n \in \mathbb{N}^*$, $a \in \mathbb{C} - \{-1, 0, 1\}$. Rút gọn:

$$F_n = \sum_{k=0}^{n-1} \frac{a^k (X + a^{k+1})}{(X - a^k)(X - a^{k+1})(X - a^{k+2})}.$$

◊ **5.4.10** Cho $n \in \mathbb{N} - \{0, 1\}$, $p \in \{0, ..., n-1\}$, $\omega_k = \exp\left(\frac{2ik\pi}{n}\right)$ với $k \in \{0, ..., n-1\}$.

Đạt dưới dạng bất khả quy: $\sum_{k=0}^{n-1} \frac{\omega_k^p}{X - \omega_k}$

◊ **5.4.11** Cho $a, b, c \in \mathbb{C}$, $d = \frac{a+b+c}{2}$; ta giả sử rằng a, b, c, d từng đôi khác nhau.

a) Chứng minh rằng, với mọi đa thức P thuộc $\mathbb{C}[X]$ có bậc ≤ 2, ta có:

$$\frac{P}{(X-a)(X-b)(X-c)} = \sum \frac{P(a)}{(a-b)(a-c)} \cdot \frac{1}{X-a}$$

(trong đó tổng gồm 3 hạng tử, do hoán vị vòng tròn).

b) Suy ra trị của $\sum \frac{a^2}{(a-b)(a-c)(b+c-a)}$.

◊ **5.4.12*** Phân tích thành phần thức đơn giản trong $\mathbb{R}(X)$ phân thức hữu tỷ F_n liên kết với hàm hữu tỷ xác định bởi $x \mapsto \tan(n\text{Arctan}(x))$, $n \in \mathbb{N} - \{0, 1\}$ cố định.

◊ **5.4.13** Cho $n \in \mathbb{N}^*$, $z_1, ..., z_n \in \mathbb{C}$ từng đôi khác nhau, $Q = \prod_{k=1}^{n} (X - z_k)$.

a) Với mọi p thuộc $\{0, ..., n-1\}$, phân tích $\frac{X^p}{Q}$ thành phân thức đơn giản.

b) Suy ra trị của $\sum_{k=1}^{n} \frac{z_k^p}{Q'(z_k)}$ với $p \in \{1, ..., n-1\}$.

◊ **5.4.14** Cho $P, Q \in \mathbb{C}[X]$, $n = \deg(Q) \geq 2$. Ta giả thiết:

$$\begin{cases} Q \text{ có } n \text{ không điểm đơn } z_1, ..., z_n \text{ trong } \mathbb{C} \\ \deg(P) \leq \deg(Q) - 2. \end{cases}$$

Chứng minh: $\sum_{k=1}^{n} \frac{P(z_k)}{Q'(z_k)} = 0$.

◊ **5.4.15*** Cho $n \in \mathbb{N}^*$, $a_0, ..., a_{n-1} \in \mathbb{C}$, $P = X^n + a_{n-1}X^{n-1} + ... + a_0$, $z_1, ..., z_n \in \mathbb{C}$, từng đôi khác nhau, $\mu_k = z_k - \frac{P(z_k)}{\prod_{\substack{1 \leq i \leq n \\ i \neq k}} (z_k - z_i)}$, với $k \in \{1, ..., n\}$. Chứng minh: $\sum_{k=1}^{n} \mu_k = -a_{n-1}$.

Chương 6

Không gian vectơ

Trong chương 6 này, K chỉ một thể giao hoán. Trong thực tế, $K = \mathbb{R}$ hoặc $K = \mathbb{C}$.

6.1 Cấu trúc không gian véctơ

♦ **Định nghĩa 1** Mọi tập hợp E được trang bị một luật trong ký hiệu là $+$, và một luật ngoài $\underset{(\lambda,x)\mapsto \lambda x}{K\times E\to E}$ sao cho:

- $(E, +)$ là một nhóm Abel
- 1) $(\forall(\lambda, \mu) \in K^2, \forall x \in E,\ (\lambda + \mu)x = \lambda x + \mu x$

  2) $\forall \lambda \in K, \forall (x, y) \in E^2,\ \lambda(x + y) = \lambda x + \lambda y$

  3) $\forall(\lambda, \mu) \in K^2, \forall x \in E,\ \lambda(\mu x) = (\lambda\mu)x$

  4) $\forall x \in E,\ 1x = x.$

gọi là K - **không gian vectơ,**

Khi cố định thể K, ta có thể nói **không gian vectơ** thay cho K - không gian vectơ.

Chúng ta sẽ viết tắt K - không gian vectơ là K-kgv, không gian vectơ là kgv.

Các phần tử của một K-kgv được gọi là **vectơ;** các phần tử của K được gọi là **vô hướng**.

VÍ DỤ:

1) Thể K là một K-kgv với luật trong $\underset{(x,y)\mapsto x+y}{K\times K\to K}$ và luật ngoài là phép nhân trong K : $\underset{(\lambda,x)\mapsto \lambda x}{K\times K\to K}$. Ở đây các phần tử của K được coi đồng thời là vectơ và là vô hướng.

2) Tổng quát hơn, giả sử L là một thể sao cho K là một thể con của L (ta cũng nói L là **thể mẹ** của K). Khi đó L là một K-kgv, với luật trong $\underset{(x,y)\mapsto x+y}{L\times L\to L}$ và luật ngoài $\underset{(\lambda,x)\mapsto \lambda x}{K\times L\to L}$ (phép nhân trong L).

Đặc biệt, $\mathbb{C}$ là một $\mathbb{R}$-kgv với các luật thông thường.

3) Giả sử $n \in \mathbb{N}^*$, $E_1, ..., E_n$, là những K-kgv. Khi đó tích $E = \prod_{i=1}^{n} E_i$ là một K-kgv với luật trong và luật ngoài xác định bởi:

- $\forall (x_1, ..., x_n), (y_1, ..., y_n) \in E^2$, $(x_1, ..., x_n) + (y_1, ..., y_n) = (x_1 + y_1, ..., x_n + y_n)$
- $\forall \lambda \in K, \forall (x_1, ..., x_n) \in E$, $\lambda(x_1, ..., x_n) = (\lambda x_1, ..., \lambda x_n)$.

Đặc biệt, với mọi $n \in \mathbb{N}^*$, với các luật thông thường, K^n là một K-kgv.

4) Giả sử X là một tập hợp khác rỗng, E là một K-kgv. Tập hợp E^X các ánh xạ từ X vào E là một K-kgv với luật trong và luật ngoài xác định bởi:

- $\forall (f, g) \in (E^X)^2, \forall x \in X$, $(f + g)(x) = f(x) + g(x)$
- $\forall \lambda \in K, \forall f \in E^X, \forall x \in X$, $(\lambda f)(x) = \lambda f(x)$.

Chẳng hạn, với các luật thông thường, tập hợp $\mathbb{R}^{\mathbb{N}}$ các dãy số thực là một $\mathbb{R}$-kgv.

5) Chúng ta thấy (5.1.4, Mệnh đề 3) rằng tập hợp $K[X]$ các đa thức một ẩn với hệ số trong K là một K-kgv với phép cộng và phép nhân ngoài. Thông thường ta chứng minh E là một không gian vectơ bằng cách chứng minh E là một kgvc của một kgv đã biết (theo 6.2, Mệnh đề 1, và bài tập 6.2.5).

NHẬN XÉT:

Đổi thể

Giả sử L là một thể mẹ của K. Mọi L-kgv E có thể được coi như là một K-kgv bằng cách trang bị cho nó luật + đã được xác định trong E, và luật ngoài $K \times E \xrightarrow[(\lambda, x) \mapsto \lambda x]{} E$, thu hẹp của luật ngoài của L-kgv E.

Chẳng hạn, mọi $\mathbb{C}$-kgv có thể được coi như là một $\mathbb{R}$-kgv.

Mệnh đề 1 Giả sử E là một K-kgv. Với mọi λ, μ thuộc K và mọi x, y thuộc E, ta có:

1) $\lambda x = 0 \Leftrightarrow (\lambda = 0$ hoặc $x = 0)$

2) $(\lambda - \mu)x = \lambda x - \mu x$

3) $\lambda(x - y) = \lambda x - \lambda y$.

Ở đây ta ký hiệu 0 là phần tử trung hòa của phép cộng trong K, cũng như phần tử trung hòa của phép cộng trong E; khi cần thiết ta có thể ký hiệu 0_K và 0_E để phân biệt hai đối tượng đó.

Chứng minh:

1) • $0x = (0 + 0)x = 0x + 0x$, từ đó suy ra $0x = 0$.

- $\lambda 0 = \lambda(0 + 0) = \lambda 0 + \lambda 0$ từ đó suy ra $\lambda 0 = 0$.
- Nếu $\lambda x = 0$ và nếu $\lambda \neq 0$, thì bằng cách ký hiệu λ^{-1} là nghịch đảo của λ trong thể K:

$$x = 1x = (\lambda^{-1}\lambda)x = \lambda^{-1}(\lambda x) = \lambda^{-1}0 = 0.$$

2) $\lambda x = ((\lambda - \mu) + \mu)x = (\lambda - \mu)x + \mu x$, từ đó suy ra $(\lambda - \mu)x = (\lambda x) - (\mu x)$, phần tử này được viết là $(\lambda - \mu)x$.

3) $\lambda x = \lambda((x - y) + y) = \lambda(x - y) + \lambda y$, từ đó suy ra $\lambda(x - y) = \lambda x - \lambda y$. ■

Ta dễ dàng chứng minh (bằng quy nạp) Mệnh đề sau:

♦ **Mệnh đề 2** **(Sử dụng ký hiệu Σ trong các kgv)**

Giả sử E là một K-kgv, $n, p \in \mathbb{N}^*$, x, x_i, y_i, x_{ij} là những phần tử của E, λ, λ_i,... những phần tử của K. Ta có:

1) $\left(\sum_{i=1}^{n} x_i\right) + \left(\sum_{i=n+1}^{p} x_i\right) = \sum_{i=1}^{p} x_i$ (nếu $p \geq n+1$)

2) $\sum_{i=1}^{n} (x_i + y_i) = \sum_{i=1}^{n} x_i + \sum_{i=1}^{n} y_i$

3) $\sum_{i=1}^{n} \left(\sum_{j=1}^{p} x_{ij}\right) = \sum_{j=1}^{p} \left(\sum_{i=1}^{n} x_{ij}\right)$

4) $\forall \sigma \in \mathfrak{S}_n$, $\sum_{i=1}^{n} x_{\sigma(i)} = \sum_{i=1}^{n} x_i$

5) $\sum_{i=1}^{n} (\lambda x_i) = \lambda \sum_{i=1}^{n} x_i$

6) $\sum_{i=1}^{n} (\lambda_i x) = \left(\sum_{i=1}^{n} \lambda_i\right) x.$

- Theo quy ước, tổng của một họ rỗng những phần tử của K (tương ứng: E) bằng 0.
- Theo 5) và 6), ta có thể ký hiệu $\sum_{i=1}^{n} \lambda x_i$ và $\sum_{i=1}^{n} \lambda_i x$ thay cho $\sum_{i=1}^{n} (\lambda x_i)$ và $\sum_{i=1}^{n} (\lambda_i x)$ tương ứng.

♦ **Định nghĩa 2** Một tập hợp A cùng với một luật trong ký hiệu +, một luật ngoài $K \times A \to A$, $(\lambda, x) \mapsto \lambda x$, và một luật trong (được gọi là luật thứ ba) ở đây được ký hiệu là $*$, sao cho:

1) $(A, +, \cdot)$ là một K-kgv

2) $*$ phân phối đối với +

3) $\forall \lambda \in K$, $\forall (x, y) \in A^2$, $\lambda(x * y) = (\lambda x) * y = x * (\lambda y)$,

gọi là K - **đại số.**

Một K-đại số A gọi là:

- **kết hợp** khi và chỉ khi $*$ có tính kết hợp
- **giao hoán** khi và chỉ khi $*$ có tính giao hoán
- **có đơn vị** (hoặc: **đơn vị**) khi và chỉ khi A có phần tử trung hòa đối với $*$.

VÍ DỤ:

1) Mọi thể giao hoán K là một K-đại số kết hợp, giao hoán, có đơn vị, nếu lấy luật thứ ba là phép nhân.

2) Tổng quát hơn nếu L là một thể mẹ của K, thì L là một K-đại số kết hợp, và có đơn vị nếu lấy luật thứ ba là phép nhân trong L.

Chẳng hạn, $\mathbb{C}$ là một $\mathbb{R}$-đại số kết hợp, giao hoán, có đơn vị đối với các luật thông thường.

3) Giả sử X là một tập hợp khác rỗng. Chúng ta đã thấy (Ví dụ 4), rằng K^X là một K-kgv với các luật thông thường. Bằng cách trang bị cho K^X luật thứ ba, được xác định bởi:

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

K^X là một K-đại số kết hợp, giao hoán, có đơn vị, phần tử trung hòa đối với luật thứ ba là ánh xạ hằng bằng một.

4) Chúng ta đã thấy (5.1.4, Mệnh đề 3) rằng $K[X]$ là một K-đại số kết hợp, giao hoán, có đơn vị.

5) Dưới đây ta sẽ thấy đại số $\mathcal{L}(E)$ các tự đồng cấu của một K-kgv E, với luật thứ ba là luật $\circ$ của phép hợp thành (7.2.2, Mệnh đề 5), và đại số $\mathbf{M}_n(K)$ các ma trận vuông cấp n với hệ số trong K, mà luật thứ ba là phép nhân ma trận (8.1.4, Mệnh đề 4).

Thông thường ta sẽ chứng minh A là một đại số bằng cách chứng minh A là một đại số con của một đại số đã biết (xem 6.2, Mệnh đề 6 và bài tập 6.4.10).

6.2 Không gian vectơ con

♦ **Định nghĩa 1** Giả sử E là một K-kgv, $F \in \mathfrak{P}(E)$. Ta nói F là một **không gian vectơ con** của E khi và chỉ khi:

$$\begin{cases} 1) & F \neq \varnothing \\ 2) & \forall (x, y) \in F^2, \quad x + y \in F \\ 3) & \forall \lambda \in K, \forall x \in F, \quad \lambda x \in F. \end{cases}$$

Chúng ta viết tắt không gian vectơ con là kgvc. Để nhắc lại thể K đang sử dụng, thỉnh thoảng ta nói K-kgvc thay cho kgvc.

Dễ dàng chứng minh Mệnh đề sau:

♦ **Mệnh đề 1** Giả sử E là một K-kgv, $F \in \mathfrak{P}(E)$. Nếu F là một kgvc của E, thì F là một K-kgv với luật + : $\underset{(x,y)\mapsto x+y}{F \times F \to F}$ và luật ngoài $\underset{(\lambda,x)\mapsto \lambda x}{K \times F \to F}$ cảm sinh bởi các luật của E.

VÍ DỤ:

1) $\mathbb{R} \times \{0\}$ là một kgvc của $\mathbb{R}$-kgv $\mathbb{R}^2$.

2) Với mọi n thuộc $\mathbb{N}$, $K_n[X]$ là một kgvc của K-kgv $K[X]$ (xem 5.1.4).

NHẬN XÉT:

1) $\{0\}$ và E là hai kgvc của K-kgv E.

2) Nếu F là một kgvc của kgv E và nếu G là một kgvc của F, thì G là một kgvc của E; người ta nói khái niệm không gian vécto con có tính bắc cầu.

♦ **Mệnh đề 2** Giả sử E là một K-kgv, $(F_i)_{i\in I}$ là một họ kgvc của E; thế thì $\bigcap_{i\in I} F_i$ là một kgvc của E.

Chứng minh:

Đặt $F = \bigcap_{i\in I} F_i$.

1) $F \neq \varnothing$; thực vậy, $0 \in F$ vì $(\forall i \in I, 0 \in F_i)$.

2) Giả sử $(x, y) \in F^2$. Ta có: $(\forall i \in I, (x \in F_i \text{ và } y \in F_i))$, vì vậy $(\forall i \in I, x + y \in F_i)$, do đó $x + y \in F$.

3) Giả sử $(\lambda, x) \in K \times F$.

Ta có: $(\forall i \in I, x \in F_i)$, vì vậy $(\forall i \in I, \lambda x \in F_i)$, do đó $\lambda x \in F$. ■

Đặc biệt, nếu F_1, F_2 là hai kgvc của E thì $F_1 \cap F_2$ là một kgvc của E.

♦ **Mệnh đề - Định nghĩa 3**

Giả sử E là một K-kgv, F_1, F_2 là hai kgvc của E.

Ta ký hiệu $F_1 + F_2 = \{x \in E;\ \exists (x_1, x_2) \in F_1 \times F_2,\ x = x_1 + x_2\}$

$$= \{x_1 + x_2;\ (x_1, x_2) \in F_1 \times F_2\},$$

gọi là **tổng của** F_1 **và** F_2 (xem 2.1, Định nghĩa 12), và $F_1 + F_2$ là một kgvc của E.

Chứng minh:

1) $F_1 + F_2 \neq \emptyset$ vì $0 = 0 + 0 \in F_1 + F_2$.

2) Giả sử $(x, y) \in (F_1 + F_2)^2$. Tồn tại $(x_1, x_2) \in F_1 \times F_2$, $(y_1, y_2) \in F_1 \times F_2$ sao cho: $x = x_1 + x_2$, $y = y_1 + y_2$.

Vậy ta có: $x + y = (x_1 + x_2) + (y_1 + y_2) = (x_1 + y_1) + (x_2 + y_2) \in F_1 + F_2$.

3) Giả sử $(\lambda, x) \in K \times (F_1 + F_2)$. Tồn tại $(x_1, x_2) \in F_1 + F_2$ sao cho $x = x_1 + x_2$. Ta có:

$$\lambda x = \lambda(x_1 + x_2) = \lambda x_1 + \lambda x_2 \in F_1 + F_2. \qquad \blacksquare$$

♦ **Mệnh đề 4** Giả sử E là một K-kgv; đối với mọi kgvc F_1, F_2, F_3 của E ta có:

1) $F_1 + F_2 = F_2 + F_1$	1') $F_1 \cap F_2 = F_2 \cap F_1$
2) $F_1 \subset F_1 + F_2$	2') $F_1 \cap F_2 \subset F_1$
3) $\begin{cases} F_1 \subset F_3 \\ F_2 \subset F_3 \end{cases} \Leftrightarrow F_1 + F_2 \subset F_3$	3') $\begin{cases} F_3 \subset F_1 \\ F_3 \subset F_2 \end{cases} \Leftrightarrow F_3 \subset F_1 \cap F_2$
4) $F_1 \subset F_2 \Rightarrow F_1 + F_3 \subset F_2 + F_3$	4') $F_1 \subset F_2 \Rightarrow F_1 \cap F_3 \subset F_2 \cap F_3$
5) $F_1 + F_1 = F_1$	5') $F_1 \cap F_1 = F_1$
6) $F_1 + \{0\} = F_1$	6') $F_1 \cap \{0\} = \{0\}$
7) $F_1 + E = E$	7') $F_1 \cap E = F_1$
8) $(F_1 + F_2) + F_3 = F_1 + (F_2 + F_3)$	8') $(F_1 \cap F_2) \cap F_3 = F_1 \cap (F_2 \cap F_3)$.

Chứng minh:

Các phép chứng minh rất đơn giản. Chẳng hạn, đối với 2): với mọi x thuộc F_1, ta có thể viết $x = x + 0$, trong đó $x \in F_1$ và $0 \in F_2$, nên $x \in F_1 + F_2$.

NHẬN XÉT:

Ký hiệu $\mathbf{V}(E)$ chỉ tập hợp các kgvc của E.

Các luật trong + và $\cap$ trong $\mathbf{V}(E)$, luật này không phân phối đối với luật kia (trừ trường hợp đặc biệt của E) (xem bài tập 6.2.1).

♦ **Định nghĩa 2** Giả sử E là một K-kgv, F_1, F_2 là hai kgvc của E. Ta nói rằng F_1, F_2 **có tổng trực tiếp** khi và chỉ khi $F_1 \cap F_2 = \{0\}$.

Khi F_1 và F_2 có tổng trực tiếp, ta ký hiệu $F_1 \oplus F_2$ thay cho $F_1 + F_2$.

VÍ DỤ:

Với $K = \mathbb{R}$, $E = \mathbb{R}^3$, các kgvc $F_1 = \mathbb{R} \times \{0\} \times \{0\}$ và $F_2 = \{0\} \times \mathbb{R} \times \{0\}$ có tổng trực tiếp.

NHẬN XÉT:

Ký hiệu $F_1 \oplus F_2$ chỉ xác định khi F_1 và F_2 có tổng trực tiếp; $\oplus$ không phải là một phép toán mới.

◆ **Mệnh đề 5** Để hai kgvc F_1, F_2 của một K-kgv E có tổng trực tiếp, thì cần và đủ là mọi phần tử của $F_1 + F_2$ phân tích một cách duy nhất thành tổng của một phần tử của F_1 và một phần tử của F_2.

Chứng minh:

1) Giả sử F_1 và F_2 có tổng trực tiếp, và giả sử $x \in F_1 + F_2$.

- Từ định nghĩa của $F_1 + F_2$ suy ra tồn tại $(x_1, x_2) \in F_1 \times F_2$ sao cho $x = x_1 + x_2$.
- Giả sử $(x_1, x_2) \in F_1 \times F_2$, $(y_1, y_2) \in F_1 \times F_2$ sao cho $x = x_1 + x_2 = y_1 + y_2$.

Thế thì: $x_1 - y_1 = y_2 - x_2$.

Vì $(x_1 - y_1 \in F_1, y_2 - x_2 \in F_2, F_1 \cap F_2 = \{0\})$, nên $x_1 - y_1 = y_2 - x_2 = 0$, do đó $x_1 = y_1$, $x_2 = y_2$.

Như vậy, x được phân tích một cách duy nhất trên F_1 và F_2.

2) Ngược lại, giả sử mọi phần tử của $F_1 + F_2$ được phân tích một cách duy nhất trên F_1 và F_2.

Giả sử $x \in F_1 \cap F_2$. Ta có hai cách phân tích của 0 trên F_1 và F_2: $0 = 0 + 0$ và $0 = x + (-x)$, từ đó suy ra $x = 0$. Như vậy $F_1 \cap F_2 = \{0\}$, F_1 và F_2 có tổng trực tiếp.

◆ **Định nghĩa 3** Hai kgvc F_1, F_2 của một K-kgv E được gọi là **bù nhau trong** E khi và chỉ khi: $F_1 \cap F_2 = \{0\}$ và $F_1 + F_2 = E$.

Điều đó có nghĩa là: F_1 và F_2 có tổng trực tiếp và $F_1 \oplus F_2 = E$.

VÍ DỤ:

1) $K = \mathbb{R}$, $E = \mathbb{R}^2$, $F_1 = \mathbb{R} \times \{0\}$, $F_2 = \{0\} \times \mathbb{R}$; F_1 và F_2 là hai kgvc của E bù nhau trong E.

2) $K = \mathbb{R}$, $E = \mathbb{R}^{\mathbb{R}}$, F_1 (tương ứng: F_2) là tập hợp các ánh xạ chẵn (tương ứng: lẻ) từ $\mathbb{R}$ vào $\mathbb{R}$; F_1, F_2 là hai kgvc của E bù nhau trong E. Thực vậy:

- Nếu $f \in F_1 \cap F_2$, thì f là chẵn và lẻ, nên $(\forall x \in \mathbb{R}, f(x) = -f(x))$, vì vậy $f = 0$.
- Mọi $f \in E$ có thể viết dưới dạng $f = g + h$ trong đó $g \in F_1$, $h \in F_2$ được xác định bởi:

$$\forall x \in \mathbb{R},\ g(x) = \frac{1}{2}(f(x) + f(-x)),\ h(x)) = \frac{1}{2}(f(x) - f(-x)).$$

(xem Tập 1, 4.1.3, Mệnh đề).

NHẬN XÉT:

1) Một kgvc F của E có thể có nhiều phần bù trong E. Chẳng hạn, nếu $K = \mathbb{R}$ và $E = \mathbb{R}^2$, thì kgvc $F = \mathbb{R} \times \{0\}$ có vô hạn phần bù trong E, đó là tất cả các $\mathbb{R}x$, $x \in E - F$.

2) Sau này ta sẽ chứng minh (6.4, Mệnh đề) rằng, nếu E là một không gian hữu hạn chiều, thì mọi kgvc của E có ít nhất một phần bù trong E.

3) Sự tồn tại một phần bù đối với một kgvc bất kỳ là tương đương lôgic với *tiên đề chọn*, mà việc nghiên cứu nằm ngoài phạm vi cuốn sách này.

♦ **Định nghĩa 4** Giả sử A là một K-đại số với luật thứ ba ký hiệu là $*$, $B \in \mathfrak{P}(A)$. Ta nói B là một **đại số con** của A khi và chỉ khi:

$$\begin{cases} B \text{ là một kgvc của } K\text{-kgv } A \\ \forall (x, y) \in B, \quad x * y \in B. \end{cases}$$

Nói cách khác, một bộ phận B của một đại số A là một đại số con của A khi và chỉ khi:

$$\begin{cases} B \neq \varnothing \\ \forall (x, y) \in B^2, \ x + y \in B \\ \forall (\lambda, x) \in K \times B, \ \lambda x \in B \\ \forall (x, y) \in B^2, \quad x * y \in B \end{cases}$$

■

Dễ dàng suy ra mệnh đề sau:

♦ **Mệnh đề 6** Giả sử A là một K-đại số, $B \in \mathfrak{P}(A)$. Nếu B là một đại số con của A, thì B là một K-đại số đối với các luật $+ : \underset{(x,y)\mapsto x+y}{B \times B \to B}$, luật ngoài: $\underset{\lambda x \mapsto \lambda x}{K \times B \to B}$, $* : \underset{(x,y)\mapsto x*y}{B \times B \to B}$ cảm sinh bởi các luật của E.

VÍ DỤ:

$A = \mathbb{R}^{\mathbb{R}}$ là một $\mathbb{R}$ - đại số đối với các luật thông thường (luật thứ ba là phép nhân) và tập hợp B các ánh xạ bị chặn từ $\mathbb{R}$ vào $\mathbb{R}$ là một đại số con của A (xem Tập 1, 4.1.8, Mệnh đề 3).

Bài tập

◊ **6.2.1** Cho E là một K-kgv, F, G, H là những kgvc của E.

a) 1) Chứng minh: $(F \cap G) + (F \cap H) \subset F \cap (G + H)$.

2) Chứng minh: $(G \subset F \text{ hoặc } H \subset F) \Rightarrow (F \cap G) + (F \cap H) = F \cap (G + H)$.

3) Cho một ví dụ về K, E, F, G, H sao cho trong kết quả của a), 1) không xảy ra đẳng thức.

b) 1) Chứng minh: $F + (G \cap H) \subset (F + G) \cap (F + H)$.

2) Chứng minh: $(F \subset G \text{ hoặc } F \subset H) \Rightarrow F + (G \cap H) = (F + G) \cap (F + H)$.

3) Cho một ví dụ về K, E, F, G, H sao cho trong kết quả b) 1) không xảy ra đẳng thức.

◊ **6.2.2** Giả sử E là một K-kgv, F, G là hai kgvc của E sao cho $F \cup G = E$. Chứng minh: $F = E$ hoặc $G = E$.

◊ **6.2.3** Cho E là một K-kgv, I là một tập hợp khác rỗng $(F_i)_{i \in I}$ là một họ những không gian con của E.

Giả sử: $\forall (i, j) \in I^2, \exists k \in I, \ F_i \cup F_j \subset F_k$. Chứng minh rằng $\bigcup_{i \in I} F_i$ là một kgvc của E.

◊ **6.2.4** Cho một ví dụ về thể hữu hạn K, K-kgv E, các kgvc F_1, F_2, F_3 của E sao cho:

$$F_1 \cup F_2 \cup F_3 = E \quad \text{và} \quad (\forall i \in \{1, 2, 3\}, F_i \neq E).$$

◊ **6.2.5** Giả sử E là tập hợp các ánh xạ $f : \mathbb{R} \to \mathbb{R}$ sao cho tồn tại $A \in \mathbb{R}_+^*$ và $g, h : \mathbb{R} \to \mathbb{R}$ tăng sao cho: $\forall x \in \mathbb{R}, (|x| \geq A \Rightarrow f(x) = g(x) - h(x))$.

Chứng tỏ rằng E là một $\mathbb{R}$-kgv đối với các luật thông thường.

◊ **6.2.6** Giả sử $N \in \mathbb{N}^*$, $a_0, \ldots, a_N \in \mathbb{R}$ khác nhau từng đôi, $E = \mathbb{R}^{\mathbb{R}}$, $F = \{f \in \mathbb{R}^{\mathbb{R}}; \forall i \in \{0, \ldots, N\}, f(a_i) = 0\}$, G là tập các ánh xạ đa thức từ $\mathbb{R}$ vào $\mathbb{R}$ với bậc $\leq N$. Chứng tỏ rằng F và G là hai kgvc của E, bù nhau trong E (E được trang bị các luật thông thường).

◊ **6.2.7** Cho A là một K-đại số. Với mọi bộ phận X của A, ta gọi bộ phận của A, viết là X', xác định bởi: $X' = \{y \in A; \forall x \in X, xy = yx\}$ là **hoán tập** của X.

a) Chứng tỏ rằng, nếu A có tính kết hợp, thì X' là một đại số con của A. Đặc biệt, **tâm** của A, được định nghĩa là A', là một đại số con của A (nếu A có tính kết hợp).

b) Chứng minh: 1) $\forall (X, Y) \in (\mathfrak{P}(A))^2, (X \subset Y \Rightarrow X' \supset Y')$

2) $\forall X \in \mathfrak{P}(A), X \subset X''$.

6.3 Tính phụ thuộc tuyến tính và tính độc lập tuyến tính

6.3.1 Họ phụ thuộc, họ độc lập

♦ **Định nghĩa 1** Cho E là một K-kgv, $n \in \mathbb{N}^*$, $(x_1, ..., x_n) \in E^n$. Mọi phần tử x thuộc E sao cho tồn tại $(\lambda_1, ..., \lambda_n) \in K^n$ thỏa mãn

$x = \lambda_1 x_1 + ... + \lambda_n x_n = \sum_{i=1}^{n} \lambda_i x_i$ gọi là một **tổ hợp tuyến tính** của $x_1, ..., x_n$.

Tổng quát hơn, nếu $(x_i)_{i \in I}$ là một họ phần tử (có thể vô hạn) của một K-kgv E, mọi phần tử x thuộc E sao cho tồn tại một bộ phận hữu hạn J của I và một họ phần tử $(\lambda_i)_{i \in J}$ của K thỏa mãn $x = \sum_{i \in J} \lambda_i x_i$, gọi là **tổ hợp tuyến tính** của họ $(x_i)_{i \in I}$.

Theo quy ước: $\sum_{i \in \varnothing} x_i = 0$ (xem 6.1).

♦ **Mệnh đề** Cho E là một K-kgv, $F \in \mathfrak{P}(E)$.

Để F là một kgvc của E, thì cần và đủ là F khác rỗng và F ổn định đối với phép tổ hợp tuyến tính.

(nghĩa là : $\forall(\lambda, \mu) \in K^2$, $\forall(x, y) \in F^2$, $\quad \lambda x + \mu y \in F$).

Chứng minh:

1) Nếu F là một kgvc của E thì $F \neq \varnothing$ và với mọi (λ, μ) thuộc K^2 và mọi (x, y) thuộc F^2, λx và μy đều thuộc F, và do đó $\lambda x + \mu y \in F$.

2) Ngược lại, giả sử $F \neq \varnothing$ và: $\forall(\lambda, \mu) \in K^2$, $\forall(x, y) \in F^2$, $\lambda x + \mu y \in F$. Bằng cách chọn $\mu = 0$, sau đó $\lambda = \mu = 1$, ta kết luận F là một kgvc của E.

NHẬN XÉT: Để một bộ phận F của một kgv E là một kgvc của E, thì cần và đủ là:

$$\begin{cases} F \neq \varnothing \\ \forall \lambda \in K, \forall (x, y) \in F^2, \lambda x + y \in F. \end{cases}$$

♦ **Định nghĩa 2** Cho E là một K-kgv, $n \in \mathbb{N}^*$, $(x_1, ..., x_n) \in E^n$.

1) Ta nói họ hữu hạn $(x_1, ..., x_n)$ là **phụ thuộc (tuyến tính)** khi và chỉ khi:

$$\exists(\lambda_1, ..., \lambda_n) \in K^n - \{(0, ..., 0)\}, \quad \sum_{i=1}^{n} \lambda_i x_i = 0.$$

2) Ta nói họ hữu hạn $(x_1, ..., x_n)$ **độc lập (tuyến tính)** khi và chỉ khi nó không phụ thuộc tuyến tính, nghĩa là:

$$\forall(\lambda_1, ..., \lambda_n) \in K^n, \ (\sum_{i=1}^{n} \lambda_i x_i = 0 \Rightarrow (\forall i \in \{1, ..., n\}, \lambda_i = 0)).$$

Một họ hữu hạn phần tử của E còn được gọi là một **hệ** phần tử của E.

Tổng quát hơn, giả sử $(x_i)_{i\in I}$ là một họ phần tử (có thể vô hạn) của E.

1) Ta nói họ $(x_i)_{i\in I}$ là **phụ thuộc (tuyến tính)** khi và chỉ khi có một họ con hữu hạn của $(x_i)_{i\in I}$ là phụ thuộc tuyến tính, nghĩa là, khi và chỉ khi có một bộ phận hữu hạn J của I sao cho $(x_i)_{i\in J}$ là phụ thuộc tuyến tính.

2) Ta nói họ $(x_i)_{i\in I}$ **độc lập (tuyến tính)** khi và chỉ khi nó không phụ thuộc tuyến tính, nghĩa là khi và chỉ khi mọi họ con hữu hạn của $(x_i)_{i\in I}$ là độc lập tuyến tính.

Để nhấc lại rằng ta đang dùng thể K, đôi khi người ta nói **K-độc lập** (tuyến tính) (tương ứng: **K-phụ thuộc** (tuyến tính)) thay cho độc lập tuyến tính (tương ứng: phụ thuộc tuyến tính).

Ta nói hai vectơ x, y thuộc $E-\{0\}$ là **đồng phương** (hay: **cộng tuyến**) khi và chỉ khi tồn tại $\lambda \in K$ sao cho $y = \lambda x$.

NHẬN XÉT:

1) Để một họ (x) có một phần tử duy nhất là phụ thuộc tuyến tính, thì cần và đủ là : $x = 0$.

2) Đối với mọi $x \in E$, họ (x, x) là phụ thuộc tuyến tính vì $1x + (-1)x = 0$ và $(1, -1) \neq (0, 0)$.

3) Nếu họ phần tử $(x_i)_{i\in I}$ của E là phụ thuộc tuyến tính, thì mọi **họ mẹ** của $(x_i)_{i\in I}$ (nghĩa là, mọi họ phần tử của E nhận họ $(x_i)_{i\in I}$ làm một họ con) là phụ thuộc tuyến tính. Chẳng hạn, mọi họ chứa 0 là phụ thuộc tuyến tính.

4) Nếu họ phần tử $(x_i)_{i\in I}$ của E là độc lập tuyến tính, thì mọi họ con của $(x_i)_{i\in I}$ là độc lập tuyến tính.

5) Nếu họ phần tử $(x_i)_{i\in I}$ của E là độc lập (tuyến tính), thì các $(x_i)(i \in I)$ khác nhau từng đôi một. Thực vậy, giả sử $(i, j) \in I^2$ sao cho $i \neq j$; khi đó từ 3) suy ra họ (x_i, x_j) với hai phần tử là độc lập (tuyến tính), vì vậy (xem 2)): $x_i \neq x_j$.

6) Tính phụ thuộc (tuyến tính) và tính độc lập (tuyến tính) của một họ $(x_i)_{i\in I}$ không phụ thuộc vào "thứ tự" các phần tử. Nói cách khác, nếu σ là một hoán vị của I, họ $(x_{\sigma(i)})_{i\in I}$ là phụ thuộc tuyến tính (tương ứng: độc lập tuyến tính) khi và chỉ khi họ $(x_i)_{i\in I}$ là phụ thuộc (tuyến tính) (tương ứng: độc lập tuyến tính).

Nhận xét 6) trên đây cho phép đưa ra định nghĩa sau.

♦ **Định nghĩa 3** Một bộ phận A của E được gọi là **độc lập tuyến tính** khi và chỉ khi họ $(x)_{x\in A}$ là độc lập tuyến tính.

Đặc biệt, một bộ phận hữu hạn $\{x_1, ..., x_n\}$ của E (trong đó $n \in \mathbb{N}^*$ và $x_1, ..., x_n$ khác nhau từng đôi một) là độc lập tuyến tính khi và chỉ khi họ $(x_1, ..., x_n)$ là độc lập tuyến tính.

VÍ DỤ:

1) $E = \mathbb{R}^3$, $n = 2$, $x_1 = (1, 0, 1)$, $x_2 = (2, 1, -1)$; họ (x_1, x_2) là độc lập tuyến tính.

2) $E = \mathbb{R}^3$, $n = 3$, $x_1 = (1, 1)$, $n_2 = (2, 1)$, $x_3 = (-1, 0)$; họ (x_1, x_2, x_3) là phụ thuộc tuyến tính vì $x_1 - x_2 - x_3 = 0$.

3) $E = \mathbb{R}^{\mathbb{R}}$ và với mọi $\alpha \in \mathbb{R}$, $f_\alpha : \mathbb{R} \to \mathbb{R}$, $x \mapsto e^{\alpha x}$; họ $(f_\alpha)_{\alpha\in\mathbb{R}}$ là độc lập tuyến tính (xem bài tập 6.3.4).

Bài tập

◊ **6.3.1** Cho E là một $\mathbb{R}$-kgv, $x, y, z \in E$ sao cho (x, y, z) độc lập tuyến tính, $u = x + y$, $v = y + z$, $w = z + x$.

Chứng minh rằng (u, v, w) độc lập tuyến tính.

◊ **6.3.2** Giả sử $(N, n) \in (\mathbb{N} - \{0, 1\})^2$ sao cho: $\forall k \in \mathbb{N}, N \neq k^n$.

a) Chứng minh: $\sqrt[n]{N} \notin \mathbb{Q}$.

b) Chứng minh rằng $(1, \sqrt[n]{N})$ là $\mathbb{Q}$ - độc lập tuyến tính.

◊ **6.3.3** Cho $n \in \mathbb{N}$, $z_0, \ldots, z_n \in \mathbb{C}$ khác nhau từng đôi một. Chứng minh rằng $((X - z_k)^n)_{0 \leq k \leq n}$ độc lập tuyến tính trong $\mathbb{C}[X]$.

◊ **6.3.4** Chứng minh rằng các họ hàm số sau độc lập tuyến tính (đối với các luật thông thường):

a) $\left(\begin{array}{l} f_a :]0;1[\to \mathbf{R} \\ \qquad x \mapsto \dfrac{1}{1-ax} \end{array} \right)_{a \in]0;1[}$

b) $\left(\begin{array}{l} f_a : \mathbf{R} \to \mathbf{R} \\ \qquad x \mapsto \dfrac{1}{x^2+a^2+1} \end{array} \right)_{a \in [0;+\infty[}$

c) $\left(\begin{array}{l} f_a :]0;1[\to \mathbf{R} \\ \qquad x \mapsto \begin{cases} 1 \text{ nếu } x \geq a \\ 0 \text{ nếu } x < a \end{cases} \end{array} \right)_{a \in \mathbf{R}^2}$

d) $\left(\begin{array}{l} f_a : \mathbf{R} \to \mathbf{R} \\ \qquad x \mapsto e^{ax} \end{array} \right)_{a \in \mathbf{R}}$

e) $\left(\begin{array}{l} f_{a,b} : \mathbf{R}^2 \to \mathbf{R} \\ \qquad (x,y) \mapsto e^{ax+by} \end{array} \right)_{(a,\,b) \in \mathbf{R}^2}$

f) $\left(\begin{array}{l} f_a :]0;+\infty[\to \mathbf{R} \\ \qquad x \mapsto x^a \end{array} \right)_{a \in \mathbf{R}}$

g) $\left(\begin{array}{l} f_{a,b} :]0;+\infty[^2 \to \mathbf{R} \\ \qquad (x,y) \mapsto x^a y^b \end{array} \right)_{(a,b) \in \mathbf{R}^2}$

h) $\left(\begin{array}{l} f_n : \mathbf{R} \to \mathbf{R} \\ \qquad x \mapsto \sin(x^n) \end{array} \right)_{n \in \mathbf{N}^*}$

i) $\left(f, f \circ f, f \circ f \circ f\right)$, trong đó $f : \begin{array}{l} \mathbf{R} \to \mathbf{R} \\ x \mapsto \sin x \end{array}$.

◊ **6.3.5** Với mọi (a, h) của $\mathbb{R} \times \mathbf{R}_+^*$, ta ký hiệu $f_{a,h} : \mathbb{R} \to \mathbb{R}$ là ánh xạ xác định bởi:

$$f_{a,h}(x) = \begin{cases} 0 & \text{nếu } x \leq a \\ \dfrac{1}{h}(x-a) & \text{nếu } a \leq x \leq a+h \\ 1 & \text{nếu } a+h \leq x \end{cases}$$

Đối với các luật thông thường, họ $(f_{a,h})_{(a,h) \in \mathbf{R} \times \mathbf{R}_+^*}$ có độc lập tuyến tính không?

6.3.2 Không gian con sinh bởi một bộ phận

♦ **Định nghĩa 1** Cho E là một K-kgv, $A \in \mathfrak{P}(E)$. Giao của tất cả các kgvc của E chứa A:

$$\text{Vect}(A) = \bigcap_{\substack{F \in \mathbf{V}(E) \\ F \supset A}} F$$

gọi là **kgvc sinh bởi** A và ký hiệu là $\text{Vect}(A)$.

♦ **Mệnh đề 1** Cho E là một K-kgv, $A \in \mathfrak{P}(E)$.

1) $\text{Vect}(A)$ là kgvc nhỏ nhất (theo nghĩa bao hàm) trong các kgvc của E có chứa A.

2) • Nếu $A \neq \varnothing$, thì $\text{Vect}(A)$ là tập hợp các tổ hợp tuyến tính của các phần tử của A.

• $\text{Vect}(\varnothing) = \{0\}$.

Chứng minh:

1) • Theo 6.2, Mệnh đề 2, $\text{Vect}(A)$ là một kgvc của E vì nó là giao của những kgvc của E.

• Theo định nghĩa của $\text{Vect}(A)$, ta suy ra: $A \subset \text{Vect}(A)$.

• Giả sử F là một kgvc của E chứa A. Theo định nghĩa của $\text{Vect}(A)$, ta suy ra: $\text{Vect}(A) \subset F$. Như vậy, $\text{Vect}(A)$ là một kgvc của E chứa A, và nó nằm trong mọi kgvc của E có chứa A.

2) Hiển nhiên, tập hợp chỉ có một phần tử $\{0\}$ là kgvc nhỏ nhất của E có chứa $\varnothing$.

Giả sử $A \neq \varnothing$ và ký hiệu C là tập hợp các tổ hợp tuyến tính các phần tử của A:

$$C = \left\{ x \in E : \exists n \in \mathbb{N}^*, \exists (a_1, \ldots, a_n) \in A^n, \exists (\lambda_1, \ldots, \lambda_n) \in K^n, x = \sum_{i=1}^{n} \lambda_i a_i \right\}.$$

Ta chứng minh rằng C là kgvc nhỏ nhất của E có chứa A.

a) • Hiển nhiên $C \neq \varnothing$.

• Giả sử $(x, y) \in C^2$. Tồn tại $n \in \mathbb{N}^*$, $(a_1, \ldots, a_n) \in A^n$, $(\lambda_1, \ldots, \lambda_n) \in K^n$ sao cho $x = \sum_{i=1}^{n} \lambda_i a_i$ và $p \in \mathbb{N}^*$, $(b_1, \ldots, b_p) \in A^p$, $(\mu_1, \ldots, \mu_p) \in K^p$ sao cho $y = \sum_{j=1}^{p} \mu_j b_j$.

Đặt $c_k = \begin{cases} a_k & \text{nếu } 1 \leq k \leq n \\ b_{k-n} & \text{nếu } n+1 \leq k \leq n+p \end{cases}$, $\nu_k = \begin{cases} \lambda_k & \text{nếu } 1 \leq k \leq n \\ \mu_{k-n} & \text{nếu } n+1 \leq k \leq n+p, \end{cases}$

ta có: $\begin{cases} \forall k \in \{1, \ldots, n+p\}, c_k \in A \\ x + y = \sum_{i=1}^{n} \lambda_i a_i + \sum_{j=1}^{p} \mu_j b_j = \sum_{k=1}^{n+p} \nu_k c_k \end{cases}$, vì vậy $x + y \in C$.

• Tương tự, ta chứng minh rằng: $\forall \lambda \in K, \forall x \in C, \quad \lambda x \in C$.

Như vậy C là một kgvc của E.

b) Vì mọi phần tử a thuộc A là một tổ hợp tuyến tính các phần tử của A (chỉ cần viết $a = 1a$), nên C chứa A.

c) Giả sử G là một kgvc của E có chứa A, và $x \in C$. Tồn tại $n \in \mathbb{N}^*$, $(a_1, ..., a_n) \in A^n$, $(\lambda_1, ..., \lambda_n) \in K^n$ sao cho $x = \sum_{i=1}^{n} \lambda_i a_i$. Vì G chứa A và G là một kgvc, nên ta suy ra $x \in G$, điều đó chứng tỏ $C \subset G$.

Như vậy ta đã chứng minh rằng C là kgvc nhỏ nhất của E có chứa A, và do đó: $C = \text{Vect}(A)$. ■

Đặc biệt, kgvc sinh bởi tập hợp gồm một phần tử $\{x\}$ (trong đó $x \in E$) là Kx, nghĩa là $\{\lambda x; \lambda \in K\}$.

♦ **Định nghĩa 2** Cho E là một K-kgv, $(x_i)_{i \in I}$ là một họ phần tử của E. kgvc sinh bởi bộ phận $\{x_i : i \in I\}$ của E gọi là **kgvc sinh bởi** $(x_i)_{i \in I}$, và ký hiệu là $\text{Vect}((x_i)_{i \in I})$.

Đặc biệt, kgvc của E sinh bởi một họ hữu hạn khác rỗng các phần tử $(x_1, ..., x_n)$ của E là $\left\{\sum_{i=1}^{n} \lambda_i x_i ; (\lambda_1, ..., \lambda_n) \in K^n\right\}$.

♦ **Mệnh đề 2** Cho E là một K-kgv, $A, B \in \mathfrak{P}(E)$. Ta có

1) $A \subset B \Rightarrow \text{Vect}(A) \subset \text{Vect}(B)$

2) A là một kgvc của E khi và chỉ khi $\text{Vect}(A) = A$

3) $\text{Vect}(\text{Vect}(A)) = \text{Vect}\, A$

4) $\text{Vect}(A \cup B) = \text{Vect}(A) + \text{Vect}(B)$.

Chứng minh:

Dễ dàng suy ra 1), 2), 3). Ta chứng minh 4).

• $\begin{cases} A \subset A \cup B \\ B \subset A \cup B \end{cases} \overset{1)}{\Rightarrow} \begin{cases} \text{Vect}(A) \subset \text{Vect}(A \cup B) \\ \text{Vect}(B) \subset \text{Vect}(A \cup B) \end{cases} \Rightarrow \text{Vect}(A) + \text{Vect}(A) \subset \text{Vect}(A \cup B)$,

xem 6.2, Mệnh đề 4, 3).

• Ngược lại, giả sử $x \in \text{Vect}(A \cup B)$. Tồn tại $n \in \mathbb{N}^*$, $(c_1, ..., c_n) \in (A \cup B)^n$, $(\lambda_1, ..., \lambda_n) \in K^n$ sao cho $x = \sum_{i=1}^{n} \lambda_i c_i$. Bằng cách nhóm các phần tử của A lại với nhau và các phần tử của B lại với nhau, ta suy ra rằng tồn tại $a \in \text{Vect}(A)$, $b \in \text{Vect}(B)$ sao cho $x = a + b$.

Điều đó chứng tỏ: $\text{Vect}(A \cup B) \subset \text{Vect}(A) + \text{Vect}(B)$.

6.3.3 Tổng của nhiều kgvc

Bây giờ chúng ta sẽ tổng quát hóa việc khảo sát tổng của hai kgvc đã được thực hiện ở 6.2.

◆ **Định nghĩa 1** Cho E là một K-kgv, $n \in \mathbb{N}^*$, $F_1, F_2, ..., F_n$ là những kgvc của E. Ta định nghĩa tổng của $F_1, ..., F_n$, ký hiệu $F_1 + F_2 + ... + F_n$ (hay $\sum_{i=1}^{n} F_i$), là :

$$F_1 + ... + F_n = \{x \in E;\ \exists (x_1, ..., x_n) \in F_1 \times ... \times F_n,\ x = x_1 + ... + x_n\}$$
$$= \{x_1 + ... + x_n;\ (x_1, ..., x_n) \in F_1 \times ... \times F_n\}.$$

Ta quy ước rằng: $\sum_{i \in \varnothing} F_i = \{0\}$.

Dễ dàng chứng minh (bằng quy nạp) Mệnh đề sau.

◆ **Mệnh đề** Cho E là một K-kgv, $n \in \mathbb{N}^*$, $F_1, ..., F_n$ là những kgvc của E. Ta có:

1) $\forall \sigma \in \mathfrak{S}_n,\ \sum_{i=1}^{n} F_{\sigma(i)} = \sum_{i=1}^{n} F_i$

2) Với mọi phân hoạch H của $\{1, 2, ..., n\}$: $\sum_{I \in H} \left(\sum_{i \in I} F_i \right) = \sum_{i=1}^{n} F_i$.

Nói cách khác:

1) Tổng của nhiều kgvc không phụ thuộc vào thứ tự các kgvc đó.

2) Trong tổng của nhiều kgvc, ta có thể "gộp" nhiều hạng tử thành từng nhóm.

Đặc biệt, với mọi kgvc con F_1, F_2, F_3 của E, ta có:

$$(F_1 + F_2) + F_3 = F_1 + (F_2 + F_3) = F_1 + F_2 + F_3.$$

NHẬN XÉT:

Với mọi kgvc $F_1, ..., F_n$ của một K-kgv E, ta có: $\sum_{i=1}^{n} F_i = \text{Vect}\left(\bigcup_{i=1}^{n} F_i \right)$.

Đặc biệt, với mọi $(x_1, ..., x_n)$ thuộc E^n, ta có: $\text{Vect}(x_1, ..., x_n) = \sum_{i=1}^{n} Kx_i$.

◆ **Định nghĩa 2** Cho E là một K-kgv, $n \in \mathbb{N}^*$, $F_1, ..., F_n$ là những kgvc của E. Ta nói rằng $F_1, ..., F_n$ **có tổng trực tiếp** khi và chỉ khi:

$$\forall (x_1, ..., x_n) \in F_1 \times ... \times F_n,\ (x_1 + ... + x_n = 0 \Rightarrow x_1 = ... = x_n = 0).$$

Khi $F_1, ..., F_n$ có tổng trực tiếp, thay cho $F_1 + ... + F_n$ ta viết $F_1 \oplus ... \oplus F_n$, hay $\bigoplus_{i=1}^{n} F_i$.

Thay cho cách nói $F_1, ..., F_n$ **có tổng trực tiếp**, ta còn nói $F_1 + ... + F_n$ **là tổng trực tiếp**, hay $F_1, ..., F_n$ **độc lập tuyến tính.**

◆ **Định lý** Cho E là một K-kgv, $n \in \mathbb{N}^*$, $F_1, ..., F_n$ là những kgvc của E. Các tính chất sau đây tương đương từng đôi một:

1) $F_1, ..., F_n$ có tổng trực tiếp

2) Mọi phần tử của $\sum_{i=1}^{n} F_i$ được phân tích một cách duy nhất thành tổng những phần tử của $F_1, ..., F_n$

3) $\forall i \in \{1, ..., n\}, \quad F_i \cap \left(\sum_{\substack{1 \le j \le n \\ j \ne i}} F_j \right) = \{0\}$

4) $\forall i \in \{2, ..., n\}, \quad F_i \cap \left(\sum_{1 \le j \le i-1} F_j \right) = \{0\}$

5) Với mọi $(x_1, ..., x_n)$ thuộc $(F_1 - \{0\}) \times ... \times (F_n - \{0\})$, $(x_1, ..., x_n)$ độc lập tuyến tính (ta giả thiết rằng mọi $F_1, ..., F_n$ đều $\neq \{0\}$).

Chứng minh:

1) $\Rightarrow$ 2): Giả sử $F_1, ..., F_n$ có tổng trực tiếp.

Giả sử $x \in F_1 + ... + F_n$, $(x_1, ..., x_n) \in F_1 \times ... \times F_n$, $(y_1, ..., y_n) \in F_1 \times ... \times F_n$ sao cho:

$$x = \sum_{i=1}^{n} x_i = \sum_{i=1}^{n} y_i .$$

Khi đó: $\begin{cases} \forall i \in \{1,...,n\}, \quad x_i - y_i \in F_i \\ \sum_{i=1}^{n} (x_i - y_i) = 0 \end{cases}$, do đó vì $F_1 + ... + F_n$ là tổng trực tiếp nên:

$\forall i \in \{1, ..., n\}$, $x_i - y_i = 0$, và vì vậy $(x_1, ..., x_n) = (y_1, ..., y_n)$.

2) $\Rightarrow$ 3): Giả sử mọi phần tử của $\sum_{i=1}^{n} F_i$ đều phân tích một cách duy nhất thành tổng những phần tử của $F_1, ..., F_n$.

Giả sử $i \in \{1, ..., n\}$ và $x \in F_i \cap \left(\sum_{\substack{1 \le j \le n \\ j \ne i}} F_j \right)$.

Thế thì $x \in F_i$ và tồn tại $(x_1, ..., x_{i-1}, x_{i+1}, ..., x_n) \in F_1 \times ... \times F_{i-1} \times F_{i+1} \times ... \times F_n$ sao cho: $x = \sum_{\substack{1 \le j \le n \\ j \ne i}} x_j$. Đặt $x_i = -x$, ta sẽ nhận được: $\begin{cases} \forall j \in \{1,...,n\}, \ x_j \in F_j \\ \sum_{j=1}^{n} x_j = 0 \end{cases}$.

Do đó, vì 0 cũng được phân tích thành $0 = 0 + ... + 0$ $(0 \in F_i)$, nên từ 2) ta suy ra:

$$\forall j \in \{1, ..., n\}, x_j = 0.$$

Đặc biệt $x = -x_i = 0$ nên $F_i \cap \left(\sum_{\substack{1 \le j \le n \\ j \ne i}} F_j \right) = \{0\}$.

3) $\Rightarrow$ 4): Hiển nhiên vì: $\sum_{1\le j\le i-1} F_j \subset \sum_{\substack{1\le j\le n \\ j\neq i}} F_j$.

4) $\Rightarrow$ 5): Giả sử 4) đúng.

Cho $x_1 \in F_1 - \{0\}, ..., x_n \in F_n - \{0\}, (\lambda_1, ..., \lambda_n) \in K^n$ sao cho $\sum_{i=1}^{n} \lambda_i x_i = 0$.

- Ta có $\lambda_n x_n \in F_n$ và $\lambda_n x_n = -\sum_{i=1}^{n-1} \lambda_i x_i \in \sum_{1\le j\le n-1} F_j$, nên theo 4) ta suy ra: $\lambda_n x_n = 0$, do đó vì $x_n \neq 0$ nên: $\lambda_n = 0$.

- Lập lại lập luận trên, ta sẽ suy ra: $\lambda_n = 0$, $\lambda_{n-1} = 0$, ..., $\lambda_1 = 0$. Như vậy, $(x_1, ..., x_n)$ độc lập tuyến tính.

5) $\Rightarrow$ 1): Giả sử $F_1, ..., F_n$ đều $\neq \{0\}$ và điều kiện 5) được thỏa mãn.

Cho $(x_1, ..., x_n) \in F_1 \times ... \times F_n$ sao cho $\sum_{i=1}^{n} x_i = 0$. Đặt $I = \{i \in \{1, ..., n\}; x_i \neq 0\}$.

Giả sử $I \neq \varnothing$ và đặt $J = \{1, ..., n\} - I$.

Vì $F_1, ..., F_n$ đều $\neq \{0\}$ nên tồn tại $(y_1, ..., y_n)$ thuộc $(F_1 - \{0\}) \times ... \times (F_n - \{0\})$.

Với $i \in \{1, ..., n\}$, đặt: $z_i = \begin{cases} x_i & \text{nếu } i \in I \\ y_i & \text{nếu } i \in J \end{cases}$.

Họ $(z_1, ..., z_n)$ phụ thuộc tuyến tính vì là một họ mẹ $\left(\sum_{i\in I} x_i = 0\right)$ của họ phụ thuộc tuyến tính $(x_i)_{i\in I}$. Hơn nữa : $\forall i \in I, z_i \in F_i - \{0\}$. Điều này mâu thuẫn với giả thiết 5).

Từ đó suy ra $I = \varnothing$, nghĩa là: $\forall i \in \{1, ..., n\}, x_i = 0$.

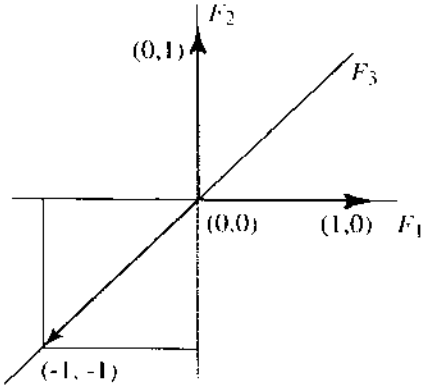
NHẬN XÉT:

1) Nếu F_1, F_2, F_3 là những kgvc của một kgv E, ta có thể có $F_1 \cap F_2 = F_1 \cap F_3 = F_2 \cap F_3 = \{0\}$, mà F_1, F_2, F_3 không có tổng trực tiếp, như trong ví dụ sau:

$K = \mathbb{R}$, $E = \mathbb{R}^2$, $F_1 = \mathbb{R} \times \{0\}$,

$F_2 = \{0\} \times \mathbb{R}$, $F_3 = \{(x, x); x \in \mathbb{R}\}$.

Trong ví dụ này, F_1, F_2, F_3 không có tổng trực tiếp vì $(1, 0) \in F_1$, $(0, 1) \in F_2$, $(-1, -1) \in F_3$, chúng đều khác không nhưng có tổng bằng $(0, 0)$.



2) Nếu F_1, F_2, F_3 là những kgvc của một kgv E, ta có thể có $F_1 \cap F_2 \cap F_3 = \{0\}$ mà F_1, F_2, F_3 không có tổng trực tiếp (cũng xem ví dụ trên).

3) Sự kiện các không gian con $F_1, ..., F_n$ có tổng trực tiếp không phụ thuộc vào thứ tự của $F_1, ..., F_n$. Nói cách khác, nếu $F_1, ..., F_n$ có tổng trực tiếp, thì với mọi hoán vị σ của $\mathfrak{S}_n$, $F_{\sigma(1)}, ..., F_{\sigma(n)}$ cũng có tổng trực tiếp.

4) Nếu các kgvc $F_1, ..., F_n$ có tổng trực tiếp, thì với mọi p thuộc $\{1, ..., n\}$, các kgvc $F_1, ..., F_p$ cũng có tổng trực tiếp.

Bài tập

◊ **6.3.6** Cho E là một K-kgv, F, G, F', G' là những kgvc của E sao cho:

$$\begin{cases} F \text{ và } G \text{ bù nhau trong } E \\ F' \text{ và } G' \text{ bù nhau trong } E \\ F' \subset G \end{cases}$$

Chứng minh rằng $F, F', G \cap G'$ có tổng trực tiếp và: $F \oplus F' \oplus (G \cap G') = E$.

◊ **6.3.7** Giả sử E là một K-kgv, $n \in \mathbb{N}^*$, $(x_1, ..., x_n) \in E^n$. Chứng minh rằng $(x_1, ..., x_n)$ độc lập tuyến tính khi và chỉ khi:

$$\begin{cases} \forall i \in \{1, ..., n\}, x_i \neq 0 \\ \sum_{i=1}^{n} Kx_i \text{ có tổng trực tiếp} \end{cases}$$

◊ **6.3.8** Cho E là một K-kgv, $n \in \mathbb{N}^*$, $F_1, ..., F_n, G_1, ..., G_n$ là những kgvc của E sao cho:

$$\begin{cases} F_1, ..., F_n \text{ có tổng trực tiếp} \\ \forall i \in \{1, ..., n\}, G_i \subset F_i \end{cases}$$

Chứng minh rằng $G_1, ..., G_n$ có tổng trực tiếp.

6.3.4 Họ sinh, cơ sở

◆ **Định nghĩa 1** Cho E là một K-kgv, G là một họ phần tử của E. Ta nói G là một **họ sinh của** E (hay: G **sinh ra** E) khi và chỉ khi:

$$\text{Vect}\,(G) = E.$$

Dễ dàng suy ra Mệnh đề sau.

◆ **Mệnh đề 1** Nếu $G = (x_1, ..., x_n)$ là một họ hữu hạn phần tử của một K-kgv E, thì G sinh ra E khi và chỉ khi:

$$\forall x \in E, \exists\, (\lambda_1, ..., \lambda_n) \in K^n, \quad x = \sum_{i=1}^{n} \lambda_i x_i \ .$$

Một bộ phận G của một K-kgv E được gọi là một **tập sinh của** E khi và chỉ khi: $\text{Vect}\,(G) = E$. Điều đó có nghĩa là họ $(x)_{x \in G}$ các phần tử của G sinh ra E theo nghĩa Định nghĩa 1.

◆ **Định nghĩa 2** Ta nói họ phần tử $\mathcal{B}$ của một K-kgv E là một **cơ sở** của E khi và chỉ khi: $\mathcal{B}$ độc lập tuyến tính và là một họ sinh của E.

NHẬN XÉT:

$\varnothing$ là một cơ sở của $\{0\}$.
Dễ dàng suy ra Mệnh đề sau.

◆ **Mệnh đề - Định nghĩa 2** Một họ hữu hạn $\mathcal{B} = (e_1, ..., e_n)$ những phần tử của một K-kgv E là một cơ sở của E khi và chỉ khi:

$$\forall x \in E, \exists!\, (x_1, ..., x_n) \in K^n, \quad x = \sum_{i=1}^{n} x_i e_i \ .$$

Nếu E có một cơ sở hữu hạn $\mathcal{B} = (e_1, ..., e_n)$, thì với mọi x thuộc E, các phần tử $x_1, ..., x_n$ được xác định trên đây được gọi là **các tọa độ** (hay: **các thành phần**) **của** x **trong cơ sở** $\mathcal{B}$; x_i được gọi là **tọa độ** (hay: **thành phần**) **thứ** i **của** x **trong cơ sở** $\mathcal{B}$.

Bài tập

◊ **6.3.9** Cho E là một K-kgv, $n \in \mathbb{N}^*$, $F_1, ..., F_n$ là những kgvc của E.

a) Chứng minh rằng, nếu $F_1, ..., F_n$ có tổng trực tiếp và nếu với mọi i thuộc $\{1, ..., n\}$, $\mathcal{L}_i$ là một họ độc lập tuyến tính trong F_i, thì $\bigcup_{i=1}^{n} \mathcal{L}_i$ độc lập tuyến tính trong E.

b) Chứng minh rằng, nếu $F_1 + ... + F_n = E$ và nếu, $\mathcal{G}_i$ là một họ sinh của F_i với mọi i thuộc $\{1, ..., n\}$, thì $\bigcup_{i=1}^{n} \mathcal{G}_i$ là một họ sinh của E.

c) Chứng minh rằng, nếu $F_1, ..., F_n$ có tổng trực tiếp và có tổng bằng E, và nếu $\mathcal{B}_i$ là một cơ sở của F_i với mọi i thuộc $\{1, ..., n\}$, thì $\bigcup_{i=1}^{n} \mathcal{B}_i$ là một cơ sở của E.

6.4 Lý thuyết về số chiều

Trong §6.4 này, E chỉ một K-kgv.

♦ **Mệnh đề 1** Cho $(n, p) \in (\mathbb{N}^*)^2$, $(x_1, ..., x_{n+p}) \in E^{n+p}$,
$\mathcal{F} = (x_1, ..., x_p)$, $\mathcal{F}' = (x_1, ..., x_p, x_{p+1}, ..., x_{n+p})$.

1) Nếu $\mathcal{F}'$ độc lập tuyến tính, thì $\mathcal{F}$ độc lập tuyến tính

2) Nếu $\mathcal{F}$ là một họ sinh của E, thì $\mathcal{F}'$ là một họ sinh của E.

Chứng minh:

1) Xem 6.3.1, Nhận xét 4).

2) Giả sử $x \in E$. Vì $\mathcal{F}$ sinh ra E nên tồn tại $(\lambda_1, ..., \lambda_p) \in K^p$ sao cho $x = \sum_{i=1}^{p} \lambda_i x_i$.

Do đó, nếu đặt $\lambda_{p+1} = ... = \lambda_{n+p} = 0$ thì ta có $x = \sum_{i=1}^{n+p} \lambda_i x_i$.

Điều đó chứng tỏ rằng $\mathcal{F}'$ sinh ra E. ■

Mệnh đề trên được tổng quát hóa cho một họ bất kỳ (không nhất thiết hữu hạn):

1) Nếu $\mathcal{F} \subset \mathcal{F}'$ và nếu $\mathcal{F}'$ độc lập tuyến tính, thì $\mathcal{F}$ độc lập tuyến tính.

2) Nếu $\mathcal{F} \subset \mathcal{F}'$ và nếu $\mathcal{F}$ là một họ sinh của E, thì $\mathcal{F}'$ là một họ sinh của E.

(Trong đó $\mathcal{F} \subset \mathcal{F}'$ có nghĩa là $\mathcal{F}$ là một họ con của $\mathcal{F}'$).

♦ **Mệnh đề 2** Cho $n \in \mathbb{N}^*$, $(x_1, ..., x_{n+1}) \in E^{n+1}$, $\mathcal{F} = (x_1, ..., x_n)$, $\mathcal{F}' = (x_1, ..., x_n, x_{n+1})$.

1) Nếu $\mathcal{F}$ độc lập tuyến tính và nếu $x_{n+1} \notin \text{Vect}(\mathcal{F})$, thì $\mathcal{F}'$ độc lập tuyến tính.

2) Nếu $\mathcal{F}'$ là một họ sinh của E và nếu $x_{n+1} \in \text{Vect}(\mathcal{F})$, thì $\mathcal{F}$ là một họ sinh của E.

Chứng minh:

1) Giả sử $(\lambda_1, ..., \lambda_{n+1}) \in K^{n+1}$ sao cho $\sum_{i=1}^{n+1} \lambda_i x_i = 0$. Nếu $\lambda_{n+1} \neq 0$ thì ta suy ra

$x_{n+1} = \sum_{i=1}^{n} \left(-\lambda_{n+1}^{-1} \lambda_i\right) x_i \in \text{Vect}(\mathcal{F})$, mâu thuẫn.

Vì vậy $\lambda_{n+1} = 0$, do đó $\sum_{i=1}^{n} \lambda_i x_i = 0$, từ đó suy ra $\lambda_1 = ... = \lambda_n = 0$, vì $\mathcal{F}$ độc lập tuyến tính.

2) Giả sử : $x \in E$. Vì $\mathcal{F}'$ là họ sinh của E nên tồn tại $(\lambda_1, ..., \lambda_{n+1}) \in K^{n+1}$ sao cho

$x = \sum_{i=1}^{n+1} \lambda_i x_i$.

Vì $x_{n+1} \in \text{Vect}(\mathcal{F})$ nên tồn tại $(\mu_1, ..., \mu_n) \in K^n$ sao cho : $x_{n+1} = \sum_{i=1}^{n} \mu_i x_i$.

Ta suy ra : $x = \left(\sum_{i=1}^{n} \lambda_i x_i\right) + \lambda_{n+1} x_{n+1} = \sum_{i=1}^{n} (\lambda_i + \lambda_{n+1}\mu_i) x_i \in \text{Vect}(\mathcal{G})$.

Điều đó chứng tỏ $\mathcal{G}$ là họ sinh của E. ■

Mệnh đề trên được tổng quát hóa cho các họ tùy ý (không nhất thiết hữu hạn):

1) Nếu $\mathcal{G}$ độc lập tuyến tính và nếu $x \notin \text{Vect}(\mathcal{G})$, thì $\mathcal{G} \cup \{x\}$ độc lập tuyến tính (trong đó $\mathcal{G} \cup \{x\}$ thu được bằng cách thêm x vào họ $\mathcal{G}$).

2) Nếu $\mathcal{G} \cup \{x\}$ là họ sinh của E và nếu $x \in \text{Vect}(\mathcal{G})$, thì $\mathcal{G}$ là họ sinh của E. ■

Có thể phát biểu mệnh đề trên dưới dạng:

1) Nếu thêm vào một họ độc lập tuyến tính một vectơ không phân tích được trên họ đó, thì ta sẽ được một họ mới độc lập tuyến tính.

2) Nếu đưa ra khỏi một họ sinh của E một vectơ phân tích được theo các phần tử khác của họ, thì ta sẽ thu được một họ sinh mới của E.

♦ Bổ đề (Định lý thay thế)

Cho $\mathcal{G} = (x_1, ..., x_p)$, $\mathcal{L} = (y_1, ..., y_r)$ là hai họ hữu hạn phần tử của E. Nếu $\mathcal{G}$ là một họ sinh của E và nếu $\mathcal{L}$ độc lập tuyến tính thì:

1) $r \leq p$

2) Có ít nhất một cách thay thế r vectơ thuộc $\mathcal{G}$ bằng những vectơ thuộc $\mathcal{L}$ để thu được một họ sinh của E.

Chứng minh.

• Vì $\mathcal{G}$ sinh ra E nên tồn tại $(\lambda_{1,1}, ..., \lambda_{1,p}) \in K^p$ sao cho $y_1 = \sum_{j=1}^{p} \lambda_{1,j} x_j$.

Ta có : $(\lambda_{1,1}, ..., \lambda_{1,p}) \neq (0, ..., 0)$, vì nếu không như thế thì $y_1 = 0$, điều này mâu thuẫn với tính độc lập tuyến tính của $\mathcal{L}$.
Nếu cần ta hoán vị $x_1, ..., x_p$ (và $\lambda_{1,1}, ..., \lambda_{1,p}$), ta có thể quy về trường hợp: $\lambda_{1,1} \neq 0$.

Khi đó, nếu đặt $\mathcal{G}_1 = (y_1, x_2, ..., x_p)$ thì ta có $x_1 = \lambda_{1,1}^{-1} y_1 - \sum_{j=2}^{p} \lambda_{1,1}^{-1} \lambda_{1,j} x_j \in \text{Vect}(\mathcal{G}_1)$.

Vì $\mathcal{G}$ sinh ra E nên $(y_1, x_1, ..., x_p)$ sinh ra E (theo Mệnh đề 1, 2)), do đó vì $x_1 \in \text{Vect}(\mathcal{G}_1)$, nên $\mathcal{G}_1$ sinh ra E (theo Mệnh đề 2,2).

Như vậy, ta đã thay một trong các vectơ của $\mathcal{G}$ bởi y_1 để thu được một họ sinh $\mathcal{G}_1 = (y_1, x_2, ..., x_p)$.

• Cho $s \in \mathbb{N}^*$ sao cho $s \leq \text{Min}(p - 1, r - 1)$. Giả sử (có thể sau một hoán vị của x_1, ..., x_p) rằng họ $\mathcal{G}_s = (y_1, ..., y_s, x_{s+1}, ..., x_p)$ là một họ sinh của E.

Tồn tại $(\lambda_{s+1,1}, ..., \lambda_{s+1,p}) \in K^p$ sao cho : $y_{s+1} = \sum_{j=1}^{s} \lambda_{s+1,j} y_j + \sum_{j=s+1}^{p} \lambda_{s+1,j} x_j$.

Nếu $(\lambda_{s+1,s+1}, ..., \lambda_{s+1,p}) = (0, ..., 0)$ thì $y_{s+1} = \sum_{j=1}^{s} \lambda_{s+1,j} y_j$, điều này mâu thuẫn với tính độc lập tuyến tính của $(y_1, ..., y_{s+1})$, (do đó của $\mathcal{L}$). Nếu cần ta có thể hoán vị

$x_{s+1}, ..., x_p$ (và $\lambda_{s+1,s+1}, ..., \lambda_{s+1,p}$), ta có thể quy về trường hợp $\lambda_{s+1,s+1} \neq 0$. Khi đó, nếu đặt $\mathcal{G}_{s+1} = (y_1, ..., y_s, y_{s+1}, x_{s+2}, ..., x_p)$, thì cũng với lập luận như ở trên, ta suy ra rằng $\mathcal{G}_{s+1}$ là một họ sinh của E.

Như vậy ta đã thay thế những vectơ của $\mathcal{G}$ bằng những vectơ của $\mathcal{L}$ để nhận được một họ sinh.

- Giả sử $r > p$.

Với các ký hiệu trên đây, $\mathcal{G}_p = (y_1, ..., y_p)$ là một họ sinh của E, vì vậy $y_{p+1} \in \text{Vect}(\mathcal{G}_p)$, điều này mâu thuẫn với tính độc lập tuyến tính của $(y_1, ..., y_{p+1})$, do đó của $\mathcal{L}$.

Như vậy $r \leq p$ và $\mathcal{G}_r = (y_1, ..., y_r, x_{r+1}, ..., x_p)$ là một họ sinh của E.

♦ **Định nghĩa 1** Một K-kgv E được gọi là **hữu hạn chiều** khi và chỉ khi E có ít nhất một họ sinh hữu hạn.

VÍ DỤ:

1) $\{0\}$ và K^n ($n \in \mathbb{N}^*$) là hai K-kgv hữu hạn chiều.

2) $K[X]$ là một K-kgv không hữu hạn chiều, vì nếu $K[X]$ có một họ sinh hữu hạn $(P_1, ..., P_n)$, thì với mọi P thuộc $K[X]$, ta sẽ có $\deg(P) \leq \underset{1 \leq i \leq n}{\text{Max}} (\deg(P_i))$.

♦ **Định lý - Định nghĩa 1** Giả sử E là một K-kgv hữu hạn chiều. Thế thì:

1) E có ít nhất một cơ sở hữu hạn

2) Mọi cơ sở của E có cùng lực lượng
Lực lượng của một cơ sở của E được gọi là **số chiều** của E và ký hiệu là $\dim_K(E)$, hoặc $\dim(E)$.

Chứng minh:

1) Vì E hữu hạn chiều, nên E có ít nhất một họ sinh $\mathcal{G} = (x_1, ..., x_p)$. Nếu $\mathcal{G}$ độc lập tuyến tính thì $\mathcal{G}$ là một cơ sở hữu hạn của E.

Giả sử $\mathcal{G}$ phụ thuộc tuyến tính: tồn tại $(\lambda_1, ..., \lambda_p) \in K^p - \{(0, ..., 0)\}$ sao cho $\sum_{i=1}^{p} \lambda_i x_i = 0$.

Nếu cần ta hoán vị $x_1, ..., x_p$ (và $\lambda_1, ..., \lambda_p$), ta có thể quy về $\lambda_p \neq 0$, do đó, nếu đặt $\mathcal{G}_1 = (x_1, ..., x_{p-1})$ thì $x_p = -\sum_{i=1}^{p-1} \lambda_p^{-1} \lambda_i x_i \in \text{Vect}(\mathcal{G}_1)$.

Do đó theo Mệnh đề 2, 2), $\mathcal{G}_1$ là một họ sinh của E.

Ta lập lại quá trình trên.

Nếu tồn tại $r \in \{1, ..., p\}$ sao cho họ sinh $\mathcal{G}_r = (x_1, ..., x_{p-r})$ độc lập tuyến tính, thì $\mathcal{G}_r$ là một cơ sở của E.

Nếu không như thế thì $\mathcal{G}_1 = (x_1)$ phụ thuộc tuyến tính và là một họ sinh, khi đó $E = \{0\}$, và $\varnothing$ là một cơ sở hữu hạn của E.

2) Theo 1), E có ít nhất một cơ sở hữu hạn $\mathcal{B}$; gọi n là số phần tử của $\mathcal{B}$.

Giả sử $\mathcal{B}'$ là một cơ sở (khác) của E. Nếu $\mathcal{B}'$ là vô hạn hoặc hữu hạn với lực lượng $> n$, thì $\mathcal{B}'$ chứa ít nhất một họ hữu hạn độc lập tuyến tính $\mathcal{L}$ có $n + 1$ phần tử. Nhưng $\mathcal{B}$ là

một họ sinh với n phần tử và $\mathcal{L}$ là một họ độc lập tuyến tính với $n + 1$ phần tử, điều này mâu thuẫn với kết quả 1) của định lý thay thế.

Do vậy, $\mathcal{B}'$ hữu hạn với lực lượng $\leq n$.

Tương tự, vì $\mathcal{B}$ độc lập tuyến tính với n phần tử và $\mathcal{B}'$ là một họ sinh, nên kết quả 1) của định lý thay thế chứng tỏ rằng : $n \leq \text{Card}(\mathcal{B}')$.

Như vậy $\mathcal{B}'$ hữu hạn và có n phần tử. ■

NHẬN XÉT:

Phép chứng minh trên đã xác lập một cách chính xác rằng mọi họ sinh hữu hạn của một K-kgv hữu hạn chiều có chứa ít nhất một cơ sở. ■

Ta nói một kgv con F của một kgv E là **hữu hạn chiều** khi và chỉ khi kgv F là hữu hạn chiều.

Đôi khi người ta nói một kgv không hữu hạn chiều là kgv **"vô hạn chiều"**.

NHẬN XÉT:

1) Với mọi kgv hữu hạn chiều E: $\dim(E) = 0 \Leftrightarrow E = \{0\}$.

2) Số chiều của một K-kgv hữu hạn chiều "phụ thuộc" vào thể K. Chẳng hạn:

$$\dim_{\mathbb{C}}(\mathbb{C}^2) = 2, \text{ nhưng } \dim_{\mathbb{R}}(\mathbb{C}^2) = 4.$$

3) Sự kiện rằng tồn tại đối với mọi kgv (không nhất thiết hữu hạn chiều), ít nhất một cơ sở, là tương đương lôgic của *tiên đề chọn*, mà việc nghiên cứu nằm ngoài phạm vi cuốn sách này.

♦ **Định lý 2 (Định lý về cơ sở không đầy đủ)**

Cho E là một K-kgv hữu hạn chiều, $\mathcal{L} = (v_1, ..., v_r)$ là một họ độc lập tuyến tính trong E.

Dạng thứ 1 (dạng mạnh)

Giả sử $\mathcal{B} = (e_1, ..., e_n)$ là một cơ sở của E. Có ít nhất một cách bổ sung $n - r$ vectơ thuộc $\mathcal{B}$ vào $\mathcal{L}$ để được một cơ sở của E.

Dạng thứ 2 (dạng yếu)

Có ít nhất một cách bổ sung $n - r$ vectơ thuộc E vào $\mathcal{L}$ để được một cơ sở của E.

Chứng minh:

Để có dạng thứ 1, ta chỉ cần áp dụng định lý thay thế cho họ sinh $\mathcal{B}$ và họ độc lập tuyến tính $\mathcal{L}$.

Từ dạng thứ 1 và sự tồn tại ít nhất một cơ sở hữu hạn của E, ta dễ dàng suy ra dạng thứ 2.

♦ **Mệnh đề 3** Cho E là một K-kgv hữu hạn chiều và $n = \dim(E)$.

1) Mọi họ độc lập tuyến tính của E là hữu hạn và có nhiều nhất n phần tử

2) Mọi họ của E có chứa ít nhất $(n + 1)$ phần tử là phụ thuộc tuyến tính

3) Mọi họ sinh của E có ít nhất n phần tử.

Chứng minh:

Theo Định lý - Định nghĩa 1, E có ít nhất một cơ sở $\mathcal{B} = \{e_1, ..., e_n\}$.

1) Giả sử $\mathcal{L}$ là một họ độc lập tuyến tính trong E. Nếu $\mathcal{L}$ là vô hạn hoặc hữu hạn với lực lượng $> n$, thì sẽ mâu thuẫn với kết quả *1)* của định lý thay thế, vì $\mathcal{B}$ là một họ sinh.

2) Là phản - đảo của *1)*.

3) Giả sử $\mathcal{G}$ là một họ sinh của E. Vì $\mathcal{B}$ là độc lập tuyến tính nên từ kết quả *1)* của định lý thay thế, ta suy ra rằng $\mathcal{G}$ có ít nhất n phần tử.

♦ **Mệnh đề 4** Giả sử E là một K-kgv hữu hạn chiều, $n = \dim(E)$ và $\mathcal{F}$ là một họ hữu hạn những phần tử của E. Hai tính chất bất kỳ trong ba tính chất sau kéo theo tính chất thứ 3:

1) $\mathcal{F}$ có n phần tử

2) $\mathcal{F}$ độc lập tuyến tính

3) $\mathcal{F}$ là họ sinh của E.

Chứng minh:

- (1 và 2) $\Rightarrow$ 3:

Giả sử $\text{Card}(\mathcal{G}) = n$ và $\mathcal{G}$ độc lập tuyến tính; E có ít nhất một cơ sở $\mathcal{B} = \{e_1, ..., e_n\}$. Theo định lý thay thế, vì $\mathcal{B}$ là một họ sinh và $\mathcal{G}$ độc lập tuyến tính, nên có ít nhất một cách thay thế n vectơ của $\mathcal{B}$ bởi những vectơ của $\mathcal{G}$ để thu được một họ sinh. Nhưng, vì $\mathcal{B}$ có n phần tử, nên họ sinh thu được chính là $\mathcal{G}$.

- (1 và 3) $\Rightarrow$ 2:

Giả sử $\text{Card}(\mathcal{G}) = n$ và $\mathcal{G}$ là họ sinh. Lập luận phản chứng: giả sử $\mathcal{G}$ phụ thuộc tuyến tính.

Tồn tại $(\lambda_1, ..., \lambda_n) \in K^n - \{(0, ..., 0)\}$ sao cho $\sum_{i=1}^{n} \lambda_i x_i = 0$.

Nếu cần ta hoán vị $x_1, ..., x_n$ (và $\lambda_1, ..., \lambda_n$), và ta có thể quy về trường hợp $\lambda_n \neq 0$, do đó:

$$x_n = -\sum_{i=1}^{n-1} \lambda_n^{-1} \lambda_i x_i \in \text{Vect}(x_1, ..., x_{n-1}).$$

Theo Mệnh đề 2, 2), $(x_1, ..., x_{n-1})$ là một họ sinh của E, điều này mâu thuẫn với Mệnh đề 3, *3)*.

Kết quả đó chứng tỏ rằng $\mathcal{G}$ độc lập tuyến tính.

- (2) và 3) $\Rightarrow$ 1: Suy ra từ Định lý - Định nghĩa 1.

♦ **Mệnh đề 5** Cho E là một K-kgv hữu hạn chiều. Mọi kgvc F của E đều hữu hạn chiều và:

$$\dim(F) \leq \dim(E).$$

Chứng minh:

Kết quả là hiển nhiên khi $F = \{0\}$.

Giả sử $F \neq \{0\}$. Tồn tại $x_1 \in F$ sao cho $x_1 \neq 0$; đặt $\mathcal{L}_1 = (x_1)$, họ này độc lập tuyến tính.

Nếu $\mathcal{L}_1$ sinh ra F, thì F hữu hạn chiều và $\dim(F) = 1$.

Nếu trái lại thì tồn tại $x_2 \in F$ sao cho $x_2 \notin \text{Vect}(\mathcal{L}_1)$.

Theo Mệnh đề 2, *1)*, họ $\mathcal{L}_2 = (x_1, x_2)$ độc lập tuyến tính, và ta lặp lại lập luận trên đây.

Giả sử $p \in \mathbb{N}^*$; giả sử đã xác định $x_1, ..., x_p$ trong F sao cho $\mathcal{L}_p = (x_1, ..., x_p)$ độc lập tuyến tính.

Nếu $\mathcal{L}_p$ sinh ra F thì F thì F là hữu hạn chiều và $\dim(F) = p$.

Nếu trái lại thì tồn tại $x_{p+1} \in F$ sao cho $x_{p+1} \notin \text{Vect}(L_p)$, và họ $L_{p+1} = (x_1, ..., x_{p+1})$ độc lập tuyến tính trong F.

Đặt $n = \dim(E)$, vì mọi họ có ít nhất $(n + 1)$ phần tử của E đều phụ thuộc tuyến tính, nên tồn tại $p \in \{1, ..., n\}$ sao cho $\mathcal{L}_p$ sinh ra F.

Như vậy, F hữu hạn chiều và $\dim(F) \leq n$.

♦ **Định nghĩa 2** Mọi kgv hoặc kgvc 1 chiều (tương ứng: 2 chiều) được gọi là **đường thẳng vectơ** (tương ứng: **mặt phẳng vectơ**). Một đường thẳng vectơ được sinh (người ta còn nói: được **định phương**) bởi một vectơ $\neq 0$ bất kỳ của nó.

Trong một không gian vectơ n chiều ($n \geq 1$), mọi kgvc $n - 1$ chiều được gọi là **siêu phẳng**.

♦ **Mệnh đề 6** Giả sử E là một K-kgv hữu hạn chiều, $n = \dim E$, F là một kgvc của E, $p = \dim(F)$.

1) F có ít nhất một phần bù trong E.

2) Mọi phần bù của F trong E đều có chiều là $n - p$.

Chứng minh:

1) Theo Định lý - Định nghĩa 1 và Mệnh đề trên đây, E có ít nhất một cơ sở $\mathcal{B} = (e_1, ..., e_n)$, F có ít nhất một cơ sở $\mathcal{C} = (f_1, ..., f_p)$, và $p \leq n$.

Theo định lý về cơ sở không đầy đủ, dạng mạnh (Định lý 2), nếu cần ta hoán vị trong $\mathcal{B}$ và trong $\mathcal{C}$, họ $\mathcal{B}' = \{f_1, ..., f_p, e_{p+1}, ..., e_n\}$ là một cơ sở của E.

Đặt $G = \text{Vect}(e_{p+1}, ..., e_n)$ và ta sẽ chứng minh rằng G là một phần bù của F trong E.

- Cho $x \in E$. Tồn tại $(\lambda_1, ..., \lambda_n) \in K^n$ sao cho $x = \sum_{i=1}^{p} \lambda_i f_i + \sum_{i=p+1}^{n} \lambda_i e_i$, nên $x \in F + G$. Điều đó chứng tỏ rằng $F + G = E$.

- Cho $x \in F \cap G$. Tồn tại $(\lambda_1, ..., \lambda_n) \in K^n$ sao cho $x = \sum_{i=1}^{p} \lambda_i f_i = \sum_{i=p+1}^{n} \lambda_i e_i$. Vậy ta có $\sum_{i=1}^{p} \lambda_i f_i + \sum_{i=p+1}^{n} (-\lambda_i) e_i = 0$, do đó, vì $\mathcal{B}'$ độc lập tuyến tính, ta suy ra:

$\lambda_1 = ... = \lambda_p = \lambda_{p+1} = ... = \lambda_n = 0$, và vì vậy $x = 0$. Điều đó chứng tỏ: $F \cap G = \{0\}$.

Như vậy G là một phần bù của F trong E.

2) Giả sử H là một phần bù của F trong E.

Theo Mệnh đề 5, H hữu hạn chiều. Theo Định lý - Định nghĩa 1, F (tương ứng: H) có ít nhất một cơ sở $(f_1, ..., f_p)$ (tương ứng: $(h_{p+1}, ..., h_q)$).

Ta chứng minh $\mathcal{F} = (f_1, ..., f_p, h_{p+1}, ..., h_q)$ là một cơ sở của E.

- Giả sử $(\lambda_1, ..., \lambda_q) \in K^q$ sao cho $\sum_{i=1}^{p} \lambda_i f_i + \sum_{i=p+1}^{q} \lambda_i h_i = 0$.

Vậy: $\sum_{i=1}^{p} \lambda_i f_i = -\sum_{i=p+1}^{q} \lambda_i h_i \in F \cap G = \{0\}$, nên: $\sum_{i=1}^{p} \lambda_i f_i = 0$ và $\sum_{i=p+1}^{q} \lambda_i h_i = 0$, do đó, vì $(f_1, ..., f_p)$ và $(h_{p+1}, ..., h_q)$ độc lập tuyến tính, ta suy ra $\lambda_1 = ... = \lambda_p = \lambda_{p+1} = ... = \lambda_q = 0$. Điều này chứng tỏ $\mathcal{F}$ độc lập tuyến tính.

- Cho $x \in E$. Vì $E = F + H$, tồn tại $(f, h) \in F \times H$ sao cho $x = f + h$. Hơn nữa, tồn tại $(\lambda_1, ..., \lambda_p) \in K^p$ và $(\lambda_{p+1}, ..., \lambda_q) \in K^{q-p}$ sao cho $f = \sum_{i=1}^{p} \lambda_i f_i$ và $h = \sum_{i=p+1}^{q} \lambda_i h_i$.

Ta được $x = \sum_{i=1}^{p} \lambda_i f_i + \sum_{i=p+1}^{q} \lambda_i h_i$, điều này chứng tỏ $\mathcal{F}$ sinh ra E. ■

NHẬN XÉT:

Nói chính xác, phép chứng minh trên xác lập rằng :

Nếu { E là một K-kgv hữu hạn chiều; F, G là hai kgvc của E, bù nhau trong E; $\mathcal{B}$ (tương ứng: $\mathcal{C}$) là một cơ sở của F (tương ứng: G) }

thì $\mathcal{B} \cup \mathcal{C}$ là một cơ sở của E.

♦ **Hệ quả 1** Giả sử E là một K-kgv hữu hạn chiều, F, G là hai kgvc của E có tổng trực tiếp. Thế thì ta có:

$$\dim(F \oplus G) = \dim(F) + \dim(G).$$

Chứng minh:

Suy ra từ Mệnh đề 6, áp dụng cho $F \oplus G$ thay vì E.

NHẬN XÉT:

Trong Hệ quả 1, có thể thay giả thiết E hữu hạn chiều bằng: F và G hữu hạn chiều (cụm từ "hữu hạn chiều" giữ nguyên).

♦ **Hệ quả 2** Giả sử E là một K-kgv hữu hạn chiều, $n \in \mathbb{N}^*$, $F_1, ..., F_n$ là những kgvc của E có tổng trực tiếp. Thế thì ta có: $\dim\left(\bigoplus_{i=1}^{n} F_i\right) = \sum_{i=1}^{n} \dim(F_i)$

Chứng minh:

Quy nạp theo n.

- Trường hợp $n = 1$ là tầm thường, trường hợp $n = 2$ chính là Hệ quả 1.
- Giả sử tính chất đã được thiết lập đối với một số nguyên n, và giả sử $F_1, ..., F_{n+1}$ là những kgvc của E có tổng trực tiếp. Thế thì $F_1, ..., F_n$ có tổng trực tiếp (xem 6.3.3, Nhận xét 4)), và $\bigoplus_{i=1}^{n} F_i$ và F_{n+1} có tổng trực tiếp, do đó

$$\dim\left(\bigoplus_{i=1}^{n+1} F_i\right) = \dim\left(\left(\bigoplus_{i=1}^{n} F_i\right) \oplus F_{n+1}\right) =$$

$$= \dim\left(\bigoplus_{i=1}^{n} F_i\right) + \dim(F_{n+1}) = \sum_{i=1}^{n} \dim(F_i) + \dim(F_{n+1}) = \sum_{i=1}^{n+1} \dim(F_i).$$

♦ **Hệ quả 3** Cho E là một K-kgv hữu hạn chiều, F, G là hai kgvc của E.

Nếu $\begin{cases} F \subset G \\ \dim(F) = \dim(G) \end{cases}$, thì $F = G$.

Chứng minh:

F có ít nhất một phần bù H trong G, và $\dim(H) = \dim(G) - \dim(F) = 0$, từ đó suy ra $H = \{0\}$, $G = F + H = F$.

♦ **Định lý 3** Giả sử E là một K-kgv hữu hạn chiều.

Với mọi kgvc F, G của E, ta có:

$$\dim(F + G) = \dim(F) + \dim(G) - \dim(F \cap G).$$

Chứng minh:

Theo Mệnh đề 6, $F \cap G$ có ít nhất một phần bù F' trong F.

1) Ta chứng minh rằng F' và G có tổng trực tiếp và $F' \oplus G = F \oplus G$.

- $F' \subset F$ nên $F' \cap G = (F' \cap F) \cap G = F' \cap (F \cap G) = \{0\}$.
- $F + G = (F' + (F \cap G)) + G = F' + ((F \cap G) + G) = F' + G$.

2) Theo Hệ quả 1: $\begin{cases} \dim(F+G) = \dim(F' \oplus G) = \dim(F') + \dim(G) \\ \dim(F) = \dim(F' \oplus (F \cap G)) = \dim(F') + \dim(F \cap G) \end{cases}$

từ đó suy ra hệ thức cần chứng minh.

NHẬN XÉT:

Trong định lý trên, có thể thay giả thiết E hữu hạn chiều bằng giả thiết: F và G hữu hạn chiều.

♦ **Mệnh đề 7** Cho E, F là hai K-kgv hữu hạn chiều. Thế thì $E \times F$ hữu hạn chiều và: $\dim(E \times F) = \dim(E) + \dim(F)$.

Chứng minh:

Theo Định lý - Định nghĩa 1, E và F tương ứng có các cơ sở hữu hạn $(e_1, ..., e_n)$, $(f_1, ..., f_p)$, trong đó $n = \dim(E)$, $p = \dim(F)$.

Ta chứng minh $\mathcal{B} = ((e_1, 0), ..., (e_n, 0), (0, f_1), ..., (0, f_p))$ là một cơ sở của $E \times F$.

1) Giả sử $(\lambda_1, ..., \lambda_n, \mu_1, ..., \mu_p) \in K^{n+p}$ thỏa mãn $\sum_{i=1}^{n} \lambda_i (e_i, 0) + \sum_{j=1}^{p} \mu_j (0, f_j) = 0$. Vậy ta có: $\left(\sum_{i=1}^{n} \lambda_i e_i, \sum_{j=1}^{p} \mu_j f_j \right) = (0, 0)$, nên $\sum_{i=1}^{n} \lambda_i e_i = 0$ và $\sum_{j=1}^{p} \mu_j f_j = 0$, và do đó $\lambda_1 = ... = \lambda_n = \mu_1 = ... = \mu_p = 0$, vì $(e_1, ..., e_n)$ và $(f_1, ..., f_p)$ độc lập tuyến tính. Điều này chứng tỏ rằng $\mathcal{B}$ độc lập tuyến tính.

2) Giả sử $(x, y) \in E \times F$. Vì $(e_1, ..., e_n)$ và $(f_1, ..., f_p)$ tương ứng sinh ra E và F, nên tồn tại $(\lambda_1, ..., \lambda_n) \in K^n$ và $(\mu_1, ..., \mu_p) \in K^p$ sao cho $x = \sum_{i=1}^{n} \lambda_i e_i$, $y = \sum_{j=1}^{p} \mu_j f_j$. Vậy ta có: $(x, y) = \left(\sum_{i=1}^{n} \lambda_i e_i, \sum_{j=1}^{p} \mu_j f_j \right) = \sum_{i=1}^{n} \lambda_i (e_i, 0) + \sum_{j=1}^{p} \mu_j (0, f_j)$.

Điều này chứng tỏ rằng $\mathcal{B}$ sinh ra $E \times F$.

Như vậy $\mathcal{B}$ là một cơ sở của $E \times F$, vì vậy $E \times F$ hữu hạn chiều và:

$$\dim(E \times F) = \mathrm{Card}(\mathcal{B}) = n + p = \dim(E) + \dim(F).$$

♦ **Hệ quả** Giả sử $n \in \mathbb{N}^*$, $E_1, ..., E_n$ là những K-kgv hữu hạn chiều. Thế thì $\prod_{i=1}^{n} E_i$ hữu hạn chiều và: $\dim\left(\prod_{i=1}^{n} E_i \right) = \sum_{i=1}^{n} \dim(E_i)$.

Chứng minh:

Bằng một phép quy nạp đơn giản từ Mệnh đề trên. ■

Đặc biệt, với mọi $n \in \mathbb{N}^*$, K^n là một K-kgv hữu hạn chiều và $\dim(K^n) = n$. Họ phần tử $(e_1, ..., e_n)$ của K^n xác định bởi $e_i = (0, ..., 0, 1, 0, ..., 0)$ trong đó "1" nằm ở vị trí thứ i, là một cơ sở của K^n được gọi là cơ sở chính tắc của K^n.

Hạng của một họ hữu hạn vectơ

♦ **Định nghĩa 3** Giả sử E là một K-kgv, $\mathcal{F}$ là một họ hữu hạn phần tử của E. Số tự nhiên $\dim(\mathrm{Vect}(\mathcal{F}))$ được gọi là **hạng** của $\mathcal{F}$ và ký hiệu là $\mathrm{rank}(\mathcal{F})$: $\mathrm{rank}(\mathcal{F}) = \dim(\mathrm{Vect}(\mathcal{F}))$.

♦ **Mệnh đề 8** Đối với mọi họ hữu hạn $\mathcal{F}$, $\mathcal{F}'$ những phần tử của E:

1) $\mathcal{F} \subset \mathcal{F}' \Rightarrow \mathrm{rank}(\mathcal{F}) \leq \mathrm{rank}(\mathcal{F}')$

2) $\mathrm{Max}(\mathrm{rank}(\mathcal{F}), \mathrm{rank}(\mathcal{F}')) \leq \mathrm{rank}(\mathcal{F} \cup \mathcal{F}') \leq \mathrm{rank}(\mathcal{F}) + \mathrm{rank}(\mathcal{F}')$.

Chứng minh:

1) $\mathcal{F} \subset \mathcal{F}' \Rightarrow \mathrm{Vect}(\mathcal{F}) \subset \mathrm{Vect}(\mathcal{F}') \Rightarrow \dim(\mathrm{Vect}(\mathcal{F})) \leq \dim(\mathrm{Vect}(\mathcal{F}'))$

2) $\begin{cases} \mathcal{F} \subset \mathcal{F} \cup \mathcal{F}' \\ \mathcal{F}' \subset \mathcal{F} \cup \mathcal{F}' \end{cases} \Rightarrow \begin{cases} \mathrm{rank}(\mathcal{F}) \leq \mathrm{rank}(\mathcal{F} \cup \mathcal{F}') \\ \mathrm{rank}(\mathcal{F}') \leq \mathrm{rank}(\mathcal{F} \cup \mathcal{F}') \end{cases}$

$\Rightarrow \mathrm{Max}(\mathrm{rank}(\mathcal{F}), \mathrm{rank}(\mathcal{F}')) \leq \mathrm{rank}(\mathcal{F} \cup \mathcal{F}')$.

3) $\text{rank}(\mathcal{F} \cup \mathcal{F}') = \dim(\text{Vect}(\mathcal{F} \cup \mathcal{F}')) = \dim(\text{Vect}(\mathcal{F}) + \text{Vect}(\mathcal{F}'))$

$\leq \dim(\text{Vect}(\mathcal{F})) + \dim(\text{Vect}(\mathcal{F}'))$ (dùng 6.3.2, Mệnh đề 2, 4)).

◆ **Mệnh đề 9** Giả sử E là một K-kgv, $\mathcal{F}$ là một họ hữu hạn phần tử của E.

1) Hạng của $\mathcal{F}$ là lực lượng lớn nhất của các họ con độc lập tuyến tính của $\mathcal{F}$.

2) $\mathcal{F}$ độc lập tuyến tính khi và chỉ khi: $\text{Card}(\mathcal{F}) = \text{rank}(\mathcal{F})$.

Chứng minh:

1) • Vì $\mathcal{F}$ hữu hạn, nên $\text{Vect}(\mathcal{F})$ hữu hạn chiều. Theo Nhận xét ở 6.4, Định lý - Định nghĩa 1, tồn tại một họ con $\mathcal{B}$ của $\mathcal{F}$, là một cơ sở của $\text{Vect}(\mathcal{F})$, vì vậy $\mathcal{B}$ là họ con của $\mathcal{F}$ thỏa mãn $\text{Card}(\mathcal{B}) = \text{rank}(\mathcal{F})$.

• Giả sử $\mathcal{L}$ là một họ con độc lập tuyến tính của $\mathcal{F}$. Theo Mệnh đề 3, *1)*:

$$\text{Card}(\mathcal{L}) \leq \dim(\text{Vect}(\mathcal{F})) = \text{rank}(\mathcal{F}).$$

2) • Nếu $\mathcal{F}$ độc lập tuyến tính, thì theo *1)*: $\text{rank}(\mathcal{F}) = \text{Card}(\mathcal{F})$.

• Ngược lại, nếu $\text{Card}(\mathcal{F}) = \text{rank}(\mathcal{F})$, thì, vì $\mathcal{F}$ sinh ra $\text{Vect}(\mathcal{F})$ nên theo Mệnh đề 4, $\mathcal{F}$ là một cơ sở của $\text{Vect}(\mathcal{F})$, và vì vậy độc lập tuyến tính.

VÍ DỤ:

$K = \mathbb{R}$, $E = \mathbb{R}^3$, $\mathcal{F} = (V_i)_{1 \leq i \leq 4}$ trong đó:

$$V_1 = (1, -1, 1), V_2 = (-1, 1, -1), V_3 = (0, 1, 1), V_4 = (1, 0, 2).$$

Vì (V_1, V_3) độc lập tuyến tính và vì $V_2 = -V_1$, $V_4 = V_1 + V_3$ nên ta có: $\text{rank}(\mathcal{F}) = 2$.

Dưới đây (8.1.7), ta sẽ thấy một thuật toán (*phương pháp Gauss*) cho phép tính hạng của một họ hữu hạn vectơ.

Bài tập

◊ **6.4.1** Chứng minh rằng tập hợp F xác định bởi $F = \left\{ (x, y, z) \in \mathbb{C}^3 ; \begin{cases} x + y + z = 0 \\ x + iy - z = 0 \end{cases} \right\}$ là một kgvc của $\mathbb{C}^3$ và xác định một cơ sở và số chiều của nó.

◊ **6.4.2** Xác định một cơ sở và số chiều của kgvc F của $\mathbb{R}^{]-1;1[}$ được sinh ra bởi $(f_i)_{1 \leq i \leq 4}$ trong đó với mọi x thuộc $]-1; 1[$:

$$f_1(x) = \sqrt{\frac{1-x}{1+x}}, f_2(x) = \sqrt{\frac{1+x}{1-x}}, f_3(x) = \frac{1}{\sqrt{1-x^2}}, f_4(x) = \frac{x}{\sqrt{1-x^2}}.$$

◊ **6.4.3** Trong $\mathbb{R}^4$, cho $u = (1, 0, 1, 0)$, $v = (0, 1, -1, 0)$, $w = (1, 1, 1, 1)$, $x = (0, 0, 1, 0)$, $y = (1, 1, 0, -1)$, $F = \text{Vect}(u, v, w)$, $G = \text{Vect}(x, y)$. Tìm số chiều của F, G, $F + G$, $F \cap G$.

◊ **6.4.4** Giả sử E là một K-kgv hữu hạn chiều, F là một kgvc của E sao cho $F \neq \{0\}$ và $F \neq E$. Chứng tỏ rằng F có ít nhất hai phần bù khác nhau trong E.

◊ **6.4.5** Giả sử E là một K-kgv hữu hạn chiều, F, G là hai kgvc của E. Chứng minh rằng hai tính chất bất kỳ trong ba tính chất sau kéo theo tính chất thứ 3:

1) $F \cap G = \{0\}$ 2) $F + G = E$ 3) $\dim(F) + \dim(G) = \dim(E)$.

◊ **6.4.6** Giả sử E, F là hai K-kgv. Chứng tỏ rằng nếu $E \times F$ hữu hạn chiều, thì E và F cũng hữu hạn chiều.

◊ **6.4.7** Với $a \in \mathbb{R}$, ký hiệu $f_a : \begin{matrix}\mathbb{R} \to \mathbb{R} \\ x \mapsto \cos(x+a)\end{matrix}$.

Giả sử $(a_1, a_2, a_3) \in \mathbb{R}^3$; xác định hạng của $(f_{a_1}, f_{a_2}, f_{a_3})$ trong $\mathbb{R}^{\mathbb{R}}$ (được trang bị các luật thông thường).

◊ **6.4.8** Giả sử E là một K-kgv hữu hạn chiều, $\mathcal{G}$ là một họ hữu hạn phần tử của E. Chứng minh rằng các tính chất sau là tương đương:

1) $\mathcal{G}$ là một cơ sở của E

2) $\begin{cases} \mathcal{G} \text{ là một họ sinh của } E \\ \text{Với mọi họ sinh } \mathcal{G}_1 \text{ của } E : \mathcal{G}_1 \subset \mathcal{G} \Rightarrow \mathcal{G}_1 = \mathcal{G} \\ \text{(người ta nói } \mathcal{G} \text{ là một } \textit{họ sinh tối tiểu} \text{ của } E\text{).} \end{cases}$

3) $\begin{cases} \mathcal{G} \text{ độc lập tuyến tính} \\ \text{Với mọi họ độc lập tuyến tính } \mathcal{L} \text{ của } E : \mathcal{G} \subset \mathcal{L} \Rightarrow \mathcal{G} = \mathcal{L} \\ \text{(người ta nói } \mathcal{G} \text{ là họ } \textit{độc lập tuyến tính tối đại} \text{ của } E\text{).} \end{cases}$

◊ **6.4.9** Giả sử E là một K-kgv hữu hạn chiều.

a) Chứng minh rằng, với mọi họ sinh hữu hạn $\mathcal{G}$ của E, tồn tại một cơ sở $\mathcal{B}_1$ của E sao cho $\mathcal{B}_1 \subset \mathcal{G}$.

b) Chứng minh rằng, với mọi họ độc lập tuyến tính $\mathcal{L}$ của E, tồn tại một cơ sở $\mathcal{B}_2$ của E sao cho $\mathcal{L} \subset \mathcal{B}_2$.

c) Chứng minh rằng, với mọi họ sinh hữu hạn $\mathcal{G}$ của E và mọi họ độc lập tuyến tính $\mathcal{L}$ của E sao cho $\mathcal{L} \subset \mathcal{G}$, tồn tại một cơ sở $\mathcal{B}_3$ của E sao cho $\mathcal{L} \subset \mathcal{B}_3 \subset \mathcal{G}$.

d) Chứng minh rằng, với mọi họ sinh hữu hạn $\mathcal{G}$ của E và mọi họ độc lập tuyến tính $\mathcal{L}$ của E, tồn tại một cơ sở $\mathcal{B}_4$ của E sao cho $\mathcal{L} \subset \mathcal{B}_4 \subset \mathcal{L} \cup \mathcal{G}$.

◊ **6.4.10** Ký hiệu $A = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \,;\, (a, b, c, d) \in \mathbb{Q}^4\}$.

a) Chứng minh rằng A là một $\mathbb{Q}$ - đại số với các luật thông thường (luật thứ 3 là phép nhân).

b) Chứng minh rằng A là một $\mathbb{Q}$-kgv hữu hạn chiều và $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ là một cơ sở của E.

c) Chứng minh rằng A là một thể con của $\mathbb{R}$.

Ví dụ: Phân tích nghịch đảo của $4 + 3\sqrt{2} - 2\sqrt{3} - \sqrt{6}$ theo cơ sở $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ của A.

Chương 7

Ánh xạ tuyến tính

Trong chương 7 này K sẽ chỉ một thể giao hoán. Trên thực tế: $K = \mathbb{R}$ hoặc $K = \mathbb{C}$.

Ta sẽ viết tắt không gian vectơ là kgv, và không gian vectơ con là kgvc.

7.1 Đại cương

7.1.1 Các định nghĩa

♦ **Định nghĩa 1**

1) Cho E và F là hai K-kgv ; một ánh xạ $f : E \to F$ được gọi là **tuyến tính** (hay K **-tuyến tính** ; hoặc : là một **đồng cấu** K**-kgv**) khi và chỉ khi:

$$\begin{cases} \forall (x, y) \in E^2, & f(x+y) = f(x) + f(y) \\ \forall \lambda \in K, \forall x \in E, & f(\lambda x) = \lambda f(x) \end{cases}$$

Ta ký hiệu tập hợp các ánh xạ tuyến tính từ E vào F là $\mathcal{L}(E, F)$ (hoặc : $\mathcal{L}_K(E,F)$).

2) Cho E một K-kgv, $f : E \to E$ là một ánh xạ . Ta nói f là một **tự đồng cấu** của E khi và chỉ khi f là tuyến tính.

Ta ký hiệu tập hợp các tự đồng cấu của E là $\mathcal{L}(E)$ (hoặc : $\mathcal{L}_K(E)$)

Như vậy , ta có $\mathcal{L}(E) = \mathcal{L}(E,E)$.

NHẬN XÉT

Với mọi f thuộc $\mathcal{L}(E,F)$, $f(0) = 0$ vì: $f(0)=f(0+0) = f(0) + f(0)$; xem thêm 2.2.3, Mệnh đề 1, *1*).

♦ **Định nghĩa 2**

1) Cho E và F là hai K-kgv, $f : E \to F$ là một ánh xạ .Ta nói f là một **đẳng cấu** từ E lên F khi và chỉ khi f là tuyến tính và song ánh.

2) Cho E là một K-kgv, $f : E \to E$ là một ánh xạ .Ta nói f là một **tự đẳng cấu** của E khi và chỉ khi f là tuyến tính và là song ánh.

Ta ký hiệu tập hợp các tự đẳng cấu của kgv E là $\mathcal{GL}(E)$ (hoặc $\mathcal{GL}_K(E)$).

◆ **Định nghĩa 3** Cho E là một K - kgv . **Dạng tuyến tính** trên E là mọi ánh xạ tuyến tính φ từ E vào K. Ký hiệu E^* là tập hợp các dạng tuyến tính trên E ; E^* được gọi là **đối ngẫu** của E .

Như vậy ta có : $E^* = \mathcal{L}(E,K)$.

◆ **Mệnh đề 1** Giả sử E và F là hai K-kgv, $f: E \to F$ là một ánh xạ ; f tuyến tính khi và chỉ khi :

$$\forall\, \lambda \in K\ ,\ \forall (x,y) \in E^2\ ,\ \ f(\lambda x + y) = \lambda f(x) + f(y).$$

Chứng minh:

1) Nếu f là tuyến tính , thì với mọi (λ, x, y) thuộc $K \times E \times E$:

$$f(\lambda x + y) = f(\lambda x) + f(y) = \lambda f(x) + f(y).$$

2) Ngược lại, nếu điều kiện trên được thỏa mãn , thì:

- Lấy $\lambda = 1$, ta nhận được $f(x + y) = f(x) + f(y)$, và vì vậy $f(0) = 0$
- Lấy $y = 0$, ta nhận được $f(\lambda x) = \lambda f(x)$, và vì vậy f là tuyến tính.

◆ **Mệnh đề 2** Giả sử E và F là hai K -kgv , $f \in \mathcal{L}(E,F)$. Với mọi n thuộc $\mathbb{N}^*$, $(\lambda_1, \ldots, \lambda_n)$ thuộc K^n , $(x_1, \ldots, x_n)$ thuộc E^n , ta có :

$$f\left(\sum_{i=1}^{n} \lambda_i x_i\right) = \sum_{i=1}^{n} \lambda_i f(x_i)\,.$$

Chứng minh :

Quy nạp theo n

Tính chất là hiển nhiên với $n = 1$; và với $n = 2$:

$$f(\lambda_1 x_1 + \lambda_2 x_2) = f(\lambda_1 x_1) + f(\lambda_2 x_2) = \lambda_1 f(x_1) + \lambda_2 f(x_2).$$

Nếu tính chất đúng với một n thuộc $\mathbb{N}^*$, thì với mọi $(\lambda_1, \ldots, \lambda_{n+1})$ thuộc K^{n+1} và $(x_1, \ldots, x_{n+1})$ thuộc E^{n+1} :

$$f\left(\sum_{i=1}^{n+1} \lambda_i x_i\right) = f\left(\sum_{i=1}^{n} \lambda_i x_i + \lambda_{n+1} x_{n+1}\right)$$

$$= f\left(\sum_{i=1}^{n} \lambda_i x_i\right) + f\left(\lambda_{n+1} x_{n+1}\right)$$

$$= \sum_{i=1}^{n} \lambda_i f(x_i) + \lambda_{n+1} f(x_{n+1}) = \sum_{i=1}^{n+1} \lambda_i f(x_i)\,. \qquad \blacksquare$$

Ta suy ra Hệ quả sau:

◆ **Hệ quả** Giả sử E là một K-kgv hữu hạn chiều, F là một K-kgv, $\mathcal{B} = \{e_1, ..., e_n\}$ là một cơ sở của E, $f \in \mathcal{L}(E, F)$, $x \in E$, $(x_1, ..., x_n)$ là các thành phần của x trong cơ sở $\mathcal{B}$ (nghĩa là : $x = \sum_{i=1}^{n} x_i e_i$). Thế thì, ta có :

$$f(x) = \sum_{i=1}^{n} x_i f(e_i).$$

Nói cách khác, một ánh xạ tuyến tính được xác định hoàn toàn bởi ảnh của các vectơ của một cơ sở.

NHẬN XÉT :

Hệ quả trên được tổng quát cho trường hợp E không hữu hạn chiều bằng cách dùng khái niệm "tổng với giá hữu hạn", vốn không thuộc phạm vi của cuốn sách này. ■

VÍ DỤ:

1) **Phép vị tự**

Giả sử E là một K-kgv. Với mọi α thuộc K, ta gọi ánh xạ $h_\alpha : \underset{x \mapsto \alpha x}{E \to E}$ là **phép vị tự (vectơ) với tỷ số** α ; hiển nhiên $h_\alpha \in \mathcal{L}(E)$.

Đặc biệt : $h_0 = 0$, $h_1 = \mathrm{Id}_E$. Để đơn giản cách viết, ta thường viết e thay cho Id_E.

2) **Phép chiếu**

Giả sử E là một K- kgv, F, G là hai kgvc của E bù nhau trong E : $E = F \oplus G$.

Với mọi $x \in E$ tồn tại duy nhất $(x', x'') \in F \times G$ sao cho $x = x' + x''$.

Ánh xạ $p : \underset{x \mapsto x'}{E \to E}$ là một tự đồng cấu của E. Thực vậy, nếu $\lambda \in K$ và $(x, y) \in E^2$, thì tồn tại $(x', x'') \in F \times G$ và $(y', y'') \in F \times G$ sao cho $x = x' + x''$ và $y = y' + y''$, nên

$$\begin{cases} \lambda x + y = \lambda(x'+x'') + (y'+y'') = (\lambda x'+y') + (\lambda x''+y'') \\ (\lambda x'+y', \lambda x''+y'') \in F \times G \end{cases}$$

và vì vậy $p(\lambda x + y) = \lambda x' + y' = \lambda p(x) + p(y)$.

Ánh xạ $p : \underset{x \mapsto x'}{E \to E}$ được gọi là **phép chiếu lên F song song với G.**

Hiển nhiên ánh xạ $q : \underset{x \mapsto x''}{E \to E}$ là phép chiếu lên G song song với F.

Ta có: $q = e - p$, nghĩa là: $\forall x \in E, q(x) = x - p(x)$.

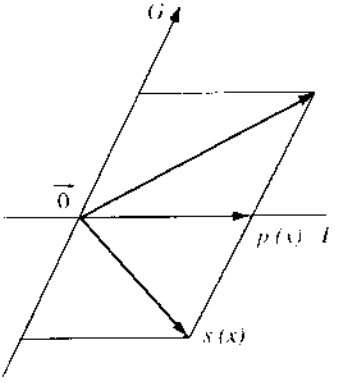
3) Phép đối xứng

Giả sử E là một K-kgv, F, G là hai kgvc của E bù nhau trong E : $E = F \oplus G$. Ký hiệu p là phép chiếu lên F song song với G.

Ánh xạ $s = 2p - e$, xác định bởi:

$$s : \begin{array}{ccc} E & \to & E \\ x & \mapsto & 2p(x) - x \end{array}$$

là một tự đồng cấu của E, gọi là **phép đối xứng qua F song song với G**.



4) Phép nhúng chính tắc

Giả sử E là một K-kgv, F là một kgvc của E. **Phép nhúng** (hoặc: **đơn ánh**) **chính tắc** $i_{F,E} : \begin{array}{ccc} F & \to & E \\ x & \mapsto & x \end{array}$ (xem 1.3.1, Ví dụ 2)) là tuyến tính.

5) Phép chiếu chính tắc

Giả sử $n \in \mathbb{N}^*$, E_1, ..., E_n là những K-kgv. Với mọi i thuộc $\{1, ..., n\}$, **phép chiếu chính tắc thứ** i $\mathrm{pr}_i : \begin{array}{ccc} E_1 \times ... \times E_n & \to & E_i \\ (x_1, ..., x_n) & \mapsto & x_i \end{array}$ (xem 1.3.1, Ví dụ 6)) là tuyến tính.

6) Giá trị

Giả sử X là một tập khác rỗng, F là một K-kgv. Với mọi a thuộc X, ánh xạ

$E_a : \begin{array}{ccc} F^X & \to & F \\ \varphi & \mapsto & \varphi(a) \end{array}$ được gọi là **giá trị tại** a, là tuyến tính vì:

$$\forall \lambda \in K, \forall \varphi, \psi \in F^X, \quad E_a(\lambda\varphi + \mu) = (\lambda\varphi + \psi)(a) = \lambda\varphi(a) + \mu(a) = \lambda E_a(\varphi) + E_a(\mu).$$

7) Toán tử đạo hàm

Giả sử I là một khoảng của $\mathbb{R}$, khác rỗng và không thu về một điểm, $D^1(I, \mathbb{R})$ là $\mathbb{R}$-kgv các ánh xạ từ I vào $\mathbb{R}$ khả vi trên I. Ánh xạ $D : \begin{array}{ccc} D^1(I, \mathbb{R}) & \to & \mathbb{R}^I \\ f & \mapsto & f' \end{array}$ là tuyến tính

(xem Tập 1, 5.1.3, Định lý 1).

8) Tích phân

Giả sử $(a, b) \in \mathbb{R}^2$ sao cho $a \le b$. $\mathcal{U}$ là $\mathbb{R}$-kgv các ánh xạ từ $[a ; b]$ vào $\mathbb{R}$, liên tục từng khúc (xem Tập 1, 1.6.2, Mệnh đề 1). Ánh xạ $\mu : \begin{array}{ccc} \mathcal{U} & \to & \mathbb{R} \\ f & \mapsto & \int_a^b f \end{array}$ là tuyến tính (xem

Tập 1, 6.2.4, Mệnh đề).

Đại số

♦ Định nghĩa 4

1) Cho A, B là hai K-đại số (phép toán thứ 3 được ký hiệu theo lối nhân); một ánh xạ $f : A \to B$ được gọi là **đồng cấu đại số** khi và chỉ khi:

$$\begin{cases} \forall (x, y) \in A^2 & f(x + y) = f(x) + f(y) \\ \forall \lambda \in K, \forall x \in A, & f(\lambda x) = \lambda f(x) \\ \forall (x, y) \in A^2 & f(xy) = f(x)f(y). \end{cases}$$

2) Giả sử A là một K-đại số, $f : A \to A$ là một ánh xạ. Ta nói f là một **tự đồng cấu của đại số** A khi và chỉ khi f là một đồng cấu đại số từ A vào A.

NHẬN XÉT:

Với các ký hiệu trên của 1), f là một đồng cấu đại số khi và chỉ khi:

$$\begin{cases} f \text{ tuyến tính (từ kgv } A \text{ vào kgv } B) \\ f \text{ là một đồng cấu đối với luật thứ 3.} \end{cases}$$

♦ Định nghĩa 5

1) Cho A, B là hai K-đại số, $f : A \to B$ là một ánh xạ. Ta nói f là **một đẳng cấu đại số** từ A lên B khi và chỉ khi f là một đồng cấu đại số và là song ánh.

2) Cho A là một K-đại số, $f : A \to A$ là một ánh xạ. Ta nói f là một **tự đẳng cấu của đại số** A khi và chỉ khi f là một tự đồng cấu của đại số A và là song ánh.

7.1.2 Hạt nhân và ảnh

♦ **Mệnh đề 1** Cho E, F là hai K-kgv, $f \in \mathcal{L}(E, F)$.

1) Với mọi kgvc F_1 của F, nghịch ảnh $f^{-1}(F_1)$ là một kgvc của E.

2) Với mọi kgvc E_1 của E, ảnh $f(E_1)$ là một kgvc của F.

Ta nhắc lại (xem 1.3.5, Định nghĩa):

• $f^{-1}(F_1) = \{x \in E; f(x) \in F_1\}$ • $f(E_1) = \{y \in F; \exists x \in E_1, y = f(x)\}$.

Chứng minh:

1) • $f^{-1}(F_1) \neq \varnothing$: $0 \in f^{-1}(F_1)$ vì $f(0) = 0 \in F_1$.

• Giả sử $\lambda \in K$, $(x, y) \in (f^{-1}(F_1))^2$. Ta có: $(f(x), f(y)) \in (F_1)^2$, nên $f(\lambda x + y) = \lambda f(x) + f(y) \in F_1$, và vì vậy $\lambda x + y \in f^{-1}(F_1)$.

2) • $f(E_1) \neq \varnothing$: $0 \in f(E_1)$ vì $0 = f(0)$.

• Giả sử $\lambda \in K$, $(x', y') \in (f(E_1))^2$. Tồn tại $(x, y) \in (E_1)^2$ sao cho $x' = f(x)$ và $y' = f(y)$. Khi đó ta có $\lambda x' + y' = \lambda f(x) + f(y) = f(\lambda x + y) \in f(E_1)$. ■

Ta nhắc lại rằng, theo 1.3.1, Định nghĩa 3, một kgvc V của một kgv E được gọi là **ổn định** đối với một tự đồng cấu f của E khi và chỉ khi: $f(V) \subset V$. ■

♦ **Định nghĩa** Giả sử E, F là hai K-kgv, $f \in \mathcal{L}(E, F)$. **Hạt nhân** của f, ký hiệu là $\mathrm{Ker}(f)$, là kgvc của E xác định bởi:

$$\mathrm{Ker}(f) = f^{-1}(\{0\}) = \{x \in E; f(x) = 0\}.$$

Ảnh của f, ký hiệu là $\mathrm{Im}(f)$, là kgvc của F xác định bởi:

$$\mathrm{Im}(f) = f(E) = \{y \in F; \exists x \in E, y = f(x)\}.$$

♦ **Mệnh đề 2** Giả sử E, F là hai K-kgv, $f \in \mathcal{L}(E, F)$.

1) f là đơn ánh khi và chỉ khi $\mathrm{Ker}(f) = \{0\}$.

2) f là toàn ánh khi và chỉ khi $\mathrm{Im}(f) = F$.

Chứng minh:

1) • Giả sử f là đơn ánh, và giả sử $x \in \mathrm{Ker}(f)$. Khi đó $f(x) = 0 = f(0)$, do đó vì f là đơn ánh nên: $x = 0$. Như vậy: $\mathrm{Ker}(f) = \{0\}$.

• Ngược lại, giả sử $\mathrm{Ker}(f) = \{0\}$, và giả sử $(x, y) \in E^2$ sao cho $f(x) = f(y)$. Thế thì: $f(x - y) = f(x) - f(y) = 0$, nên $x - y \in \mathrm{Ker}(f) = 0$, từ đó suy ra $x = y$.

Điều này chứng tỏ f là đơn ánh.

2) (f toàn ánh) $\Leftrightarrow (\forall y \in F, \exists x \in E, y = f(x)) \Leftrightarrow f(E) = F \Leftrightarrow \mathrm{Im}f = F$.

7.1.3 Ánh xạ tuyến tính và họ vectơ

Trong §7.1.3 này:

- E, F chỉ hai K-kgv.
- $f \in \mathcal{L}(E, F)$
- $\mathcal{F} = (x_1, ..., x_n)$ là một họ hữu hạn những phần tử của E.

♦ **Mệnh đề 1** Với mọi f thuộc $\mathcal{L}(E, F)$ và mọi họ $\mathcal{F}$ gồm hữu hạn phần tử của E:

$$f(\mathrm{Vect}(\mathcal{F})) = \mathrm{Vect}(f(\mathcal{F})).$$

Chứng minh:

1) Giả sử $y \in f(\mathrm{Vect}(\mathcal{F}))$. Tồn tại $x \in \mathrm{Vect}(\mathcal{F})$ sao cho $y = f(x)$, do vậy tồn tại $(\lambda_i)_{1 \leq i \leq n} \in K^n$ sao cho $x = \sum_{i=1}^{n} \lambda_i x_i$. Khi đó ta có:

$$y = f(x) = f\left(\sum_{i=1}^{n} \lambda_i x_i\right) = \sum_{i=1}^{n} \lambda_i f(x_i) \in \mathrm{Vect}(f(\mathcal{F})).$$

Điều này chứng tỏ: $f(\mathrm{Vect}(\mathcal{F})) \subset \mathrm{Vect}(f(\mathcal{F}))$.

2) Bao hàm thức ngược lại chứng minh tương tự.

♦ **Hệ quả** Nếu $f \in \mathcal{L}(E, F)$ là toàn ánh và nếu $\mathcal{F}$ sinh ra E, thì $f(\mathcal{F})$ sinh ra F.

Chứng minh: $F = f(E) = f(\text{Vect}(\mathcal{F})) = \text{Vect}(f(\mathcal{F}))$.

♦ **Mệnh đề 2** Giả sử $f \in \mathcal{L}(E, F)$ và $\mathcal{F}$ là một họ phần tử của E.
1) Nếu $\mathcal{F}$ phụ thuộc tuyến tính, thì $f(\mathcal{F})$ phụ thuộc tuyến tính.
2) Nếu $f(\mathcal{F})$ độc lập tuyến tính, thì $\mathcal{F}$ độc lập tuyến tính.

Chứng minh:

1) Vì $\mathcal{F}$ phụ thuộc tuyến tính, nên tồn tại $(\lambda_1, ..., \lambda_n) \in K^n - \{(0, ..., 0)\}$ sao cho $\sum_{i=1}^{n} \lambda_i x_i = 0$. Khi đó ta có $\sum_{i=1}^{n} \lambda_i f(x_i) = f\left(\sum_{i=1}^{n} \lambda_i x_i\right) = f(0) = 0$, và vì vậy $f(\mathcal{F})$ phụ thuộc tuyến tính.

2) Suy từ 1) bằng lập luận phản đảo.

♦ **Mệnh đề 3** Giả sử $f \in \mathcal{L}(E, F)$, $\mathcal{F}$ là một họ phần tử của E. Nếu f là đơn ánh và nếu $\mathcal{F}$ độc lập tuyến tính, thì $f(\mathcal{F})$ độc lập tuyến tính.

Chứng minh:

Giả sử $(\lambda_1, ..., \lambda_n) \in K^n$ sao cho $\sum_{i=1}^{n} \lambda_i f(x_i) = 0$. Thế thì: $f\left(\sum_{i=1}^{n} \lambda_i x_i\right) = \sum_{i=1}^{n} \lambda_i f(x_i) = 0$,

do đó vì f là đơn ánh nên: $\sum_{i=1}^{n} \lambda_i x_i = 0$. Cuối cùng, vì $\mathcal{F}$ độc lập tuyến tính nên:

$\forall i \in \{1, ..., n\}$, $\lambda_i = 0$.

♦ **Mệnh đề 4** Giả sử E là một K-kgv hữu hạn chiều, F là một K-kgv, $f \in \mathcal{L}(E, F)$. Các tính chất sau tương đương từng đôi một:
(i) f là song ánh
(ii) Với mọi cơ sở $\mathcal{B}$ của E, $f(\mathcal{B})$ là một cơ sở của F
(iii) Tồn tại một cơ sở $\mathcal{B}$ của E sao cho $f(\mathcal{B})$ là một cơ sở của F.

Chứng minh:

(i) ⇒ (ii) :
Giả sử f là song ánh. Giả sử $\mathcal{B}$ là một cơ sở của E. Vì f là toàn ánh và $\mathcal{B}$ là một họ sinh của E nên $f(\mathcal{B})$ là một họ sinh của F (xem Hệ quả). Vì f là đơn ánh và $\mathcal{B}$ độc lập tuyến tính, nên $f(\mathcal{B})$ độc lập tuyến tính (Xem Mệnh đề 3).

(ii) ⇒ (iii):
Suy ra từ sự tồn tại một cơ sở của E (xem 6.4, Định lý - Định nghĩa 1).

(iii) ⇒ (i):
Giả sử tồn tại một cơ sở $\mathcal{B} = (e_1, ..., e_n)$ của E sao cho $f(\mathcal{B}) = (f(e_1), ..., f(e_n))$ là một cơ sở của F.

- Giả sử $x \in \mathrm{Ker}(f)$. Tồn tại $(x_1, ..., x_n) \in K^n$ sao cho $x = \sum_{i=1}^{n} x_i e_i$. Ta có:

$$0 = f(x) = f\left(\sum_{i=1}^{n} x_i e_i\right) = \sum_{i=1}^{n} x_i f(e_i),$$

do vậy, vì $f(\mathcal{B})$ độc lập tuyến tính: $\forall i \in \{1, ..., n\}, x_i = 0$, suy ra $x = 0$.

Như vậy: $\mathrm{Ker}(f) = \{0\}$, do đó f là đơn ánh.

- Giả sử $y \in F$.

Vì $f(\mathcal{B})$ sinh ra F, nên tồn tại $(x_1, ..., x_n) \in K^n$ sao cho $y = \sum_{i=1}^{n} x_i f(e_i)$, từ đó suy ra

$$y = f\left(\sum_{i=1}^{n} x_i e_i\right) \in \mathrm{Im}(f).$$

Điều đó chứng tỏ f là toàn ánh. Như vậy f là song ánh. ■

NHẬN XÉT:
Kết quả của §7.1.3 này vẫn đúng cho mọi họ $\mathcal{Y}$ những phần tử của E (không nhất thiết hữu hạn).

Bài tập

◊ **7.1.1** Cho E, F là hai K-kgv, $f \in \mathcal{L}(E, F)$, A, B là hai kgvc của E. Chứng minh rằng:

$$f(A) \subset f(B) \Leftrightarrow A + \mathrm{Ker}(f) \subset B + \mathrm{Ker}(f).$$

◊ **7.1.2** Cho E, F là hai K-kgv, G là một kgvc của $E \times F$ sao cho:
$\forall a \in E, \exists!\, b \in F, (a, b) \in G$.
Ký hiệu f $\begin{matrix} E \to F \\ a \mapsto b \end{matrix}$ xác định trên đây.

Chứng minh rằng ánh xạ f tuyến tính.

◊ **7.1.3** Chứng minh rằng ánh xạ $f : \mathbb{R}[X] \to \mathbb{R}[X]$ tuyến tính và xác định $\mathrm{Ker}(f)$ và $\mathrm{Im}(f)$.

$$P \mapsto P - XP'$$

◊ **7.1.4** Cho $n \in \mathbb{N}$, $E = K_n[X]$ là K-kgv các đa thức với bậc $\le n$, f : $\begin{matrix} E \to E \\ P \mapsto P - P' \end{matrix}$.

Chứng minh rằng f là một tự đẳng cấu của E và hãy biểu diễn f^{-1}.

◊ **7.1.5** Cho $T \in \mathbb{R}_+^*$, E là tập hợp các ánh xạ từ $\mathbb{R}$ vào $\mathbb{R}$, T - tuần hoàn và thuộc lớp $\mathcal{C}^\infty$.

a) Kiểm chứng rằng E là một $\mathbb{R}$-kgv (đối với các luật thông thường) và: $\forall f \in E, f' \in E$.

b) Ký hiệu ϕ : $\begin{matrix} E \to E \\ f \mapsto f' \end{matrix}$. Kiểm chứng rằng ϕ tuyến tính, và hãy xác định $\mathrm{Ker}(\phi)$ và $\mathrm{Im}(\phi)$.

◊ **7.1.6*** Giả sử E là một K-kgv, $f \in \mathcal{L}(E)$ sao cho, với mọi $x \in E$, $(x, f(x))$ phụ thuộc tuyến tính. Chứng minh rằng f là một phép vị tự.

◊ **7.1.7** Giả sử E là một K-kgv, $f \in \mathcal{L}(E)$, $n \in \mathbb{N}^*$, $\lambda_1, ..., \lambda_n \in K$ khác nhau từng đôi một; ký hiệu $N_i = \mathrm{Ker}(f - \lambda_i e)$ với $1 \le i \le n$, trong đó $e = \mathrm{Id}_E$.

Chứng minh rằng các kgvc N_i ($1 \le i \le n$) độc lập tuyến tính (nghĩa là:

$$\forall (x_1, ..., x_n) \in N_1 \times ... \times N_n, \quad (x_1 + ... + x_n = 0 \Rightarrow x_1 = ... = x_n = 0).$$

xem 6.3.3, Định nghĩa 2).

7.2 Các phép toán trên các ánh xạ tuyến tính

7.2.1 Không gian vectơ $\mathcal{L}(E, F)$

♦ **Mệnh đề**

$\mathcal{L}(E, F)$ là một K-kgv đối với các luật thông thường.

Ta nhắc lại rằng (xem 6.1, Ví dụ 4)) các luật thông thường trên $\mathcal{L}(E, F)$ được xác định bởi:

$$\begin{cases} \forall f, g \in F^E, \forall x \in E, \ (f+g)(x) = f(x) + g(x) \\ \forall \lambda \in K, \forall f \in F^E, \quad (\lambda f)(x) = \lambda f(x). \end{cases}$$

Chứng minh:

Ta sẽ chứng tỏ rằng $\mathcal{L}(E, F)$ là một K-kgvc của F^E.

1) $\mathcal{L}(E, F) \neq \varnothing$ vì hiển nhiên ánh xạ không $0 : E \xrightarrow[x \mapsto 0]{} F$ tuyến tính.

2) Giả sử $\alpha \in K, f, g \in \mathcal{L}(E, F)$. Với mọi λ thuộc K, và mọi x, y thuộc E, ta có:

$$\begin{aligned}(\alpha f + g)(\lambda x + y) &= \alpha f(\lambda x + y) + g(\lambda x + y) = \alpha(\lambda f(x) + f(y)) + (\lambda g(x) + g(y)) \\ &= \lambda(\alpha f(x) + g(x)) + (\alpha f(y) + g(y)) = \lambda(\alpha f + g)(x) + (\alpha f + g)(y).\end{aligned}$$

Điều này chứng tỏ $\alpha f + g$ tuyến tính, vì vậy $\alpha f + g \in \mathcal{L}(E, G)$.

7.2.2 Phép hợp

♦ **Mệnh đề 1** Giả sử E, F, G là ba K-kgv. Ta có:

$$\forall f \in \mathcal{L}(E, F), \forall g \in \mathcal{L}(F, G), \ g \circ f \in \mathcal{L}(E, G).$$

Chứng minh: $\forall \lambda \in K, \forall (x, y) \in E^2$,

$$\begin{aligned}(g \circ f)(\lambda x + y) &= g(f(\lambda x + y)) = g(\lambda f(x) + f(y)) = \\ &= \lambda g(f(x)) + g(f(y)) = \lambda(g \circ f)(x) + (g \circ f)(y).\end{aligned}$$ ■

Nói cách khác: Hợp của hai ánh xạ tuyến tính là tuyến tính.

♦ **Mệnh đề 2** Giả sử E, F, G là ba K-kgv. Ta có:

1) $\forall f_1, f_2 \in \mathcal{L}(E, F), \forall g \in \mathcal{L}(F, G), \quad g \circ (f_1 + f_2) = g \circ f_1 + g \circ f_2$
(giả phân phối trái)

2) $\forall f \in \mathcal{L}(E, F), \forall g_1, g_2 \in \mathcal{L}(F, G), (g_1 + g_2) \circ f = g_1 \circ f + g_2 \circ f$
(giả phân phối phải)

3) $\forall \alpha \in K, \forall f \in \mathcal{L}(E, F), \forall g \in \mathcal{L}(F, G), (\alpha g) \circ f = g \circ (\alpha f) = \alpha(g \circ f)$.

Chứng minh:

Các phép kiểm chứng hầu như "tự động".

1) $\forall x \in E$,

$$(g \circ (f_1 + f_2))(x) = g((f_1 + f_2)(x)) = g(f_1(x)) + g(f_2(x))$$
$$= (g \circ f_1)(x) + (g \circ f_2)(x) = (g \circ f_1 + g \circ f_2)(x).$$

2) $\forall x \in E$,

$$((g_1 + g_2) \circ f)(x) = (g_1 + g_2)(f(x)) = g_1(f(x)) + g_2(f(x))$$
$$= (g_1 \circ f)(x) + (g_2 \circ f)(x) = (g_1 \circ f + g_2 \circ f)(x).$$

3) $\forall x \in E$,

$$\begin{cases} ((\alpha g) \circ f)(x) = (\alpha g)(f(x)) = \alpha g(f(x)) = \alpha(g \circ f)(x) = (\alpha(g \circ f))(x) \\ (g \circ (\alpha f))(x) = g(\alpha f(x)) = \alpha g(f(x)). \end{cases}$$

NHẬN XÉT:

- Công thức 1) có sử dụng tính chất tuyến tính của g, nhưng không dùng đến tính chất đó của f_1 và f_2
- Công thức 2) không sử dụng đến tính chất tuyến tính (của g_1, g_2, f)
- Công thức $(\alpha g) \circ f = \alpha(g \circ f)$ không sử dụng đến tính chất tuyến tính
- Công thức $g \circ (\alpha f) = \alpha(g \circ f)$ sử dụng tính chất tuyến tính của g, nhưng không dùng đến tính chất đó của f.

♦ **Mệnh đề 3** Cho E, F là hai K-kgv, $f \in \mathcal{L}(E, F)$. Nếu f là một đẳng cấu của E lên F, thì f^{-1} là một đẳng cấu từ F lên E.

Chứng minh:

Giả sử f tuyến tính và là song ánh, ta chứng minh $f^{-1} : F \to E$, vốn đã là song ánh (xem 1.3.2, Mệnh đề 3), cũng tuyến tính.

Giả sử $\lambda \in K$, $(x', y') \in F^2$. Ta có:

$$f^{-1}(\lambda x' + y') = f^{-1}(\lambda f(f^{-1}(x')) + f(f^{-1}(y'))$$
$$= f^{-1}(f(\lambda f^{-1}(x') + f^{-1}(y'))) = \lambda f^{-1}(x') + f^{-1}(y'),$$

và vì vậy f^{-1} tuyến tính. Xem thêm 2.1, Mệnh đề 5, *3*).

♦ **Định nghĩa 1** Hai K-kgv E, F được gọi là **đẳng cấu** khi và chỉ khi tồn tại một đẳng cấu K-kgv từ E lên F.

NHẬN XÉT:

Quan hệ "đẳng cấu" giữa các K-kgv là một quan hệ tương đương trong mọi tập hợp những K-kgv (nhưng không tồn tại **tập hợp** tất cả các K-kgv).

♦ **Mệnh đề 4**

1) Cho E, F là hai K-kgv hữu hạn chiều. Để E và F đẳng cấu, thì cần và đủ là: $\dim(E) = \dim(F)$.

2) Giả sử $n \in \mathbb{N}^*$. Mọi K-kgv n chiều đều đẳng cấu với K^n.

Chứng minh:

1) • Giả sử E và F đẳng cấu. Tồn tại một đẳng cấu f từ E lên F. Kgv E có ít nhất một cơ sở $\mathcal{B}$ và vì vậy (theo 7.1.3, Mệnh đề 4), $f(\mathcal{B})$ là một cơ sở của F, do đó:

$$\dim(F) = \mathrm{Card}(f(\mathcal{B})) = \mathrm{Card}(\mathcal{B}) = \dim(E).$$

• Ngược lại, giả sử $\dim(E) = \dim(F)$. Khi đó E (tương ứng: F) có một cơ sở $\mathcal{B} = (e_1, ..., e_n)$ (tương ứng: $\mathcal{C} = (e'_1, ..., e'_n)$, trong đó $n = \dim E \in \mathbb{N}$.

Xét $f \in \mathcal{L}(E, F)$, $g \in \mathcal{L}(F, E)$ xác định bởi

$$\forall i \in \{1, ..., n\}, \quad (f(e_i) = e'_i \text{ và } g(e'_i) = e_i).$$

Rõ ràng: $g \circ f = \mathrm{Id}_E$ và $f \circ g = \mathrm{Id}_F$, vì vậy (xem 1.3.2, Mệnh đề 5), f và g là những song ánh nghịch đảo lẫn nhau. Như vậy f là một đẳng cấu K-kgv từ E lên F.

2) Suy từ 1), vì $\dim(E) = \dim(K^n) = n$.

♦ Mệnh đề 5

$(\mathcal{L}(E), +, \cdot, \circ)$ là một K-đại số kết hợp và có đơn vị.

Chứng minh:

1) Chúng ta đã thấy rằng $(\mathcal{L}(E), +, \cdot)$ là một K-kgv, xem 7.2.1, Mệnh đề.

2) Luật $\circ$ là luật hợp thành trong trong $\mathcal{L}(E)$ (xem Mệnh đề 1), phân phối đối với $+$ (xem Mệnh đề 2, *1*) và 2)), và thỏa mãn công thức $(\alpha g) \circ f = g \circ (\alpha f) = \alpha(g \circ f)$ (xem Mệnh đề 2, *3*)).

3) Luật $\circ$ có tính kết hợp (trong E^E).

4) $\mathrm{Id}_E \in \mathcal{L}(E)$ và Id_E là phần tử trung hòa đối với $\circ$.

NHẬN XÉT:

1) Theo Mệnh đề 5, $(\mathcal{L}(E), +, \circ)$ là một vành.

2) Luật $\circ$ không có tính kết hợp, trừ khi: E hữu hạn chiều và $\dim(E) \leq 1$.

Thực vậy, ta giả thiết rằng $e_1, e_2 \in E$ sao cho (e_1, e_2) độc lập tuyến tính và ta *thừa nhận* rằng kgvc $\mathrm{Vect}(e_1, e_2)$ có ít nhất một phần bù F trong E. Xét các ánh xạ f, $g : E \to E$ xác định theo cách sau. Với mọi x thuộc E, tồn tại duy nhất $(\lambda_1, \lambda_2, y) \in K \times K \times F$ sao cho $x = \lambda_1 e_1 + \lambda_2 e_2 + y$, và đặt $f(x) = \lambda_2 e_1$ và $g(x) = \lambda_1 e_2$. Rõ ràng rằng f, g là những ánh xạ tuyến tính, $(g \circ f)(e_1) = 0$ và $(f \circ g)(e_1) = e_1$, vậy $g \circ f \neq f \circ g$. ■

Cách viết theo ma trận sẽ làm sáng tỏ ví dụ này (xem 8.1.3, Mệnh đề 2).

♦ **Định nghĩa 2** Một tự đồng cấu f của một K-kgv E được gọi là **lũy linh** khi và chỉ khi tồn tại $p \in \mathbb{N}^*$ sao cho $f^p = 0$.

Ở đây, f^p ký hiệu $f \circ ... \circ f$ (p nhân tử).

Nếu f là lũy linh, tập hợp $\{k \in \mathbb{N}; f^k = 0\}$ là một bộ phận khác rỗng của $\mathbb{N}$, do đó có phần tử nhỏ nhất, ở đây được ký hiệu là $\nu(f)$, và được gọi là **chỉ số lũy linh** của f. Ta có:

• $\forall k \in \mathbb{N}$, $(k < \nu(f) \Rightarrow f^k \neq 0)$, theo định nghĩa của $\nu(f)$

• $\forall k \in \mathbb{N}$, $(k \geq \nu(f) \Rightarrow f^k = 0)$, vì $f^k = f^{k-\nu(f)} \circ f^{\nu(f)} = f^{k-\nu(f)} \circ 0 = 0$. ■

♦ **Mệnh đề 6 (Dán các ánh xạ tuyến tính)**

Cho E, F là hai K-kgv, $n \in \mathbb{N}^*$, E_1, ..., E_n là những kgvc của E có tổng trực tiếp sao cho $E = \bigoplus_{i=1}^{n} E_i$, $f_i \in \mathcal{L}(E_i, F)$ $(1 \le i \le n)$.

Tồn tại một phần tử và chỉ một f thuộc $\mathcal{L}(E, F)$ sao cho $\forall i \in \{1, ..., n\}$, $f\big|_{E_i} = f_i$, và ta có: $f = \sum_{i=1}^{n} f_i \circ p_i$, trong đó, với mọi i thuộc $\{1, ..., n\}$, $p_i : E \to E_i$ được xác định bởi: $\forall (x_1, ..., x_n) \in E_1 \times ... \times E_n$, $p_i(x_1 + ... + x_n) = x_i$.

Chứng minh:

1) Giả sử $f \in \mathcal{L}(E, F)$ sao cho: $\forall i \in \{1, ..., n\}$, $f\big|_{E_i} = f_i$. Với mọi x thuộc E, ta có:

$$f(x) = f\left(\sum_{i=1}^{n} p_i(x)\right) = \sum_{i=1}^{n} f(p_i(x)) = \sum_{i=1}^{n} f_i(p_i(x)) = \left(\sum_{i=1}^{n} f_i \circ p_i\right)(x),$$

và vì vậy : $f = \sum_{i=1}^{n} f_i \circ p_i$.

2) Ngược lại, $\sum_{i=1}^{n} f_i \circ p_i \in \mathcal{L}(E, F)$ và, nếu ký hiệu $j_i : E_i \to E$ là đơn ánh chính tắc $(1 \le i \le n)$, thì với mọi k thuộc $\{1, ..., n\}$, ta có:

$$\left(\sum_{i=1}^{n} f_i \circ p_i\right)\Big|_{E_k} = \left(\sum_{i=1}^{n} f_i \circ p_i\right) \circ j_k = \sum_{i=1}^{n} (f_i \circ p_i \circ j_k) = f_k,$$

vì $p_i \circ j_k = \begin{cases} Id_{E_k} \text{ nếu } i = k \\ 0 \quad \text{nếu } i \neq k \end{cases}$.

Một cách viết theo lược đồ là :

Nếu $i = k$: $E_i \xrightarrow{j_i} E \xrightarrow{p_i} E_i$, Id_{E_i} ; nếu $i \neq k$: $E_k \xrightarrow{j_k} E \xrightarrow{p_i} E_i$, 0 ■

Phép chiếu

Giả sử E là một K-kgv.

1) Ta đã thấy rằng (7.1.1, Ví dụ 2)), với mọi cặp (F, G) những kgvc của E bù nhau trong E, phép chiếu lên F song song với G là ánh xạ tuyến tính $p : E \to E$, $x \mapsto x'$ trong đó $(x', x'') \in F \times G$, sao cho $x = x' + x''$.

• Với các ký hiệu trên, $x' = x' + 0$ và $(x', 0) \in F \times G$, do đó $p(x') = x'$, nói cách khác: $(p \circ p)(x) = p(x)$.

• Ta xác định $\mathrm{Im}(p)$.

Với các ký hiệu trên: $p(x) = x' \in F$, nên $\mathrm{Im}(p) \subset F$.

Mặt khác, với mọi x thuộc F, ta có $x = x + 0$ và $(x, 0) \in F \times G$, vì vậy $x = p(x) \in \mathrm{Im}(p)$.
Như vậy: $\mathrm{Im}(p) = F$.

• Ta xác định $\mathrm{Ker}(p)$.

Với mọi x thuộc G, $x = 0 + x$ và $(0, x) \in F \times G$, vì vậy $p(x) = 0$, do đó $G \subset \mathrm{Ker}(p)$.
Mặt khác, với các ký hiệu trên thì với mọi x thuộc E ta có:

$$p(x) = 0 \Leftrightarrow x' = 0 \Leftrightarrow x = x'' \Rightarrow x \in G,$$

do vậy $\mathrm{Ker}(p) \subset G$.
Như vậy: $\mathrm{Ker}(p) = G$.

2) Ngược lại, giả sử $p \in \mathcal{L}(E)$ sao cho $p \circ p = p$ (ta nói p là một phần tử *lũy đẳng* của vành $\mathcal{L}(E)$). Ta chứng tỏ rằng $\mathrm{Im}(p)$ và $\mathrm{Ker}(p)$ là hai kgvc của E, bù nhau trong E, và p là phép chiếu lên $\mathrm{Im}(p)$ song song với $\mathrm{Ker}(p)$.

• Giả sử $x \in \mathrm{Ker}(p) \cap \mathrm{Im}(p)$. Khi đó ta có $p(x) = 0$, và tồn tại $y \in E$ sao cho $x = p(y)$, từ đó suy ra:

$$0 = p(x) = p(p(y)) = \big(p \circ p\big)(y) = p(y) = x.$$

Điều đó chứng tỏ: $\mathrm{Im}(p) \cap \mathrm{Ker}(p) = \{0\}$.

• Giả sử $x \in E$. Ta có dạng phân tích: $x = p(x) + (x - p(x))$

và: $\begin{cases} p(x) \in \mathrm{Im}(p) \\ x - p(x) \in \mathrm{Ker}(p), \text{ vì } p(x - p(x)) = p(x) - (p \circ p)(x) = 0. \end{cases}$

Điều đó chứng tỏ: $E = \mathrm{Im}(p) + \mathrm{Ker}(p)$.

• Vì, với mọi x thuộc E: $\begin{cases} x = p(x) + (x - p(x)) \\ p(x) \in \mathrm{Im}(p), \\ x - p(x) \in \mathrm{Ker}(p) \end{cases}$

nên p là phép chiếu lên $\mathrm{Im}(p)$ song song với $\mathrm{Ker}(p)$.

Tóm lại, ta có :

♦ Mệnh đề 7

1) Giả sử F, G là hai kgvc của E bù nhau trong E, p là phép chiếu lên F, song song với G. Ta có: $p \circ p = p$, $\mathrm{Im}(p) = F$, $\mathrm{Ker}(p) = G$.

2) Ngược lại, nếu $p \in \mathcal{L}(E)$ sao cho $p \circ p = p$, thì $\mathrm{Im}(p)$ và $\mathrm{Ker}(p)$ là hai kgvc của E bù nhau trong E, và p là phép chiếu lên $\mathrm{Im}(p)$ song song với $\mathrm{Ker}(p)$.

Hơn nữa, với mọi x thuộc E:

$$x = p(x) + (x - p(x)), \quad p(x) \in \mathrm{Im}(p), \quad x - p(x) \in \mathrm{Ker}(p).$$

NHẬN XÉT:

Giả sử p là một phép chiếu của E. Ký hiệu $e = \mathrm{Id}_E$.

1) $e - p$ là một phép chiếu của E vì $(e - p)^2 = e - 2p + p^2 = e - p$, gọi là **phép chiếu liên kết** với phép chiếu p.

Rõ ràng là $\mathrm{Im}(e - p) = \mathrm{Ker}(p)$ và $\mathrm{Ker}(e - p) = \mathrm{Im}(p)$.

2) $s = 2p - e$ là phép đối xứng qua $\mathrm{Im}(p)$ song song với $\mathrm{Ker}(p)$ (xem 7.1.1, Ví dụ 3)): ta có: $s^2 = (2p - e)^2 = 4p^2 - 4p + e = e$.

Giả sử $2 \neq 0$ trong K, ta chứng minh dễ dàng rằng $\mathrm{Ker}(s - e) = \mathrm{Im}(p)$ và $\mathrm{Ker}(s + e) = \mathrm{Ker}(p)$, và vì vậy, với mọi (x', x'') thuộc $\mathrm{Im}(p) \times \mathrm{Ker}(p)$: $s(x' + x'') = x' - x''$.

(vì $s(x') = 2p(x') - x' = x'$ và $s(x'') = 2p(x'') - x'' = -x''$).

7.2.3 Nhóm $\mathcal{GL}(E)$

♦ **Mệnh đề - Định nghĩa**

Cho E là một K-kgv. Tập hợp $\mathcal{GL}(E)$ các tự đẳng cấu của E là một nhóm đối với $\circ$, được gọi là **nhóm tuyến tính** của E.

Chứng minh:

1) $\circ$ là luật hợp thành trong trong $\mathcal{GL}(E)$ vì, nếu $f, g : E \to E$ tuyến tính và song ánh, thì $g \circ f$ tuyến tính (xem 7.2.2, Mệnh đề 1) và song ánh (xem 1.3.2, Mệnh đề 1).

2) $\mathrm{Id}_E \in \mathcal{GL}(E)$ và Id_E là phần tử trung hòa đối với $\circ$.

3) Luật $\circ$ có tính kết hợp (trong E^E).

4) Cho $f \in \mathcal{GL}(E)$. Theo 7.2.2, Mệnh đề 3, f^{-1} là một tự đẳng cấu của E, nghĩa là $f^{-1} \in \mathcal{GL}(E)$.

NHẬN XÉT:

1) Nhóm $\mathcal{GL}(E)$ không giao hoán trừ khi: E hữu hạn chiều và $\dim(E) \leq 1$: lập luận như trong 7.2.2, Nhận xét 2), với:

$$f(x) = \lambda_1(e_1 + e_2) - \lambda_2 e_2 + y, \quad g(x) = \lambda_1 e_1 + \lambda_2(e_1 + e_2) + y.$$

Cách viết theo ma trận sẽ làm sáng tỏ ví dụ này (xem 8.1.4, Nhận xét 1)).

2) Nếu E hữu hạn chiều và nếu $\dim(E) = 1$, thì $(\mathcal{GL}(E), \circ)$ là một nhóm đẳng cấu với nhóm $(K - \{0\}, \cdot)$ qua đẳng cấu nhóm $K - \{0\} \to \mathcal{GL}(E)$, $\alpha \mapsto h_\alpha$, trong đó

$h_\alpha : E \to E$, $x \mapsto \alpha x$ là phép vị tự tỷ số α.

3) $\mathcal{GL}(E)$ cũng là tập hợp các phần tử khả nghịch của vành $(\mathcal{L}(E), +, \circ)$ (xem 7.2.2, Mệnh đề 3).

Bài tập

◊ **7.2.1** Giả sử E là $\mathbb{K}$-kgv các ánh xạ từ $\mathbb{K}$ vào $\mathbb{K}$ thuộc lớp C^∞ trên $\mathbb{K}$, $\varphi : \underset{f \mapsto f'}{E \to E}$.

$\psi : E \to E$ xác định bởi: $\forall f \in E, \forall x \in \mathbb{K}\ (\psi(f))(x) = \int_0^x f(t)dt$.

a) Kiểm chứng rằng φ và ψ là những ánh xạ tuyến tính.

b) Biểu diễn $\psi \circ \varphi$ và $\varphi \circ \psi$.

c) Xét tính đơn ánh, toàn ánh, song ánh của φ và của ψ.

◊ **7.2.2** Giả sử E là một K-kgv, $n \in \mathbb{N}^*$, $f \in \mathcal{L}(E)$ thỏa mãn $f^n = e$ (trong đó $e = \mathrm{Id}_E$), $\alpha \in K$ sao cho $\alpha^n \neq 1$, và $g = f - \alpha e$. Chứng tỏ rằng g là song ánh, và tính g^{-1}.

◊ **7.2.3** Giả sử E, F là hai K-kgv, $g \in \mathcal{L}(E, F)$, $\varphi : \underset{(x,y) \mapsto (x+g(y),y)}{E \times F \to E \times F}$. Chứng minh rằng φ là một tự đẳng cấu của $E \times F$.

◊ **7.2.4** Giả sử E là một K-kgv, $f \in \mathcal{L}(E)$. Giả sử tồn tại duy nhất một g thuộc $\mathcal{L}(E)$ thỏa mãn $f \circ g = \mathrm{Id}_E$. Chứng minh: $f \in \mathcal{GL}(E)$.

◊ **7.2.5** Giả sử E là một K-kgv, $E \neq \{0\}$, $f \in \mathcal{L}(E)$ là lũy linh, p là chỉ số lũy linh của f (nghĩa là $p \in \mathbb{N}^*$, $f^p = 0$, $f^{p-1} \neq 0$). Chứng minh rằng họ $(\mathrm{Id}_E, f, \ldots, f^{p-1})$ độc lập tuyến tính.

◊ **7.2.6** Giả sử E là một K-kgv, $n \in \mathbb{N}^*$, $E_1, \ldots, E_n$ là những kgvc của E, f: $\underset{(x_1,\ldots,x_n) \mapsto \sum_{i=1}^n x_i}{E_1 \times \ldots \times E_n \to E}$.

Chứng minh rằng $E_1, \ldots, E_n$ độc lập tuyến tính khi và chỉ khi f là đơn ánh.

◊ **7.2.7** Giả sử E là một K-kgv, $E_1, \ldots, E_n$ là những kgvc của E độc lập tuyến tính và thỏa mãn $\bigoplus_{i=1}^n E_i = E$, $f_i \in \mathcal{L}(E)$ với $i \in \{1, \ldots, n\}$, $f : E \to E$ xác định bởi: với mọi x thuộc E, tồn tại duy nhất $(x_1, \ldots, x_n) \in E_1 \times \ldots \times E_n$ sao cho $x = x_1 + \ldots + x_n$, và ta đặt $f(x) = \sum_{i=1}^n f_i(x_i)$.

Chứng minh : a) $\mathrm{Ker}(f) = \bigoplus_{i=1}^n \mathrm{Ker}(f_i)$ b) $\mathrm{Im}(f) = \bigoplus_{i=1}^n \mathrm{Im}(f_i)$.

◊ **7.2.8** Giả sử E là một K-kgv, $f, g \in \mathcal{L}(E)$ thỏa mãn $f \circ g = g \circ f$. Chứng minh rằng $\mathrm{Ker}(f)$ và $\mathrm{Im}(f)$ ổn định đối với g.

◊ **7.2.9** Giả sử E, F, G là ba K-kgv, $f \in \mathcal{L}(E, F)$, $g \in \mathcal{L}(F, G)$. Chứng minh :

a) $\mathrm{Ker}(g \circ f) = f^{-1}(\mathrm{Ker}(g))$ và $\mathrm{Ker}(g \circ f) \supset \mathrm{Ker}(f)$

b) $\mathrm{Im}(g \circ f) = g(\mathrm{Im}(f))$ và $\mathrm{Im}(g \circ f) \subset \mathrm{Im}(g)$.

◊ **7.2.10** Giả sử E, F, G là ba K-kgv, $f \in \mathcal{L}(E, F)$, $g, h \in \mathcal{L}(F, G)$. Chứng minh :

$\mathrm{Ker}(g \circ f) = \mathrm{Ker}(h \circ f) \Leftrightarrow \mathrm{Im}(f) \cap \mathrm{Ker}(g) = \mathrm{Im}(f) \cap \mathrm{Ker}(h)$.

◊ **7.2.11** Cho E là một K-kgv, $f, g \in \mathcal{L}(E)$, $\lambda \in K$, V là một kgvc của E.

a) Chứng minh rằng nếu V ổn định đối với f và đối với g, thì V ổn định đối với $f+g$, λf, $g \circ f$.

b) Chứng minh rằng nếu V ổn định đối với f, thì, với mọi $n \in \mathbb{N}^*$, V ổn định đối với f^n.

c) Cho một ví dụ về một kgv E trên $\mathbb{R}$, về $f \in \mathcal{L}(E)$ và về kgvc V của E sao cho:

$$f \text{ là song ánh, } f(V) \subset V, f(V) \neq V.$$

◊ **7.2.12** Giả sử E là một K-kgv, p, q là hai phép chiếu của E sao cho: $p \neq 0$, $q \neq 0$, $p \neq q$. Chứng minh rằng (p, q) độc lập tuyến tính trong $\mathcal{L}(E)$.

◊ **7.2.13** Giả sử E là một K-kgv, p, q là hai phép chiếu của E sao cho $p \circ q = q \circ p$ và $\mathrm{Ker}(p) = \mathrm{Ker}(q)$. Chứng minh $p = q$.

◊ **7.2.14** Giả sử E là một K-kgv (trong đó $K = \mathbb{R}$ hoặc $K = \mathbb{C}$), p, q là hai phép chiếu của E. Chứng minh rằng $p + q$ là một phép chiếu khi và chỉ khi $p \circ q = q \circ p = 0$.

◊ **7.2.15** Giả sử E là một K-kgv, $f, g \in \mathcal{L}(E)$. Chứng minh rằng hai tính chất sau là tương đương:

(i) $f \circ g = g$ và $g \circ f = f$

(ii) f, g là những phép chiếu và $\mathrm{Im}(f) = \mathrm{Im}(g)$.

◊ **7.2.16** Giả sử E là một K-kgv, p là một phép chiếu của E, $q = e - p$ (trong đó $e = \mathrm{Id}_E$).

$L = \{f \in \mathcal{L}(E);\ \exists u \in \mathcal{L}(E), f = u \circ p\}$, $M = \{g \in \mathcal{L}(E);\ \exists v \in \mathcal{L}(E), g = v \circ q\}$.

Chứng minh rằng L và M là những không gian con của $\mathcal{L}(E)$ bù nhau trong $\mathcal{L}(E)$.

Trong các bài tập 7.2.17 tới 7.2.22, ta thừa nhận rằng mọi kgvc có ít nhất một phần bù.

◊ **7.2.17*** Giả sử E, F là hai K-kgv, $f \in \mathcal{L}(E, F)$.

a) Chứng minh rằng f là toàn ánh khi và chỉ khi tồn tại $g \in \mathcal{L}(F, E)$ sao cho $f \circ g \in \mathrm{Id}_F$.

b) Chứng minh rằng f là đơn ánh khi và chỉ khi tồn tại $h \in \mathcal{L}(F, E)$ sao cho $h \circ f = \mathrm{Id}_E$.

◊ **7.2.18*** **Nhân tử hóa một ánh xạ tuyến tính**

Cho E, F, G là ba K-kgv.

a) Giả sử $f \in \mathcal{L}(E, F)$, $g \in \mathcal{L}(E, G)$.

Chứng minh : $\mathrm{Ker}(f) \subset \mathrm{Ker}(g) \Leftrightarrow (\exists h \in \mathcal{L}(F, G), g = h \circ f)$.

b) Giả sử $f \in \mathcal{L}(F, G)$, $g \in \mathcal{L}(E, G)$.

Chứng minh : $\mathrm{Im}(f) \supset \mathrm{Im}(g) \Leftrightarrow (\exists k \in \mathcal{L}(E, F), g = f \circ k)$.

◊ **7.2.19*** Giả sử E, F, G là ba K-kgv thỏa mãn $E \neq \{0\}$ và $G \neq \{0\}$. Ký hiệu:

$\phi : \mathcal{L}(E, F) \to \mathcal{L}(\mathcal{L}(F, G), \mathcal{L}(E, G))$ và $\psi : \mathcal{L}(F, G) \to \mathcal{L}(\mathcal{L}(E, F), \mathcal{L}(E, G))$

là các ánh xạ tuyến tính xác định bởi:

$$\forall f \in \mathcal{L}(E, F),\ \forall g \in \mathcal{L}(F, G),\ (\phi(f))(g) = (\psi(g))(f) = g \circ f.$$

Chứng minh rằng, với mọi (f, g) thuộc $\mathcal{L}(E, F) \times \mathcal{L}(F, G)$:

a) $\phi(f)$ là đơn ánh $\Leftrightarrow f$ là toàn ánh

b) $\phi(f)$ là toàn ánh $\Leftrightarrow f$ là đơn ánh

c) $\psi(g)$ là đơn ánh $\Leftrightarrow g$ là đơn ánh

d) $\psi(g)$ là toàn ánh $\Leftrightarrow g$ là toàn ánh.

(Có thể sử dụng bài tập 7.2.18).

◊ **7.2.20*** Giả sử E là một K-kgv, F, G là hai kgvc của E. Chứng tỏ rằng các tính chất sau là tương đương:

(i) $\exists f \in \mathcal{L}(E)$, $\mathrm{Im}(f) = F$ và $\mathrm{Ker}(f) = G$.

(ii) Tồn tại một phần bù H của G trong E sao cho H đẳng cấu với F.

◊ **7.2.21*** Giả sử E, F' là hai K-kgv, E' là một kgvc của E, F là một kgvc của F', $\phi : \mathcal{L}(E, F) \to \mathcal{L}(E', F')$ là ánh xạ được xác định bởi:

$$\forall f \in \mathcal{L}(E, F), \forall x' \in E', \ (\phi(f))(x') = f(x').$$

a) Kiểm chứng rằng ϕ tuyến tính

b) Xác định $\mathrm{Ker}(\phi)$ và $\mathrm{Im}(\phi)$.

◊ **7.2.22*** Giả sử E, F là hai K-kgv, $f \in \mathcal{L}(E, F)$. Chứng minh rằng tồn tại $g \in \mathcal{L}(F, E)$ sao cho:

$$f \circ g \circ f = f \quad \text{và} \quad g \circ f \circ g = g.$$

◊ **7.2.23*** Giả sử E là một K-kgv, E_1, E_2 là hai kgvc của E bù nhau trong E; ký hiệu:

$$G = \{f \in \mathcal{L}(E); \ \mathrm{Ker}(f) = E_1 \text{ và } \mathrm{Im}(f) = E_2\}.$$

a) Giả sử $f \in G$. Chứng tỏ rằng E_2 ổn định đối với f và tự đồng cấu f' của E_2 cảm sinh bởi f (nghĩa là: $\forall x \in E_2, f'(x) = f(x)$) là một tự đẳng cấu của E_2.

b) Chứng minh rằng G là một nhóm (đối với $\circ$), đẳng cấu với $(GL(E_2)$.

7.3 Trường hợp hữu hạn chiều

Trong §7.3 này, các kgv được giả thiết là hữu hạn chiều (trừ khi có nói ngược lại).

Nếu E, F là hai K-kgv hữu hạn chiều và $f \in \mathcal{L}(E, F)$, nhằm phục vụ việc nghiên cứu các ma trận (chương 8), nên ta sẽ ký hiệu n là số chiều của F và p là số chiều của E (thay vì ngược lại).

7.3.1 Định lý về hạng và các hệ quả

♦ **Định nghĩa** Giả sử E, F là hai K-kgv hữu hạn chiều, $f \in \mathcal{L}(E, F)$. Số tự nhiên xác định bởi

$$\text{rank}(f) = \dim(\text{Im}(f))$$

gọi là **hạng** của f, và ký hiệu là rank(f).

NHẬN XÉT:

1) Im(f) đúng là hữu hạn chiều vì Im(f) là một kgvc con của F và F hữu hạn chiều, hoặc nói cách khác, vì E hữu hạn chiều. Tổng quát hơn, giả sử E, F là hai K-kgv (không nhất thiết hữu hạn chiều), $f \in \mathcal{L}(E, F)$. Ta nói rằng f có **hạng hữu hạn** khi và chỉ khi Im(f) hữu hạn chiều, và trong trường hợp này, ta gọi là **hạng** của f là số tự nhiên, ký hiệu là rank(f), xác định bởi:

$$\text{rank}(f) = \dim(\text{Im}(f)).$$

2) Nếu $\mathcal{B}$ là một cơ sở của E, thì, với mọi $f \in \mathcal{L}(E, F)$:

$$\text{rank}(f) = \dim(f(\text{Vect}(\mathcal{B}))) = \dim(\text{Vect}(f(\mathcal{B}))) = \text{rank}(f(\mathcal{B})),$$

xem 6.4, Định nghĩa 3 và 7.1.3, Mệnh đề 1.

3) Với mọi f thuộc $\mathcal{L}(E, F)$: $\text{rank}(f) \leq \text{Min}(\dim(E), \dim(F))$. Thực vậy:

- E có ít nhất một cơ sở $\mathcal{B}$, và ta có

$$\text{rank}(f) = \text{rank}(f(\mathcal{B})) \text{ và } \text{Card}(f(\mathcal{B})) \leq \dim(E)$$

- $\text{rank}(f) = \dim(\text{Im}(f)) \leq \dim(F)$.

♦ **Định lý 1 (Định lý về hạng)**

Giả sử E, F là hai K-kgv, $f \in \mathcal{L}(E, F)$. Ta có:

$$\text{rank}(f) = \dim(E) - \dim(\text{Ker}(f)).$$

Chứng minh:

Ký hiệu $p = \dim(E)$, $n = \dim(F)$; kgvc Ker(f) của E có ít nhất một cơ sở $(e_1, ..., e_q)$, trong đó $q = \dim(\text{Ker}(f)) \in \mathbb{N}$. Theo định lý về cơ sở không đầy đủ, dạng yếu (6.4, Định lý 2), ta có thể bổ sung vào $(e_1, ..., e_q)$ để được một cơ sở $(e_1, ..., e_q, e_{q+1}, ..., e_p)$ của E. Ta sẽ chứng tỏ rằng $(f(e_{q+1}), ..., f(e_p))$ là một cơ sở của Im(f).

1) Hiển nhiên $f(e_{q+1}), ..., f(e_p)$ thuộc $\mathrm{Im}(f)$.

2) Giả sử $(\lambda_{q+1}, ..., \lambda_p) \in K^{p-q}$ thỏa mãn $\sum_{i=q+1}^{p} \lambda_i f(e_i) = 0$.

Vậy: $f\left(\sum_{i=q+1}^{p} \lambda_i e_i\right) = \sum_{i=q+1}^{p} \lambda_i f(e_i) = 0$, nên $\sum_{i=q+1}^{p} \lambda_i e_i \in \mathrm{Ker}(f)$.

Do đó tồn tại $(\mu_1, ..., \mu_q) \in K^q$ sao cho $\sum_{i=q+1}^{p} \lambda_i e_i = \sum_{i=1}^{q} \mu_i e_i$,

từ đó suy ra : $\mu_1 e_1 + ... + \mu_q e_q - \lambda_{q+1} e_{q+1} - ... - \lambda_p e_p = 0$.

Do $(e_1, ..., e_p)$ độc lập tuyến tính nên suy ra: $\lambda_{q+1} = ... = \lambda_p = 0$.

Điều này chứng tỏ $(f(e_{q+1}), ..., f(e_p))$ độc lập tuyến tính.

3) Giả sử $y \in \mathrm{Im}(f)$. Tồn tại $x \in E$ sao cho $y = f(x)$; vả lại, vì $(e_1, ..., e_p)$ sinh ra E nên tồn tại $(\alpha_1, ..., \alpha_p) \in K^p$ sao cho $x = \sum_{i=1}^{p} \alpha_i e_i$.

Ta có: $y = f(x) = f\left(\sum_{i=1}^{p} \lambda_i e_i\right) = \sum_{i=1}^{p} \lambda f(e_i) = \sum_{i=q+1}^{p} \lambda_i f(e_i)$,

vì $f(e_1) = ... = f(e_q) = 0$.

Điều này chứng tỏ $(f(e_{q+1}, ..., f(e_p))$ sinh ra $\mathrm{Im}(f)$.

Vì $(f(e_{q+1}), ..., f(e_p))$ là một cơ sở của $\mathrm{Im}(f)$, nên ta kết luận:

$$\mathrm{rank}(f) = \dim(\mathrm{Im}(f)) = p - q = \dim(E) - \dim(\mathrm{Ker}(f)).$$ ■

NHẬN XÉT:

1) Phép chứng minh trên cũng chứng tỏ rằng, với mọi phần bù E_1 của $\mathrm{Ker}(f)$ trong E, ánh xạ tuyến tính $E_1 \to \mathrm{Im}(f)$, $x \mapsto f(x)$ là một đẳng cấu kgv.

Như vậy, mọi phần bù của $\mathrm{Ker}(f)$ trong E đều đẳng cấu với $\mathrm{Im}(f)$.

2) Tuy $\dim(\mathrm{Ker}(f)) + \dim(\mathrm{Im}(f)) = \dim(E)$, nhưng "nói chung" $\mathrm{Ker}(f)$ và $\mathrm{Im}(f)$ không bù nhau trong E.

Thực vậy, trước hết $\mathrm{Im}(f)$ là một kgvc của F, chứ không phải của E.

Sau đó, thậm chí nếu $F = E$, $\mathrm{Ker}(f)$ và $\mathrm{Im}(f)$ có thể không bù nhau trong E, như trong ví dụ sau: $K = \mathbb{R}$, $E = F = \mathbb{R}^2$, $f : \mathbf{R}^2 \to \mathbf{R}^2$, $(x,y) \mapsto (y,0)$, trong trường hợp này ta có

$\mathrm{Ker}(f) = \mathrm{Im}(f) = \mathrm{Vect}((1, 0))$.

♦ **Mệnh đề** Giả sử E, F là hai K-kgv hữu hạn chiều, $f \in \mathcal{L}(E, F)$. Ta có:

1) (f là đơn ánh) $\Leftrightarrow$ $\mathrm{rank}(f) = \dim(E)$

2) (f là toàn ánh) $\Leftrightarrow$ $\mathrm{rank}(f) = \dim(F)$.

Chứng minh:

1) Áp dụng định lý về hạng:

(f đơn ánh) $\Leftrightarrow$ $\mathrm{Ker}(f) = \{0\}$ $\Leftrightarrow$ $\dim(\mathrm{Ker}(f)) = 0$ $\Leftrightarrow$ $\mathrm{rank}(f) = \dim(E)$.

2) (f toàn ánh) $\Leftrightarrow \mathrm{Im}(f) = F \Leftrightarrow \mathrm{rank}(f) = \dim(F)$ ■

(xem 6.4, Hệ quả 3).

Một phần tử f của $\mathcal{L}(E)$ được gọi là:

- **khả nghịch trái** đối với $\circ$ trong $\mathcal{L}(E)$ khi và chỉ khi:
$$\exists f' \in \mathcal{L}(E), f' \circ f = \mathrm{Id}_E$$
- **khả nghịch phải** đối với $\circ$ trong $\mathcal{L}(E)$ khi và chỉ khi:
$$\exists f'' \in \mathcal{L}(E), f \circ f'' = \mathrm{Id}_E$$
- **khả nghịch** đối với $\circ$ trong $\mathcal{L}(E)$ khi và chỉ khi:
$$\exists f' \in \mathcal{L}(E), f' \circ f = f \circ f' = \mathrm{Id}_E.$$

(xem 2.1, Định nghĩa 8).

Ta nhắc lại rằng một phần tử f của $\mathcal{L}(E)$ được gọi là:

- **chính quy trái** đối với $\circ$ trong $\mathcal{L}(E)$ khi và chỉ khi:
$$\forall (g, h) \in (\mathcal{L}(E))^2, (f \circ g = f \circ h \Rightarrow g = h)$$
- **chính quy phải** đối với $\circ$ trong $\mathcal{L}(E)$ khi và chỉ khi:
$$\forall (g, h) \in (\mathcal{L}(E))^2, (g \circ f = h \circ f \Rightarrow g = h)$$
- **chính quy** đối với $\circ$ trong $\mathcal{L}(E)$ khi và chỉ khi f là chính quy trái và chính quy phải đối với $\circ$ trong $\mathcal{L}(E)$ (xem 2.1, Định nghĩa 5).

◆ **Định lý 2** Giả sử E là một K-kgv hữu hạn chiều, $f \in \mathcal{L}(E)$. Các tính chất sau tương đương với nhau từng đôi một :

1. f khả nghịch trái đối với $\circ$ trong $\mathcal{L}(E)$
2. f khả nghịch phải đối với $\circ$ trong $\mathcal{L}(E)$
3. f khả nghịch đối với $\circ$ trong $\mathcal{L}(E)$
4. f chính quy trái đối với $\circ$ trong $\mathcal{L}(E)$
5. f chính quy phải đối với $\circ$ trong $\mathcal{L}(E)$
6. f chính quy đối với $\circ$ trong $\mathcal{L}(E)$
7. f là đơn ánh
8. f là toàn ánh
9. f là song ánh.

Chứng minh:

1 ⇒ 4:

Giả sử f khả nghịch trái đối với $\circ$ trong $\mathcal{L}(E)$; tồn tại $f' \in \mathcal{L}(E)$ sao cho $f' \circ f = e$ $(= \mathrm{Id}_E)$. Khi đó: $\forall (f, g) \in (\mathcal{L}(E))^2$, $(f \circ g = f \circ h \Rightarrow f' \circ f \circ g = f' \circ f \circ h \Rightarrow g = h)$, vậy f chính quy trái đối với $\circ$ trong $\mathcal{L}(E)$.

Ta chứng minh tương tự **2 ⇒ 5**, và suy ra: **3 ⇒ 6**.

4 ⇒ 7:

Giả sử f chính quy trái đối với $\circ$ trong $\mathcal{L}(E)$. Kgvc $\mathrm{Ker}(f)$ của kgv hữu hạn chiều E có ít nhất một phần bù E_1 trong E.

Xét phép chiếu p lên E_1 song song với $\mathrm{Ker}(f)$. Ta có:

$$\forall x \in E, \quad f(x) = f(p(x) + (x - p(x))) = f(p(x)) + f(x - p(x)) = f(p(x)),$$

vì $x - p(x) \in \mathrm{Ker}(f)$.

Như vậy, $f \circ e = f \circ p$, do đó vì f chính quy trái: $e = p$, và vì vậy $E = e(E) = p(E) = E_1$, $\mathrm{Ker}(f) = \{0\}$, f là đơn ánh.

5 ⇒ 8:

Giả sử f chính quy phải đối với $\circ$ trong $\mathcal{L}(E)$. Kgvc $\mathrm{Im}(f)$ của kgv hữu hạn chiều E có ít nhất một phần bù E_2 trong E. Xét phép chiếu q lên $\mathrm{Im}(f)$ song song với E_2. Ta có: $\forall x \in E, f(x) = q(f(x))$, vì $f(x) \in \mathrm{Im}(f)$.

Như vậy: $e \circ f = q \circ f$, do đó vì f chính quy phải: $e = q$, và vì vậy $E = e(E) = q(E)$ $= \mathrm{Im}(f)$, f là toàn ánh.

Cũng như **(4 ⇒ 7)** và **(5 ⇒ 8)**, ta suy ra: **6 ⇒ 9**.

7 ⇒ 8:

Áp dụng định lý về hạng và 6.4, Hệ quả 3, ta được:

$$(f \text{ đơn ánh}) \Leftrightarrow \mathrm{Ker}(f) = \{0\} \Leftrightarrow \dim(\mathrm{Ker}(f)) = 0 \Leftrightarrow \mathrm{rank}(f) = \dim(E)$$

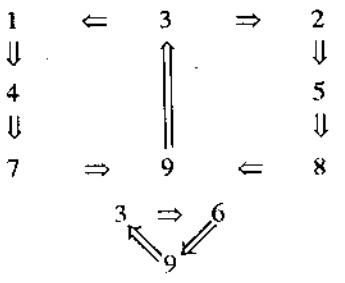
$$\Leftrightarrow \dim(\mathrm{Im}(f)) = \dim(E) \Leftrightarrow \mathrm{Im}(f) = E \Leftrightarrow (f \text{ toàn ánh}).$$

Từ tương tương thức **7 ⇔ 8**, dễ dàng suy ra: **(7 ⇒ 9)** và **(8 ⇒ 9)**.

9 ⇒ 3:

Nếu f tuyến tính và là song ánh, thì f^{-1} tuyến tính (xem 7.2.2, Mệnh đề 3), vì vậy f có một nghịch đảo đối với $\circ$ trong $\mathcal{L}(E)$.

(3 ⇒ 1) và **(3 ⇒ 2)**: hiển nhiên.



"Chu trình" $1 \Rightarrow 4 \Rightarrow 7 \Rightarrow 9 \Rightarrow 3 \Rightarrow 1$ chứng tỏ rằng các tính chất 1, 4, 7, 9, 3 tương đương với nhau từng đôi một .

Tương tự, 2, 5, 8, 9, 3 tương đương với nhau từng đôi một và 3, 6, 9 tương đương với nhau từng đôi một.

Như vậy, chín tính chất đang xét tương đương với nhau từng đôi một.

NHẬN XÉT:

1) • Các phép suy diễn $3 \Rightarrow 1, 3 \Rightarrow 2, 6 \Rightarrow 4, 6 \Rightarrow 5, 9 \Rightarrow 7, 9 \Rightarrow 8$ là tầm thường.

• Các phép suy diễn $1 \Rightarrow 4, 2 \Rightarrow 5, 3 \Rightarrow 6$ vẫn đúng khi E không hữu hạn chiều.

• Các phép suy diễn $4 \Rightarrow 7, 5 \Rightarrow 8, 6 \Rightarrow 9, 7 \Rightarrow 1, 8 \Rightarrow 2, 9 \Rightarrow 3$ vẫn đúng khi E không hữu hạn chiều, với điều kiện thừa nhận sự tồn tại của một phần bù của F trong E đối với mọi kgvc F của E, điều này cần đến *tiên đề chọn* (xem bài tập 7.2.17).

• Các suy diễn $1 \Rightarrow 2, 2 \Rightarrow 1, 4 \Rightarrow 5, 5 \Rightarrow 4, 7 \Rightarrow 8, 8 \Rightarrow 7$ có thể không đúng nếu E không hữu hạn chiều.

2) Dưới đây (8.1.5, Định lý) ta sẽ thấy những đặc trưng khác được phát biểu bằng những hệ thức ma trận.

7.3.2 Số chiều của $\mathcal{L}(E, F)$

♦ **Mệnh đề** Giả sử E, F là hai K-kgv hữu hạn chiều. Khi đó $\mathcal{L}(E, F)$ hữu hạn chiều và: $\dim(\mathcal{L}(E, F)) = \dim(E).\dim(F)$.

Chứng minh:

Ta sẽ xây dựng một cơ sở cho $\mathcal{L}(E, F)$ liên kết với một cơ sở cho trước của E và một cơ sở cho trước của F.

Ký hiệu $p = \dim(E)$, $n = \dim(F)$, $\mathcal{B} = \{e_1, ..., e_p\}$ là một cơ sở của E, $\mathcal{C} = (e'_1, ..., e'_n)$ là một cơ sở của F.

Với mọi (i, j) thuộc $\{1, ..., n\} \times \{1, ..., p\}$, ký hiệu φ_{ij} là ánh xạ tuyến tính từ E vào F xác định bởi:

$\forall k \in \{1, ..., p\}$, $\varphi_{ij}(e_k) = \delta_{kj} e'_i$, trong đó δ_{kj} là *ký hiệu Kronecker* xác định bởi:

$$\delta_{kj} = \begin{cases} 1 & \text{nếu } k = j \\ 0 & \text{nếu } k \neq j \end{cases}.$$

Ta chứng tỏ rằng họ $\Phi = \left(\varphi_{ij}\right)_{\substack{1 \le i \le n \\ 1 \le j \le p}}$ là một cơ sở của $\mathcal{L}(E, F)$.

1) Giả sử $\left(\lambda_{ij}\right)_{\substack{1 \le i \le n \\ 1 \le j \le p}} \in K^{np}$ sao cho $\sum_{\substack{1 \le i \le n \\ 1 \le j \le p}} \lambda_{ij} \varphi_{ij} = 0$.

Khi đó, với mọi k thuộc $\{1, ..., p\}$, ta có:

$$0 = \left(\sum_{\substack{1 \le i \le n \\ 1 \le j \le p}} \lambda_{ij} \varphi_{ij} \right)(e_k) = \sum_{\substack{1 \le i \le n \\ 1 \le j \le p}} \lambda_{ij} \varphi_{ij}(e_k) = \sum_{\substack{1 \le i \le n \\ 1 \le j \le p}} \lambda_{ij} \delta_{kj} e'_i = \sum_{i=1}^{n} \lambda_{ik} e'_i \ .$$

Vì $(e'_1, ..., e'_n)$ độc lập tuyến tính nên: $\forall k \in \{1, ..., p\}, \forall i \in \{1, ..., n\}, \lambda_{ik} = 0$.

Điều đó chứng tỏ Φ độc lập tuyến tính.

2) Giả sử $f \in \mathcal{L}(E, F)$.

Với mọi j thuộc $\{1, ..., p\}$, $f(e_j)$ phân tích được trên cơ sở $(e'_1, ..., e'_n)$ của F, và vì vậy tồn tại $(\lambda_{1j}, ..., \lambda_{nj}) \in K^n$ sao cho: $f(e_j) = \sum_{i=1}^{n} \lambda_{ij} e'_i$.

Khi đó ta có, như trong 1): $\forall k \in \{1,..., p\} \left(\sum_{\substack{1 \le i \le n \\ 1 \le j \le p}} \lambda_{ij} \varphi_{ij} \right) (e_k) = \sum_{i=1}^{n} \lambda_{ik} e'_i = f(e_k)$,

do đó $f = \sum_{\substack{1 \le i \le n \\ 1 \le j \le p}} \lambda_{ij} \varphi_{ij}$.

Điều này chứng tỏ rằng Φ sinh ra $\mathcal{L}(E, F)$.

Như vậy Φ là một cơ sở của $\mathcal{L}(E, F)$, và:

$$\dim \mathcal{L}(E, F) = \text{Card}(\Phi) = pn = \dim(E).\dim(F).$$

NHẬN XÉT:

Phép chứng minh trên (xây dựng các φ_{ij}) sẽ được sáng tỏ trên quan điểm ma trận (xem 8.1.3, Mệnh đề 2).

Bài tập

◊ **7.3.1** Giả sử $n \in \mathbb{N}^*$, $E_n = \mathbb{R}_n[X]$ là $\mathbb{R}$-kgv các đa thức bậc $\le n$. Chứng tỏ:

$$\forall Q \in E_n, \exists! P \in E_n, \quad Q = \sum_{i=0}^{n} P^{(i)}\left(\frac{X}{2^i}\right).$$

◊ **7.3.2** Giả sử E là một K-kgv 2 chiều, D_1, D_2, D_3 (tương ứng: Δ_1, Δ_2, Δ_3) là ba đường thẳng vectơ khác nhau từng đôi một. Chứng tỏ: $\exists f \in \mathcal{GL}(E), \forall i \in \{1, 2, 3\}, f(D_i) = \Delta_i$.

◊ **7.3.3** Giả sử E là một K-kgv hữu hạn chiều, $f \in \mathcal{L}(E)$ thỏa mãn: $\forall x \in E, \exists p_x \in \mathbb{N}^*$, $f^{p_x}(x) = x$. Chứng minh rằng: $\exists p \in \mathbb{N}^*, f^p = \text{Id}_E$.

◊ **7.3.4** Giả sử E là một K-kgv hữu hạn chiều, $e = \text{Id}_E$, $f, g \in \mathcal{L}(E)$. Giả sử tồn tại $h \in \mathcal{L}(E)$ sao cho: $e - f \circ g = f \circ h$ và $f \circ h = h \circ f$. Chứng minh rằng: $f \circ g = g \circ f$.

◊ **7.3.5*** Giả sử $K = \mathbb{R}$ hoặc $\mathbb{C}$, E là một K-kgv hữu hạn chiều, L_1, L_2 là hai kgvc của $\mathcal{L}(E)$ sao cho:

$$\begin{cases} L_1 \oplus L_2 = \mathcal{L}(E) \\ \forall (f_1, f_2) \in L_1 \times L_2, \ f_1 \circ f_2 + f_2 \circ f_1 = 0 \end{cases}$$

Chứng minh: $L_1 = \{0\}$ hoặc $L_2 = \{0\}$.

◊ **7.3.6** Giả sử E là một K-kgv hữu hạn chiều, $f \in \mathcal{L}(E)$. Chứng minh rằng: $\dim(\text{Ker}(f^2)) \le 2\dim(\text{Ker}(f))$.

◊ **7.3.7** Giả sử E là một K-kgv hữu hạn chiều, $\lambda \in K, f \in \mathcal{L}(E)$. Tính $\text{rank}(\lambda f)$ theo $\text{rank}(f)$.

◊ **7.3.8** Giả sử E_1, E_2, F_1, F_2 là những K-kgv hữu hạn chiều, $f_1 \in \mathcal{L}(E_1, F_1), f_2 \in \mathcal{L}(E_2, F_2)$, $\varphi : \begin{matrix} E_1 \times E_2 \to F_1 \times F_2 \\ (x_1, x_2) \mapsto (f_1(x_1), f_2(x_2)) \end{matrix}$. Chứng minh rằng φ tuyến tính và $\text{rank}(\varphi) = \text{rank}(f_1) + \text{rank}(f_2)$.

◊ **7.3.9** Giả sử E là một K-kgv hữu hạn chiều, $f, g \in \mathcal{L}(E)$ sao cho:

$$f + g = \text{Id}_E \text{ và } \text{rank}(f) + \text{rank}(g) \leq \dim(E).$$

Chứng minh rằng f và g là những phép chiếu.

◊ **7.3.10*** Giả sử E, F là hai K-kgv hữu hạn chiều, $f, g \in \mathcal{L}(E, F)$. Chứng minh:

$$\text{rank}(f + g) = \text{rank}(f) + \text{rank}(g) \Leftrightarrow \begin{cases} \text{Im}(f) \cap \text{Im}(g) = \{0\} \\ \text{Ker}(f) + \text{Ker}(g) = E \end{cases}$$

◊ **7.3.11** Giả sử E, F, G là ba K-kgv hữu hạn chiều, $f \in \mathcal{L}(E, F), g \in \mathcal{L}(F, G)$.

a) Chứng minh $\text{Ker}(g|_{\text{Im}(f)}) = \text{Ker}(g) \cap \text{Im}(f)$

b) Từ đó suy ra: $\text{rank}(g \circ f) = \text{rank}(f) - \dim(\text{Ker}(g) \cap \text{Im}(f))$.

c) Chứng minh: $\text{rank}(g \circ f) \geq \text{rank}(f) + \text{rank}(g) - \dim F$.

Bổ sung

◊ **C7.1 Các kgvc ổn định đối với các tự đồng cấu hoán vị**

Giả sử $n \in \mathbb{N} - \{0, 1\}$, E là một $\mathbb{C}$-kgv n chiều, $\mathcal{B} = (e_1, ..., e_n)$ là một cơ sở của E.

Với mọi σ thuộc $\mathfrak{S}_n$, ta ký hiệu f_σ là tự đồng cấu của E xác định bởi: $\forall i \in \{1, ..., n\}, f_\sigma(e_i) = e_{\sigma(i)}$.

Ký hiệu $s = \sum_{i=1}^{n} e_i$, D là đường thẳng vectơ sinh bởi s, H là siêu phẳng có phương trình $\sum_{i=1}^{n} x_i = 0$, $\mathfrak{F}$ là tập hợp các kgvc F của E sao cho: $\forall \sigma \in \mathfrak{S}_n, f_\sigma(F) \subset F$.

1) Chứng minh: $D \in \mathfrak{F}$ và $H \in \mathfrak{F}$.

2) Chứng minh rằng D và H bù nhau trong E, và nếu ký hiệu p là phép chiếu lên D song song với H, thì ta có: $p = \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}} f_\sigma$.

3) Giả sử $F \in \mathfrak{F}$ sao cho $F \not\subset D$. Chứng minh: $F \supset H$.

4) Kết luận rằng: $\mathfrak{F} = \{\{0\}, D, H, E\}$.

Chương 8

Ma trận

Trong chương 8 này K chỉ một thể giao hoán.

Tất cả các K-kgv xét đến đều được giả thiết hữu hạn chiều và có số chiều ≥ 1.

8.1 Phép tính ma trận

8.1.1 Khái niệm ma trận

Cho $n, p \in \mathbb{N}^*$.

◆ **Định nghĩa** Mọi ánh xạ từ $\{1, ..., n\} \times \{1, ..., p\}$ vào K gọi là **ma trận n dòng, p cột và với phần tử** (hoặc : **hệ tử**) **thuộc** K.

Một ánh xạ $A : \{1,..., n\} \times \{1,..., p\} \to K$ được ký hiệu dưới dạng một
$(i, j) \mapsto a_{ij}$ (hoặc $a_{i,j}$)
bảng :

$$A = (a_{ij})_{\substack{1\leq i\leq n\\ 1\leq j\leq p}} = (a_{ij})_{1\leq i\leq n;1\leq j\leq p} = (a_{ij})_{ij} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1p} \\ a_{21} & a_{22} & \cdots & a_{2p} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{np} \end{pmatrix}$$

Trong ký pháp này, các chỉ số ở ngoài dấu ngoặc theo thứ tự chỉ dòng và cột.

Cặp (n, p) được gọi là **cấp** của ma trận A, n là **số dòng**, p là **số cột** của A.

Với $(i, j) \in \{1, ..., n\} \times \{1, ..., p\}$, số hạng a_{ij} nằm ở dòng thứ i và cột thứ j được gọi là **hạng tử** (hoặc: **hệ số**) thứ (i, j) của A.

Ta nói rằng:

• A là một ma trận **vuông** khi và chỉ khi $n = p$, khi đó ta nói A là một ma trận **vuông cấp** n.

• A là một **ma trận cột** (hay: **ma trận một cột**) khi và chỉ khi $p = 1$.

• A là một **ma trận dòng** (hay:**ma trận một dòng**) khi và chỉ khi $n = 1$.

Nếu $A = (a_{ij})_{1\leq i,j\leq n}$ là ma trận vuông cấp n, các a_{ii} $(1 \leq i \leq n)$ được gọi là các **phần tử chéo** của A và $(a_{11},....,a_{nn})$ được gọi là **đường chéo** của A.

♦ **Ký hiệu** Với $(n, p) \in (\mathbb{N}^*)^2$, ta ký hiệu:
$\mathbf{M}_{n,p}(K)$ là tập hợp các ma trận n dòng, p cột và với hạng tử thuộc K.
$\mathbf{M}_n(K) = \mathbf{M}_{n,n}(K)$ là tập hợp các ma trận vuông cấp n với phần tử thuộc K.
Giả sử $A = (a_{ij})_{1\le i\le n;1\le j\le p} \in \mathbf{M}_{n,p}(K)$.

• Với $i \in \{1, ..., n\}$, ma trận dòng $(a_{ij})_{1\le j\le p} = (a_{i1}, ..., a_{ip})$ thuộc $\mathbf{M}_{1,p}(K)$ được gọi là **dòng thứ** i của A.

• Với $j \in \{1, ..., p\}$, ma trận cột $(a_{ij})_{1\le i\le n} = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix}$ thuộc $\mathbf{M}_{n,1}(K)$ được gọi là **cột thứ** j của A.

8.1.2 Ma trận và ánh xạ tuyến tính

♦ **Định nghĩa1** Giả sử E là một K-kgv, $n = \dim(E)$, $\mathcal{B} = (e_1, ..., e_n)$ là một cơ sở của E, $x \in E$, $(x_1, ..., x_n)$ là các thành phần của x trong $\mathcal{B}$: $x = \sum_{i=1}^{n} x_i e_i$.

Ma trận cột $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ được gọi là **ma trận cột các thành phần của** x **trong** $\mathcal{B}$ và được ký hiệu là $\mathrm{Mat}_{\mathcal{B}}(x)$.

Như vậy : $\mathrm{Mat}_{\mathcal{B}}(x) \in \mathbf{M}_{n,1}(K)$.

Rõ ràng ánh xạ $\mathrm{Mat}_{\mathcal{B}} : \underset{x \mapsto \mathrm{Mat}_{\mathcal{B}}(x)}{E \to \mathbf{M}_{n,1}(K)}$ là một song ánh.

Khi $X = \mathrm{Mat}_{\mathcal{B}}(x)$, ta nói rằng x **được biểu diễn bởi** X trong cơ sở $\mathcal{B}$, hoặc X **biểu diễn** x trong $\mathcal{B}$.

♦ **Định nghĩa 2** Giả sử E là một K-kgv, $n = \dim(E)$, $\mathcal{B} = (e_1, ..., e_n)$ là một cơ sở của E, $p \in \mathbb{N}^*$, $\mathcal{F} = (V_1, ..., V_p)$ là một họ hữu hạn gồm p phần tử của E, và với mỗi j thuộc $\{1, ..., p\}$, $(a_{1j}, ..., a_{nj})$ là các thành phần của V_j trong $\mathcal{B}$:

$$\forall j \in \{1, ..., p\}, V_j = \sum_{i=1}^{n} a_{ij} e_i .$$

Ma trận $(a_{ij})_{1\le i\le n;1\le j\le p} = \begin{pmatrix} a_{11} & \cdots & a_{1p} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{np} \end{pmatrix}$ thuộc $\mathbf{M}_{n,p}(K)$ được gọi là **ma trận của họ** $(V_1, ..., V_p)$ **đối với cơ sở** $\mathcal{B}$ và được ký hiệu là $\mathrm{Mat}_{\mathcal{B}}(\mathcal{F})$.

NHẬN XÉT:

$\mathrm{Mat}_{\mathcal{B}}(V_1, ..., V_p)$ thu được bằng cách đặt "kề nhau" các ma trận cột $\mathrm{Mat}_{\mathcal{B}}(V_1)$, ..., $\mathrm{Mat}_{\mathcal{B}}(V_p)$.

♦ Định nghĩa 3

1) Giả sử | E, F là hai K-kgv, $p = \dim(E)$, $n = \dim(F)$,
$\mathcal{B} = (e_1, ..., e_p)$ là một cơ sở của E, $\mathcal{C} = \{f_1, ..., f_n\}$ là một cơ sở của F,
$f \in \mathcal{L}(E, F)$.

Với mỗi j thuộc $\{1, ..., p\}$, ta ký hiệu $(a_{1j}, ..., a_{nj})$ là các thành phần của $f(e_j)$ trong $\mathcal{C}$:

$$f(e_j) = \sum_{i=1}^{n} a_{ij} f_i .$$

Ma trận thuộc $\mathbf{M}_{n,p}(K)$ xác định bởi :

$$\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f) = (a_{ij})_{1 \le i \le n; 1 \le j \le p}$$

gọi là **ma trận của** f **đối với các cơ sở** $\mathcal{B}$ **và** $\mathcal{C}$ và ký hiệu là $\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f)$.

2) Giả sử E là một K-kgv, $n = \dim(E)$, $\mathcal{B} = (e_1, ..., e_n)$ là một cơ sở của E, $f \in \mathcal{L}(E)$. Ma trận thuộc $\mathbf{M}_n(K)$ xác định bởi :

$$\mathrm{Mat}_{\mathcal{B}}(f) = \mathrm{Mat}_{\mathcal{B},\mathcal{B}}(f)$$

gọi là **ma trận của** f **đối với cơ sở** $\mathcal{B}$ và ký hiệu là $\mathrm{Mat}_{\mathcal{B}}(f)$.

Rõ ràng rằng ánh xạ $\mathrm{Mat}_{\mathcal{B},\mathcal{C}} : \mathcal{L}(E, F) \to \mathbf{M}_{n,p}(K)$ là một song ánh.
$f \mapsto \mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f)$

Khi $A = \mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f)$, ta nói rằng f **được biểu diễn bởi** A **trong các cơ sở** $\mathcal{B}, \mathcal{C}$, hoặc A **biểu diễn** f **trong các cơ sở** $\mathcal{B}$, $\mathcal{C}$.

8.1.3 Không gian véctơ $\mathbf{M}_{n,p}(K)$

Chúng ta sẽ "chuyển" cấu trúc vectơ của $\mathcal{L}(E, F)$ lên $\mathbf{M}_{n,p}(K)$ bằng song ánh $\mathrm{Mat}_{\mathcal{B},\mathcal{C}}$, trong đó $\mathcal{B} = (e_1, ..., e_p)$, $C = (f_1, ..., f_n)$ là những cơ sở cố định tương ứng của E, F.

Giả thiết $\lambda \in K$, $f, g \in \mathcal{L}(E, F)$, $A = (a_{ij})_{ij} = \mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f)$, $B = (b_{ij})_{ij} = \mathrm{Mat}_{\mathcal{B},\mathcal{C}}(g)$.

Như vậy ta có:

$$\forall j \in \{1, ..., p\}, \begin{cases} f(e_j) = \sum_{i=1}^{n} a_{ij} f_i \\ g(e_j) = \sum_{i=1}^{n} b_{ij} f_i \end{cases}$$

do đó: $\forall j \in \{1, ..., p\}, (\lambda f + g)(e_j) = \sum_{i=1}^{n} (\lambda a_{ij} + b_{ij}) f_i$.

Điều này dẫn ta tới định nghĩa sau.

♦ Định nghĩa

1) Luật hợp thành trong trong $\mathbf{M}_{n,p}(K)$, ký hiệu là +, xác định bởi:

$$\forall (a_{ij})_{ij} \in \mathbf{M}_{n,p}(K), \forall (b_{ij})_{ij} \in \mathbf{M}_{n,p}(K), \quad (a_{ij})_{ij} + (b_{ij})_{ij} = (a_{ij} + b_{ij})_{ij}$$

gọi là **phép cộng** trong $M_{n,p}(K)$

2) Luật ngoài $K \times \mathbf{M}_{n,p}(K) \to \mathbf{M}_{n,p}(K)$, thể hiện bằng cách không viết dấu nào cả (hoặc bởi một điểm), xác định bởi:

$$\forall \alpha \in K, \forall (a_{ij})_{ij} \in \mathbf{M}_{n,p}(K), \quad \alpha (a_{ij})_{ij} = (\alpha a_{ij})_{ij}$$

gọi là **phép nhân** với vô hướng.

NHẬN XÉT:

Chỉ có thể cộng các ma trận cùng cấp.

♦ Mệnh đề 1

1) $(\mathbf{M}_{n,p}(K), +, \cdot)$ là một K-kgv.

2) Với mọi K-kgv (p chiều) E và (n chiều) F, và với mọi cơ sở $\mathcal{B}$ của E và $\mathcal{C}$ của F, ánh xạ : $\mathrm{Mat}_{\mathcal{B},\mathcal{C}} : \mathcal{L}(E, F) \to \mathbf{M}_{n,p}(K)$ là một đẳng cấu K-kgv.
$f \mapsto \mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f)$

Chứng minh:

Ánh xạ $\mathrm{Mat}_{\mathcal{B},\mathcal{C}}$ là một song ánh, và:

$$\forall \alpha \in K, \quad \forall (f, g) \in (\mathcal{L}(E,F))^2, \quad \mathrm{Mat}_{\mathcal{B},\mathcal{C}}(\alpha f + g) = \alpha \mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f) + \mathrm{Mat}_{\mathcal{B},\mathcal{C}}(g),$$

do đó bằng việc chuyển cấu trúc ta dễ dàng suy ra rằng $\mathbf{M}_{n,p}(K)$ là một K-kgv và $\mathrm{Mat}_{\mathcal{B},\mathcal{C}}$ là một đẳng cấu K-kgv. ■

Tương tự, với mọi K-kgv n chiều và mọi cơ sở $\mathcal{B}$ của E, ánh xạ $\mathrm{Mat}_{\mathcal{B}} : E \to \mathbf{M}_{n,1}(K)$ là
$x \mapsto \mathrm{Mat}_{\mathcal{B}}(x)$

một đẳng cấu K-kgv.

♦ Ký hiệu

1) Ký hiệu $0_{n,p}$ hoặc đơn giản hơn, O (hoặc: 0) chỉ ma trận thuộc $\mathbf{M}_{n,p}(K)$ có tất cả các hạng tử bằng không.

2) Với $(n, p) \in (\mathbb{N}^*)^2$ và $(i, j) \in \{1, ..., n\} \times \{1, ..., p\}$, ta ký hiệu ma trận thuộc $\mathbf{M}_{n,p}(K)$ có hạng tử thứ (i, j) bằng 1 và các hạng tử khác bằng không là $E_{i,j}$. Các ma trận E_{ij} được gọi là các **ma trận sơ cấp**.

NHẬN XÉT:

1) Trong ký hiệu E_{ij}, ta không nhắc tới cấp (n, p).

2) Nếu **ký hiệu Kronecker** là δ, xác định bởi : $\delta_{xy} = \begin{cases} 1 & \text{nếu } x = y \\ 0 & \text{nếu } x \neq y \end{cases}$, thì rõ ràng ta có: $E_{ij} = \left(\delta_{ki}\delta_{lj}\right)_{\substack{1 \le k \le n \\ 1 \le l \le p}}$.

♦ Mệnh đề 2

1) $\left(E_{ij}\right)_{(i,j) \in \{1,\ldots,n\} \times \{1,\ldots,p\}}$ là một cơ sở của $\mathbf{M}_{n,p}(K)$, gọi là **cơ sở chính tắc** của $\mathbf{M}_{n,p}(K)$.

2) $\dim(\mathbf{M}_{n,p}(K)) = np$.

Chứng minh :

1) Hiển nhiên với mọi ma trận $A = \left(a_{ij}\right)_{ij}$ thuộc $\mathbf{M}_{n,p}(K)$ ta có: $A = \sum_{\substack{1 \le i \le n \\ 1 \le j \le p}} a_{ij} E_{ij}$, điều đó chứng tỏ $(E_{ij})_{ij}$ sinh ra $\mathbf{M}_{n,p}(K)$.

2) Nếu $\left(a_{ij}\right)_{ij}$ thỏa mãn $\sum_{i,j} a_{ij} E_{ij} = 0$ thì $\left(a_{ij}\right)_{ij} = 0$, điều đó chứng tỏ $(E_{ij})_{ij}$ độc lập tuyến tính. Xem thêm 7.3.2, Mệnh đề. ■

VÍ DỤ :

Cơ sở chính tắc của $\mathbf{M}_2(K)$ là $(E_{11}, E_{12}, E_{21}, E_{22})$, trong đó: $E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $E_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $E_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, $E_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, và với mọi ma trận $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ thuộc $\mathbf{M}_2(K)$ ta có:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11}E_{11} + a_{12}E_{12} + a_{21}E_{21} + a_{22}E_{22}.$$

8.1.4 Phép nhân ma trận

Giả sử | E, F, G là ba K-kgv, tương ứng q, p, n chiều
$\mathcal{B} = (e_1, ..., e_q)$, $\mathcal{C} = (f_1, ..., f_p)$, $\mathcal{D} = (g_1, ..., g_n)$ tương ứng là những cơ sở của E, F, G
$f \in \mathcal{L}(E, F)$, $g \in \mathcal{L}(F, G)$
$A = (a_{jk})_{jk} = \mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f)$, $B = (b_{ij})_{ij} = \mathrm{Mat}_{\mathcal{C},\mathcal{D}}(g)$.

Ta xác định ma trận của $g \circ f$ đối với các cơ sở $\mathcal{B}$ và $\mathcal{D}$.

Giả sử $k \in \{1, ..., q\}$. Từ định nghĩa của A ta có: $f(e_k) = \sum_{j=1}^{p} a_{jk} f_j$.

Suy ra: $(g \circ f)(e_k) = g\left(\sum_{j=1}^{p} a_{jk} f_j\right) = \sum_{j=1}^{p} a_{jk}\, g(f_j)$.

Từ định nghĩa của B: $\forall j \in \{1, ..., p\}, g(f_j) = \sum_{i=1}^{n} b_{ij} g_i$.

Do vậy: $(g \circ f)(e_k) = \sum_{j=1}^{p} a_{jk}\left(\sum_{i=1}^{n} b_{ij} g_i\right) = \sum_{j=1}^{p}\sum_{i=1}^{n} b_{ij} a_{jk} g_i = \sum_{i=1}^{n}\left(\sum_{j=1}^{p} b_{ij} a_{jk}\right) g_i$.

Do đó $\mathrm{Mat}_{\mathcal{B},\mathcal{D}}(g \circ f) = (c_{ik})_{ik}$, trong đó: $\forall (i, k) \in \{1, ..., n\} \times \{1, ..., q\}, c_{ik} = \sum_{j=1}^{p} b_{ij} a_{jk}$.

Điều này dẫn ta tới định nghĩa sau, sau khi đổi chỗ A và B.

♦ **Định nghĩa 1** Giả sử $A = (a_{ij})_{ij} \in \mathbf{M}_{n,p}(K)$, $B = (b_{jk})_{jk} \in \mathbf{M}_{p,q}(K)$. Ma trận thuộc $\mathbf{M}_{n,q}(K)$ xác định bởi:

$AB = (c_{ik})_{ik}$, trong đó: $\forall (i, k) \in \{1, ..., n\} \times \{1, ..., q\}, c_{ik} = \sum_{j=1}^{p} a_{ij} b_{jk}$,

gọi là **tích của A với B** và ký hiệu là AB.

Ánh xạ $\mathbf{M}_{n,p}(K) \times \mathbf{M}_{p,q}(K) \to \mathbf{M}_{n,q}(K)$, $(A, B) \mapsto AB$ được gọi là **phép nhân ma trận**.

NHẬN XÉT:

Tích AB tồn tại khi và chỉ khi số cột của A bằng số dòng của B. ■

Chúng ta đã chứng minh kết quả sau đây:

♦ Mệnh đề 1

Giả sử | E, F, G là ba K-kgv,
| $\mathcal{B}, \mathcal{C}, \mathcal{D}$ tương ứng là những cơ sở của E, F, G
| $f \in \mathcal{L}(E, F), g \in \mathcal{L}(F, G)$

Ta có: $\mathrm{Mat}_{\mathcal{B},\mathcal{D}}(g \circ f) = (\mathrm{Mat}_{\mathcal{C},\mathcal{D}}(g))(\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f))$.

Nói cách khác: (trong những cơ sở thích hợp) ma trận của một tích hai ánh xạ tuyến tính bằng tích các ma trận của các ánh xạ tuyến tính đó (theo cùng thứ tự). ■

♦ Mệnh đề 2

Giả sử | E, F là hai K-kgv,
| $\mathcal{B}, \mathcal{C}$ tương ứng là những cơ sở của E, F
| $f \in \mathcal{L}(E, F), x \in E$.

Ta có: $\mathrm{Mat}_{\mathcal{C}}(f(x)) = (\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f))\,(\mathrm{Mat}_{\mathcal{B}}(x))$.

Chứng minh:

Đặt $\mathcal{B} = (e_1, \ldots, e_p)$, $\mathcal{C} = \{f_1, \ldots f_n\}$, $X = \mathrm{Mat}_{\mathcal{B}}(x) = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}$,

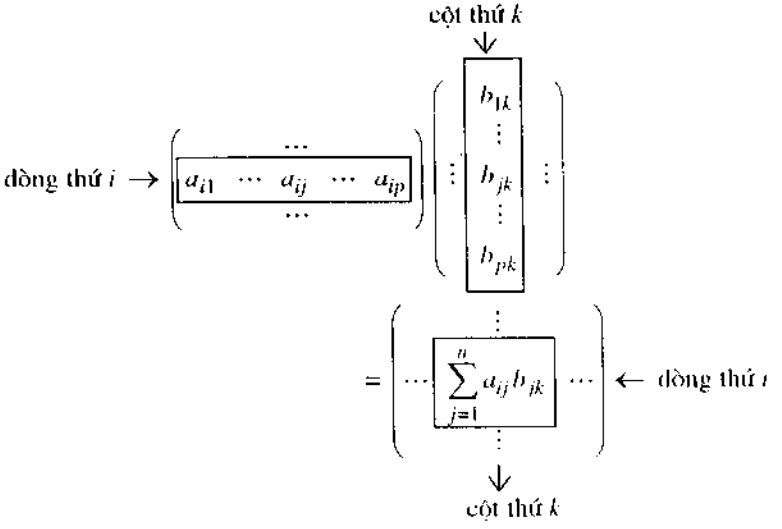
$A = \mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f) = (a_{ij})_{\substack{1 \le i \le n \\ 1 \le j \le p}}$.

Ta có : $f(x) = f\left(\sum_{j=1}^{p} x_j e_j\right) = \sum_{j=1}^{p} x_j f(e_j) = \sum_{j=1}^{p}\left(x_j \sum_{i=1}^{n} a_{ij} f_i\right)$

$= \sum_{j=1}^{p}\sum_{i=1}^{n} a_{ij} x_j f_i = \sum_{i=1}^{n}\left(\sum_{j=1}^{p} a_{ij} x_j\right) f_i$.

Do đó: $\mathrm{Mat}_{\mathcal{C}}(f(x)) = \left(\sum_{j=1}^{p} a_{ij} x_j\right)_{1 \le i \le n} = AX$. ■

Trong thực tế, để tính tích AB của hai ma trận, ta tiến hành theo cách sau:



NHẬN XÉT:

Nếu $A \in \mathbf{M}_{n,p}(K)$ và $B \in \mathbf{M}_{p,q}(K)$, thì $AB \in \mathbf{M}_{n,q}(K)$. Như vậy cấp (n, q) của AB có được từ các cấp (n, p) của A, và (p, q) của B "giống như theo hệ thức Chasles".

VÍ DỤ :

1) • $\begin{pmatrix}2 & 3\end{pmatrix}\begin{pmatrix}1\\11\end{pmatrix} = \begin{pmatrix}35\end{pmatrix}$.

• Tổng quát hơn : $\begin{pmatrix}x_1, \ldots, x_n\end{pmatrix}\begin{pmatrix}y_1\\ \vdots \\ y_n\end{pmatrix} = \begin{pmatrix}\sum_{i=1}^{n} x_i y_i\end{pmatrix}$.

2) • $\begin{pmatrix}1\\11\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix} = \begin{pmatrix}2 & 3\\22 & 33\end{pmatrix}$.

• Tổng quát hơn: $\begin{pmatrix}x_1\\ \vdots \\ x_n\end{pmatrix}\begin{pmatrix}y_1, \ldots, y_p\end{pmatrix} = \begin{pmatrix}x_1y_1 & \cdots & x_1y_p\\ \vdots & & \vdots \\ x_ny_1 & \cdots & x_ny_p\end{pmatrix}$.

3) $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix} = \begin{pmatrix}ax+by\\ cx+dy\end{pmatrix}$.

4) $\begin{pmatrix}u, v\end{pmatrix}\begin{pmatrix}\alpha & \alpha' & \alpha''\\ \beta & \beta' & \beta''\end{pmatrix} = \begin{pmatrix}u\alpha+v\beta & u\alpha'+v\beta' & u\alpha''+v\beta''\end{pmatrix}$.

5) $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}x & y\\ z & t\end{pmatrix} = \begin{pmatrix}ax+bz & ay+bt\\ cx+dz & cy+dt\end{pmatrix}$.

6) $\begin{pmatrix}1 & -2\\ 3 & 7\\ -4 & 6\end{pmatrix}\begin{pmatrix}4 & 1 & -3 & 2\\ 6 & -5 & 9 & 0\end{pmatrix} = \begin{pmatrix}-8 & 11 & -21 & 2\\ 54 & -32 & 54 & 6\\ 20 & -34 & 66 & -8\end{pmatrix}$. ■

Xuất phát từ các tính chất quen thuộc về các phép toán đại số với các ánh xạ tuyến tính, ta suy ra các tính chất về các phép toán đại số đối với các ma trận:

Mệnh đề 3

1) **(Giả phân phối trái)**

$$\forall A \in \mathbf{M}_{n,p}(K),\ \forall B, C \in \mathbf{M}_{p,q}(K),\quad A(B + C) = AB + AC$$

2) **(Giả phân phối phải)**

$$\forall A, B \in \mathbf{M}_{n,p}(K),\ \forall C \in \mathbf{M}_{p,q}(K),\quad (A + B)C = AC + BC$$

3) $\forall \lambda \in K,\ \forall A \in \mathbf{M}_{n,p}(K),\ \forall B \in \mathbf{M}_{p,q}(K)$

$$(\lambda A)\, B = \lambda(AB) = A(\lambda B).$$

4) **(Giả kết hợp)**

$$\forall A \in \mathbf{M}_{n,p}(K),\ \forall B \in \mathbf{M}_{p,q}(K),\ \forall C \in \mathbf{M}_{q,r}(K)$$

$$(AB)C = A(BC).$$

Đối với các ma trận A,B,C có cấp tương ứng (n,p), (p,q), (q,r) ta có thể viết ABC thay cho $(AB)C$ hoặc $A(BC)$. ■

Mệnh đề 4

1) $(\mathbf{M}_n(K), +, \bullet, \times)$ là một K-đại số kết hợp và có đơn vị.

2) Với mọi K-kgv n chiều E và mọi cơ sở $\mathcal{B}$ của E, ánh xạ $\mathrm{Mat}_{\mathcal{B}} : \mathcal{L}(E) \to \mathbf{M}_n(K)$ là một đẳng cấu K- đại số có đơn vị.

$$f \mapsto \mathrm{Mat}_{\mathcal{B}}(f)$$

Chứng minh :

Ta đã thấy $(\mathbf{M}_n(K), +, \bullet)$ là một K-kgv (8.1.3, Mệnh đề) và phép nhân là luật hợp thành trong $\mathbf{M}_n(K)$.

Vì $\mathrm{Mat}_{\mathcal{B}}$ là một song ánh và do

$$\forall (f,g) \in (\mathcal{L}(E))^2,\quad \mathrm{Mat}_{\mathcal{B}}(g \circ f) = (\mathrm{Mat}_{\mathcal{B}}(g))\,(\mathrm{Mat}_{\mathcal{B}}(f)),$$

và vì $(\mathcal{L}(E), +, \bullet, \circ)$ là một K-đại số kết hợp, có đơn vị, nên bằng việc chuyển cấu trúc, ta suy ra $(\mathbf{M}_n(K), +, \bullet, \times)$ cũng là một K- đại số kết hợp, có đơn vị và $\mathrm{Mat}_{\mathcal{B}}$ là một đẳng cấu K- đại số có đơn vị.

Ký hiệu Ta ký hiệu $\mathbf{I}_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in \mathbf{M}_n(K)$, là phần tử trung hòa của phép nhân trong $\mathbf{M}_n(K)$.

NHẬN XÉT:

1) Nếu $n \geq 2$, đại số $\mathbf{M}_n(K)$ không giao hoán như trong ví dụ sau (với $n = 2$):

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix};\quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

2) Nếu $n \geq 2$, có thể xảy ra là tích của hai ma trận thuộc $\mathbf{M}_n(K)$ bằng không mà không có ma trận nào trong hai ma trận đó bằng không, như trong ví dụ sau (với $n = 2$):

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

3) Người ta thường đồng nhất một phần tử x thuộc K và ma trận (x) thuộc $\mathbf{M}_1(K)$.

- Cho $A \in \mathbf{M}_{n,1}(K)$, ta có $A \cdot (x) = xA$, nhưng $(x)A$ không xác định (khi $n \geq 2$).
- Cho $B \in \mathbf{M}_{1,n}(K)$, ta có $(x)B = xB$, nhưng $B(x)$ không xác định (khi $n \geq 2$).

♦ **Định nghĩa 2** Một ma trận vuông A thuộc $\mathbf{M}_n(K)$ được gọi là **lũy linh** khi và chỉ khi tồn tại $k \in \mathbb{N}^*$ sao cho $A^k = 0$.

VÍ DỤ:

1) $A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ thuộc $\mathbf{M}_3(\mathbb{R})$ là lũy linh, vì $A^2 = 0$.

2) $A = \begin{pmatrix} -9 & 7 & 3 \\ -13 & 10 & 4 \\ 4 & -3 & -1 \end{pmatrix}$ thuộc $\mathbf{M}_3(\mathbb{R})$ là lũy linh, vì $A^3 = 0$.

♦ **Mệnh đề - Định nghĩa 5** Giả sử $A \in \mathbf{M}_n(K)$ là lũy linh.
Tập hợp $\{k \in \mathbb{N}^*;\ A^k = 0\}$ có phần tử nhỏ nhất $\nu(A)$, được gọi là **chỉ số lũy linh** của A, và ta có: $\forall k \in \mathbb{N}^*,\ (k \geq \nu(A) \Rightarrow A^k = 0)$.

Chứng minh:

- $\{k \in \mathbb{N}^*;\ A^k = 0\}$ là một bộ phận khác rỗng của $\mathbb{N}^*$, nên có phần tử nhỏ nhất $\nu(A)$.
- Với mọi k sao cho $k \geq \nu(A)$: $A^k = A^{k-\nu(A)}A^{\nu(A)} = 0$.

♦ **Định nghĩa 3** Giả sử $A \in \mathbf{M}_{n,p}(K)$.

1) **Hạt nhân** của A là kgvc của $\mathbf{M}_{p,1}(K)$, ký hiệu là $\mathrm{Ker}(A)$, được xác định bởi :
$$\mathrm{Ker}(A) = \{X \in \mathbf{M}_{p,1}(K);\ AX = 0\}.$$

2) **Ảnh** của A là kgvc của $\mathbf{M}_{n,1}(K)$, ký hiệu là $\mathrm{Im}(A)$, được xác định bởi :
$$\mathrm{Im}(A) = \{Y \in \mathbf{M}_{n,1}(K);\ \exists X \in \mathbf{M}_{p,1}(K),\ Y = AX\} = \{AX;\ X \in \mathbf{M}_{p,1}(K)\}.$$

Giả sử $A \in \mathbf{M}_{n,p}(K)$. Đặt $f : \mathbf{M}_{p,1}(K) \to \mathbf{M}_{n,1}(K)$, thì f là ánh xạ tuyến tính và:
$$X \mapsto AX$$
$\mathrm{Ker}(f) = \mathrm{Ker}(A)$ và $\mathrm{Im}(f) = \mathrm{Im}(A)$.
Các ký hiệu $\mathrm{Ker}(A)$, $\mathrm{Im}(A)$ khiến cho ta có thể coi A như là một ánh xạ tuyến tính. ■

Trong Tập 6 ta sẽ thấy các khái niệm *phân tích thành khối* và *đa thức ma trận*.

Bài tập

◊ **8.1.1** Giả sử $n, p, q \in \mathbb{N}^*$, $i \in \{1, \ldots, n\}$; $j, k \in \{1, \ldots, p\}$; $l \in \{1, \ldots, q\}$, E_{ij}, E_{kl} là các ma trận sơ cấp của $\mathbf{M}_{n,p}(K)$ và $\mathbf{M}_{p,q}(K)$. Tính $E_{ij}E_{kl}$.

◊ **8.1.2** Giả sử $A \in \mathbf{M}_n(K)$ thỏa mãn : $\forall X \in \mathbf{M}_n(K)$, $(XA)^2 = 0$. Chứng minh : $A = 0$.

◊ **8.1.3** Cho $A, B \in \mathbf{M}_n(K)$ sao cho tồn tại $(\alpha, \beta) \in (K - \{0\})^2$ thỏa mãn $AB + \alpha A + \beta B = 0$. Chứng minh : $AB = BA$.

◊ **8.1.4** Giải phương trình $X^2 - 2X = \begin{pmatrix} -1 & 0 \\ 0 & 3 \end{pmatrix}$ với ẩn $X \in \mathbf{M}_2(\mathbb{R})$.

◊ **8.1.5** Giải hệ phương trình $\begin{cases} XYX = I_2 \\ YXY = I_2 \end{cases}$ với ẩn $(X, Y) \in (\mathbf{M}_2(\mathbb{R}))^2$.

◊ **8.1.6** Giả sử $U = \begin{pmatrix} 1 & -1 & 1 \\ 1 & 1 & 1 \\ 1 & -1 & 1 \end{pmatrix} \in \mathbf{M}_n(\mathbb{C})$, $E = \{aU ; a \in \mathbb{C}\}$. Chứng minh rằng E là một thể đối với các luật thông thường ; E có phải là một thể con của vành $\mathbf{M}_n(\mathbb{C})$ không?

◊ **8.1.7** Cho $E = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} ; a \in K \right\}$

a) Chứng minh rằng E là một giả vành con của vành $\mathbf{M}_2(K)$.

b) E có phải là một vành con của vành $\mathbf{M}_2(K)$ không?

◊ **8.1.8** Xét $E = \left\{ \begin{pmatrix} a & b & b & c \\ b & a & c & b \\ b & c & a & b \\ c & b & b & a \end{pmatrix} ; (a, b, c) \in \mathbb{C}^3 \right\}$

a) Chứng minh rằng E là một đại số con kết hợp và có đơn vị của $\mathbf{M}_4(\mathbb{C})$, và $\dim(E) = 3$.

b) Giải phương trình $X^2 = I_4$, với ẩn $X \in E$.

◊ **8.1.9** Cho $a, b \in \mathbb{C}$, $M_{a,b} = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \in \mathbf{M}_n(\mathbb{C})$, $k \in \mathbb{N}^*$. Tính $M_{a,b}^k$.

◊ **8.1.10** Giả sử $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathbf{M}_n(K)$, $k \in \mathbb{N}^*$. Tính A^k.

◊ **8.1.11** Tìm tất cả các ma trận $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ thuộc $\mathbf{M}_2(\mathbb{R})$ sao cho:

$$\forall k \in \mathbb{N}^*, \quad A^k = \begin{pmatrix} a^k & b^k \\ c^k & d^k \end{pmatrix}.$$

8.1.5 Nhóm $\mathbf{GL}_n(K)$

Cho $n \in \mathbb{N}^*$.

♦ **Định nghĩa** Một ma trận A thuộc $\mathbf{M}_n(K)$ được gọi là **khả nghịch** khi và chỉ khi tồn tại $A' \in \mathbf{M}_n(K)$ sao cho $AA' = A'A = \mathbf{I}_n$.

Nếu A khả nghịch thì A' là duy nhất và được gọi là **nghịch đảo** của A và ký hiệu là A^{-1}.

Ta ký hiệu tập hợp các ma trận khả nghịch thuộc $\mathbf{M}_n(K)$ là $\mathbf{GL}_n(K)$.

♦ **Mệnh đề - Định nghĩa**

1) Phép nhân là luật hợp thành trong trong $\mathbf{GL}_n(K)$, và $\mathbf{GL}_n(K)$ là một nhóm, gọi là **nhóm tuyến tính.**

2) Với mọi K- kgv n chiều E và mọi cơ sở $\mathcal{B}$ của E, ánh xạ $f \longrightarrow \mathrm{Mat}_{\mathcal{B}}(f)$ là một đẳng cấu từ nhóm $(\mathcal{GL}(E), \circ)$ lên nhóm $(\mathbf{GL}_n(K), \cdot)$.

Chứng minh:

1) • Với mọi (A, B) thuộc $(\mathbf{GL}_n(K))^2$, $(AB)(B^{-1}A^{-1}) = (B^{-1}A^{-1})AB = \mathbf{I}_n$, do đó $AB \in \mathbf{GL}_n(K)$.

• $\mathbf{I}_n \in \mathbf{GL}_n(K)$.

• Với mọi A thuộc $\mathbf{GL}_n(K)$, $A^{-1}A = A\,A^{-1} = \mathbf{I}_n$, do vậy $A^{-1} \in \mathbf{GL}_n(K)$.

2) • Với mọi f thuộc $\mathcal{GL}(E)$, vì

$$(\mathrm{Mat}_{\mathcal{B}}(f))\,(\mathrm{Mat}_{\mathcal{B}}(f^{-1})) = (\mathrm{Mat}_{\mathcal{B}}(f^{-1}))\,(\mathrm{Mat}_{\mathcal{B}}(f)) = \mathrm{Mat}_{\mathcal{B}}(\mathrm{Id}_E) = \mathbf{I}_n,$$

nên ta có: $\mathrm{Mat}_{\mathcal{B}}(f) \in \mathbf{GL}_n(K)$.

• Ngược lại, với mọi A thuộc $\mathbf{GL}_n(K)$, tồn tại duy nhất $(f, g) \in (\mathcal{L}(E))^2$ sao cho $\mathrm{Mat}_{\mathcal{B}}(f) = A$ và $\mathrm{Mat}_{\mathcal{B}}(g) = A^{-1}$, và ta có:

$$\mathrm{Mat}_{\mathcal{B}}(g \circ f) = (\mathrm{Mat}_{\mathcal{B}}(g))\,(\mathrm{Mat}_{\mathcal{B}}(f)) = A^{-1}A = \mathbf{I}_n$$

$$\mathrm{Mat}_{\mathcal{B}}(f \circ g) = (\mathrm{Mat}_{\mathcal{B}}(f))\,(\mathrm{Mat}_{\mathcal{B}}(g)) = A\,A^{-1} = \mathbf{I}_n;$$

Do đó $g \circ f = f \circ g = \mathrm{Id}_E$, nên $f \in \mathcal{GL}(E)$.

• Cuối cùng: $\forall (f, g) \in (\mathcal{GL}(E))^2$, $\mathrm{Mat}_{\mathcal{B}}(g \circ f) = (\mathrm{Mat}_{\mathcal{B}}(g))\,(\mathrm{Mat}_{\mathcal{B}}(f))$. ■

NHẬN XÉT:

Với $n \geq 2$, nhóm $\mathbf{GL}_n(K)$ không giao hoán, như trong ví dụ sau (với $n = 2$) :

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

Từ Định lý 2 của 7.3.1, ta suy ra Định lý sau.

♦ **Định lý** Giả sử $A \in \mathbf{M}_n(K)$, f là một tự đồng cấu biểu diễn bởi A trong một cơ sở. Các tính chất sau tương đương với nhau từng đôi một:

1) f là song ánh

2) A khả nghịch trái

3) A khả nghịch phải

4) A khả nghịch

5) A chính quy trái

6) A chính quy phải

7) A chính quy.

Ta nhắc lại rằng (xem 2.1, Định nghĩa 5), A được gọi là :

- **chính quy trái** khi và chỉ khi: $\forall (B, C) \in (\mathbf{M}_n(K))^2, (AB = AC \Rightarrow B = C)$
- **chính quy phải** khi và chỉ khi: $\forall (B, C) \in (\mathbf{M}_n(K))^2, (BA = CA \Rightarrow B = C)$
- **chính quy** khi và chỉ khi A chính quy trái và chính quy phải.

NHẬN XÉT:

Một ma trận A thuộc $\mathbf{M}_n(K)$ là khả nghịch khi và chỉ khi:

$\forall X \in \mathbf{M}_{n,1}(K), (AX = 0 \Rightarrow X = 0)$ (xem chẳng hạn C8.1.1).

Dưới đây ta sẽ thấy các đặc trưng khác của tính khả nghịch của một ma trận vuông, có liên quan tới hạng (8.1.6, Mệnh đề 3), định thức (9.4, Mệnh đề 2. 4)), các trị riêng (Tập 6, 2.1).

Đôi khi ma trận vuông được gọi là **suy biến** khi và chỉ khi nó không chính quy. ■

Thực hành tính A^{-1}

Đặt $AX = Y$, trong đó $X, Y \in \mathbf{M}_{n,1}(K)$, ta biểu diễn X theo Y bằng cách giải một hệ phương trình tuyến tính (vì nếu A khả nghịch: $AX = Y \Leftrightarrow X = A^{-1}Y$).

VÍ DỤ: Chứng tỏ $A = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \in \mathbf{M}_4(\mathbb{R})$ là khả nghịch và tính A^{-1}.

Đặt $X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$ và $Y = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix}$, ta có : $AX = Y \Leftrightarrow \begin{cases} x_2 + x_3 + x_4 = y_1 \\ x_1 + x_3 + x_4 = y_2 \\ x_1 + x_2 + x_4 = y_3 \\ x_1 + x_2 + x_3 = y_4 \end{cases}$.

Ta có thể thêm vào hệ phương trình tuyến tính này phương trình nhận được bằng cách cộng bốn phương trình lại:

$$3(x_1 + x_2 + x_3 + x_4) = y_1 + y_2 + y_3 + y_4 .$$

và do vậy: $AX = Y \Leftrightarrow \begin{cases} 3x_1 = (y_1 + y_2 + y_3 + y_4) - 3y_1 \\ 3x_2 = (y_1 + y_2 + y_3 + y_4) - 3y_2 \\ 3x_3 = (y_1 + y_2 + y_3 + y_4) - 3y_3 \\ 3x_4 = (y_1 + y_2 + y_3 + y_4) - 3y_4 \end{cases}$

Điều đó chứng tỏ A khả nghịch và : $A^{-1} = \frac{1}{3}\begin{pmatrix} -2 & 1 & 1 & 1 \\ 1 & -2 & 1 & 1 \\ 1 & 1 & -2 & 1 \\ 1 & 1 & 1 & -2 \end{pmatrix}$.

Đối với các ma trận vuông cấp lớn, hoặc với các hạng tử là số, ta sẽ sử dụng một phần mềm tính nghịch đảo các ma trận khả nghịch.

Bài tập

◊ **8.1.12** Chứng tỏ rằng $E = \left\{\begin{pmatrix} x+y & 3y \\ -y & x-y \end{pmatrix} : (x, y) \in \mathbf{R}^2\right\}$ là một thể con của vành $\mathbf{M}_2(\mathbb{R})$, đẳng cấu với $\mathbb{C}$.

◊ **8.1.13** Giả sử $\alpha \in \mathbb{R}$, $E_\alpha = \left\{\begin{pmatrix} x & \alpha y \\ y & x \end{pmatrix} ; (x, y) \in \mathbf{R}^2\right\}$.

a) Chứng tỏ rằng E_α là một đại số con giao hoán và có đơn vị, của $\mathbf{M}_2(\mathbb{R})$.

b) Chứng minh rằng:

- Nếu $\alpha < 0$ thì E_α là một thể đẳng cấu với $\mathbb{C}$
- Nếu $\alpha \geq 0$ thì E_α là một vành và không phải là vành nguyên.

◊ **8.1.14** Trong các ví dụ sau, chứng tỏ rằng ma trận A khả nghịch (trong $\mathbf{M}_n(\mathbb{R})$, $n \geq 2$) và tính nghịch đảo của nó :

a) $A = \begin{pmatrix} 1 & 1 & 0 \\ & \ddots & 1 \\ 0 & & 1 \end{pmatrix}$ b) $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ c) $A = \begin{pmatrix} 1 & 2 & \cdots & n \\ & \ddots & & \vdots \\ & & \ddots & 2 \\ 0 & & & 1 \end{pmatrix}$.

◊ **8.1.15** Giả sử $t \in K$, $A = a(a_{ij})_{ij}$, $B = (b_{ij})_{ij} \in \mathbf{M}_n(K)$ xác định bởi:

$$a_{ij} = \begin{cases} t^{j-i} C_j^i & \text{nếu } i \leq j \\ 0 & \text{nếu } i > j \end{cases}, \quad b_{ij} = \begin{cases} (-1)^{i+j} t^{j-i} C_j^i & \text{nếu } i \leq j \\ 0 & \text{nếu } i > j \end{cases}$$

Chứng tỏ rằng A và B là nghịch đảo của nhau.

◊ **8.1.16** Giả sử $A, B \in \mathbf{M}_n(K)$ sao cho B và $B - AB^{-1}A$ khả nghịch. Giải hệ phương trình $\begin{cases} AX + BY = 0 \\ BX - AY = \mathbf{I}_n \end{cases}$ với ẩn $(X, Y) \in (\mathbf{M}_n(K))^2$.

◊ **8.1.17** Giải trong $(\mathbf{M}_2(\mathbb{R}))^3$: $XY = \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}$, $YZ = \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix}$, $ZX = \begin{pmatrix} 2 & 0 \\ 2 & 0 \end{pmatrix}$.

◊ **8.1.18** Giả sử $S \in \mathbf{M}_n(K)$, $E = \{M \in \mathbf{M}_n(K) ; MS = 0\}$, $F = \{\mathbf{I}_n + M ; M \in E\}$.

a) Chứng tỏ rằng E là một kgvc của $\mathbf{M}_n(K)$.

b) α) Chứng tỏ rằng F ổn định đối với phép nhân.

β) Chứng minh : $\forall A \in F \cap \mathbf{GL}_n(K)$, $A^{-1} \in F$.

◊ **8.1.19** a) Chứng tỏ rằng : $\forall (i, j) \in \{1, ..., n\}^2$, $(i \neq j \Rightarrow \mathbf{I}_n + \mathbf{E}_{ij} \in \mathbf{GL}_n(K))$.

b) Từ đó suy ra rằng $\{A \in \mathbf{M}_n(K) ; \forall X \in \mathbf{GL}_n(K), AX = XA\}$, gọi là **hoàn tập** của $\mathbf{GL}_n(K)$ trong $\mathbf{M}_n(K)$, bằng $K\mathbf{I}_n$.

8.1.6 Hạng của một ma trận

◆ **Định nghĩa** Giả sử $A \in \mathbf{M}_{n,p}(K)$. Ta gọi hạng của họ các cột của A trong $\mathbf{M}_{n,1}(K)$ là **hạng** của A, ký hiệu là rank(A).

Như vậy, nếu ký hiệu $A=\begin{pmatrix} a_{11} & \cdots & a_{1p} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{np} \end{pmatrix}$ và $C_1 = \begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix}, ..., C_p = \begin{pmatrix} a_{1p} \\ \vdots \\ a_{np} \end{pmatrix}$ là các cột của A, thì : rank(A) = rank(C_1, ..., C_p).

◆ **Mệnh đề 1** Giả sử E, F là hai K-kgv, $\mathcal{B}$, $\mathcal{C}$ tương ứng là các cơ sở của E, F, $f \in \mathcal{L}(E, F)$, $A = \text{Mat}_{\mathcal{B},\mathcal{C}}(f)$. Ta có rank($f$) = rank($A$).

Chứng minh :

Đặt $\mathcal{B} = (e_1, ..., e_p)$, $\mathcal{C} = (f_1, ..., f_n)$, $A = (a_{ij})_{ij}$, $C_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix}$ với $1 \le j \le p$.

Ta có : $\forall j \in \{1, ..., p\}$, $f(e_j) = \sum_{i=1}^{n} a_{ij} f_i$.

Vì θ: $\mathbf{M}_{n,1}(K) \to F$ là một đẳng cấu K-kgv nên ta có:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \sum_{i=1}^{n} x_i f_i$$

rank (A) = dim(Vect (C_1, ..., C_p)) = dim (Vect(θ(C_1)), ..., θ(C_p)))

= dim (Vect ($f(e_1)$, ..., $f(e_p)$)) = rank(f). ■

Như vậy:

- Hạng của một ma trận A là hạng của ánh xạ tuyến tính bất kỳ được biểu diễn bởi A.
- Hạng của một ánh xạ tuyến tính f là hạng của ma trận bất kỳ biểu diễn f.
- Hạng của một họ hữu hạn vectơ $\mathcal{F}$ thuộc một K- kgv E là hạng của ma trận của $\mathcal{F}$ trong bất kỳ cơ sở nào của E. ■

◆ **Mệnh đề 2**

$$\forall A \in \mathbf{M}_{n,p}(K), \text{ rank}(A) \le \text{Min}(n, p).$$

Chứng minh: Với các ký hiệu trên :

- Rank (A) = rank (C_1, C_2, ..., C_p) $\le p$.
- Rank (A) = dim(Vect (C_1, ..., C_p)) $\le$ dim ($\mathbf{M}_{n,1}(K)$) = n. ■

Mệnh đề 3

$$\forall A \in \mathbf{M}_n(K),\ (\text{rank}\ (A) = n \Leftrightarrow A \in \mathbf{GL}_n(K)).$$

Chứng minh:

Giả sử f là tự đồng cấu của $\mathbf{M}_{n,1}(K)$ biểu diễn bởi A trong cơ sở chính tắc của $\mathbf{M}_{n,1}(K)$. Vì $(C_1, ..., C_n)$ là một cơ sở của $\mathbf{M}_{n,1}(K)$ khi và chỉ khi f là song ánh, nên ta kết luận : Rank $(A) = n \Leftrightarrow A \in \mathbf{GL}_n(K)$. ■

Mệnh đề 4

$$\forall A \in M_{n,p}(K)\ ,\ \begin{cases} \forall P \in \mathbf{GL}_p(K), & \text{rank}(AP) = \text{rank}(A) \\ \forall Q \in \mathbf{GL}_n(K), & \text{rank}(QA) = \text{rank}(A) \end{cases}.$$

Chứng minh:

1) Hiển nhiên $\text{Im}(AP) \subset \text{Im}(A)$, nên rank $(AP) \leq$ rank (A).

Thay (A, P) bởi (AP, P^{-1}), ta suy ra : $\text{rank}(A) = \text{rank}((AP).P^{-1}) \leq$ rank (AP).

2) Hiển nhiên Ker (A) $\subset$ Ker (QA) , nên theo định lý về hạng:

$$\text{rank (A)} = p - \dim (\text{Ker}(A)) \geq p - \dim (\text{Ker}(QA)) = \text{rank}(QA).$$

Thay (A, Q) bởi $(QA\ ,\ Q^{-1})$, ta suy ra:

$$\text{rank}(QA) \geq \text{rank}(Q^{-1}(QA)) = \text{rank}(A)$$ ■

Nói cách khác, khi nhân một ma trận với một ma trận khả nghịch, thì hạng của ma trận không đổi.

NHẬN XÉT :

Ta chứng minh một cách tương tự :

$$\forall (A, B, C) \in \mathbf{M}_{n,p}(K) \times \mathbf{M}_{p,q}(K) \times \mathbf{M}_{q,r}(K),\ \ \text{rank}(ABC) \leq \text{rank}(B).$$

Bài tập

◊ **8.1.20** Với $(a, b) \in \mathbb{C}^2$, hãy xác định hạng của $M_{a,b} = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \in M_n(\mathbb{C})$.

◊ **8.1.21** Giả sử $A \in \mathbf{M}_{n,p}(K)$, $C_1, \ldots, C_p$ là các cột của A. Chứng minh :

a) $\text{rank}(A) = n \Leftrightarrow ((C_1,\ldots,C_p)$ sinh ra $M_{n,1}(K))$

b) $\text{rank}(A) = p \Leftrightarrow ((C_1,\ldots,C_p)$ độc lập tuyến tính).

◊ **8.1.22** Giả sử $A \in \mathbf{M}_{n,p}(K)$, E, F là hai K-kgv tương ứng p,n chiều, $\mathcal{B}$ (tương ứng: $\mathcal{C}$) là một cơ sở của E (tương ứng: F), $f \in \mathcal{L}(E,F)$ sao cho $\text{Mat}_{\mathcal{B},\mathcal{C}}(f) = A$. Chứng minh :

a) $\text{rank}(A) = n \Leftrightarrow f$ là toàn ánh

b) $\text{rank}(A) = p \Leftrightarrow f$ là đơn ánh.

◊ **8.1.23** Giả sử $A \in \mathbf{M}_{n,p}(K)$, $s \in \mathbb{N}$. Chứng minh :

$$\text{rank}(A) \le s \Leftrightarrow \left(\exists q \in \mathbb{N}^*, \exists B \in \mathbf{M}_{p,q}(K), \begin{cases} AB = 0 \\ \text{rank}(B) \ge p - s \end{cases} \right).$$

◊ **8.1.24** Giả sử $A \in \mathbf{M}_{n,p}(K)$, $B \in \mathbf{M}_{p,q}(K)$, $C \in \mathbf{M}_{q,r}(K)$ sao cho $\text{rank}(B) = \text{rank}(AB)$. Chứng minh : $\text{rank}(BC) = \text{rank}(ABC)$.

◊ **8.1.25*** Giả sử $A \in \mathbf{M}_{3,4}(\mathbb{R})$, $B \in \mathbf{M}_{4,2}(\mathbb{R})$, $C \in \mathbf{M}_{2,3}(\mathbb{R})$ sao cho

$$ABC = \begin{pmatrix} 0 & -1 & -1 \\ -1 & 0 & -1 \\ 1 & 1 & 2 \end{pmatrix}.$$

Tính CAB và chứng minh rằng $(BCA)^2 = BCA$.

◊ **8.1.26*** a) Giả sử $A, B \in \mathbf{M}_n(K)$ sao cho : A là lũy linh, $AB = BA$, $B \neq 0$.

Chứng minh: $\text{rank}(AB) \le \text{rank}(B)-1$.

b) Giả sử $p \in \mathbb{N}^*$, $A_1,\ldots,A_p \in \mathbf{M}_n(K)$ là lũy linh và giao hoán được với nhau từng đôi một.

Chứng tỏ: $\text{rank}\left(\prod_{i=1}^{p} A_i\right) \le (n-p)^+ = \begin{cases} n-p & \text{nếu} \quad n-p \ge 0 \\ 0 & \text{nếu} \quad n-p < 0 \end{cases}$

c) Từ đó suy ra rằng, nếu $A_1, \ldots, A_n \in \mathbf{M}_n(K)$ là lũy linh và giao hoán với nhau từng đôi một, thì $\prod_{i=1}^{n} A_i = 0$.

8.1.7 Các phép biến đổi sơ cấp

Giả sử $(n, p) \in (\mathbb{N} - \{0,1\})^2$, $A = (a_{ij})_{ij} \in \mathbf{M}_{np}(K)$.

Các phép biến đổi sơ cấp trên cột của A là các phép biến đổi sau đây (trong đó C_j ký hiệu cột thứ j của ma trận A, $1 \le j \le p$):

- Hoán vị hai cột của A
- Thay một cột C_j của A bởi αC_j, trong đó $\alpha \in K - \{0\}$
- Thay một cột C_j của A bởi $C_j + \alpha C_k$, trong đó $\alpha \in K$ và $k \in \{1,..., p\} - \{j\}$.

Ta định nghĩa một cách tương tự **các phép biến đổi sơ cấp trên dòng** của A (đó là các phép biến đổi sơ cấp trên cột của chuyển vị của A, xem 8.1.8, Định nghĩa).

Bây giờ chúng ta xét các phép biến đổi sơ cấp trên cột hoặc trên dòng của A như là phép nhân với những ma trận vuông khả nghịch nào đó. Ta nhắc lại (xem bài tập 8.1.1):

$$\forall (i, j, k, l) \in \{1, ..., p\}^4, \quad E_{ij}E_{kl} = \delta_{jk}E_{il}.$$

1) Với $(j, k) \in \{1, ..., p\}^2$ sao cho $j < k$, đặt

$$P_{jk} = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 0 & & 1 & & \\ & & & 1 & & & \\ & & \vdots & & \ddots & & \\ & & 1 & & 0 & & \\ & & & & & 1 & \\ 0 & & & & & & \ddots \\ & & & & & & & 1 \end{pmatrix} = I_p + (E_{jk} + E_{kj} - E_{jj} - E_{kk}) \in \mathbf{M}_p(K).$$

cột thứ j cột thứ k

Ta có: $AP_{jk} = \begin{pmatrix} a_{11} \cdots a_{1\,j-1} & a_{1k} & a_{1\,j+1} \cdots a_{1\,k-1} & a_{1j} & a_{1\,k+1} \cdots & a_{1p} \\ \vdots \quad\quad \vdots & \vdots & \vdots \quad\quad \vdots & \vdots & \vdots \quad\quad \vdots & \vdots \\ a_{n1} \cdots a_{n\,j-1} & a_{nk} & a_{n\,j+1} \cdots a_{n\,k-1} & a_{nj} & a_{n\,k+1} \cdots & a_{np} \end{pmatrix}$

Hơn nữa, P_{jk} khả nghịch, vì $P_{jk}^2 = I_p$.

Như vậy, việc hoán vị các cột thứ j và thứ k của A quy về việc nhân phải (người ta cũng nói: **nhân sau**) với ma trận khả nghịch P_{jk}.

2) Với $j \in \{1,..., p\}$ và $\alpha \in K - \{0\}$, đặt

$$D_{j,\alpha} = \begin{pmatrix} 1 & & & & \\ & \ddots & & 0 & \\ & & 1 & & \\ & & & \alpha & \\ & 0 & & & 1 \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix} = I_p + (\alpha - 1) E_{jj} \in M_n(K),$$

cột thứ j

ta có : $AD_{j,\alpha} = \begin{pmatrix} a_{11} \cdots \alpha a_{1j} \cdots & a_{1p} \\ \vdots & \vdots \\ a_{n1} & \alpha a_{nj} \cdots & a_{np} \end{pmatrix}$

Hơn nữa $D_{j,\alpha}$ khả ghịch, vì $D_{j,\alpha} D_{j,\alpha^{-1}} = I_p$.

Như vậy, việc thay thế cột thứ j của A bởi tích cột đó với α ($\alpha \in K$ và $\alpha \neq 0$) quy về việc nhân phải (nhân sau) với ma trận khả nghịch $D_{j,\alpha}$.

3) Với $(j, k) \in \{1, ..., p\}^2$ sao cho $j \neq k$ và $\alpha \in K$, đặt

$$T_{jk,\alpha} = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & 0 & \\ & & 1 & \cdots & 0 & \\ & & \vdots & \ddots & \vdots & \\ & & \alpha & \cdots & 1 & \\ & 0 & & & & \ddots \\ & & & & & & 1 \end{pmatrix} = I_n + \alpha E_{jk} \in M_p(K)$$

cột thứ k cột thứ j

ta có : $A\,T_{jk,\alpha} = \begin{pmatrix} a_{11} \cdots a_{1k} + \alpha a_{1j} \cdots a_{1p} \\ \vdots \qquad\quad \vdots \\ a_{n1} \quad a_{nk} + \alpha a_{nj} \cdots a_{np} \end{pmatrix}$.

cột thứ k

Hơn nữa, $T_{jk,\alpha}$ khả nghịch , vì : $T_{jk,\alpha} \cdot T_{jk,-\alpha} = (I_n + \alpha E_{jk})(I_n - \alpha E_{jk}) = I_n$.

Như vậy, việc thay C_k bởi $C_k + \alpha C_j$ ($k \neq j$) quy về việc nhân sau với ma trận khả nghịch $T_{jk,\alpha}$. ■

Tương tự, các phép biến đổi sơ cấp trên dòng ($L_j \leftrightarrow L_k$, $L_j \leftrightarrow \alpha L_j$ $L_k \leftrightarrow L_k + \alpha L_j$) quy về việc nhân trái (**nhân trước**) với các ma trận khả nghịch P_{jk}, $D_{j,\alpha}$, $T_{kj,\alpha}$. ■

Theo 8.1.6 , Mệnh đề 4, ta suy ra kết quả sau.

♦ **Mệnh đề**

Các phép biến đổi sơ cấp trên dòng hoặc trên cột không làm thay đổi hạng.

Nói cách khác, nếu $B \in \mathbf{M}_{n,p}(K)$ suy ra từ $A \in \mathbf{M}_{n,p}(K)$ bằng những phép biến đổi sơ cấp, thì rank (B) = rank (A).

Phương pháp Gauss

Cho $A \in \mathbf{M}_{n,p}(K)$.

Bằng những phép biến đổi sơ cấp, ta sẽ xây dựng một ma trận T có cùng hạng với A, và sao cho hạng của T là hiển nhiên.

Nếu dòng thứ nhất của A bằng không, thì ma trận thuộc $\mathbf{M}_{n-1,p}(K)$ thu được bằng cách bỏ đi dòng thứ nhất của ma trận A, có cùng hạng với A. Vì vậy ta có thể giả thiết rằng dòng thứ nhất của A là khác không.

Bằng cách hoán vị cột, ta quy về một ma trận có cùng hạng với A, và có hạng tử thứ (1,1) khác không. Nhân cột thứ nhất với nghịch đảo của hạng tử này, ta quy về một ma trận $A_1 = (\alpha_{ij})_{ij}$ với $\alpha_{11} = 1$.

Với mỗi j thuộc $\{2,..., p\}$, việc thay cột C_j bởi cột $C_j - \alpha_{1j}C_1$ sẽ làm xuất hiện ma trận A_2, có cùng hạng với A, và có hàng thứ nhất là $(1, 0, ..., 0)$:

$$A_1 = \begin{pmatrix} 1 & \alpha_{12} & \cdots & \alpha_{1p} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2p} \\ \vdots & \vdots & & \vdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{np} \\ C_1 & C_2 & \cdots & C_p \end{pmatrix} \text{ ^^^> } A_2 = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ \alpha_{21} & \alpha_{22} - \alpha_{12}\alpha_{21} & \cdots & \alpha\alpha_{2p} - \alpha_{1p}\alpha_{21} \\ \vdots & \vdots & & \vdots \\ \alpha_{n1} & \alpha_{n2} - \alpha_{12}\alpha_{n1} & \cdots & \alpha_{np} - \alpha_{1p}\alpha_{n1} \\ C_1 & C_2 - \alpha_{12}C_1 & \cdots & C_p - \alpha_{1p}C_1 \end{pmatrix}$$

Lặp lại thủ tục cho ma trận với n - 1 dòng và p - 1 cột nằm ở phần dưới bên phải trong A_2, sau một số hữu hạn phép biến đổi sơ cấp trên cột và bỏ đi những dòng hoặc cột bằng không (nếu có), ta đi đến một ma trận T (có cùng hạng với A) có dạng

$$T = \begin{pmatrix} 1 & & \\ & \ddots & 0 \\ & & 1 \\ & \cdots & \end{pmatrix}$$

Vì các cột của T tạo thành một họ độc lập tuyến tính, nên hiển nhiên hạng của T bằng số cột của T (số đó không nhất thiết bằng số cột của A).

VÍ DỤ :

Tính hạng của ma trận $A = \begin{pmatrix} 2 & 3 & 5 \\ 1 & 4 & 0 \\ -1 & -3 & -1 \\ 3 & 6 & 6 \end{pmatrix} \in \mathbf{M}_{4,3}(\mathbb{R})$.

$$A \rightsquigarrow \begin{pmatrix} 1 & 3 & 5 \\ \frac{1}{2} & 4 & 0 \\ -\frac{1}{2} & -3 & -1 \\ \frac{3}{2} & 6 & 6 \end{pmatrix} \quad \text{qua } C_1 \leftarrow \frac{1}{2} C_1$$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ \frac{1}{2} & \frac{5}{2} & -\frac{5}{2} \\ -\frac{1}{2} & -\frac{3}{2} & \frac{3}{2} \\ \frac{3}{2} & \frac{3}{2} & -\frac{3}{2} \end{pmatrix} \quad \text{qua } C_2 \leftarrow C_2 - 3C_1 \text{ và } C_3 \leftarrow C_3 - 5C_1$$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 \\ \frac{1}{2} & 1 \\ -\frac{1}{2} & -\frac{3}{5} \\ \frac{3}{2} & \frac{3}{5} \end{pmatrix} \quad \text{qua } C_2 \leftarrow \frac{2}{5} C_2 ,$$

Vì cột cuối cùng, đồng phương với C_2, có thể loại bỏ.

Như vậy : rank(A) = 2.

NHẬN XÉT:

1) Phương pháp Gauss có thể áp dụng cho các dòng (thay cho các cột). Ta cũng có thể dùng hỗn hợp những phép biến đổi sơ cấp trên dòng và trên cột.

2) Nếu A khả nghịch (do đó vuông), thì các phép biến đổi sơ cấp trên dòng và trên cột cho phép đưa A về $\mathbf{I}_n$, do vậy cho phép tính được A^{-1}.

8.1.8 Chuyển vị

◆ **Định nghĩa** Với mọi ma trận $A=(a_{ij})_{\substack{1\le i\le n\\1\le j\le p}}=\begin{pmatrix}a_{11}\dots a_{1p}\\ \vdots\quad\ \vdots\\ a_{n1}\dots a_{np}\end{pmatrix}$ thuộc $\mathbf{M}_{n,p}(K)$, **chuyển vị** của A là ma trận thuộc $\mathbf{M}_{p,n}(K)$, ký hiệu là ${}^tA$, xác định bởi :

$$ {}^tA=(a_{ij})_{\substack{1\le j\le p\\1\le i\le n}}=\begin{pmatrix}a_{11}\dots a_{n1}\\ \vdots\quad\ \vdots\\ a_{1p}\dots a_{np}\end{pmatrix}. $$

Nói cách khác : ${}^tA$ thu được từ A bằng cách lấy đối xứng qua "đường chéo" (dẫu rằng A là hình chữ nhật).

Chẳng hạn, nếu $A=\begin{pmatrix}a & b & c\\ \alpha & \beta & \gamma\end{pmatrix}$ thì ${}^tA=\begin{pmatrix}a & \alpha\\ b & \beta\\ c & \gamma\end{pmatrix}$.

Ta cũng có thể nói rằng ${}^tA$ thu được từ A bằng cách trao đổi các khái niệm dòng và cột.

Nói riêng, chuyển vị của một ma trận dòng là một ma trận cột và ngược lại :

$${}^t\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}=(x_1\dots x_n),\quad {}^t(x_1\dots x_n)=\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}$$

◆ **Mệnh đề**

1) $\forall A\in\mathbf{M}_{n,p}(K)$, ${}^{tt}A=A$.

2) $\forall\alpha\in K$, $\forall(A,B)\in(\mathbf{M}_{n,p}(K))^2$, ${}^t(\alpha A+B)=\alpha{}^tA+{}^tB$.

3) $\forall A\in\mathbf{M}_{n,p}(K)$, $\forall B\in\mathbf{M}_{p,q}(K)$, ${}^t(AB)={}^tB{}^tA$.

4) $\forall A\in\mathbf{GL}_n(K)$, (${}^tA\in\mathbf{GL}_n(K)$ và $({}^tA)^{-1}={}^t(A^{-1})$).

Chứng minh :

1) Hiển nhiên .

2) Đặt $A=(a_{ij})_{ij}$, $B=(b_{ij})_{ij}$, ta có $\alpha A+B=(\alpha a_{ij}+b_{ij})_{ij}$, vì vậy ${}^t(\alpha A+B)=(\alpha a_{ij}+b_{ij})_{ji}$ và $\alpha{}^tA+{}^tB=\alpha(a_{ij})_{ji}+(b_{ij})_{ji}=(\alpha a_{ij}+b_{ij})_{ji}$, do đó ${}^t(\alpha A+B)=\alpha{}^tA+{}^tB$.

3) Đặt $A=(a_{ij})_{ij}$, $B=(b_{jk})_{jk}$, ta có ${}^tA=(\alpha_{ji})_{ji}$, ${}^tB=(\beta_{kj})_{kj}$, trong đó $\alpha_{ji}=a_{ij}$ và $\beta_{kj}=b_{jk}$, và $AB=(c_{ik})_{ik}$, ${}^tB{}^tA=(\gamma_{ki})_{ki}$ trong đó $c_{ik}=\sum_{j=1}^{p}a_{ij}b_{jk}$ và

$$\gamma_{ki}=\sum_{j=1}^{p}\beta_{kj}\alpha_{ji}=\sum_{j=1}^{p}b_{jk}a_{ij}=c_{ik}\ .$$

Như vậy : ${}^tB{}^tA={}^t(AB)$.

4) Giả sử $A\in\mathbf{GL}_n(K)$.

Vì ${}^tA\,{}^t(A^{-1})={}^t(A^{-1}A)={}^tI_n=I_n$, nên ${}^tA$ khả nghịch và $({}^tA)^{-1}={}^t(A^{-1})$. ■

Theo 4) trên đây, với $A\in\mathbf{GL}_n(K)$, ta có thể viết ${}^tA^{-1}$ thay vì $({}^tA)^{-1}$ hoặc ${}^t(A^{-1})$.

Bài tập

◊ **8.1.27** Giả sử $a \in K - \{0\}$, $A = \begin{pmatrix} 0 & a & & \dots & a^{n-1} \\ \frac{1}{a} & & \ddots & & \vdots \\ \vdots & \ddots & & \ddots & a \\ \frac{1}{a^{n-1}} & \dots & \frac{1}{a} & & 0 \end{pmatrix} \in \mathbf{M}_n(K)$,

nghĩa là $A = UV - I_n$, trong đó $U = \begin{pmatrix} 1 \\ \frac{1}{a} \\ \vdots \\ \frac{1}{a^{n-1}} \end{pmatrix}$, $V = \begin{pmatrix} 1 \\ a \\ \vdots \\ a^{n-1} \end{pmatrix}$.

a) Tính A^k với $k \in \mathbb{N}^*$.

b) Chứng tỏ rằng A khả nghịch và tính A^{-1}.

c) Tính A^k với $k \in \mathbb{Z}$.

8.1.9 Vết của một ma trận vuông

♦ **Định nghĩa** Với mọi ma trận vuông $A = (a_{ij})_{ij} \in \mathbf{M}_n(K)$, ta định nghĩa **vết** của A, ký hiệu là $\mathrm{tr}(A)$, là: $\mathrm{tr}(A) = \sum_{i=1}^{n} a_{ii}$.

Nói cách khác, vết của A là tổng các phần tử chéo của A.

♦ **Mệnh đề**

1) Ánh xạ $\mathrm{tr} : \mathbf{M}_n(K) \to K$, $A \mapsto \mathrm{tr}(A)$ là một dạng tuyến tính.

2) $\forall A \in \mathbf{M}_{n,p}(K)$, $\forall B \in \mathbf{M}_{p,n}(K)$, $\mathrm{tr}(AB) = \mathrm{tr}(BA)$.

Chứng minh:

1) Đặt $A = (a_{ij})_{ij}$, $B = (b_{ij})_{ij}$:

$$\mathrm{tr}(\alpha A + B) = \sum_{i=1}^{n} (\alpha a_{ii} + b_{ii}) = \alpha \sum_{i=1}^{n} a_{ii} + \sum_{i=1}^{n} b_{ii} = \alpha \mathrm{tr}(A) + \mathrm{tr}(B).$$

2) Trước hết nhận xét rằng AB và BA là những ma trận vuông.

Đặt $A = (a_{ij})_{ij}$, $B = (b_{ij})_{ij}$, ta có :

$$\mathrm{tr}(AB) = \sum_{i=1}^{n} \left(\sum_{j=1}^{p} a_{ij} b_{ji} \right) = \sum_{j=1}^{p} \left(\sum_{i=1}^{n} b_{ji} a_{ij} \right) = \mathrm{tr}(BA) .$$

Bài tập

◊ **8.1.28** **Đẳng thức Wagner**

Chứng minh : $\forall A, B, C \in \mathbf{M}_2(K)$, $(AB - BA)^2C - C(AB - BA)^2 = 0$.

◊ **8.1.29** Chứng tỏ rằng không tồn tại $(A, B, C, D) \in (\mathbf{M}_n(\mathbb{R}))^4$ sao cho $\begin{cases} AC + DB = \mathrm{I}_n \\ CA + BD = 0 \end{cases}$

◊ **8.1.30** Giải (S) $\begin{cases} \mathrm{tr}(X)Y + \mathrm{tr}(Y)X = \begin{pmatrix} 4 & 8 \\ 4 & -4 \end{pmatrix} \\ XY = \begin{pmatrix} 1 & 1 \\ 4 & -2 \end{pmatrix} \end{cases}$, với ẩn $(X, Y) \in (\mathbf{M}_2(\mathbb{R}))^2$.

◊ **8.1.31** Cho $H \in \mathbf{M}_n(K)$ sao cho $\mathrm{rank}(H) \leq 1$.

a) Chứng minh rằng tồn tại $U, V \in \mathbf{M}_{n,1}(K)$ sao cho: $H = UV$ và $\mathrm{tr}(H) = {}^tVU$.

b) Từ đó suy ra : $H^2 = \mathrm{tr}(H)H$.

◊ **8.1.32** Chứng tỏ rằng với mọi $A \in \mathbf{M}_3(\mathbb{C})$: $A^2 = 0 \Leftrightarrow \begin{cases} \mathrm{rank}(A) \leq 1 \\ \mathrm{tr}(A) = 0 \end{cases}$

(Có thể sử dụng bài tập 8.1.31).

◊ **8.1.33** Cho $A \in \mathbf{M}_{n,p}(K)$, $B = \mathbf{M}_{q,n}(K)$. Chứng minh:

$$\forall X \in \mathbf{M}_{p,q}(K), \quad \mathrm{tr}(AXB) = 0) \Leftrightarrow BA = 0.$$

◊ **8.1.34** a) Tìm tất cả các ánh xạ tuyến tính $f : \mathbf{M}_n(K) \to \mathbf{M}_n(K)$ sao cho:

$$\forall A, B \in \mathbf{M}_n(K), \quad f(AB) = f(BA).$$

b) Tìm tất cả các ánh xạ tuyến tính $f: \mathbf{M}_n(K) \to \mathbf{M}_n(K)$ sao cho :

$$\forall A, B, C \in \mathbf{M}_n(K), \quad f(ABC) = f(BAC).$$

8.2 Đổi cơ sở

8.2.1 Ma trận chuyển cơ sở

♦ **Định nghĩa** Cho E là một K-kgv n chiều, $\mathcal{B}$, $\mathcal{B}'$ là hai cơ sở của E.

Ma trận chuyển cơ sở từ $\mathcal{B}$ sang $\mathcal{B}'$, ký hiệu là $\text{Pass}(\mathcal{B},\mathcal{B}')$, là ma trận thuộc $\mathbf{M}_n(K)$ có các cột được tạo bởi các thành phần của các vectơ của $\mathcal{B}'$ biểu thị trên cơ sở $\mathcal{B}$, nghĩa là :

$$\text{Pass}(\mathcal{B},\mathcal{B}') = \text{Mat}_{\mathcal{B}}(\mathcal{B}').$$

VÍ DỤ :

Giả sử $\mathcal{B} = (e_1, e_2)$ là cơ sở chính tắc của K^2, nghĩa là $e_1 = (1, 0)$ và $e_2 = (0, 1)$, và $u = (2, 4)$, $v = (3, -1)$. Thế thì $\mathcal{B}' = (u, v)$ là một cơ sở của K^2 và ma trận chuyển cơ sở từ $\mathcal{B}$ sang $\mathcal{B}'$ là $\begin{pmatrix} 2 & 3 \\ 4 & -1 \end{pmatrix}$ vì $u = 2e_1 + 4e_2$, $v = 3e_1 - e_2$.

♦ **Mệnh đề 1**

Với mọi cơ sở $\mathcal{B}$, $\mathcal{B}'$ của E: $\text{Pass}(\mathcal{B}, \mathcal{B}') = \text{Mat}_{\mathcal{B}',\mathcal{B}}(\text{Id}_E)$.

Chứng minh :

Đặt $\mathcal{B}' = \{e'_1, ..., e'_n\}$. Với mỗi j thuộc $\{1, ..., n\}$, cột thứ j của $\text{Mat}_{\mathcal{B}',\mathcal{B}}(\text{Id}_E)$ được tạo bởi các thành phần của $\text{Id}_E(e_j)$, nghĩa là e_j, trong cơ sở $\mathcal{B}$. ■

Ta chú ý rằng, ở đây ta đã biểu diễn ma trận của một tự đồng cấu (phép đồng nhất) theo hai cơ sở khác nhau đối với nguồn và đích, điều này rất ít gặp.

♦ **Mệnh đề 2** Giả sử E là một K-kgv, $\mathcal{B}$, $\mathcal{B}'$, $\mathcal{B}''$ là những cơ sở của E. Ta có:

1) $\text{Pass}(\mathcal{B},\mathcal{B}'') = \text{Pass}(\mathcal{B},\mathcal{B}')\,\text{Pass}(\mathcal{B}',\mathcal{B}'')$

2) $\text{Pass}(\mathcal{B},\mathcal{B}) = \mathrm{I}_n$

3) $\text{Pass}(\mathcal{B},\mathcal{B}')$ khả nghịch và $(\text{Pass}(\mathcal{B},\mathcal{B}'))^{-1} = \text{Pass}(\mathcal{B}',\mathcal{B})$.

Chứng minh:

1) $\text{Pass}(\mathcal{B},\mathcal{B}'') = \text{Mat}_{\mathcal{B}'',\mathcal{B}}(\text{Id}_E) = (\text{Mat}_{\mathcal{B}',\mathcal{B}}(\text{Id}_E))(\text{Mat}_{\mathcal{B}'',\mathcal{B}'}(\text{Id}_E))$
$= \text{Pass}(\mathcal{B},\mathcal{B}')\text{Pass}(\mathcal{B}',\mathcal{B}'')$.

2) $\text{Pass}(\mathcal{B},\mathcal{B}) = \text{Mat}_{\mathcal{B},\mathcal{B}}(\text{Id}_E) = \mathrm{I}_n$

3) $\text{Pass}(\mathcal{B},\mathcal{B}')\text{Pass}(\mathcal{B}',\mathcal{B}) = \text{Pass}(\mathcal{B},\mathcal{B}) = \mathrm{I}_n$.

NHẬN XÉT :

Giả sử E là một K-kgv n chiều, $\mathcal{B}$ là một cơ sở của E. Hiển nhiên ánh xạ $\mathcal{B}' \mapsto \text{Pass}(\mathcal{B},\mathcal{B}')$ là một song ánh từ tập hợp các cơ sở của E lên $\mathbf{GL}_n(K)$. Như vậy:

- Mọi ma trận chuyển cơ sở là khả nghịch
- Mọi ma trận khả nghịch có thể được xem như ma trận chuyển cơ sở (thậm chí ta có thể chọn cơ sở nguồn hoặc cơ sở đích).

8.2.2 Đổi cơ sở đối với một vectơ

◆ **Mệnh đề** Giả sử E là một K-kgv, $\mathcal{B}, \mathcal{B}'$ là hai cơ sở của E, $P = \text{Pass}(\mathcal{B}, \mathcal{B}')$, $x \in E$, $X = \text{Mat}_{\mathcal{B}}(x)$, $X' = \text{Mat}_{\mathcal{B}'}(x)$. Thế thì :

$$\boxed{X = PX'}$$

Chứng minh:

$$X = \text{Mat}_{\mathcal{B}}(x) = (\text{Mat}_{\mathcal{B}',\mathcal{B}}(\text{Id}_E))(\text{Mat}_{\mathcal{B}'}(x)) = PX'.$$

VÍ DỤ :

Trong K^2, giả sử (e_1, e_2) là cơ sở chính tắc, $u_1 = (-2, 1)$, $u_2 = (3, -2)$, $x = (x_1, x_2) \in K^2$. Rõ ràng (u_1, u_2) là một cơ sở của K^2. Ký hiệu X_1, X_2 là các thành phần của x trong cơ sở (u_1, u_2), ta có :

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} -2 & 3 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} = \begin{pmatrix} -2X_1 + 3X_2 \\ X_1 - 2X_2 \end{pmatrix}.$$

NHẬN XÉT:

Vậy trong một phép đổi cơ sở đối với một vectơ, tự nhiên là ta sẽ biểu diễn *các tọa độ cũ* (tọa độ của x trong $\mathcal{B}$) theo các *tọa độ mới* (tọa độ của x trong $\mathcal{B}'$). Nếu muốn biểu diễn toạ mới của x theo tọa độ cũ của x, ta có công thức $X' = P^{-1}X$, nhưng cần phải tính nghịch đảo của P khi sử dụng.

8.2.3 Đổi cơ sở đối với một ánh xạ tuyến tính

1) Công thức đổi cơ sở

◆ Mệnh đề

Giả sử | E, F là hai K-kgv
| $\mathcal{B}, \mathcal{B}'$ là hai cơ sở của E, $P = \text{Pass}(\mathcal{B}, \mathcal{B}')$
| $\mathcal{C}, \mathcal{C}'$ là hai cơ sở của F, $Q = \text{Pass}(\mathcal{C}, \mathcal{C}')$
| $f \in \mathcal{L}(E, F)$, $A = \text{Mat}_{\mathcal{B},\mathcal{C}}(f)$, $A' = \text{Mat}_{\mathcal{B}',\mathcal{C}'}(f)$.

Thế thì

$$\boxed{A' = Q^{-1}AP}$$

Chứng minh:

$$A' = \text{Mat}_{\mathcal{B}',\mathcal{C}'}(f) = \text{Mat}_{\mathcal{B}',\mathcal{C}'}(\text{Id}_F \circ f \circ \text{Id}_E)$$
$$= (\text{Mat}_{\mathcal{C},\mathcal{C}'}(\text{Id}_F))(\text{Mat}_{\mathcal{B},\mathcal{C}}(f))(\text{Mat}_{\mathcal{B}',\mathcal{B}}(\text{Id}_E)) = Q^{-1}AP.$$

2) Ma trận tương đương

♦ **Định nghĩa** Giả sử $A, B \in \mathbf{M}_{n,p}(K)$. Ta nói A **tương đương** với B và ký hiệu A tđ B, khi và chỉ khi:

$$\exists (P,Q) \in \mathbf{GL}_p(K) \times \mathbf{GL}_n(K), \quad B = Q^{-1}AP.$$

Theo Mệnh đề trên, A tđ B khi và chỉ khi A và B biểu diễn (trong những cơ sở) cùng một ánh xạ tuyến tính.

♦ **Mệnh đề 1**

Quan hệ tđ là một quan hệ tương đương trong $\mathbf{M}_{n,p}(K)$.

Chứng minh:

1) *Phản xạ*: $\forall A \in \mathbf{M}_{n,p}(K), \ A = \mathrm{I}_n A \mathrm{I}_p$.

2) *Đối xứng* :

Nếu tồn tại $(P,Q) \in \mathbf{GL}_p(K) \times \mathbf{GL}_n(K)$ sao cho $B = Q^{-1}AP$, thì $A = (Q^{-1})^{-1} BP^{-1}$ và $(P^{-1},Q^{-1}) \in \mathbf{GL}_p(K) \times \mathbf{GL}_n(K)$, do vậy B tđ A.

3) *Bắc cầu* :

Giả sử A tđ B và B tđ C. Tồn tại $P \in \mathbf{GL}_p(K)$, $Q \in \mathbf{GL}_n(K)$, $R \in \mathbf{GL}_p(K)$, $S \in \mathbf{GL}_n(K)$ sao cho $B = Q^{-1}AP$ và $C = S^{-1}BR$.

Khi đó : $C = S^{-1}Q^{-1}APR = (QS)^{-1}A(PR)$ và $(PR,QS) \in \mathbf{GL}_p(K) \times \mathbf{GL}_n(K)$, suy ra A tđ C. ■

Vì quan hệ tđ là đối xứng, nên ta có thể biểu thị A tđ B bởi : A và B là tương đương.

♦ **Mệnh đề 2** Giả sử $A \in \mathbf{M}_{n,p}(K)$, $r = \mathrm{rank}(A)$. Thế thì A tương đương với ma trận $J_{n,p,r}$ xác định bởi:

$$J_{n,p,r} = \begin{pmatrix} 1 & \ddots & 0 & 0 \\ 0 & & 1 & \\ & 0 & & 0 \end{pmatrix} \begin{matrix} \updownarrow r \\ \updownarrow n-r \end{matrix} = \begin{pmatrix} \mathrm{I}_r & 0_{r,p-r} \\ 0_{n-r,r} & 0_{n-r,p-r} \end{pmatrix}$$

(cột: $\leftrightarrow r$, $\leftrightarrow p-r$)

(đặc biệt $J_{n,p,0} = 0$).

Chứng minh :

Giả sử E, F là hai K-kgv tương ứng p,n chiều (luôn luôn tồn tại), $\mathcal{B}$ và $\mathcal{C}$ tương ứng là các cơ sở của E và F (luôn tồn tại), $f \in \mathcal{L}(E,F)$ biểu diễn bởi A trong các cơ sở $\mathcal{B}$ và $\mathcal{C}$: $\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f) = A$.

Theo định lý về hạng (7.3.1, Định lý 1), kgvc $\mathrm{Ker}(f)$ của E là $p - r$ chiều, do vậy có ít nhất một cơ sở $(e_{r+1}, \ldots, e_p)$.

Theo định lý về cơ sở không đầy đủ, dạng yếu (6.4, Định lý 2), tồn tại $e_1, \ldots, e_r \in E$ sao cho $\mathcal{B}' = (e_1,\ldots,e_r, e_{r+1},\ldots,e_p)$ là một cơ sở của E.

Đặt $f_1 = f(e_1), \ldots, f_r = f(e_r)$.

Họ $(f_1, ..., f_r)$ độc lập tuyến tính; thực vậy, nếu $(\lambda_1, ..., \lambda_r) \in K^r$ thỏa mãn $\sum_{i=1}^{r} \lambda_i f_i = 0$,

thì: $\sum_{i=1}^{r} \lambda_i f_i \in \mathrm{Ker}(f) \cap \mathrm{Vect}(e_1, ... e_r) = \{0\}$,

do vậy $\lambda_1 = ... = \lambda_r = 0$ (xem thêm 7.3.1).

Theo định lý về cơ sở không đầy đủ, dạng yếu, tồn tại $f_{r+1}, ..., f_n \in F$ sao cho

$\mathcal{C}' = (f_1, ..., f_r, f_{r+1}, ..., f_n)$ là một cơ sở của F.

Vì $f(e_1) = f_1, ..., f(e_r) = f_r, f(e_{r+1}) = 0, ... f(e_p) = 0$, nên ma trận của f trong $\mathcal{B}'$ và $\mathcal{C}'$ là $J_{n,p,r}$ và do vậy A tđ $J_{n,p,r}$.

♦ Hệ quả 1

$$\forall A, B \in (\mathbf{M}_{n,p}(K))^2, \quad (A \text{ tđ } B \Leftrightarrow \mathrm{rank}(A) = \mathrm{rank}(B)).$$

Chứng minh:

1) Nếu A tđ B, thì A và B biểu diễn cùng một ánh xạ tuyến tính (trong những cơ sở), vì vậy có cùng hạng.

2) Ngược lại, nếu $\mathrm{rank}(A) = \mathrm{rank}(B)$, thì A và B tương đương với $J_{n,p,r}$, do vậy chúng tương đương với nhau.

♦ Hệ quả 2

$$\forall A \in \mathbf{M}_{n,p}(K), \ \mathrm{rank}({}^tA) = \mathrm{rank}(A).$$

Chứng minh:

Đặt $r = \mathrm{rank}(A)$, tồn tại $(P,Q) \in \mathbf{GL}_p(K) \times \mathbf{GL}_n(K)$ sao cho $A = Q^{-1} J_{n,p,r} P$. Khi đó ta có : ${}^tA = {}^tP\,{}^tJ_{n,p,r}\,{}^t(Q^{-1}) = ({}^tP^{-1})^{-1} J_{p,n,r}\,{}^t(Q^{-1})$,

và do vậy $\mathrm{rank}({}^tA) = \mathrm{rank}(J_{p,n,r}) = r$.

Bài tập

◊ **8.2.1** Giả sử $A \in \mathbf{M}_{n,p}(K)$, $r = \text{rank}(A)$. Chứng minh rằng tồn tại $A_1, \ldots, A_r \in \mathbf{M}_{n,p}(K)$ sao cho :

$$\begin{cases} A = \sum_{k=1}^{r} A_k \\ \forall k \in \{1, \ldots, r\}, \quad \text{rank}(A_k) = 1 \end{cases}$$

◊ **8.2.2** Xác lập rằng : $\forall A \in \mathbf{M}_n(\mathbb{C}), \exists (B, C) \in (\mathbf{GL}_n(\mathbb{C}))^2$, $A = B + C$.

◊ **8.2.3** Cho $A \in \mathbf{M}_{n,p}(K)$ và $r \in \mathbb{N}^*$ sao cho $r \leq \text{Min}(n,p)$. Chứng minh :

$$\text{rank}(A) \leq r \Leftrightarrow (\exists (B, C) \in \mathbf{M}_{n,r}(K) \times \mathbf{M}_{r,p}(K) , A = BC).$$

Đặc biệt : $\text{rank}(A) \leq 1 \Leftrightarrow (\exists (U, V) \in \mathbf{M}_{n,1}(K) \times \mathbf{M}_{p,1}(K), A = UV^t)$.

◊ **8.2.4*** a) Giả sử $A \in \mathbf{M}_{n,p}(K)$. Chứng minh rằng, bằng một dãy hữu hạn những phép biến đổi sơ cấp trên cột và trên hàng, ta có thể đưa A về $J_{n,p,r}$, trong đó $r = \text{rank}(A)$.

b) Từ đó suy ra rằng với mọi (A, B) thuộc $(\mathbf{M}_{n,p}(K))^2$, hai tính chất sau là tương đương:

(i) $\text{rank}(A) = \text{rank}(B)$

(ii) Có thể đưa A về B bằng một dãy hữu hạn những phép biến đổi sơ cấp trên cột và trên dòng.

c) Chứng tỏ rằng bộ phận của $\mathbf{GL}_n(K)$ tạo bởi các ma trận của các phép biến đổi sơ cấp (tức là các $P_{j,k}$, $D_{j,\alpha}$, $T_{j,k,\alpha}$, xem 8.1.7) sinh ra nhóm $\mathbf{GL}_n(K)$.

◊ **8.2.5*** Cho E, F là hai K-kgv hữu hạn chiều, $f, g \in \mathcal{L}(E, F)$.

a) Giả sử $\text{rank}(g) \leq \text{rank}(f)$. Chứng minh rằng :

α) $\exists h \in \mathcal{GL}(F), \exists k \in \mathcal{L}(E), \quad h \circ g = f \circ k$

β) $\exists u \in \mathcal{GL}(E), \exists v \in \mathcal{L}(F), \quad v \circ u = v \circ f$.

b) Giả sử $\text{rank}(g) = \text{rank}(f)$. Chứng minh rằng : $\exists h \in \mathcal{GL}(F), \exists k \in \mathcal{GL}(E), \quad h \circ g = f \circ k$.

8.2.4 Đổi cơ sở đối với một tự đồng cấu

Mệnh đề sau là một trường hợp đặc biệt của Mệnh đề 8.2.3,*1*).

♦ **Mệnh đề 1**

Cho | E là một K-kgv n chiều
| $\mathcal{B}$, $\mathcal{B}'$ là hai cơ sở của E, $P = \text{Pass}(\mathcal{B}, \mathcal{B}')$
| $f \in \mathcal{L}(E)$, $A = \text{Mat}_{\mathcal{B}}(f)$, $A' = \text{Mat}_{\mathcal{B}'}(f)$.

Thế thì:

$$A' = P^{-1}AP$$

♦ **Định nghĩa 1**

Cho $A, B \in \mathbf{M}_n(K)$. Ta nói A **đồng dạng** với B, và ký hiệu $A \sim B$, khi và chỉ khi tồn tại $P \in \mathbf{GL}_n(K)$ sao cho : $B = P^{-1}AP$.

♦ **Mệnh đề 2**

Quan hệ $\sim$ là một quan hệ tương đương trong $\mathbf{M}_n(K)$.

Chứng minh:

1) *Phản xạ* : $\forall A \in \mathbf{M}_n(K)$, $A = \mathbf{I}_n A \mathbf{I}_n$.

2) *Đối xứng* :

Nếu tồn tại $P \in \mathbf{GL}_n(K)$ sao cho $B = P^{-1}AP$,

thì $A = (P^{-1})^{-1} BP^{-1}$ và $P^{-1} \in \mathbf{GL}_n(K)$, do vậy $B \sim A$.

3) *Bắc cầu* :

Giả sử $A \sim B$ và $A \sim C$. Tồn tại $P, Q \in \mathbf{GL}_n(K)$ sao cho $B = P^{-1}AP$ và $C = Q^{-1}BQ$.

Thế thì, $C = Q^{-1}P^{-1}APQ = (PQ)^{-1}A(PQ)$ và $PQ \in \mathbf{GL}_n(K)$ do vậy $A \sim C$. ■

Vì quan hệ $\sim$ là đối xứng, nên ta có thể biểu thị $A \sim B$ bởi: A và B **đồng dạng** với nhau.

Quan hệ $\sim$ được gọi là **sự đồng dạng của các ma trận vuông**.

♦ **Mệnh đề 3**

$$\forall A, B \in (\mathbf{M}_n(K))^2 , (A \sim B \Rightarrow \text{tr}(A) = \text{tr}(B)) .$$

Chứng minh :

Giả sử $A \sim B$. Tồn tại $P \in \mathbf{GL}_n(K)$ sao cho $B = P^{-1}AP$, nên (xem 8.1.9, Mệnh đề 2)):

$$\text{tr}(B) = \text{tr}(P^{-1}(AP)) = \text{tr}((AP)P^{-1}) = \text{tr}(A).$$

NHẬN XÉT :

1) Hiển nhiên rằng nếu hai ma trận vuông đồng dạng thì chúng tương đương .

2) Nhưng (nếu $n \geq 2$) hai ma trận tương đương có thể không đồng dạng, chẳng hạn, với $n = 2$, các ma trận $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ và $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ tương đương vì hạng của chúng đều bằng 1, nhưng không đồng dạng vì chúng không có cùng vết.

3) Giả sử $A \in \mathbf{M}_n(K)$. Nếu tồn tại $\alpha \in K$ sao cho $A \sim \alpha \mathbf{I}_n$, thì $A = \alpha \mathbf{I}_n$. Thực vậy, với mọi $P \in \mathbf{GL}_n(K)$: $P(\alpha \mathbf{I}_n)P^{-1} = \alpha \mathbf{I}_n$.

4) Nếu $n \geq 2$, hai ma trận vuông có thể có cùng vết mà không đồng dạng. Chẳng hạn, với $n = 2$, các ma trận $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ và $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ có cùng vết, nhưng không đồng dạng, vì chúng thậm chí không tương đương (ma trận thứ nhất có hạng bằng 0, còn ma trận thứ hai có hạng bằng 1).

♦ **Định nghĩa 2** Giả sử E là một K-kgv hữu hạn chiều, $f \in \mathcal{L}(E)$. **Vết** của f, ký hiệu là $\mathrm{tr}(f)$, là vết của ma trận bất kỳ biểu diễn tự đồng cấu f.

Định nghĩa này là đúng đắn, vì theo Mệnh đề trên, mọi ma trận biểu diễn tự đồng cấu f đều có cùng vết. ■

Từ các tính chất của vết của một ma trận vuông, dễ dàng suy ra Mệnh đề sau đây.

♦ **Mệnh đề 4** Giả sử E là một K-kgv.

1) Ánh xạ $\mathrm{tr} : \mathcal{L}(E) \to K$, $f \to \mathrm{tr}(f)$ là một dạng tuyến tính.

2) $\forall (f, g) \in (\mathcal{L}(E))^2$, $\mathrm{tr}(g \circ f) = \mathrm{tr}(f \circ g)$.

3) $\forall f \in \mathcal{L}(E), \forall h \in \mathcal{GL}(E)$, $\mathrm{tr}(h^{-1} \circ f \circ h) = \mathrm{tr}(f)$.

Bài tập

◊ **8.2.6** Đặt $S : \mathbf{M}_n(K) \to K$, $A = (a_{ij})_{ij} \mapsto \sum_{1 \leq i, j \leq n} a_{ij} a_{ji}$

Chứng minh : $\forall A, B \in \mathbf{M}_n(K)$, $(A \sim B \Rightarrow S(A) = S(B))$.

◊ **8.2.7** Các ma trận thuộc $\mathbf{M}_4(\mathbb{R})$ $A = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ và $B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ có đồng dạng không?

8.3 Các ma trận đáng chú ý

8.3.1 Ma trận đối xứng, ma trận phản đối xứng

Trong § 8.3.1 này, ta giả thiết rằng $2.1_K \neq 0$ (trong đó 1_K là phần tử trung hòa đối với phép nhân); như vậy 2 (được đồng nhất với 2.1_K) có một nghịch đảo trong K, ký hiệu là $\frac{1}{2}$. Ta cũng nói K có **đặc số** $\neq 2$ (xem bài tập 2.3.4). Đó là trường hợp khi $K = \mathbb{R}$ hoặc $K = \mathbb{C}$.

Cho $n \in \mathbb{N}^*$.

1) Ma trận đối xứng

♦ Định nghĩa

Một ma trận vuông A thuộc $\mathbf{M}_n(K)$ được gọi là **đối xứng** khi và chỉ khi ${}^tA = A$.

Ta ký hiệu tập hợp các ma trận đối xứng cấp n với hệ tử trong K là $\mathbf{S}_n(K)$.

♦ Mệnh đề 1

$\mathbf{S}_n(K)$ là một kgvc của $\mathbf{M}_n(K)$.

Chứng minh:

1) $0 \in \mathbf{S}_n(K)$.

2) Giả sử $\alpha \in K$, $A, B \in \mathbf{S}_n(K)$. Ta có ${}^t(\alpha A + B) = \alpha {}^tA + {}^tB = \alpha A + B$, vì vậy $\alpha A + B \in \mathbf{S}_n(K)$.

NHẬN XÉT:

1) Rõ ràng là họ $(E_{ii})_{1 \leq i \leq n} \cup (E_{ij} + E_{ji})_{1 \leq i < j \leq n}$ là một cơ sở của $\mathbf{S}_n(K)$, và vì vậy $\dim(\mathbf{S}_n(K)) = \frac{n(n+1)}{2}$.

Chẳng hạn, với $n=2$, $\left(\begin{pmatrix}1&0\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\0&1\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}\right)$ là một cơ sở của $\mathbf{S}_2(K)$; mọi ma trận đối xứng cấp 2 viết được một cách duy nhất dưới dạng $\begin{pmatrix}a&b\\b&d\end{pmatrix}$ (trong đó $(a, b, d) \in K^3$), nghĩa là : $a\begin{pmatrix}1&0\\0&0\end{pmatrix} + d\begin{pmatrix}0&0\\0&1\end{pmatrix} + b\begin{pmatrix}0&1\\1&0\end{pmatrix}$.

2) Nếu $n \geq 2$, tích của hai ma trận đối xứng có thể không đối xứng, như trong ví dụ sau :

$$\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1&0\\0&0\end{pmatrix} = \begin{pmatrix}0&0\\1&0\end{pmatrix}.$$

Tuy nhiên công thức ${}^t(AB) = {}^tB\,{}^tA$ chứng minh Mệnh đề sau đây.

♦ **Mệnh đề 2**

$$\forall (A, B) \in (\mathbf{S}_n(K))^2, \quad (AB \in \mathbf{S}_n(K) \Leftrightarrow AB = BA). \qquad \blacksquare$$

♦ **Mệnh đề 3**

$$\forall A \in \mathbf{S}_n(K) \cap \mathbf{GL}_n(K), \ A^{-1} \in S_n(K).$$

Chứng minh:

Giả sử $A \in \mathbf{S}_n(K) \cap \mathbf{GL}_n(K)$; thế thì ta có : ${}^t(A^{-1}) = ({}^tA)^{-1} = A^{-1}$, do vậy $A^{-1} \in \mathbf{S}_n(K)$.

2) Ma trận phản đối xứng

♦ **Định nghĩa** Một ma trận vuông A thuộc $\mathbf{M}_n(K)$ được gọi là **phản đối xứng** khi và chỉ khi : ${}^tA = -A$. Ta ký hiệu tập hợp các ma trận phản đối xứng cấp n với hệ tử trong K là $\mathbf{A}_n(K)$.

♦ **Mệnh đề 1**

$\mathbf{A}_n(K)$ là một kgvc của $\mathbf{M}_n(K)$.

Chứng minh:

1) $0 \in \mathbf{A}_n(K)$.

2) Giả sử $\alpha \in K$, $A, B \in \mathbf{A}_n(K)$. Ta có : ${}^t(\alpha A + B) = \alpha {}^tA + {}^tB = -\alpha A - B = -(\alpha A + B)$, do vậy $\alpha A + B \in \mathbf{A}_n(K)$.

NHẬN XÉT :

1) Rõ ràng là họ $(E_{ij} - E_{ji})_{1 \le i < j \le n}$ là một cơ sở của $\mathbf{A}_n(K)$, và vì vậy $\dim(\mathbf{A}_n(K)) = \dfrac{n(n-1)}{2}$

Chẳng hạn, với $n = 3$, $\left(\begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & -1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} \right)$

là một cơ sở của $\mathbf{A}_3(K)$; mọi ma trận phản đối xứng cấp 3 được viết một cách duy nhất thành $\begin{pmatrix} 0 & -a & -b \\ a & 0 & -c \\ b & c & 0 \end{pmatrix}$ (trong đó $(a, b, c) \in K^3$), nghĩa là

$$a \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + b \begin{pmatrix} 0 & 0 & -1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} + c \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}.$$

2) Nếu $n \ge 3$, tích của hai ma trận phản đối xứng có thể không đối xứng , không phản đối xứng , như trong ví dụ sau (với $n = 3$) :

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

Tuy nhiên, giả sử $A,B \in \mathbf{M}_n(K)$ sao cho $AB = BA$. Nếu A và B đối xứng hoặc phản đối xứng (có bốn trường hợp), thì AB đối xứng hoặc phản đối xứng theo "một quy tắc về dấu", vì do ${}^tA = \varepsilon A$, ${}^tB = \varepsilon' B$. $(\varepsilon,\varepsilon') \in \{-1,1\}^2$, nên ta có:

$${}^t(AB) = {}^tB\,{}^tA = \varepsilon'\varepsilon BA = \varepsilon'\varepsilon AB.$$

♦ **Mệnh đề 2**

Các kgvc $\mathbf{S}_n(K)$ và $\mathbf{A}_n(K)$ bù nhau trong $\mathbf{M}_n(K)$.

Chứng minh:

1) Giả sử $A \in \mathbf{S}_n(K) \cap \mathbf{A}_n(K)$. Thế thì ta có ${}^tA = A$ và ${}^tA = -A$, nên $2A = 0$, do vậy $A = 0$. Như vậy : $\mathbf{S}_n(K) \cap \mathbf{A}_n(K) = \{0\}$.

2) Giả sử $M \in \mathbf{M}_n(K)$. Rõ ràng là :

$$\begin{cases} M = \dfrac{1}{2}(M + {}^tM) + \dfrac{1}{2}(M - {}^tM) \\ \dfrac{1}{2}(M + {}^tM) \in \mathbf{S}_n(K), \dfrac{1}{2}(M - {}^tM) \in \mathbf{A}_n(K) \end{cases}$$

Điều đó chứng tỏ : $\mathbf{S}_n(K) + \mathbf{A}_n(K) = \mathbf{M}_n(K)$.

Đối với $M \in \mathbf{M}_n(K)$, ma trận đối xứng $\dfrac{1}{2}(M + {}^tM)$ được gọi là **phần đối xứng** của M, và ma trận phản đối xứng $\dfrac{1}{2}(M - {}^tM)$ được gọi là **phần phản đối xứng** của M.

Ta chú ý rằng có sự tương tự với các khái niệm phần chẵn và phần lẻ của một hàm số (Tập 1, 4.1.3).

8.3.2 Ma trận tam giác

Cho $n \in \mathbb{N}^*$.

♦ **Định nghĩa** Cho $A \in \mathbf{M}_n(K)$.

1) Ta nói A là **tam giác trên** khi và chỉ khi :

$$\forall (i,j) \in \{1, \ldots, n\}^2, \quad (i > j \Rightarrow a_{ij} = 0).$$

Ta ký hiệu tập hợp các ma trận tam giác trên cấp n với hệ tử trong K là $\mathbf{T}_{n,t}(K)$.

2) Ta nói A là **tam giác dưới** khi và chỉ khi:

$$\forall (i,j) \in \{1, \ldots, n\}^2, (i < j \Rightarrow a_{ij} = 0).$$

Ta ký hiệu tập hợp các ma trận tam giác dưới cấp n với hệ tử trong K là $T_{n,d}(K)$.

3) Ta nói A là **tam giác** khi và chỉ khi A là tam giác trên hoặc tam giác dưới.

VÍ DỤ:

- $\begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}$ là tam giác trên.
- $\begin{pmatrix} 3 & 0 & 0 \\ -1 & 0 & 0 \\ 4 & 1 & 2 \end{pmatrix}$ là tam giác dưới.

NHẬN XÉT: $\forall A \in \mathbf{M}_n(K)$, $(A \in \mathbf{T}_{n,d}(K) \Leftrightarrow {}^tA \in \mathbf{T}_{n,t}(K))$

Dễ dàng suy ra Mệnh đề sau.

♦ Mệnh đề 1

$\mathbf{T}_{n,s}(K)$ và $\mathbf{T}_{n,d}(K)$ là những kgvc của $\mathbf{M}_n(K)$.

NHẬN XÉT :

Rõ ràng họ $(E_{ij})_{1 \le i \le j \le n}$ là một cơ sở của $\mathbf{T}_{n,s}(K)$, và do vậy:

$$\dim(\mathbf{T}_{n,s}(K)) = \frac{n(n+1)}{2}.$$

♦ Mệnh đề 2

$\mathbf{T}_{n,s}(K)$ là một đại số con có đơn vị của đại số có đơn vị $\mathbf{M}_n(K)$.

Chứng minh:

1) $\mathbf{T}_{n,s}(K)$ là một kgvc của $\mathbf{M}_n(K)$.

2) Giả sử $A = (a_{ij})_{ij}$, $B = (b_{ij})_{ij}$ là hai phần tử của $\mathbf{T}_{n,s}(K)$. Giả sử $(i, j) \in \{1, ..., n\}^2$ sao cho $i > j$. Hạng tử thứ (i, j) của AB bằng $\sum_{k=1}^{n} a_{ik} b_{kj}$. Với mỗi k thuộc $\{1, ..., n\}$:

- nếu $i > k$, thì $a_{ik} = 0$ (vì $A \in \mathbf{T}_{n,s}(K)$)
- nếu $k \ge i$, thì $k > j$ và do vậy $b_{kj} = 0$ (vì $B \in \mathbf{T}_{n,s}(K)$).

Như vậy : $\forall k \in \{1, ..., n\}$, $a_{ik} b_{kj} = 0$, và do vậy : $\sum_{k=1}^{n} a_{ik} b_{kj} = 0$, điều này chứng tỏ $AB \in T_{n,s}(K)$.

3) $\mathbf{I}_n \in T_{n,s}(K)$.

NHẬN XÉT:

1) Các hạng tử chéo của tích hai ma trận tam giác trên là các tích của các hạng tử chéo của hai ma trận đó:

$$\begin{pmatrix} a_{11} & \cdots & \\ & \ddots & \\ 0 & & a_{nn} \end{pmatrix} \begin{pmatrix} b_{11} & \cdots & \\ & \ddots & \\ 0 & & b_{nn} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & \cdots & \\ & \ddots & \\ 0 & & a_n b_{nn} \end{pmatrix}.$$

2) Đặc biệt, các hạng tử chéo của một lũy thừa của một ma trận tam giác là các lũy thừa của các hạng tử chéo của ma trận đó:

$$\begin{pmatrix} a_{11} & \cdots & \\ & \ddots & \\ 0 & & a_{nn} \end{pmatrix}^k = \begin{pmatrix} a_{11}^k & \cdots & \\ & \ddots & \\ 0 & & a_{nn}^k \end{pmatrix}.$$

♦ **Mệnh đề 3**

$\forall A \in \mathbf{T}_{n,t}(K) \cap \mathbf{GL}_n(K),\ A^{-1} \in \mathbf{T}_{n,t}(K)$.

Chứng minh:

Giả sử $A \in \mathbf{T}_{n,t}(K) \cap \mathbf{GL}_n(K)$.

Theo Mệnh đề 2, với mọi M thuộc $\mathbf{T}_{n,t}(K)$, AM thuộc $\mathbf{T}_{n,t}(K)$, điều đó cho phép ta xét ánh xạ $f_A : \mathbf{T}_{n,t}(K) \to \mathbf{T}_{n,t}(K)$.
$M \mapsto AM$

1) f_A tuyến tính :

$\forall \alpha \in K,\ \forall (M, N) \in (\mathbf{T}_{n,t}(K))^2,\quad f_A(\alpha M + N) = A(\alpha M + N)$

$= \alpha AM + N = \alpha f_A(M) + f_A(N)$.

2) f_A là đơn ánh vì, với mọi M thuộc $T_{n,t}(K)$:

$$f_A(M) = 0 \Leftrightarrow AM = 0 \Rightarrow A^{-1}(AM) = 0 \Rightarrow M = 0.$$

3) Vì f_A là một tự đồng cấu đơn ánh của một kgv hữu hạn chiều, nên f_A là song ánh (xem 7.3.1, Định lý 2). Vì $\mathbf{I}_n \in \mathbf{T}_{n,t}(K)$, nên tồn tại $B \in \mathbf{T}_{n,t}(K)$ sao cho $f_A(B) = \mathbf{I}_n$. Khi đó $A^{-1} = B \in \mathbf{T}_{n,t}(K)$.

♦ **Mệnh đề 4** Giả sử $A = \begin{pmatrix} a_{11} & \cdots & \\ & \ddots & \\ 0 & & a_{nn} \end{pmatrix} \in \mathbf{T}_{n,t}(K)$.

Ta có : $A \in \mathbf{GL}_n(K) \Leftrightarrow (\forall i \in \{1, .., n\},\ a_{ii} \neq 0)$.

Hơn nữa, nếu $A \in \mathbf{GL}_n(K)$, thì các hạng tử chéo của A^{-1} là nghịch đảo của các hạng tử chéo của A :

$$A^{-1} = \begin{pmatrix} a_{11}^{-1} & \cdots & \\ & \ddots & \\ 0 & & a_{nn}^{-1} \end{pmatrix}.$$

Chứng minh:

• Giả sử $A \in \mathbf{GL}_n(K)$. Theo Mệnh đề trên, $A^{-1} \in \mathbf{T}_{n,t}(K)$.

Đặt $A^{-1} = \begin{pmatrix} b_{11} & \cdots & \\ & \ddots & \\ 0 & & b_{nn} \end{pmatrix}$, ta có $\mathbf{I}_n = AA^{-1} = \begin{pmatrix} a_{11}b_{11} & \cdots & \\ & \ddots & \\ 0 & & a_{nn}b_{nn} \end{pmatrix}$, nên:

$\forall i \in \{1, ..., n\},\ a_{ii}b_{ii} = 1$, và vì vậy: $\forall i \in \{1, ..., n\},\ (a_{ii} \neq 0$ và $b_{ii} = a_{ii}^{-1})$.

• Ngược lại, nếu $(\forall i \in \{1, ..., n\},\ a_{ii} \neq 0)$, thì theo phương pháp Gauss (8.1.7), $\text{rank}(A) = n$, và do vậy A khả nghịch.

Bài tập

◊ **8.3.1** Chứng tỏ rằng: $\forall Q \in \mathbb{C}_n[X], \exists! P \in \mathbb{C}_n[X], \ Q(X) = P(X) + P'\left(\frac{X}{2}\right) + ... + P^{(n)}\left(\frac{X}{2^n}\right)$.

◊ **8.3.2** Giả sử $A = \begin{pmatrix} a_{11} & \cdots & \\ & \ddots & \\ 0 & & a_{nn} \end{pmatrix} \in \mathbf{T}_{n,t}(K)$. Chứng tỏ rằng A là lũy linh khi và chỉ khi $(\forall i \in \{1, ..., n\}, a_{ii} = 0)$ và, nếu A là lũy linh thì $A^n = 0$.

◊ **8.3.3** a) Chứng tỏ rằng $G = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} ; (x, y, z) \in K^3 \right\}$ là một nhóm nhân.

b) Tìm tâm của G, nghĩa là tìm $\{A \in G \ ; \forall M \in G, \ AM = MA\}$.

◊ **8.3.4** Xác định hoán tập của $\mathbf{T}_{n,t}(K)$ trong $\mathbf{M}_n(K)$, nghĩa là xác định tập :

$$\{A \in \mathbf{M}_n(K) \ ; \forall T \in \mathbf{T}_{n,t}(K), \ AT = TA\}.$$

8.3.3 Ma trận đường chéo

Cho $n \in \mathbb{N}^*$.

♦ **Định nghĩa** Một ma trận vuông $A = (a_{ij})_{1 \le i,j \le n}$ thuộc $\mathbf{M}_n(K)$ được gọi là **ma trận đường chéo** khi và chỉ khi:

$$\forall (i,j) \in \{1, ..., n\}^2, \quad (i \neq j \Rightarrow a_{ij} = 0).$$

Ta ký hiệu tập hợp các ma trận đường chéo cấp n với hệ tử trong K là $\mathbf{D}_n(K)$.

Với mọi $(\lambda_1, ..., \lambda_n)$ thuộc K^n, ta ký hiệu ma trận đường chéo thuộc $\mathbf{M}_n(K)$ có các hệ tử chéo $\lambda_1, ..., \lambda_n$ là diag $(\lambda_1, ..., \lambda_n)$:

$$\text{diag}\,(\lambda_1, ..., \lambda_n) = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}.$$

NHẬN XÉT : $\mathbf{T}_{n,t}(K) \cap \mathbf{T}_{n,d}(K) = \mathbf{D}_n(K)$.

Dễ dàng suy ra mệnh đề sau.

♦ **Mệnh đề 1**
$\mathbf{D}_n(K)$ là một đại số con giao hoán và có đơn vị của $\mathbf{M}_n(K)$.

NHẬN XÉT :

1) Rõ ràng họ $(E_{ii})_{1 \le i \le n}$ là một cơ sở của $\mathbf{D}_n(K)$, và vì vậy $\dim(\mathbf{D}_n(K)) = n$.

2) Với mọi $\alpha \in K$, $(\lambda_1,...,\lambda_n) \in K^n$, $(\mu_1,...\mu_n) \in K^n$, ta có :

$$\begin{cases} \alpha\text{diag}(\lambda_1,...,\lambda_n) = \text{diag}(\alpha\lambda_1,...,\alpha\lambda_n) \\ \text{diag}(\lambda_1,...,\lambda_n) + \text{diag}(\mu_1,...,\mu_n) = \text{diag}(\lambda_1 + \mu_1,...,\lambda_n + \mu_n) \\ \text{diag}(\lambda_1,...,\lambda_n)\text{diag}(\mu_1,...,\mu_n) = \text{diag}(\lambda_1\mu_1,...,\lambda_n\mu_n) \end{cases}.$$

Từ đó suy ra, bằng quy nạp theo k rằng với mọi $k \in \mathbb{N}^*$, $(\lambda_1,...,\lambda_n) \in K^n$:

$$(\text{diag}(\lambda_1, ..., \lambda_n))^k = \text{diag}(\lambda_1^k, ..., \lambda_n^k).$$

Dễ dàng suy ra mệnh đề sau.

♦ **Mệnh đề 2** Giả sử $D = \text{diag}(\lambda_1,...,\lambda_n) \in \mathbf{D}_n(K)$.
Ta có : $D \in \mathbf{GL}_n(K) \Leftrightarrow (\forall i \in \{1, ..., n\}, \lambda_i \neq 0)$.
Hơn nữa, nếu $D \in \mathbf{GL}_n(K)$, thì $D^{-1} = \text{diag}(\lambda_1^{-1},...,\lambda_n^{-1})$.

Bài tập

◊ **8.3.5** Xác định hoán tập của $\mathbf{D}_n(K)$ trong $\mathbf{M}_n(K)$, nghĩa là tập

$$\{A \in \mathbf{M}_n(K); \forall D \in \mathbf{D}_n(K), AD = DA\}.$$

◊ **8.3.6** Giả sử $\lambda_1, ..., \lambda_n \in K$ khác nhau từng đôi một, $D = \text{diag}(\lambda_1, ..., \lambda_n)$. Hãy xác định hoán tập của D, nghĩa là xác định : $\{A \in \mathbf{M}_n(K) ; AD = DA\}$.

Bổ sung

◊ C 8.1 Một bất đẳng thức về phép đếm thiết lập bằng đại số tuyến tính

I Giả sử $n \in \mathbb{N} - \{0, 1\}$, $\alpha_1, ..., \alpha_n, \beta \in \mathbb{R}_+^*$ sao cho : $\forall i \in \{1, ..., n\}$, $\alpha_i \geq \beta$.

Giả sử chỉ tồn tại nhiều nhất một chỉ số i thuộc $\{1, ..., n\}$ sao cho $\alpha_i = \beta$.

Ký hiệu $A = (a_{ij})_{ij} \in \mathbf{M}_n(\mathbb{R})$ xác định bởi

$$a_{ij} = \begin{cases} \alpha_i & \text{nếu} \quad i = j \\ \beta & \text{nếu} \quad i \neq j \end{cases}.$$

Chứng minh: $A \in \mathbf{GL}_n(\mathbb{R})$.

(Với $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbf{M}_{n,1}(\mathbb{R})$ sao cho $AX = 0$, ta có thể xét dấu của $x_1, ..., x_n$).

II Giả sử $\beta \in \mathbb{N}^*$, $(n,p) \in (\mathbb{N}^*)^2$, E là một tập hợp hữu hạn có p phần tử $u_1, ..., u_p$, $(A_j)_{1 \leq j \leq n}$ là một họ gồm n bộ phận của E khác nhau từng đôi một và sao cho :

$$\forall (i,j) \in \{1, ..., n\}^2, \quad (i \neq j \Rightarrow \mathrm{Card}(A_i \cap A_j) = \beta).$$

Xét $B = (b_{ij})_{\substack{1 \leq i \leq p \\ 1 \leq j \leq n}} \in \mathbf{M}_{p,n}(\mathbb{R})$ xác định bởi $b_{ij} = \begin{cases} 1 & \text{nếu } u_i \in A_j \\ 0 & \text{nếu trái lại} \end{cases}$

và $A = {}^tBB \in \mathbf{M}_n(\mathbb{R})$.

1) Chứng minh (dùng I): $A \in \mathbf{GL}_n(\mathbb{R})$.

2) Từ đó suy ra $n \leq p$.

Chương 9

Định thức, hệ tuyến tính

Trong chương 9 này, K chỉ một thể giao hoán. Ta giả thiết $2.1_K \neq 0$ (trong đó 1_K chỉ phần tử trung hòa đối với phép nhân); như vậy 2 (được đồng nhất với 2.1_K) có trong K một nghịch đảo, ký hiệu là $\frac{1}{2}$.

Ta cũng nói K là một thể có đặc số $\neq 2$ (xem bài tập 2.3.4). Đây là trường hợp $K = \mathbb{R}$ hay $K = \mathbb{C}$.

K-kgv xét ở chương này đều giả thiết là hữu hạn chiều và với số chiều $\neq 0$.

9.1 Ánh xạ đa tuyến tính

9.1.1 Đại cương

♦ **Định nghĩa** Giả sử $p \in \mathbb{N}^*$, $E_1, ..., E_p, F$ là những K - kgv.

Một ánh xạ $\varphi : E_1 \times ... \times E_p \to F$ được gọi là ***p*-tuyến tính** (hay: **đa tuyến tính**) khi và chỉ khi φ tuyến tính đối với từng thành phần (hay: biến), nghĩa là:

$\forall i \in \{1, ..., p\}$, $\forall \lambda \in K$, $\forall x_1 \in E_1$, ..., $\forall x_i \in E_i, \forall y_i \in E_i$, ..., $\forall x_p \in E_p$,
$\varphi(x_1, ..., x_{i-1}, \lambda x_i + y_i, x_{i+1}, ..., x_p) = \lambda\varphi(x_1, ..., x_i, ..., x_p) + \varphi(x_1, ..., y_i, ..., x_p)$.

Nếu có thêm $F = K$, thì ta nói φ là một **dạng *p* - tuyến tính**.

VÍ DỤ:

1) Khi $p = 1$, khái niệm ánh xạ 1-tuyến tính trùng với khái niệm ánh xạ tuyến tính.

2) Ánh xạ không là p - tuyến tính.

3) Tích vô hướng chính tắc trên $\mathbb{R}^2$, $\varphi : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$ là một dạng
$((x_1, x_2),(y_1,y_2)) \mapsto x_1y_1 + x_2y_2$

2-tuyến tính (hay thường gọi là : **song tuyến tính**).

4) Tích vectơ trong $\mathbb{R}^3$: $\phi : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$, xác định bởi:

$$\phi((x_1, x_2, x_3),(y_1, y_2, y_3)) = (x_2y_3 - x_3y_2, x_3y_1 - x_1y_3, x_1y_2 - x_2y_1)$$

(xem dưới đây, 10.5.2, Mệnh đề 5) là một ánh xạ song tuyến tính.

♦ **Mệnh đề** Tập hợp $\mathcal{L}_p(E_1,..., E_n; F)$ các ánh xạ p-tuyến tính từ $E_1 \times ... \times E_p$ đến F là một K -kgv.

Chứng minh:

Rõ ràng $\mathcal{L}_p(E_1, ..., E_p; F)$ là một kgvc của $F^{E_1 \times ... \times E_p}$.

9.1.2 Ánh xạ đa tuyến tính thay phiên

Cho E là một K-kgv và $p \in \mathbb{N}^*$.

♦ **Định nghĩa** Một ánh xạ p - tuyến tính $\varphi : E^p \to F$ được gọi là **thay phiên** khi và chỉ khi, với mọi cặp (i, j) thuộc $\{1,..., p\}^2$ sao cho $i \neq j$, và với mọi $(x_1,...,x_p)$ thuộc E^p: $x_i = x_j \Rightarrow \varphi(x_1,...,x_p) = 0$.

Nếu có thêm $F = K$, thì ta nói φ là một **dạng p - tuyến tính thay phiên.**

Nói cách khác, φ là thay phiên khi và chỉ khi $\varphi(x_1,...,x_p)$ bằng không với mọi bộ p phần tử $(x_1, ...,x_p)$ có chứa ít nhất một *phần tử lặp lại.*

NHẬN XÉT:

Tập hợp các ánh xạ p-tuyến tính thay phiên từ E^p đến F là một kgvc của $\mathcal{L}_p(E,...,E;F)$.

♦ **Mệnh đề 1** Một ánh xạ p -tuyến tính $\varphi : E^p \to F$ là thay phiên khi và chỉ khi:

$$\forall \sigma \in \mathfrak{S}_p, \quad \forall (x_1,...,x_p) \in E^p, \quad \varphi(x_{\sigma(1)},...,x_{\sigma(p)}) = \varepsilon(\sigma)\varphi(x_1,...,x_p).$$

Ta nhắc lại (3.3.1, Ký hiệu) rằng $\mathfrak{S}_p$ là nhóm đối xứng với chỉ số p, tạo nên bởi các hoán vị của $\{1,...,p\}$, và với mọi σ thuộc $\mathfrak{S}_p$, $\varepsilon(\sigma)$ chỉ dấu của σ.

Chứng minh:

1) Trường hợp một chuyển vị

Giả sử $(i,j) \in \{1,...,p\}^2$, $i < j$; ký hiệu $\tau_{i,j}$ là chuyển vị đổi chỗ i và j và giữ nguyên các phần tử khác của $\{1,...,p\}$ (xem 3.4.2, Định nghĩa 1).

Vì φ thay phiên nên ta có:

$$\varphi(x_1,..., x_{i-1}, x_i + x_j, x_{i+1}, ..., x_{j-1}, x_i + x_j, x_{j+1}, .., x_p) = 0$$

do đó, bằng cách khai triển theo tính chất đa tuyến tính :

$$\varphi(x_1,...,x_i,...,x_i,...,x_p) + \varphi(x_1,...,x_i,...,x_j,...,x_p) + \varphi(x_1,...,x_j,...,x_i,...,x_p) + \varphi(x_1,...,x_j,...,x_j,...,x_p) = 0,$$

và do đó $\varphi(x_1,..., x_j,...,x_i,...,x_p) = -\varphi(x_1,..., x_i,..., x_j,...,x_p)$.

Điều đó chứng tỏ: $\varphi(x_{\tau_{i,j}(1)},..., x_{\tau_{i,j}(p)}) = \varepsilon(\tau_{ij})\varphi(x_1,..., x_p)$.

2) Trường hợp tổng quát

Giả sử $\sigma \in \mathfrak{S}_p$. Theo 3.4.2, Định lý 1, σ được phân tích thành một tích những chuyển vị; tồn tại $N \in \mathbb{N}^*$ và những chuyển vị $\sigma_1,...,\sigma_N$ sao cho $\sigma = \sigma_1 \circ ... \circ \sigma_N$; hơn nữa $\varepsilon(\sigma) = (-1)^N$.

Bằng cách lặp lại kết quả của 1), ta được:

$$\varphi(x_{\sigma(1)},...,x_{\sigma(p)}) = -\varphi\left(x_{\sigma_2\circ\cdots\circ\sigma_N(1)},\ldots,\varphi_{\sigma_2\circ\cdots\circ\sigma_N(p)}\right)$$

$$= ... = (-1)^N \varphi(x_1,...,x_p) = \varepsilon(\sigma)\varphi(x_1,...,x_p).$$

♦ **Mệnh đề 2** Giả sử $E^p \to F$ là một ánh xạ p-tuyến tính thay phiên và $(x_1,...,x_p) \in E^p$. Nếu $(x_1,...,x_p)$ phụ thuộc tuyến tính thì $\varphi(x_1,..., x_p) = 0$.

Chứng minh :

Giả sử $(x_1,...,x_p)$ phụ thuộc tuyến tính, khi đó ít nhất một trong các $x_1,...,x_p$ được biểu diễn thành một tổ hợp tuyến tính của các biến khác. Theo Mệnh đề trên, ta có thể quy về trường hợp tồn tại $(\alpha_1,...,\alpha_{p-1}) \in K^{p-1}$ sao cho $x_p = \sum_{i=1}^{p-1} \alpha_i x_i$. Khi đó:

$$\varphi(x_1,...,x_p) = \sum_{i=1}^{p-1} \alpha_i \varphi(x_1,\ldots,x_{p-1},x_i) = 0 \ ,$$

vì mọi bộ-p $(x_1,...,x_{p-1}, x_i)$ đều có chứa một phần tử lặp lại.

♦ **Hệ quả** Nếu $p > \dim(E)$, thì ánh xạ p - tuyến tính thay phiên duy nhất từ E^p đến F là ánh xạ không.

Chứng minh :

Mọi họ p phần tử của E đều phụ thuộc tuyến tính.

9.2 Định thức của một họ n vectơ trong một cơ sở của một kgv n chiều

Cho $n \in \mathbb{N}^*$, E là một K-kgv n chiều.

9.2.1 Không gian $\Lambda_n(E)$

Giả sử $\mathcal{B} = (e_1,..., e_n)$ là một cơ sở của E .

1) Cho $S = (V_1, ..., V_n) \in E^n$ và, với mỗi j thuộc $\{1,...,n\}$, $(a_{i_j j})_{i_j \in \{1,...,n\}} \in K^n$ sao cho: $V_j = \sum_{i_j=1}^{n} a_{i_j j} e_{i_j}$.

Giả sử $\varphi : E^n \to K$ là một dạng n-tuyến tính thay phiên. Ta sẽ tính $\varphi(S)$ theo các $a_{i_j j}$. Ta có:

$$\varphi(S) = \varphi\left(\sum_{i_1=1}^{n} a_{i_1 1} e_{i_1}, \ldots, \sum_{i_n=1}^{n} a_{i_n n} e_{i_n}\right) = \sum_{i_1=1}^{n} a_{i_1 1}\ \varphi\left(e_{i_1}, \sum_{i_2=1}^{n} a_{i_2 2} e_{i_2}, \ldots, \sum_{i_n=1}^{n} a_{i_n n} e_{i_n}\right)$$

$$= \ldots = \sum_{i_1=1}^{n} \cdots \sum_{i_n=1}^{n} a_{i_1 1} \ldots a_{i_n n}\ \varphi\ (e_{i_1},\ldots,e_{i_n}) = \sum_{(i_1,\ldots,i_n) \in \{1,\ldots,n\}^n} a_{i_1 1} \ldots a_{i_n n}\ \varphi(e_{i_1},\ldots,e_{i_n}) .$$

Vì φ thay phiên, nên $\varphi(e_{i_1},...,e_{i_n})$ bằng không mỗi khi $i_1,..., i_n$ không khác nhau từng đôi một, vì vậy, trong tổng bội trên đây chỉ còn các hạng tử ứng với các trường hợp trong đó $(1,...,n) \to (i_1, ..., i_n)$ là một hoán vị của $\{1, ..., n\}$.

Do đó :

$$\varphi(S) = \sum_{\sigma \in \mathfrak{S}_n} a_{\sigma(1)1} \ldots a_{\sigma(n)n} \varphi(e_{\sigma(1)},\ldots,e_{\sigma(n)})$$

$$= \left(\sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1)1} \ldots a_{\sigma(n)n}\right) \varphi(e_1 \ldots, e_n) .$$

2) Ngược lại, giả sử $\lambda \in K$ và $\Psi : E^n \to K$ là ánh xạ xác định bởi

$$\psi(S) = \lambda \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1)1} \ldots a_{\sigma(n)n}$$

với mọi $S = (V_1,...,V_n)$ thuộc E^n, trong đó các $a_{i_j j}$ là các thành phần của các V_j trong cơ sở $\mathcal{B}$: $\forall j \in \{1,...,n\}, V_j = \sum_{i_j=1}^{n} a_{i_j j} e_{i_j j}$.

• Ψ là n-tuyến tính vì, với mọi i thuộc $\{1,...,n\}$, mọi α thuộc K, mọi $V_1,...,V_{i-1}$, V_i, V_i', $V_{i+1},..., V_n$ thuộc E, nếu gọi các thành phần của V_i' trong cơ sở $\mathcal{B}$ là $(a'_{ki})_{1 \le k \le n}$, ta có:

$$\Psi(V_1,...,\alpha V_i + V',...,V_n) = \lambda \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1)1}\cdots(\alpha a_{\sigma(i)i} + a'_{\sigma(i)i})\cdots a_{\sigma(n)n}$$

$$= \alpha\lambda \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1)1}\cdots a_{\sigma(n)n} + \lambda \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1)1}\cdots a'_{\sigma(i)i}\cdots a_{\sigma(n)n}$$

$$= \alpha\Psi(V_1,...,V_i,...,V_n) + \Psi(V_1,...,V'_i,...,V_n).$$

• Ψ là thay phiên vì, với mọi (i,j) thuộc $\{1,...,n\}^2$ sao cho $i < j$ và mọi $(V_1,...,V_n)$ thuộc E^n sao cho $V_i = V_j$, khi thực hiện phép đổi chỉ số $\sigma' = \sigma \circ \tau_{ij}$ trong tổng, ta sẽ có:

$$\Psi(V_1,...,V_n) = \lambda \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1)1}\cdots a_{\sigma(n)n}$$

$$= \lambda \sum_{\sigma'\in\mathfrak{S}_n} -\varepsilon(\sigma') a_{\sigma'(1)1}\cdots a_{\sigma'(j)i}\cdots a_{\sigma'(i)j}\cdots a_{\sigma'(n)n}$$

$$= -\lambda \sum_{\sigma'\in\mathfrak{S}_n} \varepsilon(\sigma') a_{\sigma'(1)1}\cdots a_{\sigma'(i)i}\cdots a_{\sigma'(j)j}\cdots a_{\sigma'(n)n}$$

vì rằng $V_i = V_j$.

Từ đó suy ra $\Psi(V_1,...,V_n) = -\Psi(V_1,...,V_n)$, $2\Psi(V_1,...,V_n) = 0$, $\Psi(V_1,...,V_n) = 0$ (vì K có đặc số $\neq 2$).

• Ta chứng tỏ rằng $\Psi \neq 0$.

Với mỗi j thuộc $\{1,...,n\}$, dạng phân tích của e_j trong cơ sở $\mathcal{B}$ là: $e_j = \sum_{i_j=1}^{n} \delta_{i_j j} e_{i_j}$,

trong đó $\delta_{i_j j}$ là ký hiệu Kronecker. Do đó $\Psi(\mathcal{B}) = \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma)\delta_{\sigma(1)1}\cdots\delta_{\sigma(n)n} = 1$, vì nếu $\sigma \neq \mathrm{Id}_{\{1,...,n\}}$, thì một trong các nhân tử $\delta_{\sigma(j)j}$ $(1 \leq j \leq n)$ phải bằng 0.

Ta tóm tắt sự khảo sát trên đây:

♦ **Định lý - Định nghĩa** Tập hợp $\Lambda_n(E)$ các dạng n - tuyến tính thay phiên trên một K - kgv n chiều ($n \geq 1$) là một K - kgv 1 chiều.

Với mọi cơ sở $\mathcal{B} = (e_1,...,e_n)$ của E, $\det_{\mathcal{B}} : E^n \to K$ ký hiệu ánh xạ xác định bởi:

$$\det_{\mathcal{B}}(V_1,...,V_n) = \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1)1}\cdots a_{\sigma(n)n},$$

với mọi $(V_1,...,V_n)$ thuộc E^n, trong đó, với mỗi j thuộc $\{1,...,n\}$, $(a_{i_j j})_{1\leq i_j\leq n}$ là các thành phần của V_j trong $\mathcal{B}$:

$$V_j = \sum_{i_j=1}^{n} a_{i_j j} e_{i_j}.$$

Phần tử $\det_{\mathcal{B}}(V_1,...,V_n)$ (của K) được gọi là **định thức của** $(V_1,...,V_n)$ **trong cơ sở** $\mathcal{B}$.

Với mọi cơ sở $\mathcal{B}$ của E, $(\det_{\mathcal{B}})$ là một cơ sở của $\Lambda_n(E)$.

Nói cách khác, với mọi cơ sở $\mathcal{B}$ của E, các phần tử của $\Lambda_n(E)$ *tỷ lệ* với $\det_{\mathcal{B}}$.

NHẬN XÉT:

Ta đã thấy ở trên rằng với mọi cơ sở $\mathcal{B}$ của E : $\det_{\mathcal{B}}(\mathcal{B}) = 1$.

9.2.2 Tính chất

Ở đây, ta sẽ ký hiệu tập hợp các cơ sở của E là $\beta(E)$.

◆ **Tính chất 1**

$$\forall \varphi \in \Lambda_n(K),\ \forall S \in E^n,\ \forall \mathcal{B} \in \beta(E),\quad \varphi(S) = \varphi(\mathcal{B})\det_{\mathcal{B}}(S)\ .$$

Chứng minh:

Giả sử $\varphi \in \Lambda_n(E)$, $\mathcal{B} \in \beta(E)$. Vì $\det_{\mathcal{B}}$ sinh ra $\Lambda_n(E)$, nên tồn tại $\alpha \in K$ sao cho $\varphi = \alpha\det_{\mathcal{B}}$. Đặc biệt: $\varphi(\mathcal{B}) = \alpha\det_{\mathcal{B}}(\mathcal{B}) = \alpha$, do đó : $\varphi = \varphi(\mathcal{B})\det_{\mathcal{B}}$ nghĩa là:

$$\forall S \in E^n,\ \varphi(S) = \varphi(\mathcal{B})\ \det_{\mathcal{B}}(S).$$

◆ **Hệ quả**

$$\forall \mathcal{B}, \mathcal{B}' \in \beta(E),\ \forall S \in E^n,\quad \det_{\mathcal{B}'}(S) = \det_{\mathcal{B}'}(\mathcal{B})\det_{\mathcal{B}}(S).$$

Chứng minh:

Chỉ cần áp dụng Mệnh đề trên cho $\varphi = \det_{\mathcal{B}'}$.

NHẬN XÉT:

1) Để nhớ công thức trên, ta chú ý đến sự tương tự đối với *hệ thức Chasles* ($\overrightarrow{B'S} = \overrightarrow{B'B} + \overrightarrow{BS}$) , hoặc phép tính về các phân thức $\left(\dfrac{s}{b'} = \dfrac{b}{b'}\cdot\dfrac{s}{b}\right)$.

2) $\forall \mathcal{B}, \mathcal{B}', \mathcal{B}'' \in \beta(E)$, $\det_{\mathcal{B}''}(\mathcal{B}) = \det_{\mathcal{B}''}(\mathcal{B}')\det_{\mathcal{B}'}(\mathcal{B})$.

3) Đặc biệt, nếu lấy $\mathcal{B}'' = \mathcal{B}$ trong kết quả trên:

$$\forall \mathcal{B}, \mathcal{B}' \in \beta(E),\quad (\det_{\mathcal{B}}(\mathcal{B}) \neq 0 \text{ và } \det_{\mathcal{B}}(\mathcal{B}') = (\det_{\mathcal{B}'}(\mathcal{B}))^{-1}).$$

◆ **Mệnh đề 2** Giả sử $\mathcal{B} \in \beta(E)$, $S \in E^n$.

Thế thì S phụ thuộc tuyến tính khi và chỉ khi $\det_{\mathcal{B}}(S) = 0$.

Chứng minh:

1) Nếu S phụ thuộc tuyến tính, thì $\det_{\mathcal{B}}(S) = 0$, vì $\det_{\mathcal{B}}$ là n - tuyến tính và thay phiên (xem 9.1.2, Mệnh đề 2).

2) Nếu S độc lập tuyến tính thì vì S có n phần tử, nên S là một cơ sở của E, và do vậy (xem Nhận xét 3 trên đây): $\det_{\mathcal{B}}(S) \neq 0$.

9.3 Định thức của một tự đồng cấu

Giả sử $n \in \mathbb{N}^*$, E là một K-kgv n chiều. Giả sử $f \in \mathcal{L}(E)$, $\varphi \in \Lambda_n(E) - \{0\}$.

Hiển nhiên ánh xạ $\varphi \circ (f \times ... \times f)$: $E^n \to K$ xác định bởi:

$$\forall (V_1,...,V_n) \in E^n, (\varphi \circ (f \times ... \times f))(V_1,...,V_n) = \varphi(f(V_1),...,f(V_n))$$

là n- tuyến tính và thay phiên.

Vì $\Lambda_n(E)$ có số chiều là 1 và $\varphi \neq 0$, nên φ sinh ra $\Lambda_n(E)$, do vậy tồn tại $\alpha \in K$ sao cho: $\varphi \circ (f \times ... \times f) = \alpha\varphi$. Ta chứng tỏ rằng α không phụ thuộc φ.

Giả sử $\Psi \in \Lambda_n(E) - \{0\}$. Vì φ sinh ra $\Lambda_n(E)$, nên tồn tại $\lambda \in K - \{0\}$ sao cho $\Psi = \lambda\varphi$. Khi đó ta có:

$$\Psi \circ (f \times ... \times f) = (\lambda\varphi) \circ (f \times ... \times f) = \lambda(\varphi \circ (f \times ... \times f)) = \lambda(\alpha\varphi) = \alpha(\lambda\varphi) = \alpha\Psi.$$

Điều đó chứng tỏ rằng α không phụ thuộc việc chọn φ trong $\Lambda_n(E) - \{0\}$.

Ta tóm tắt việc khảo sát trên:

♦ **Mệnh đề - Định nghĩa 1** Với mọi f thuộc $\mathcal{L}(E)$, tồn tại duy nhất một phần tử $\alpha \in K$ sao cho: $\forall \varphi \in \Lambda_n(E)$, $\varphi \circ (f \times ... \times f) = \alpha\varphi$.

Phần tử α đó gọi là **định thức** của f, và được ký hiệu là $\det(f)$.

Như vậy ta có:

$$\forall f \in \mathcal{L}(E), \forall \varphi \in \Lambda_n(E), \quad \varphi \circ (f \times ... \times f) = (\det(f))\varphi.$$

Dễ dàng chứng minh Mệnh đề sau.

♦ **Mệnh đề 2**

1) $\forall f \in \mathcal{L}(E), \forall \varphi \in \Lambda_n(E), \forall (V_1,...,V_n) \in E^n$

$\varphi(f(V_1),...,f(V_n)) = \det(f)\ \varphi(V_1,...,V_n)$.

2) $\forall f \in \mathcal{L}(E), \forall \mathcal{B} \in \beta(E), \forall (V_1,...,V_n) \in E^n$,

$\det_{\mathcal{B}}(f(V_1),...,f(V_n)) = \det(f)\ \det_{\mathcal{B}}(V_1,...,V_n)$.

3) $\forall f \in \mathcal{L}(E), \forall \mathcal{B} = (e_1,...,e_n) \in \beta(E)$,

$\det(f) = \det_{(e_1,...,e_n)}(f(e_1),...,f(e_n))$.

♦ **Mệnh đề 3**

1) $\det(\mathrm{Id}_E) = 1$.

2) $\forall \alpha \in K, \forall f \in \mathcal{L}(E), \det(\alpha f) = \alpha^n \det(f)$.

3) $\forall f,g \in \mathcal{L}(E), \det(g \circ f) = \det(g)\det(f)$.

4) $\forall f \in \mathcal{L}(E), (f \in G\mathcal{L}(E) \Leftrightarrow \det(f) \neq 0)$.

5) $\forall f \in G\mathcal{L}(E), \det(f^{-1}) = (\det(f))^{-1}$.

Chứng minh:

E có ít nhất một cơ sở $\mathcal{B} = (e_1, \ldots e_n)$.

1) $\det(\mathrm{Id}_E) = \det_{\mathcal{B}}(\mathcal{B}) = 1$.

2) $\det(\alpha f) = \det_{(e_1,\ldots,e_n)}(\alpha f(e_1),\ldots,\alpha f(e_n)) = \alpha^n \det_{(e_1,\ldots,e_n)}(f(e_1),\ldots f(e_n))$

$= \alpha^n \det(f)$.

3) $\det(g \circ f) = \det_{\mathcal{B}}(g(f(\mathcal{B}))) = \det(g)\det_{\mathcal{B}}(f(\mathcal{B})) = \det(g)\det(f)$.

4) $(f \in \mathcal{GL}(E)) \Leftrightarrow (f(\mathcal{B}) \in \beta(E)) \Leftrightarrow \det_{\mathcal{B}}(f(\mathcal{B})) \neq 0 \Leftrightarrow \det(f) \neq 0$.

5) Giả sử $f \in \mathcal{GL}(E)$. Ta có: $\det(f)\det(f^{-1}) = \det(f \circ f^{-1}) = \det(\mathrm{Id}_E) = 1$,

vậy $\det(f^{-1}) = (\det(f))^{-1}$.

NHẬN XÉT: Trong phép chứng minh trên, ta đã ký hiệu: $f(\mathcal{B}) = (f(e_1),\ldots,f(e_n))$, ảnh này cũng có thể ký hiệu là $(f \times \ldots \times f)(\mathcal{B})$.

9.4 Định thức của một ma trận vuông

Cho $n \in \mathbb{N}^*$.

♦ **Định nghĩa** Giả sử $A = (a_{ij})_{1\le i,j\le n} \in \mathbf{M}_n(K)$. **Định thức** của A, ký hiệu là $\det(A)$, hoặc $\begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix}$ là phần tử của K xác định bởi:

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1)1} \cdots a_{\sigma(n)n}.$$

Nói cách khác, nếu ký hiệu $C_1 = \begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix}, \ldots, C_n = \begin{pmatrix} a_{1n} \\ \vdots \\ a_{nn} \end{pmatrix}$ là các cột của A và $\mathcal{B}$ là cơ sở chính tắc của $\mathbf{M}_{n,1}(K)$, thì ta có: $\det(A) = \det_{\mathcal{B}}(C_1, \ldots, C_n)$. ■

Ta nói rằng $\begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix}$ là một định thức cấp n.

Để ghi nhớ cấp n, ta có thể viết $[n]$ ở phía dưới bên phải : $\det(A) = \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix}_{[n]}$

VÍ DỤ:

1) $\forall (a,b,c,d) \in K^4$, $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ab - bc$, vì $\mathfrak{S}_2 = \{\mathrm{Id}_{[1,2]}, \tau_{12}\}$.

2) Giả sử $A = (a_{ij})_{ij} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ & \ddots & \ddots & \vdots \\ & & \ddots & a_{n-1n} \\ 0 & & & a_{nn} \end{pmatrix} \in \mathrm{T}_{n,s}(K)$.

Với $\sigma \in \mathfrak{S}_n$, nếu tồn tại $j \in \{1,\ldots,n\}$ sao cho $\sigma(j) > j$, thì $a_{\sigma(j)j} = 0$, do đó $\prod_{k=1}^{n} a_{\sigma(k)k} = 0$. Điều đó chứng tỏ rằng tổng $\sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1)1} \cdots a_{\sigma(n)n}$ được rút về (các) hạng tử ứng với σ sao cho : $\forall j \in \{1,\ldots,n\}$, $\sigma(j) \le j$.

Với một σ như vậy, ta có $\sigma(1) \le 1$, nên $\sigma(1) = 1$, sau đó $\sigma(2) \le 2$ và $\sigma(2) \ne \sigma(1) = 1$, nên $\sigma(2) = 2$, ... Rõ ràng là với mọi j thuộc $\{1,\ldots,n-1\}$, nếu $(\sigma(1) = 1\ldots,\sigma(j) = j)$ thì $\sigma(j+1) = j+1$, vì $\sigma(j+1) \le j+1$ và $\sigma(j+1) \notin \{1,\ldots,j\}$. Như vậy, hoán vị σ duy nhất thỏa mãn $(\forall j \in \{1,\ldots,n\},\ \sigma(j) \le j)$ là hoán vị đồng nhất, do đó: $\det(A) = \prod_{j=1}^{n} a_{jj}$

(xem 9.6 dưới đây, Mệnh đề).

Dễ dàng suy ra Mệnh đề sau:

Mệnh đề 1 Giả sử E là một K -kgv n chiều, $f \in \mathcal{L}(E)$, $\mathcal{B}$ là một cơ sở của E, $A = \mathrm{Mat}_{\mathcal{B}}(f)$. Ta có:

$$\det(f) = \det(A).$$

Mệnh đề 2

1) $\det(\mathrm{I}_n) = 1$.

2) $\forall \alpha \in K, \forall A \in \mathbf{M}_n(K), \quad \det(\alpha A) = \alpha^n \det(A)$.

3) $\forall (A, B) \in (\mathbf{M}_n(K))^2, \quad \det(AB) = \det(A)\det(B)$.

4) $\forall A \in \mathbf{M}_n(K), \quad (A \in \mathbf{GL}_n(K) \Leftrightarrow \det(A) \neq 0)$.

5) $\forall A \in \mathbf{GL}_n(K), \quad \det(A^{-1}) = (\det(A))^{-1}$.

6) $\forall A \in \mathbf{M}_n(K), \quad \det({}^tA) = \det(A)$.

Chứng minh:

Các tính chất từ 1) tới 5) được suy từ Mệnh đề 1 trên đây và các tính chất của định thức của một tự đồng cấu (9.3, Mệnh đề 3).

Đặt $A = (a_{ij})_{ij} \in \mathbf{M}_n(K)$, ta có:

$$\det({}^tA) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)} = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma^{-1}(\sigma(1))\sigma(1)} \cdots a_{\sigma^{-1}(\sigma(n))\sigma(n)}$$

Vì trong K phép nhân giao hoán, nên khi sắp xếp lại theo chỉ số thứ hai, ta có :

$$a_{\sigma^{-1}(\sigma(1))\sigma(1)} \cdots a_{\sigma^{-1}(\sigma(n))\sigma(n)} = a_{\sigma^{-1}(1)1} \cdots a_{\sigma^{-1}(n)n}$$

với mọi σ thuộc $\mathfrak{S}_n$, và do vậy:

$$\det({}^tA) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma^{-1}(1)1} \cdots a_{\sigma^{-1}(n)n}.$$

Cuối cùng, vì $\mathfrak{S}_n \to \mathfrak{S}_n$ là một song ánh bảo toàn dấu (nghĩa là :

$$\sigma \mapsto \sigma^{-1}$$

$\forall \sigma \in \mathfrak{S}_n$, $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$), nên ta được:

$$\det({}^tA) = \sum_{\tau \in \mathfrak{S}_n} \varepsilon(\tau) a_{\tau(1)1} \cdots a_{\tau(n)n} = \det(A).$$

NHẬN XÉT:

1) Từ tính chất 3) ở trên, bằng quy nạp dễ dàng suy ra:

$$\forall A \in \mathbf{M}_n(K), \forall k \in \mathbb{N}^*, \quad \det(A^k) = (\det(A))^k.$$

2) Từ nhận xét trên và tính chất 5), ta suy ra:

$$\forall A \in \mathbf{GL}_n(K), \forall k \in \mathbb{Z}, \quad \det(A^k) = (\det(A))^k.$$

3) Nếu $A \in \mathbf{M}_n(K)$ là lũy linh, thì tồn tại $k \in \mathbb{N}^*$ sao cho $A^k = 0$, nên

$$(\det(A))^k = \det(A^k) = 0,$$

và do vậy: $\det(A) = 0$.

4) Nếu $A \in \mathbf{M}_n(K)$ là phản đối xứng và nếu n lẻ, thì:

$$\det(A) = \det({}^tA) = \det(-A) = (-1)^n\det(A) = -\det(A),$$

nên $\det(A) = 0$.

Bài tập

◊ **9.4.1** Chứng minh rằng, với mọi $A = (a_{ij})_{ij}$ thuộc $\mathbf{M}_n(\mathbb{C})$: $\left|\det(A)\right| \leq \prod_{j=1}^{n}\left(\sum_{i=1}^{n}\left|a_{ij}\right|\right)$.

◊ **9.4.2** a) Cho $n \in \mathbb{N}^*$. Giả sử tồn tại $A, B \in \mathbf{GL}_n(\mathbb{R})$ sao cho $AB + BA = 0$; chứng minh rằng n chẵn.

b) Cho một ví dụ về $(A,B) \in (\mathbf{GL}_2(\mathbb{R}))^2$ sao cho $AB + BA = 0$.

◊ **9.4.3** **Nhóm tuyến tính đặc biệt**

Ký hiệu $\mathbf{SL}_n(K) = \{A \in \mathbf{M}_n(K);\ \det(A) = 1\}$.

a) Kiểm chứng rằng $\mathbf{SL}_n(K)$ là một nhóm con của $\mathbf{GL}_n(K)$ đối với phép nhân, nhóm con đó được gọi là **nhóm tuyến tính đặc biệt**.

b) Chứng minh : $\forall A \in \mathbf{GL}_n(\mathbb{C}),\ \exists(\alpha, B) \in \mathbb{C}^* \times \mathbf{SL}_n(\mathbb{C}),\ A = \alpha B$.

◊ **9.4.4** Giả sử $n \in \mathbb{N} - \{0,1\}$. Tìm tất cả các A thuộc $\mathbf{M}_n(\mathbb{C})$ sao cho:

$$\forall M \in \mathbf{M}_n(\mathbb{C}),\quad \det(A + M) = \det(A) + \det(M).$$

◊ **9.4.5** Cho $n \in \mathbb{N}^*$.

a) Chứng minh : $\forall A, B \in \mathbf{M}_n(\mathbb{R}),\quad (AB = BA \Leftrightarrow \det(A^2 + B^2) \geq 0)$.

b) Có hay không: $\forall A, B \in \mathbf{M}_2(\mathbb{R}),\ \det(A^2 + B^2) \geq 0$?

◊ **9.4.6** Cho $n \in \mathbb{N}^*$, $A \in \mathbf{GL}_n(\mathbb{R})$, $B \in \mathbf{M}_n(\mathbb{R})$.

Chứng minh rằng tồn tại $\varepsilon \in \mathbb{R}_+^*$ sao cho : $\forall x \in \mathbb{R},\ (|x| < \varepsilon \Rightarrow A + xB \in \mathbf{GL}_n(\mathbb{R}))$.

◊ **9.4.7** Cho $n \in \mathbb{N}^*$, $A, B \in \mathbf{M}_n(\mathbb{R})$ sao cho $AB - BA = B$.

a) Chứng minh : $\forall k \in \mathbb{N},\ AB^k = B^k(A + k\,\mathbf{1}_n)$.

b) Từ đó suy ra: $\det(B) = 0$.

9.5 Khai triển theo một hàng

9.5.1 Phần phụ đại số và định thức con

1) Xét trường hợp $n = 3$

Giả sử $A=(a_{ij})_{ij} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \in \mathrm{M}_3(K)$.

Theo định nghĩa (xem 9.4, Định nghĩa):

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_3} \varepsilon(\sigma) a_{\sigma(1)1} a_{\sigma(2)2} a_{\sigma(3)3}$$

Vì $\mathfrak{S}_3 = \{\mathrm{Id}, \tau_{12}, \tau_{13}, \tau_{23}, c, c'\}$, trong đó $c = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ và $c' = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, nên ta được:

$$\det(A) = a_{11} a_{22} a_{33} - a_{21} a_{12} a_{33} - a_{31} a_{22} a_{13} - a_{11} a_{32} a_{23} + a_{21} a_{32} a_{13} + a_{31} a_{12} a_{23}.$$

Ta có thể nhóm lại, chẳng hạn theo cách sau:

$$\det(A) = a_{11}(a_{22} a_{33} - a_{32} a_{23}) + a_{21}(-a_{12} a_{33} + a_{32} a_{13}) + a_{31}(a_{12} a_{23} - a_{22} a_{13})$$

$$= a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{21} \begin{vmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{vmatrix} + a_{31} \begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix},$$

và được *khai triển của* $\det(A)$ *theo cột thứ nhất*.

2) Trường hợp tổng quát

- Giả sử $A = (a_{ij})_{ij} \in \mathrm{M}_n(K)$.

Đặt $\mathcal{B} = (e_1,...,e_n)$ là cơ sở chính tắc của $\mathrm{M}_{n,1}(K)$:

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, e_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

và $C_1 = \begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix}, \ldots, C_n = \begin{pmatrix} a_{1n} \\ \vdots \\ a_{nn} \end{pmatrix}$ là các cột của A.

Giả sử $j \in \{1,...,n\}$.

Khai triển theo tính chất tuyến tính đối với cột thứ j :

$$\det(A) = \det_{\mathcal{B}}\left(C_1,\ldots,C_{j-1}, \sum_{i=1}^{n} a_{ij} e_i, C_{j+1},\ldots,C_n\right) = \sum_{i=1}^{n} a_{ij} A_{ij},$$

trong đó ta đã ký hiệu:

$$A_{ij} = \det_j(C_1, \ldots, C_{j-1}, e_i, C_{j+1}, C_n) = \begin{vmatrix} a_{11} & \cdots & a_{1j-1} & 0 & a_{1j+1} & \cdots & a_{1n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ \vdots & & \vdots & 0 & \vdots & & \vdots \\ \vdots & & \vdots & 1 & \vdots & & \vdots \\ \vdots & & \vdots & 0 & \vdots & & \vdots \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & \cdots & a_{nj-1} & 0 & a_{nj+1} & \cdots & a_{nn} \end{vmatrix}$$

"1" nằm ở hàng thứ i.

Trong định thức trên ta đưa cột thứ j về cột cuối cùng, nghĩa là hoán vị các cột theo hoán vị sau:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & j-1 & j & j+1 & \cdots & n \\ 1 & 2 & \cdots & j-1 & n & j & \cdots & n-1 \end{pmatrix}$$

hoán vị này có đúng $(n\text{-}1) - j + 1$ nghịch thế (nó cũng là tích của $n - j$ chuyển vị kiểu $\tau_{k,k+1}$).

$$A_{ij} = (-1)^{n-j} \begin{vmatrix} a_{11} & \cdots & a_{1j-1} & a_{1j+1} & \cdots & a_{1n} & 0 \\ \vdots & & & \vdots & & \vdots & \vdots \\ \vdots & & & \vdots & & \vdots & 1 \\ \vdots & & & \vdots & & \vdots & \vdots \\ a_{n1} & \cdots & a_{nj-1} & a_{nj+1} & \cdots & a_{nn} & 0 \end{vmatrix}$$

Bây giờ, theo cách tương tự, ta đưa dòng thứ i về dòng cuối cùng:

$$A_{ij} = (-1)^{n-j}(-1)^{n-i} \begin{vmatrix} a_{11} & \cdots & a_{1j-1} & a_{1j+1} & \cdots & a_{1n} & 0 \\ \vdots & & & & & & \vdots \\ a_{i-11} & \cdots & a_{i-1j-1} & a_{i-1j+1} & \cdots & a_{i-1n} & 0 \\ a_{i+11} & \cdots & a_{i+1j-1} & a_{i+1j+1} & \cdots & a_{i+1n} & 0 \\ \vdots & & & \vdots & & \vdots & \vdots \\ a_{n1} & \cdots & a_{nj-1} & a_{nj+1} & \cdots & a_{nn} & 0 \\ a_{i1} & \cdots & a_{ij-1} & a_{ij+1} & \cdots & a_{in} & 1 \end{vmatrix}$$

• Xét một ma trận bất kỳ $B = (b_{uv})_{uv}$ thuộc $\mathbf{M}_{n,n-1}(K)$, và

$$B' = \begin{pmatrix} b_{11} & \cdots & b_{1n-1} & 0 \\ \vdots & & \vdots & \vdots \\ b_{n-11} & \cdots & b_{n-1n-1} & 0 \\ b_{n1} & \cdots & b_{nn-1} & 1 \end{pmatrix} \in \mathbf{M}_n(K).$$

Đặt $B' = (b'_{uv})_{uv}$, ta có:

$$b'_{uv} = \begin{cases} b_{uv} & \text{nếu } v \le n-1 \\ 1 & \text{nếu } u = v = n \\ 0 & \text{trong các trường hợp khác.} \end{cases}$$

Theo định nghĩa : $\det(B') = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) b'_{\sigma(1)1} \dots b'_{\sigma(n)n}$.

Với mọi $\sigma \in \mathfrak{S}_n$ sao cho $\sigma(n) \neq n$, ta có $b'_{\sigma(n)n} = 0$. Vì $b'_{nn} = 1$, nên ta có:

$$\det(B') = \sum_{\substack{\sigma \in \mathfrak{S}_n \\ \sigma(n)=n}} \varepsilon(\sigma) b'_{\sigma(1)1} \dots b'_{\sigma(n-1)n-1}.$$

Rõ ràng ánh xạ $\{\sigma \in \mathfrak{S}_n ; \sigma(n) = n\} \to \mathfrak{S}_{n-1}$, trong đó ρ được xác định bởi :

$$\sigma \mapsto \rho$$

$\forall k \in \{1,\dots, n-1\}$, $\rho(k) = \sigma(k)$, là một song ánh bảo toàn dấu.

Do đó:

$$\det(B') = \sum_{\rho \in \mathfrak{S}_{n-1}} \varepsilon(\rho) b'_{\rho(1)1} \dots b'_{\rho(n-1)n-1} = \sum_{\rho \in \mathfrak{S}_{n-1}} \varepsilon(\rho) b_{\rho(1)1} \dots b_{\rho(n-1)n-1}.$$

- Áp dụng kết quả này vào định thức thu được đối với A_{ij}, ta đi đến

$$A_{ij} = (-1)^{i+j} \begin{vmatrix} a_{11} & \dots & a_{1j-1} & a_{1j+1} & \dots & a_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{i-11} & & a_{i-1j-1} & a_{i-1j+1} & & a_{i-1n} \\ a_{i+11} & & a_{i+1j-1} & a_{i+1j+1} & & a_{i+1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n1} & \dots & a_{nj-1} & a_{nj+1} & \dots & a_{nn} \end{vmatrix}$$

3) Phát biểu kết quả

Cho $n \in \mathbb{N}^*$.

♦ **Định nghĩa** Cho $A = (a_{ij})_{ij} \in \mathbf{M}_n(K)$.

1) Với mỗi (i,j) thuộc $\{1,\dots,n\}^2$, **định thức con của vị trí** (i,j) **trong** A (hoặc theo cách nói lạm dụng : định thức con của a_{ij} trong A) là định thức cấp $n-1$, Δ_{ij} nhận được bằng cách trong A bỏ đi dòng thứ i và cột thứ j :

$$\Delta_{ij} = \begin{vmatrix} a_{11} & \dots & a_{1j-1} & a_{1j+1} & \dots & a_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{i-11} & \dots & a_{i-1j-1} & a_{i-1j+1} & \dots & a_{i-1n} \\ a_{i+11} & \dots & a_{i+1j-1} & a_{i+1j+1} & \dots & a_{i+1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n1} & \dots & a_{nj-1} & a_{nj+1} & \dots & a_{nn} \end{vmatrix}$$

2) Với mỗi (i,j) thuộc $\{1,...,n\}^2$ **phần phụ đại số của vị trí** (i,j) **trong** A (hoặc theo cách nói lạm dụng : phần phụ đại số của a_{ij} trong A), ký hiệu là A_{ij}, là tích của $(-1)^{i+j}$ với định thức con của vị trí (i,j) trong A :

$$A_{ij} = (-1)^{i+j}\,\Delta_{ij}.$$

NHẬN XÉT:

Các phần tử của A nằm ở dòng thứ i và các phần tử nằm ở cột thứ j không tham gia vào việc tính Δ_{ij} và A_{ij}. ■

Hàng của một ma trận hay một định thức, là mọi dòng hoặc cột của ma trận hay định thức đó.

♦ **Mệnh đề (Khai triển định thức theo một hàng)**

Giả sử $A = (a_{ij})_{ij} \in \mathbf{M}_n(K)$. Ta có:

1) $\forall j \in \{1,...,n\}$, $\det(A) = \sum_{i=1}^{n} a_{ij} A_{ij}$ (khai triển $\det(A)$ theo cột thứ j)

2) $\forall i \in \{1,...,n\}$, $\det(A) = \sum_{j=1}^{n} a_{ij} A_{ij}$ (khai triển $\det(A)$ theo dòng thứ i).

Chứng minh :

1) Xem trên đây.

2) Áp dụng 1) vào ${}^tA$ thay vì A, ta sẽ suy ra 2).

VÍ DỤ:

Khai triển theo cột thứ 4:

$$\begin{vmatrix} 2 & 6 & -3 & 4 \\ 1 & 3 & 4 & -5 \\ 4 & 1 & 2 & 0 \\ -3 & 0 & 3 & 6 \end{vmatrix} = -4\begin{vmatrix} 1 & 3 & 4 \\ 4 & 1 & 2 \\ -3 & 0 & 3 \end{vmatrix} - 5\begin{vmatrix} 2 & 6 & -3 \\ 4 & 1 & 2 \\ -3 & 0 & 3 \end{vmatrix} + 6\begin{vmatrix} 2 & 6 & -3 \\ 1 & 3 & 4 \\ 4 & 1 & 2 \end{vmatrix}$$

$$= -4\left(-3\begin{vmatrix} 3 & 4 \\ 1 & 2 \end{vmatrix} + 3\begin{vmatrix} 1 & 3 \\ 4 & 1 \end{vmatrix}\right) - 5\left(-3\begin{vmatrix} 6 & -3 \\ 1 & 2 \end{vmatrix} + 3\begin{vmatrix} 2 & 6 \\ 4 & 1 \end{vmatrix}\right)$$

$$+ 6\left(2\begin{vmatrix} 3 & 4 \\ 1 & 2 \end{vmatrix} - \begin{vmatrix} 6 & -3 \\ 1 & 2 \end{vmatrix} + 4\begin{vmatrix} 6 & -3 \\ 3 & 4 \end{vmatrix}\right)$$

$$= 1437.$$

NHẬN XÉT:

1) Để tiện thông thường ta khai triển một định thức theo một hàng nếu hàng đó có ít hạng tử khác không (nhiều hạng tử bằng không).

2) Trong việc tính toán bằng số các định thức, có những phương pháp nhanh hơn hẳn phương pháp khai triển theo các hàng.

9.5.2 Ma trận phụ hợp

Cho $n \in \mathbb{N}^*$.

♦ **Định nghĩa** Cho $A = (a_{ij})_{ij} \in \mathbf{M}_n(K)$. **Ma trận phụ hợp của** A là ma trận vuông cấp n, ký hiệu là com(A), được xác định bởi:

$$\text{com}(A) = (A_{ij})_{ij} = \begin{pmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & & \vdots \\ A_{n1} & \cdots & A_{nn} \end{pmatrix},$$

trong đó A_{ij} là phần phụ đại số của vị trí (i, j) trong A.

Chúng ta đã thấy (9.5.1, Mệnh đề) rằng:

$$\forall j \in \{1,\ldots,n\}, \quad \sum_{i=1}^{n} a_{ij} A_{ij} = \det(A).$$

Ta chú ý tới $\sum_{i=1}^{n} a_{ij} A_{ik}$, với $(j, k) \in \{1,\ldots,n\}^2$ cố định sao cho $j \neq k$.

Xét ma trận $B = (b_{ip})_{ip}$ nhận được từ A bằng cách thay thế trong A, cột thứ k bởi cột thứ j của A :

$$B = \begin{pmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1k-1} & a_{1j} & a_{1k+1} & \cdots & a_{1n} \\ \vdots & & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & \cdots & a_{nj} & \cdots & a_{nk-1} & a_{nj} & a_{nk+1} & \cdots & a_{nn} \end{pmatrix}$$

cột thứ k

Một mặt, $\det(B) = 0$, vì B có hai cột bằng nhau.

Mặt khác, nếu khai triển $\det(B)$ theo cột thứ k, ta sẽ có:

$$\det(B) = \sum_{i=1}^{n} b_{ik} B_{ik} = \sum_{i=1}^{n} a_{ij} A_{ik},$$

vì các phần phụ đại số của các phần tử của cột thứ k trong B và trong A là như nhau.

Do đó: $\sum_{i=1}^{n} a_{ij} A_{ik} = 0$.

Như vậy ta đã chứng minh:

$$\forall (j, k) \in \{1,\ldots,n\}^2, \ \sum_{i=1}^{n} a_{ij} A_{ik} = \begin{cases} \det(A) & \text{nếu } j = k \\ 0 & \text{nếu } j \neq k \end{cases}$$

Nhưng với $(j, k) \in \{1,\ldots,n\}^2$, $\sum_{i=1}^{n} a_{ij} A_{ik}$ là phần tử thứ (j,k) của tích ${}^tA$ với com(A), do đó:

$${}^tA.\text{com}(A) = \begin{pmatrix} \det(A) & & 0 \\ & \ddots & \\ 0 & & \det(A) \end{pmatrix} = \det(A)\mathrm{I}_n.$$

Áp dụng kết quả này cho ${}^tA$ thay vì A và nhận xét rằng $\text{com}({}^tA) = {}^t\text{com}(A)$ và $\det({}^tA) = \det(A)$ (xem 9.4, Mệnh đề 2, 6)), ta được:

$$A.\,{}^t\text{com}(A) = \det(A)\mathbf{I}_n,$$

và chuyển vị kết quả của trang trước: ${}^t\text{com}(A).A = \det(A).\mathbf{I}_n$

Ta phát biểu kết quả đạt được:

♦ Định lý

$$\forall A \in \mathbf{M}_n(K), \quad A \cdot {}^t\text{com}(A) = {}^t\text{com}(A) \cdot A = \det(A)\mathbf{I}_n.$$

♦ Hệ quả

$$\forall A \in \mathbf{GL}_n(K), \quad A^{-1} = \frac{1}{\det(A)}\ {}^t\text{com}(A).$$

VÍ DỤ:

Với $n = 2$, nếu $ad - bc \neq 0$, thì $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ khả nghịch, và

$$A^{-1} = \frac{1}{ad - bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

NHẬN XÉT:

Công thức trên cho ta A^{-1} thông qua $\text{com}(A)$, trong thực tế gần như không sử dụng được ngay khi $n \geq 3$. Thực vậy, nói chung công thức này yêu cầu tính một định thức cấp n ($\det(A)$) và n^2 định thức cấp n -1 (các phần phụ đại số trong A).

Bài tập

◊ **9.5.1** Cho $n \in \mathbb{N}^*$, $M \in \mathbf{M}_n(K)$, $A = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & M & \\ 0 & & \end{pmatrix} \in \mathbf{M}_{n+1}(K)$. Tính $\text{com}(A)$.

◊ **9.5.2** Giả sử $n, p \in \mathbb{N}^*$, $A \in \mathbf{M}_n(K)$. Chứng minh rằng:

$$A^p = \mathbf{I}_n \Rightarrow (\text{com}(A))^p = \mathbf{I}_n$$

◊ **9.5.3** Cho $n \in \mathbb{N}^*$. Chứng minh rằng: $\forall A \in \mathbf{GL}_n(K)$, $\begin{cases} \text{com}(A) \in \mathbf{GL}_n(K) \\ (\text{com}(A))^{-1} = \text{com}(A^{-1}). \end{cases}$

9.6 Tính định thức

9.6.1 Định thức của ma trận tam giác

(Xem thêm 9.4, Ví dụ 2)).

◆ **Mệnh đề** Định thức của một ma trận tam giác bằng tích các phần tử chéo:

$$\begin{vmatrix} a_{11} & & \cdots \\ & \ddots & \\ 0 & & a_{nn} \end{vmatrix} = \prod_{i=1}^{n} a_{ii}.$$

Chứng minh:

Quy nạp theo n. Tính chất hiển nhiên đúng cho $n = 1$.

Giả sử nó đúng cho một n thuộc $\mathbb{N}^*$, và giả sử $A = \begin{pmatrix} a_{11} & & \cdots \\ & \ddots & \\ 0 & & a_{n+1\,n+1} \end{pmatrix} \in \mathrm{T}_{n+1,\,I}(K)$

Khai triển $\det(A)$ theo dòng thứ $n + 1$, ta nhận được:

$$\det(A) = \begin{vmatrix} a_{11} & & \cdots \\ & \ddots & \\ 0 & & a_{nn} \end{vmatrix} a_{n+1\,n+1} = (a_{11} \dots a_{nn})\, a_{n+1\,n+1} = \prod_{i=1}^{n+1} a_{ii}.$$

NHẬN XÉT:

Nói riêng, định thức của một ma trận chéo bằng tích các phần tử chéo.

9.6.2 Thao tác trên dòng và cột

1) Sử dụng tính đa tuyến tính

Tính chất đa tuyến tính của định thức được thể hiện dưới dạng sơ đồ như sau:

$$\begin{vmatrix} \boxed{\text{I}} & \begin{matrix} \lambda a_{1j} + b_{1j} \\ \vdots \\ \lambda a_{nj} + b_{nj} \end{matrix} & \boxed{\text{II}} \end{vmatrix} = \lambda \begin{vmatrix} \boxed{\text{I}} & \begin{matrix} a_{1j} \\ \vdots \\ a_{nj} \end{matrix} & \boxed{\text{II}} \end{vmatrix} + \begin{vmatrix} \boxed{\text{I}} & \begin{matrix} b_{1j} \\ \vdots \\ b_{nj} \end{matrix} & \boxed{\text{II}} \end{vmatrix}$$

2) Để định thức của một ma trận bằng không, thì cần và đủ là các cột của ma trận đó phụ thuộc tuyến tính (xem 9.4, Mệnh đề 2, 4). Đặc biệt nếu một định thức có một cột bằng không hoặc hai cột đồng phương, thì định thức ấy bằng không.

Ta có kết quả tương tự đối với các dòng.

3) Thay một cột bằng tổng của cột đó với một tổ hợp tuyến tính các cột khác

Giả sử $A = (a_{ij})_{ij} \in \mathbf{M}_n(K)$, $C_1,...,C_n$ là các cột của A, $j \in \{1,...,n\}$, $(\alpha_k)_{k\neq j} \in K^{n-1}$.

Xét ma trận B nhận được từ A bằng cách thay C_j *bằng* $Cj + \sum_{k\neq j}\alpha_k C_k$.

Gọi $\mathcal{B} = (e_1, ..., e_n)$ là cơ sở chính tắc của $\mathbf{M}_{n,1}(K)$, ta có:

$$\det(B) = \det_{\mathcal{B}}\left(C_1,..., C_j + \sum_{k\neq j}\alpha_k C_k ,..., C_n\right)$$

$$= \det_{\mathcal{B}}(C_1,..., C_j,..., C_n) + \sum_{k\neq j}\alpha_k \det_{\mathcal{B}}(C_1,...,C_{j-1},C_k,C_{j+1},..C_n)$$

$$= \det(A),$$

vì mỗi $\det_{\mathcal{B}}(C_1,..., C_{j-1},C_k,C_{j+1},..., C_n)$ chứa hai lần cột C_k.

Như vậy:

Ta không làm thay đổi giá trị của một định thức khi thay một cột bằng tổng của cột đó với một tổ hợp tuyến tính của các cột khác.

Ta có kết quả tương tự đối với các dòng.

NHẬN XÉT:

Cũng có thể chứng minh kết quả trên từ nhận xét rằng: $B = AF$, trong đó:

$$F = \begin{pmatrix} 1 & & 0 & & \alpha_1 & & \\ & \ddots & & & \vdots & & 0 \\ & & 1 & & \alpha_{j-1} & & \\ & & & & 1 & & \\ & & & & \alpha_{j+1} & & \\ 0 & & & & \vdots & \ddots & \\ & & & & \alpha_n & & 1 \end{pmatrix}$$

và khai triển $\det(F)$ theo cột thứ nhất, $j - 1$ lần:

$$\det(F) = \begin{pmatrix} 1 & & 0 \\ \alpha_{j+1} & \ddots & \\ \vdots & & 1 \\ \alpha_n & & \end{pmatrix},$$

và sau đó (ma trận tam giác): $\det(F) = 1$.

4) Thay thế đồng thời nhiều cột

Giả sử $A = (a_{ij})_{ij} \in \mathbf{M}_n(K)$, $C_1,...,C_n$ là các cột của A. Ta sẽ chứng minh rằng có thể thay trong A mỗi cột bởi tổng của cột đó với một tổ hợp tuyến tính của các cột *tiếp theo* mà không làm thay đổi $\det(A)$.

Với mỗi k thuộc $\{2,...,n\}$, xét $\alpha_{kk-1},...,\alpha_{n\,k-1} \in K$.

Xét ma trận B nhận được từ A bằng cách thay:

C_1 bởi $C_1 + \alpha_{21}C_2 + ... + \alpha_{n1}C_n$

C_2 bởi $C_2 + \alpha_{32}C_3 + ... + \alpha_{n2}C_n$

$\vdots$

C_{n-1} bởi $C_{n-1} + \alpha_{n\,n-1}C_n$

C_n bởi C_n

Đặt $T = \begin{pmatrix} 1 & & & 0 \\ \alpha_{21} & 1 & & \\ \alpha_{31} & \alpha_{32} & 1 & \\ \vdots & \vdots & \ddots & \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{n\,n-1} \quad 1 \end{pmatrix}$, ta có: $B = AT$, do đó :

$\det(B) = \det(A)\det(T) = \det(A) \cdot 1 = \det(A)$ (xem 9.6.1, Mệnh đề).

Như vậy:

Ta không làm thay đổi giá trị của một định thức khi thay (đồng thời) mỗi cột bằng tổng của cột đó với một tổ hợp tuyến tính của các cột tiếp theo.

Tương tự, bằng cách sử dụng phép nhân sau A với một ma trận tam giác trên:

Ta không làm thay đổi giá trị của một định thức khi thay (đồng thời) mỗi cột bởi tổng của cột đó với một tổ hợp tuyến tính của các cột đứng trước nó.

Ta có những kết quả tương tự đối với các dòng.

VÍ DỤ:

Với $(a, b) \in K^2$ và $n \geq 2$, hãy tính $\begin{vmatrix} a & & b \\ & \ddots & \\ b & & a \end{vmatrix}_{[n]}$

$$\begin{vmatrix} a & b & & \\ b & a & & \\ & & \ddots & \\ & & & a \end{vmatrix}_{[n]} = \begin{vmatrix} a+(n-1)b & b & \cdots & b \\ \vdots & & & \\ a+(n-1)b & & & \end{vmatrix} \begin{matrix} a & b & & \\ b & a & & \\ & & \ddots & \\ & & & a \end{matrix}_{[n]} \qquad C_1 \leftarrow C_1 + \sum_{j=2}^{n} C_j$$

$$= (a+(n-1)b) \begin{vmatrix} 1 & b & \cdots & b \\ \vdots & & & \\ 1 & & & \end{vmatrix} \begin{matrix} a & b & & \\ b & a & & \\ & & \ddots & \\ & & & a \end{matrix}_{[n]}$$

$$= (a+(n-1)b) \begin{vmatrix} 1 & b & \cdots & b \\ 0 & a-b & & \\ \vdots & & \ddots & \\ 0 & & & a-b \end{vmatrix}_{[n]} \begin{matrix} D_2 \leftarrow D_2 - D_1 \\ \vdots \\ D_n \leftarrow D_n - D_1 \end{matrix}$$

$$= (a + (n-1)b)\,(a-b)^{n-1}.$$

9.6.3 Trường hợp $n = 2$, $n = 3$

1) $n = 2$: $\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{21}a_{12}$

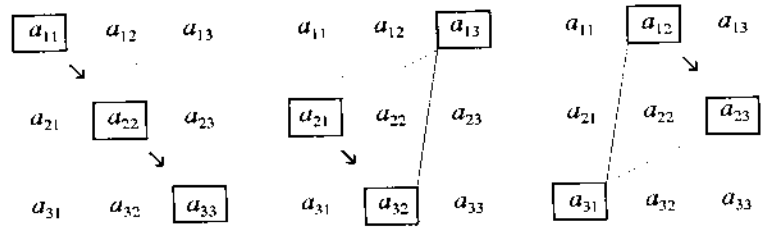
2) $n = 3$: $\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} - a_{21}a_{12}a_{33} - a_{31}a_{22}a_{13}$

$$- a_{11}a_{32}a_{23} + a_{21}a_{32}a_{13} - a_{31}a_{12}a_{23}$$

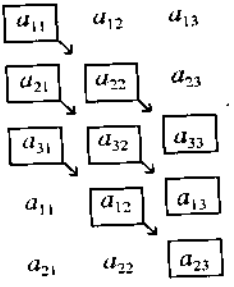
(xem 9.5.1, *1*)).

Có thể tìm được kết quả này bằng **quy tắc Sarrus**: định thức cấp 3 chứa 6 hạng tử (xem 9.4, Định nghĩa):

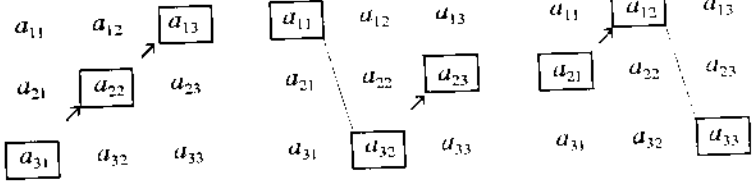
• $a_{11}a_{22}a_{33}$, $a_{21}a_{32}a_{33}$, $a_{31}a_{12}a_{23}$ tương ứng với các "đường chéo đi xuống":



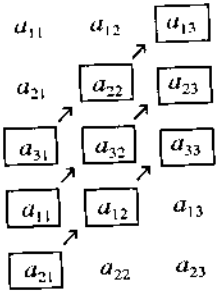
hoặc viết thêm 2 dòng xuống phía dưới:



• $-a_{31}a_{22}a_{13}$, $-a_{11}a_{32}a_{23}$, $-a_{21}a_{32}a_{13}$ tương ứng với các "đường chéo đi lên"



hoặc:



Nhưng cần chú ý: quy tắc Sarrus chỉ được áp dụng với $n = 3$ (và $n = 2$).

VÍ DỤ:

$$\begin{vmatrix} a & p & q \\ -p & a & r \\ -q & -r & a \end{vmatrix} = a^3 + pqr - pqr + aq^2 + ar^2 + ap^2 = a(a^2 + p^2 + q^2 + r^2).$$

9.64 Định thức Vandermonde

Cho $n \in \mathbb{N}^*$.

♦ **Định nghĩa** Giả sử $(x_1,...,x_n) \in K^n$. **Định thức Vandermonde**, ký hiệu là $V(x_1, ...,x_n)$, là phần tử của K xác định bởi:

$$V(x_1, ...,x_n) = \begin{vmatrix} 1 & x_1 & x_1^2 & x_1^{n-1} \\ | & \vdots & \vdots & \vdots \\ | & \vdots & \vdots & \vdots \\ 1 & x_n & x_n^2 & x_n^{n-1} \end{vmatrix} = \det((x_i^{j-1})_{1 \le i,j \le n}).$$

Ta tính $V(x_1, ..., x_n)$.

Nếu $n = 1$: $V(x_1) = 1$.

Nếu $n = 2$: $V(x_1, x_2) = \begin{vmatrix} 1 & x_1 \\ 1 & x_2 \end{vmatrix} = x_2 - x_1$.

Nếu $n = 3$: $V(x_1, x_2, x_3) = \begin{vmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ 1 & x_2 - x_1 & x_2^2 - x_1 x_2 \\ 1 & x_3 - x_1 & x_3^2 - x_1 x_3 \end{vmatrix}$

$C_2 \leftarrow C_2 - x_1 C_1, C_3 \leftarrow C_3 - x_1 C_2$

$= (x_2 - x_1)(x_3 - x_1) \begin{vmatrix} 1 & x_2 \\ 1 & x_3 \end{vmatrix} = (x_2 - x_1)(x_3 - x_1)(x_3 - x_2)$.

Với mọi n thuộc $\mathbb{N}$ mà $n \geq 3$:

$$V(x_1, ..., x_n) = \begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix}$$

$$= \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & x_2 - x_1 & x_2^2 - x_1 x_2 & \cdots & x_2^{n-1} - x_1 x_2^{n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n - x_1 & x_n^2 - x_1 x_n & \cdots & x_n^{n-1} - x_1 x_n^{n-2} \end{vmatrix}$$

$C_2 \leftarrow C_2 - x_1 C_1, C_3 \leftarrow C_3 - x_1 C_2, ..., C_n \leftarrow C_n - x_1 C_{n-1}$

$$= \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & x_2 - x_1 & (x_2 - x_1)x_2 & \cdots & (x_2 - x_1)x_2^{n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n - x_1 & (x_n - x_1)x_n & \cdots & (x_n - x_1)x_n^{n-2} \end{vmatrix}$$

$$= (x_2 - x_1) ... (x_n - x_1) \begin{vmatrix} 1 & x_2 & \cdots & x_2^{n-2} \\ \vdots & \vdots & & \vdots \\ 2 & x_n & \cdots & x_n^{n-2} \end{vmatrix},$$

ta đã khai triển theo dòng thứ nhất, sau đó nhân tử hóa trong mỗi dòng.

Như vậy ta được: $V(x_1,...,x_n) = \left(\prod_{n \geq i > 1} (x_i - x_1) \right) V(x_2,...,x_n)$

Bằng quy nạp ta kết luận:

♦ **Mệnh đề**

$$\forall n \in \mathbb{N}^*, \forall (x_1,...,x_n) \in K^n, V(x_1,...,x_n) = \prod_{n \geq i > j \geq n} (x_i - x_j).$$

♦ **Hệ quả** Với mọi $(x_1,..., x_n)$ thuộc K^n, $V(x_1,..., x_n)$ khác không khi và chỉ khi $x_1,..., x_n$ khác nhau từng đôi một.

Bài tập

◊ **9.6.1** Tính các định thức sau:

a) $$\begin{vmatrix} 1^2 & 2^2 & 3^2 & \cdots & n^2 \\ 2^2 & 3^2 & 4^2 & \cdots & (n+1)^2 \\ 3^2 & 4^2 & 5^2 & \cdots & (n+2)^2 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ n^2 & (n+1)^2 & (n+2)^2 & \cdots & (2n-1)^2 \end{vmatrix}, n \in \mathbb{N}^*$$

b) $$\begin{vmatrix} S_1 & S_1 & S_1 & \cdots & S_1 \\ S_1 & S_2 & S_2 & \cdots & S_2 \\ S_1 & S_2 & S_3 & \cdots & S_3 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ S_1 & S_2 & S_3 & \cdots & S_n \end{vmatrix}, n \in \mathbb{N}^*, S_k = \sum_{i=1}^{k} i$$

c) $$\begin{vmatrix} a_1 & a_2 & \cdots & a_n \\ & \ddots & \ddots & \vdots \\ & & \ddots & a_2 \\ & a_1 & & a_1 \end{vmatrix}, n \in \mathbb{N}^*, a_1,...,a_n \in K$$

d) $$\begin{vmatrix} a_1+b_1 & a_1 & a_1 & \cdots & a_1 \\ a_2 & a_2+b_2 & a_2 & \cdots & a_2 \\ a_3 & a_3 & a_3+b_3 & \cdots & a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_n & a_n & a_n & \cdots & a_n+b_n \end{vmatrix}, n \in \mathbb{N}^*, a_1,...,a_n, b_1,...,b_n \in K$$

e) $$\begin{vmatrix} a_1 & -a_1 & 0 & \cdots & 0 \\ -a_1 & a_1+a_2 & -a_2 & \ddots & \vdots \\ 0 & -a_2 & a_2+a_3 & \ddots & 0 \\ \vdots & \ddots & \ddots & a_{n-2}+a_{n-1} & -a_{n-1} \\ 0 & \cdots & 0 & -a_{n-1} & a_{n-1}+a_n \end{vmatrix},$$

$n \in \mathbb{N}^*, a_1,...,a_n \in K$

f) $\begin{vmatrix} a & b & & & 0 \\ c & & & & \\ & & & & b \\ & 0 & & c & a \end{vmatrix}_{[n]}$, $n \in \mathbb{N}^*$, $(a,b,c) \in \mathbb{C}^3$

(biểu diễn đáp số theo các không điểm phức của $X^2 - aX + bc$)

g) $\det\left((C_{i+j}^{j})_{0\le i,j\le n}\right) = \begin{vmatrix} C_0^0 & C_1^1 & \cdots & C_n^n \\ C_1^0 & C_2^1 & \cdots & C_{n+1}^n \\ \vdots & \vdots & \cdots & \vdots \\ C_n^0 & C_{n+1}^1 & \cdots & C_{2n}^n \end{vmatrix}_{[n+1]}$, $n \in \mathbb{N}$

h) $\begin{vmatrix} \alpha + a_1 & -1 & 0 & \cdots & 0 \\ a_2 & \alpha & -1 & \ddots & 0 \\ a_3 & 0 & \alpha & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & -1 \\ a_n & 0 & \cdots & 0 & \alpha \end{vmatrix}$ $n \in \mathbb{N}^*$, $\alpha, a_1, \ldots, a_n \in K$

i) $\begin{vmatrix} 1 & -a_1 & -a_2 & \cdots & -a_n \\ a_1 & b_1 & 0 & & \\ a_2 & 0 & b_2 & & 0 \\ \vdots & & & \ddots & \\ a_n & & 0 & & b_n \end{vmatrix}$, $n \in \mathbb{N}^*$, $a_1, \ldots, a_n, b_1, \ldots, b_n \in K$

j) $\begin{vmatrix} a & x & \cdots & x \\ y & z & & 0 \\ \vdots & & \ddots & \\ y & 0 & & z \end{vmatrix}_{[n]}$, $n \in \mathbb{N}^*$, $a, x, y, z \in K$

k) $\begin{vmatrix} -(a+1) & 1 & & 0 \\ a & -(a+2) & 2 & \\ & a & -(a+3) & \ddots \\ & & \ddots & n-1 \\ 0 & & a & -(a+n) \end{vmatrix}$, $n \in \mathbb{N}^*$, $a \in K$.

◊ **9.6.2** Chứng minh rằng: $E = \left\{ \begin{pmatrix} x & y & z \\ 2z & x & y \\ 2y & 2z & x \end{pmatrix} ; (x,y,z) \in \mathbb{Q}^3 \right\}$ là một thể con của vành $\mathbf{M}_3(\mathbb{Q})$.

◊ **9.6.3** Giả sử $A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & k \end{pmatrix} \in \mathbf{M}_3(\mathbb{R})$.

a) Chứng minh rằng không thể có: tích các phần tử trong mỗi dòng (của A) < 0 và tích các phần tử trong mỗi cột > 0.

b) Chứng minh rằng không thể có: sáu số hạng của $\det(A) = aek + bfg + cdh + (-ceg) + (-afh) + (-bdk)$ đều > 0.

◊ **9.6.4** Tính $\det(f)$, trong đó $f : \mathbf{M}_n(\mathbb{R}) \to \mathbf{M}_n(\mathbb{R})$, $X \mapsto {}^tX$.

◊ **9.6.5** Với $(p,x) \in \mathbb{N} \times \mathbb{R}$, đặt:

$$\varphi_p(x) = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 & x \\ & 2 & 0 & \cdots & 0 & x^2 \\ & 3 & 3 & \ddots & \vdots & \vdots \\ & 4 & 6 & \ddots & 0 & \vdots \\ & \vdots & \vdots & \ddots & C_p^{p-1} & x^p \\ 1 & C_{p+1}^1 & C_{p+1}^2 & \cdots & C_{p+1}^{p-1} & x^{p+1} \end{vmatrix}_{(p+1)}$$

a) Với $(p,x) \in \mathbb{N} \times \mathbb{R}$, hãy tính $\varphi_p(x+1) - \varphi_p(x)$.

b) Chứng minh: $\forall n \in \mathbb{N}^*$, $\varphi_p(n+1) = (p+1)! \sum_{k=1}^{n} k^p$.

c) Từ đó suy ra giá trị của $\sum_{k=1}^{n} k$, $\sum_{k=1}^{n} k^2$, $\sum_{k=1}^{n} k^3$ với $n \in \mathbb{N}^*$.

◊ **9.6.6** Giả sử $n \in \mathbb{N} - \{0,1\}$, $P_n = X^n - X + 1$. Gọi $x_1, \ldots, x_n$ là các không điểm của P_n trong $\mathbb{C}$.

Giả sử $A = (a_{ij})_{ij} \in \mathbf{M}_n(\mathbb{C})$, trong đó $a_{ij} = \begin{cases} 1 + x_i & \text{nếu } i = j \\ 1 & \text{nếu } i \neq j \end{cases}$. Hãy tính $\det(A)$.

◊ **9.6.7** Giả sử $n \in \mathbb{N}^*$, E là một K-kgv n chiều, $V_1, \ldots, V_n \in E$, $f \in \mathcal{L}(E)$, $\mathcal{B}$ là một cơ sở của E.

Chứng minh: $\sum_{j=1}^{n} \det_{\mathcal{B}}(V_1, \ldots, f(V_j), \ldots, V_n) = \mathrm{tr}(f) \det_{\mathcal{B}}(V_1, \ldots, V_n)$.

◊ **9.6.8** Giả sử $A = (a_{ij})_{ij} \in \mathbf{M}_n(\mathbb{R})$, sao cho: $\begin{cases} a_{ij} \in \mathbb{Z} \\ i \neq j \Rightarrow a_{ij} \text{ chẵn} \\ a_{ii} \text{ lẻ} \end{cases}$, với mọi (i,j) thuộc $\{1, \ldots, n\}^2$.

Chứng minh : $\det(A) \neq 0$

◊ **9.6.9** Cho $A = (a_{ij})_{ij} \in \mathbf{M}_n(\mathbb{R})$, sao cho:

$\begin{cases} a_{ij} \in \mathbb{Z} \\ i \neq j \Rightarrow a_{ij} \text{ lẻ} \\ a_{ij} \text{ chẵn} \end{cases}$, với mọi (i,j) thuộc $\{1, \ldots, n\}^2$. Chứng tỏ rằng, nếu n chẵn, thì $\det(A) \neq 0$.

9.7 Định hướng một không gian vectơ thực hữu hạn chiều

Giả sử $n \in \mathbb{N}^*$ và E là một $\mathbb{R}$-kgv n chiều. Ký hiệu $\beta(E)$ là tập hợp các cơ sở của E.

♦ **Định nghĩa 1** Ta nói hai cơ sở $\mathcal{B}$ và $\mathcal{B}'$ của E là :

- **cùng chiều** khi và chỉ khi : $\det_{\mathcal{B}}(\mathcal{B}') > 0$
- **ngược chiều nhau** khi và chỉ khi $\det_{\mathcal{B}}(\mathcal{B}') < 0$.

Vì $\mathbb{R}$ được sắp thứ tự toàn phần và với mọi cơ sở $\mathcal{B}$ và $\mathcal{B}'$ của E, $\det_{\mathcal{B}}(\mathcal{B}') \neq 0$, nên hai cơ sở đã cho hoặc cùng chiều hoặc ngược chiều nhau.

Gọi $\mathcal{R}$ là quan hệ xác định trong $\beta(E)$ bởi:

$$\forall\, \mathcal{B}, \mathcal{B}' \in \beta(E), \quad (\mathcal{B}\,\mathcal{R}\,\mathcal{B}' \Leftrightarrow \det_{\mathcal{B}'}(\mathcal{B}) > 0).$$

Quan hệ $\mathcal{R}$ là một quan hệ tương đương trong $\beta(E)$ vì với mọi $\mathcal{B}, \mathcal{B}', \mathcal{B}''$ thuộc $\beta(E)$:

- $\det_{\mathcal{B}}(\mathcal{B}) = 1 > 0$
- $\mathcal{B}\,\mathcal{R}\,\mathcal{B}' \Leftrightarrow \det_{\mathcal{B}'}(\mathcal{B}) > 0 \Rightarrow \det_{\mathcal{B}}(\mathcal{B}') = (\det_{\mathcal{B}'}(\mathcal{B}))^{-1} > 0 \Rightarrow \mathcal{B}'\,\mathcal{R}\,\mathcal{B}$
- $\begin{cases} \mathcal{B}\,\mathcal{R}\,\mathcal{B}' \\ \mathcal{B}'\,\mathcal{R}\,\mathcal{B}'' \end{cases} \Leftrightarrow \begin{cases} \det_{\mathcal{B}'}(\mathcal{B}) > 0 \\ \det_{\mathcal{B}''}(\mathcal{B}') > 0 \end{cases} \Rightarrow \det_{\mathcal{B}''}(\mathcal{B}) = \det_{\mathcal{B}''}(\mathcal{B}')\det_{\mathcal{B}'}(\mathcal{B}) > 0 \Rightarrow \mathcal{B}\,\mathcal{R}\,\mathcal{B}''$.

Vì $\mathbb{R}$ - kgv E là hữu hạn chiều, nên nó có ít nhất một cơ sở $\mathcal{B}_1 = (e_1,..,e_n)$; xét $\mathcal{B}_2 = (-e_1, e_2,...,e_n)$, đó là một cơ sở của E. Vì $\det_{\mathcal{B}_1}(\mathcal{B}_2) = -1 < 0$, nên $\mathcal{B}_1$ và $\mathcal{B}_2$ ngược chiều nhau.

Giả sử $\mathcal{B} \in \beta(E)$.

- Nếu $\det_{\mathcal{B}_1}(\mathcal{B}) > 0$, thì $\mathcal{B}_1\,\mathcal{R}\,\mathcal{B}$
- Nếu $\det_{\mathcal{B}_1}(\mathcal{B}) < 0$, thì $\det_{\mathcal{B}_2}(\mathcal{B}) = \det_{\mathcal{B}_2}(\mathcal{B}_1)\det_{\mathcal{B}_1}(\mathcal{B}) = -\det_{\mathcal{B}_1}(\mathcal{B}) > 0$, do vậy $\mathcal{B}_2\,\mathcal{R}\,\mathcal{B}$.

Điều đó chứng tỏ $\beta(E)$ có đúng hai lớp tương đương modulo $\mathcal{R}$, đó là lớp của $\mathcal{B}_1$ và lớp của $\mathcal{B}_2$. Do đó ta có định nghĩa sau:

♦ **Định nghĩa 2** **Định hướng** E là việc chọn, trong tập hợp $\beta(E)$ các cơ sở của E, một trong hai lớp tương đương modulo quan hệ "cùng chiều". Các cơ sở thuộc lớp này được gọi là **thuận**, các cơ sở khác (các cơ sở thuộc lớp kia) được gọi là **nghịch**. Khi đó ta nói E là một $\mathbb{R}$ - kgv **định hướng**.

Ta quy ước cơ sở chính tắc của $\mathbb{R}^n$ là thuận (điều đó tương đương với việc chọn một hướng trong $\mathbb{R}^n$).

Trục là mọi đường thẳng vectơ định hướng. ■

Cho $f \in GL(E)$. Vì $\det(f) \neq 0$ nên ta có: $\det(f) > 0$ hoặc $\det(f) < 0$.

Cho $\mathcal{B} \in \beta(E)$.

- Nếu $\det(f) > 0$, thì $\det_{\mathcal{B}}(f(\mathcal{B})) = \det(f) > 0$ và vì vậy $\mathcal{B}$ và $f(\mathcal{B})$ cùng chiều
- Nếu $\det(f) < 0$, thì $\det_{\mathcal{B}}(f(\mathcal{B})) = \det(f) < 0$ và vì vậy $\mathcal{B}$ và $f(\mathcal{B})$ ngược chiều nhau.

Từ đó ta có định nghĩa sau:

♦ **Định nghĩa 3** Giả sử $f \in GL(E)$. Ta nói rằng:

- f **bảo toàn hướng** (hoặc: **là thuận**) khi và chỉ khi: $\det(f) > 0$
- f **đổi hướng** (hoặc: **là nghịch**) khi và chỉ khi: $\det(f) < 0$.

♦ **Mệnh đề** Giả sử $f \in GL(E)$.

1) Nếu f bảo toàn hướng, thì với mọi cơ sở $\mathcal{B}$ của E, $f(\mathcal{B})$ là một cơ sở cùng chiều với $\mathcal{B}$.
2) Nếu f đổi hướng, thì với mọi cơ sở $\mathcal{B}$ của E, $f(\mathcal{B})$ là một cơ sở ngược chiều với $\mathcal{B}$.

9.8 Hạng và ma trận con

Nhắc lại về hạng

Chúng ta đã định nghĩa:

- hạng của một họ hữu hạn phần tử $\mathcal{F}$ của một K-kgv E:

$$\text{rank}(\mathcal{F}) = \dim(\text{Vect}(\mathcal{F})), \quad \text{6.4, Định nghĩa 3}$$

- hạng của một ánh xạ tuyến tính $f \in \mathcal{L}(E, F)$

$$\text{rank}(f) = \dim(\text{Im}(f)), \quad \text{7.3.1, Định nghĩa}$$

- hạng của một ma trận A thuộc $\mathbf{M}_{n,p}(K)$:

$$\text{rank}(A) = \text{rank}(C_1, \ldots, C_p) \quad \text{8.1.6, Định nghĩa}$$

trong đó $C_1, \ldots, C_p$ là các cột của A.

Các khái niệm này có liên quan mật thiết với nhau :

- Hạng của một họ hữu hạn phần tử $\mathcal{F}$ của E cũng là hạng của ma trận có các cột được tạo nên bởi các thành phần của các phần tử của $\mathcal{F}$ trong một cơ sở của E.

- Với mọi cơ sở $\mathcal{B} = (e_1, \ldots, e_n)$ của E, hạng của $f \in \mathcal{L}(E, F)$ là hạng của họ $(f(e_i))_{1 \leq i \leq n}$, và cũng là hạng của bất kỳ ma trận nào biểu diễn f.

- Hạng của một ma trận A thuộc $\mathbf{M}_{n,p}(K)$ là hạng của bất kỳ ánh xạ tuyến tính nào được biểu diễn bởi A.

Cuối cùng ta nhắc lại định lý về hạng (7.3.1, Định lý 1) :

$$\forall f \in \mathcal{L}(E, F), \quad \text{rank}(f) = \dim E - \dim(\text{Ker}(f)). \qquad \blacksquare$$

◆ **Định nghĩa** Giả sử $(n, p) \in (\mathbb{N}^*)^2$, $A = (a_{ij})_{ij} \in \mathbf{M}_{n,p}(K)$, $(u, v) \in (\mathbb{N}^*)^2$,

$\begin{cases} (i_1, \ldots, i_u) \in \{1, \ldots, n\}^u \text{ sao cho } i_1 < \ldots < i_u \\ (j_1, \ldots, j_v) \in \{1, \ldots, p\}^v \text{ sao cho } j_1 < \ldots < j_v. \end{cases}$

Ma trận con (hoặc : **ma trận được trích ra**) của A, bằng cách sử dụng các dòng $i_1, \ldots, i_u$ và các cột $j_1, \ldots, j_v$ là ma trận $(a_{i_k j_l})_{\substack{1 \leq k \leq u \\ 1 \leq l \leq v}}$ thuộc $\mathbf{M}_{u,v}(K)$.

VÍ DỤ :

Ma trận $\begin{pmatrix} a & c & d \\ a'' & c'' & d'' \end{pmatrix}$ là một ma trận con của $\begin{pmatrix} a & b & c & d \\ a' & b' & c' & d' \\ a'' & b'' & c'' & d'' \end{pmatrix}$, bằng cách sử dụng các dòng 1, 3 và các cột 1, 3 ,4 :

Dòng

1	a	b	c	d
2	a'	b'	c'	d'
3	a''	b''	c''	d''
	1	2	3	4

Cột

♦ **Định lý** Với mọi ma trận A thuộc $\mathbf{M}_{n,p}(K)$, hạng của A bằng cấp cao nhất của các ma trận con vuông khả nghịch trích ra từ A.

Chứng minh :

Ta ký hiệu r = rank (A), và s là cấp cao nhất của các ma trận con vuông khả nghịch trích ra từ A.

1) $r \geq s$

Giả sử B là một ma trận con vuông của A, α là cấp của B , và giả sử $\alpha > r$.

Ký hiệu $i_1, \ldots, i_\alpha$ $(i_1 < \ldots < i_\alpha)$ là các chỉ số của các dòng của A được sử dụng để trích ra B, $v_1, \ldots, v_\alpha$ là các cột B (trong $\mathbf{M}_{\alpha,1}(K)$), $V_1, \ldots, V_\alpha$ là các cột của A được sử dụng để trích ra B (trong $\mathbf{M}_{n,1}(K)$). Vì $\alpha > r$, họ $(V_1, \ldots, V_\alpha)$ phụ thuộc tuyến tính. Tồn tại $(\lambda_1, \ldots, \lambda_\alpha) \in K^\alpha - \{(0,\ldots,0)\}$ sao cho $\sum_{i=1}^{\alpha} \lambda_i V_i = 0$. Do đó, nếu chỉ lấy các dòng $i_1, \ldots, i_\alpha$ thì : $\sum_{i=1}^{\alpha} \lambda_i v_i = 0$, và như vậy B không khả nghịch. Điều đó chứng tỏ: $r \geq s$.

2) $r \leq s$

Giả sử $\mathcal{B} = (e_1, \ldots, e_p)$ là cơ sở chính tắc của K^p, $\mathcal{B}' = (f_1, \ldots, f_n)$ là cơ sở chính tắc của K^n, $f : K^p \to K^n$ là ánh xạ tuyến tính được biểu diễn bởi A trong các cơ sở $\mathcal{B}$ và $\mathcal{B}'$.

Vì rank (f) = rank $(A) = r$, nên tồn tại $i_1, \ldots, i_r \in \{1, \ldots, p\}$ sao cho :

$$i_1 < \ldots < i_r \text{ và } (f(e_{i_1}), \ldots, (e_{i_r})) \text{ là một cơ sở của } \mathrm{Im}(f).$$

Bằng cách hoán vị các cột của A (điều này không làm thay đổi cả r lẫn s), ta có thể quy về trường hợp $i_1 = 1, \ldots, i_r = r$.

Theo định lý về cơ sở không đầy đủ, dạng yếu (6.4, Định lý 2), tồn tại $j_{r+1}, ..., j_n \in \{1, ..., n\}$ sao cho họ $\mathcal{F} = (f(e_1), ..., f(e_r), f_{j_{r+1}}, ..., f_{j_n})$ là một cơ sở của K^n. Như vậy $\det_{\mathcal{B}'}(\mathcal{F}) \neq 0$, và :

$$\det_{\mathcal{B}'}(\mathcal{F}) = \begin{vmatrix} a_{11} & \cdots & a_{1r} & 0 & 0 & 0 \\ \vdots & & \vdots & \vdots & \vdots & \vdots \\ \vdots & & \vdots & 0 & 1 & \vdots \\ \vdots & & \vdots & 1 & 0 & \vdots \\ \vdots & & \vdots & 0 & \vdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & 1 \\ \vdots & & \vdots & \vdots & \vdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & \cdots & a_{nr} & 0 & 0 & 0 \end{vmatrix}$$

trong đó với mọi k thuộc $\{1, ..., n-r\}$, cột số $r+k$ được tạo bởi những số không, trừ một hạng tử bằng 1 nằm ở dòng j_{r+k}.

Bằng cách lập lại việc khai triển định thức này theo cột cuối cùng, và ký hiệu $j_1, ..., j_r \in \{1, ..., n\}$ sao cho $j_1 < ... < j_r$ và $\{j_1, ..., j_r\} = \complement_{\{1,...,n\}}\{j_{r+1}, ..., j_n\}$, ta được :

$$\det_{\mathcal{B}'}(\mathcal{F}) = \pm \begin{vmatrix} a_{j_1 1} & \cdots & a_{j_1 r} \\ \vdots & & \vdots \\ a_{j_r 1} & \cdots & a_{j_r r} \end{vmatrix}.$$

Như vậy ta đã làm xuất hiện một ma trận vuông cấp r, khả nghịch, trích ra từ A.

Điều đó chứng tỏ : $r \leq s$. ■

VÍ DỤ :

Hạng của ma trận $A = \begin{pmatrix} 2 & 1 & 4 & -3 \\ 4 & 0 & 6 & 1 \end{pmatrix} \in \mathbf{M}_{2,4}(\mathbb{R})$?

Một mặt, rank $(A) \leq 2$ vì $A \in \mathbf{M}_{2,4}(\mathbb{R})$.

Mặt khác, ma trận $\begin{pmatrix} 2 & 1 \\ 4 & 0 \end{pmatrix}$, cấp 2, trích ra từ A, là khả nghịch (vì có định thức là -4, khác không).

Ta kết luận rank $(A) = 2$. ■

Rõ ràng hệ quả sau đây được suy từ định lý trên.

♦ **Hệ quả**

$$\forall A \in \mathbf{M}_{n,p}(K), \quad \text{rank}\,({}^tA) = \text{rank}\,(A).$$

Cũng có thể xem 8.2.3, Hệ quả 2.

Bài tập

◊ **9.8.1** Cho $n \in \mathbb{N} - \{0, 1\}$, $A \in \mathbf{M}_n(K)$. Chứng minh:

$$\begin{cases} \text{rank}(A) \leq n-2 & \Rightarrow \text{rank}(\text{com}(A)) = 0 \\ \text{rank}(A) = n-1 & \Rightarrow \text{rank}(\text{com}(A)) = 1 \\ \text{rank}(A) = n & \Rightarrow \text{rank}(\text{com}(A)) = n. \end{cases}$$

◊ **9.8.2** Cho $n \in \mathbb{N} - \{0,1\}$, $A \in \mathbf{M}_n(K)$, $p \in \mathbb{N}^*$. Hãy tính com (com(...(com(A))...)), trong đó com được lặp lại p lần. (Có thể sử dụng bài tập 9.8.1).

◊ **9.8.3** Giả sử $n \in \mathbb{N} - \{0,1\}$, $A \in \mathbf{M}_n(K)$, sao cho $\text{rank}(A) = n-1$, $B \in \mathbf{M}_n(K)$ sao cho $AB = BA = 0$.

Chứng minh : $\exists \gamma \in K, \quad B = \gamma^t \text{com}(A)$.

◊ **9.8.4** Giả sử $n \in \mathbb{N} - \{0,1\}$, $A = \begin{pmatrix} 1-n & & \\ & \ddots & 1 \\ & 1 & \\ & & 1-n \end{pmatrix} \in \mathbf{M}_n(K)$.

Tính com(A). (Có thể sử dụng các bài tập 9.8.1 và 9.8.3).

◊ **9.8.5*** Cho $n \in \mathbb{N}$ sao cho $n \geq 3$, $A = (a_{ij})_{ij} \in \mathbf{M}_n(K)$.

Với $(i, j) \in \{1, ..., n\}^2$, ký hiệu A_{ij} là phần phụ đại số của a_{ij} trong A. Gọi B là ma trận vuông cấp $n-2$ nhận được từ A bằng cách bỏ đi các dòng thứ nhất và thứ n và các cột thứ nhất và thứ n.

Chứng minh : $\det(A)\det(B) = \begin{vmatrix} A_{11} & A_{1n} \\ A_{n1} & A_{nn} \end{vmatrix}$.

(Có thể xét định thức cấp n sau : $\begin{vmatrix} A_{11} & 0 & \cdots & 0 & A_{1n} \\ A_{21} & 1 & \ddots & & A_{2n} \\ \vdots & & \ddots & 1 & \vdots \\ A_{n-11} & & 0 & 1 & A_{n-1n} \\ A_{n1} & 0 & \cdots & 0 & A_{nn} \end{vmatrix}$).

9. 9 Hệ afin

9. 9.1 Đặt bài toán

Giả sử $A = \begin{pmatrix} a_{11} & \cdots & a_{1p} \\ \vdots & & \\ a_{n1} & \cdots & a_{np} \end{pmatrix} \in \mathbf{M}_{n,p}(K)$, $B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in \mathbf{M}_{n,1}(K)$.

Ta xét hệ phương trình :

$$(S)\begin{cases} a_{11}x_1 + \cdots + a_{1p}x_p = b_1 \\ \vdots \qquad\qquad \vdots \quad \vdots \\ a_{n1}x_1 + \cdots + a_{np}x_p = b_n \end{cases},$$

với ẩn $(x_1, \ldots, x_p) \in K^p$, được gọi là **hệ afin.**

Kí hiệu $\mathcal{S}$ là tập hợp các nghiệm của (S) trong K^p, vấn đề là xét xem $\mathcal{S}$ có rỗng hay không, và khi $\mathcal{S} \neq \varnothing$, hãy tính tường minh các phần tử của $\mathcal{S}$.

1) Dạng ma trận

Đặt $X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} \in \mathbf{M}_{p,1}(K)$, $(x_1, \ldots, x_p)$ là một nghiệm của (S) trong K^p khi và chỉ khi : $AX = B$. Như vậy việc giải hệ (S) quy về việc giải phương trình ma trận $AX = B$, với ẩn $X \in \mathbf{M}_{p,1}(K)$.

2) Dạng vectơ

Giả sử :
- E là một K-kgv p chiều
- F là một K-kgv n chiều
- $\mathcal{B}$ là một cơ sở của E, $\mathcal{C}$ là một cơ sở của F
- $f \in \mathcal{L}(E, F)$ sao cho $\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f) = A$
- $b \in F$ sao cho $\mathrm{Mat}_{\mathcal{C}}(b) = B$
- $x \in E$ sao cho $\mathrm{Mat}_{\mathcal{B}}(x) = X$.

Ta có : $AX = B \Leftrightarrow f(x) = b \Leftrightarrow x \in f^{-1}(\{b\})$.

Như vậy giải (S) là xác định nghịch ảnh qua f của đơn tử $\{b\}$.

3) Dạng afin

Với $i \in \{1, ..., n\}$ ta ký hiệu $\varphi_i : K^p \to K$ là ánh xạ xác định bởi

$$\forall (x_1, ..., x_p) \in K^p,\ \varphi_i(x_1, ..., x_p) = \sum_{j=1}^{p} a_{ij} x_j$$

Rõ ràng $\varphi_1, ..., \varphi_n$ là những dạng tuyến tính trên K^p.

Với mọi $(x_1, ..., x_p)$ thuộc K^p ta có :

$$(S) \Leftrightarrow (\forall i \in \{1, ..., n\},\ \varphi_i(x) = b_i) \Leftrightarrow x \in \bigcap_{i=1}^{n} \varphi_i^{-1}(\{b_i\})$$

Với $i \in \{1, ..., n\}$, nếu $(a_{i1}, ..., a_{ip}) \neq (0, ..., 0)$, thì $\varphi_i^{-1}(\{b_i\})$ là một siêu phẳng afin của K^p (xem Tập Hình học).

Như vậy giải (S) là xác định giao của một họ hữu hạn siêu phẳng afin.

9.9.2 Phép giải

Ta giữ lại các ký hiệu ở 9.9.1, và đặt $r = \text{rank}(A)$.

1) Hệ Cramer

Hệ (S) được gọi là **hệ Cramer** khi và chỉ khi A là ma trận vuông và khả nghịch, nghĩa là : $n = p = r$.

Ở đây, ta giả thiết điều kiện đó được thỏa mãn. Khi đó ta có : $AX = B \Leftrightarrow X = A^{-1}B$. Như vậy, (S) có một nghiệm và chỉ một, về mặt lý thuyết việc xác định nghiệm đó được suy từ việc tính A^{-1} (sau đó là $A^{-1}B$).

Với $1 \leq j \leq n$, ta kí hiệu $C_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix}$ là cột thứ j của A. Vì A khả nghịch, nên họ $\mathcal{F} = (C_1, ..., C_n)$ là một cơ sở của $\mathbf{M}_{n,1}(K)$. Vì vậy tồn tại duy nhất $(x_1, ..., x_p) \in K^p$ sao cho $B = \sum_{j=1}^{n} x_j C_j$, và do đó (S) có một nghiệm và chỉ một, đó là $(x_1, ..., x_p)$.

Giả sử $k \in \{1, ..., n\}$. Ta có :

$$\det_{\mathcal{F}}(C_1, ..., C_{k-1}, B, C_{k+1}, ..., C_n) = \det_{\mathcal{F}}\left(C_1, ..., \sum_{j=1}^{n} x_j C_j, ..., C_n\right)$$

$$= \sum_{j=1}^{n} x_j \det_{\mathcal{F}}(C_1, ..., C_j, ..., C_n) = x_k \det_{\mathcal{F}}(\mathcal{F}) = x_k,$$

vì với mọi j thuộc $\{1, ..., n\}$ sao cho $j \neq k$, $\det_{\mathcal{F}}(C_1, ..., C_j, ..., C_n) = 0$ do có một cột lặp lại.

Do đó, nếu gọi $\mathcal{B}$ là cơ sở chính của tác của $\mathbf{M}_{n,1}(K)$ thì ta có:

$$x_k = \det_{\mathcal{B}}(C_1, \ldots, C_{k-1}, B, C_{k+1}, \ldots, C_n) = \det_{\mathcal{B}}(\mathcal{B})\det_{\mathcal{B}}(C_1, \ldots, B, \ldots, C_n)$$
$$= (\det_{\mathcal{B}}(C_1, \ldots, C_n))^{-1} \det_{\mathcal{B}}(C_1, \ldots, B, \ldots, C_n).$$

Ta đã chứng minh:

◆ **Mệnh đề** Nếu $A = (a_{ij})_{ij} \in \mathbf{GL}_n(K)$ và $(b_1, \ldots, b_n) \in K^n$, thì hệ

$$(S) \begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \vdots \qquad\qquad \vdots \qquad \vdots \\ a_{n1}x_1 + \cdots + a_{nn}x_n = b_n \end{cases}$$

với ẩn $(x_1, \ldots, x_n) \in K^n$ có một nghiệm và chỉ một, và với mọi k thuộc $\{1, \ldots, n\}$:

$$x_k = \frac{1}{\det(A)} \begin{vmatrix} a_{11} & \cdots & a_{1k-1} & b_1 & a_{1k+1} & \cdots & a_{1n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & \cdots & a_{nk-1} & b_n & a_{nk+1} & \cdots & a_{nn} \end{vmatrix}.$$

Các công thức trên, cho ta $x_k (1 \le k \le n)$ được gọi là các **công thức Cramer**.

NHẬN XÉT :

Ngay khi $n \ge 3$, các công thức Cramer gần như không thể sử dụng được trong các ví dụ bằng số. Người ta thường thiên về một một phương pháp tổ hợp các phương trình và khử ẩn.

2) Trường hợp $r = n < p$

Theo 9.8, Định lý, bằng cách hoán vị các ẩn số, ta có thể giả thiết rằng ma trận vuông cấp n, $A_1 = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$, trích ra từ A, là khả nghịch.

Với mọi $(x_{n+1}, \ldots, x_p)$ thuộc K^{n-p}, hệ

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = b_1 - (a_{1n+1}x_{n+1} + \ldots + a_{1p}x_p) \\ \qquad\qquad\qquad\qquad \vdots \\ a_{n1}x_1 + \ldots + a_{nn}x_n = b_n - (a_{nn+1}x_{n+1} + \cdots a_{np}x_p) \end{cases},$$

với ẩn $(x_1, \ldots, x_n) \in K^n$, là hệ Cramer, do đó có một nghiệm và chỉ một $(x_1, \ldots, x_n)$, mà ta có thể biểu diễn tuyến tính theo $x_{n+1}, \ldots, x_p$

Chúng ta sẽ thấy (Tập Hình học) rằng tập hợp $\mathcal{S}$ các nghiệm của (S) là một không gian afin con của K^p với số chiều $p - r (= p - n)$.

VÍ DỤ:

Giải trong $\mathbb{R}^4$: $(S)\begin{cases} x+y-z+t=2 & (1)\\ 2x-2y+z-3t=1 & (2)\\ -x+y+z-2t=-2 & (3)\end{cases}$

Bằng cách thực hiện các phép biến đổi (2) -2.(1) và (3)+(1), ta có:

$$(S)\Leftrightarrow\begin{cases} x+y-z+t=2 & (1')\\ -4x+3z-5t=-3 & (2')\\ 2y-t=0 & (3')\end{cases}$$

(3') cho y theo t, sau đó thế vào (2'), ta được z, và cuối cùng, thế vào (1'), ta sẽ được x theo t :

$$(S)\Leftrightarrow\begin{cases} y=\dfrac{1}{2}t\\ z=\dfrac{1}{3}(7t-3)=\dfrac{7}{3}t-1\\ x=\dfrac{5}{6}t+1\end{cases}$$

Vậy : $\mathcal{S}=\left\{\left(\frac{5}{6}t+1,\frac{1}{2}t,\frac{7}{3}t-1\right)\ ;\ t\in\mathbb{R}\right\}$.

Trong ví dụ này, $\mathcal{S}$ là đường thẳng afin thuộc $\mathbb{R}^4$ đi qua điểm (1, 0, -1, 0), và có vectơ chỉ phương, chẳng hạn là (5, 3, 14, 6).

3) Trường hợp tổng quát: $r < n$

Thông thường, ta tiến hành tổ hợp tuyến tính các phương trình, để quy hệ phương trình về một hệ thuộc trường hợp 2) trên đây, hoặc đưa về một hệ vô nghiệm.

VÍ DỤ:

Biện luận và giải, theo $a\in\mathbb{R}$, hệ phương trình với ẩn $(x,y,z)\in\mathbb{R}^3$:

$$(S)\begin{cases} 2x+y-3z=a\\ 3x+2y+z=a+3\\ 7x+4y-5z=2a+5.\end{cases}$$

Rút y từ phương trình thứ nhất và thế vào hai phương trình còn lại:

$$(S)\ \Leftrightarrow\begin{cases} y=-2x+3z+a\\ -x+7z=-a+3\\ -x+7z=-2a+5.\end{cases}$$

Nếu $-a+3 \neq -2a+5$ (nghĩa là : $a \neq 2$), thì hai phương trình cuối không tương thích.
Nếu $a = 2$, thì:

$$(S) \Leftrightarrow \begin{cases} y = -2x + 3z + 2 \\ x = 7z - 1 \end{cases} \Leftrightarrow \begin{cases} x = 7z - 1 \\ y = -11z + 4 \end{cases}.$$

Kết luận: $\mathcal{S} = \begin{cases} \{(7z-1, -11z+4, z); z \in \mathbb{R}\} & \text{nếu } a = 2 \\ \varnothing & \text{nếu } a \neq 2 \end{cases}$

4) Trường hợp hệ tuyến tính - thuần nhất

Hệ afin (S) $\begin{cases} a_{11}x_1 + \cdots + a_{1p}x_p = b_1 \\ \vdots \\ a_{n1}x_1 + \cdots + a_{np}x_p = b_n \end{cases}$ được gọi là **tuyến tính-thuần nhất** (hoặc: **tuyến tính**; hoặc: **thuần nhất**) khi và chỉ khi: $b_1 = \ldots = b_n = 0$.

Trong trường hợp này $(0, \ldots, 0)$ là nghiệm của (S), được gọi là nghiệm tầm thường. Với các ký hiệu ở 9.9.1, 2), vì tập hợp $f^{-1}(\{0\})$ là hạt nhân của f, nên từ định lý về hạng ta suy ra kết quả sau:

♦ **Mệnh đề** Tập hợp các nghiệm của hệ phương trình tuyến tính - thuần nhất

(S_0) $\begin{cases} a_{11}x_1 + \cdots + a_{1p}x_p = 0 \\ \vdots \\ a_{n1}x_1 + \cdots + a_{np}x_p = 0 \end{cases}$ là một kgvc của K^p, với số chiều $p - r$,

trong đó $r = \operatorname{rank} \begin{pmatrix} a_{11} & \cdots & a_{1p} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{np} \end{pmatrix}$.

Nói riêng (S_0) có nghiệm, ngoài nghiệm $(0, \ldots, 0)$, khi và chỉ khi :

$$r < p.$$

Bài tập

◊ **9.9.1** Giải các hệ phương trình sau (ẩn $(x, y, z) \in \mathbb{C}^3$, các tham số $a, b, m \in \mathbb{C}$):

a) $\begin{cases} 2x+3y-z=1 \\ x+2y+3z=2 \\ 3x+4y-5z=-4 \end{cases}$

b) $\begin{cases} x+y+(2m-1)z=1 \\ mx+y+z=1 \\ x+my+z=3(m+1) \end{cases}$

c) $\begin{cases} 3mx+(3m-7)y+(m-5)z=m-1 \\ (2m-1)x+(4m-1)y+2mz=m+1 \\ 4mx+(5m-7)y+(2m-5)z=m-1 \end{cases}$

d) $\begin{cases} x-my+m^2z=m \\ mx-m^2y+mz=1 \\ mx+y-m^3z=1 \end{cases}$

e) $\begin{cases} 3x+y-z=1 \\ 5x+2y-2z=a \\ 4x+y-z=b \end{cases}$

f) $\begin{cases} ax+(b-1)y+2z=1 \\ ax+(2b-3)y+3z=1 \\ ax+(b-1)y+(b+2)z=2b-3 \end{cases}$

g) $\begin{cases} 2x+y-z=2 \\ x-y+z=4 \\ 3x+3y-z=4a \\ (2-a)x+2y-2z=-2b. \end{cases}$

◊ **9.9.2** Tìm điều kiện cần và đủ đối với $m \in \mathbb{C}$ để ba mặt phẳng vectơ của $\mathbb{C}^3$ với phương trình:

$$x - 2y + z = mx, \quad 3x - y - 2z = my, \quad 3x - 2y - z = mz$$

có chứa cùng một đường thẳng vectơ.

◊ **9.9.3** Giải các hệ phương trình sau (ẩn $(x, y, z, t) \in \mathbb{C}^4$, các tham số $a, b, m \in \mathbb{C}$) :

a) $\begin{cases} 3x+4y+z+2t=3 \\ 6x+8y+2z+6t=7 \\ 9x+12y+3z+10t=0 \end{cases}$

b) $\begin{cases} 2x-y+z+t=1 \\ x+2y-z+4t=2 \\ x+7y-4z+11t=m \end{cases}$

c) $\begin{cases} mx+y+z+t=1 \\ x+my+z+t=m \\ x+y+mz+t=m+1 \end{cases}$

d) $\begin{cases} 2x+y+z+t=3 \\ x+2y+z+t=1 \\ x+y+2z+t=2 \\ x+y+z+2t=4 \\ 4x-3y+3z-4t=a \\ 2x+7y+7z+2t=b \end{cases}$

e) $\begin{cases} ax+y+z+t=1 \\ x+ay+z+t=b \\ x+y+az+t=b^2 \\ x+y+z+at=b^3. \end{cases}$

◊ **9.9.4** Giải (ẩn $(x_1, \ldots, x_n) \in \mathbb{C}^n$, tham số $(a_1, \ldots, a_n) \in \mathbb{C}^n$):

$$\begin{cases} x_1 + x_2 &= 2a_1 \\ x_2 + x_3 &= 2a_2 \\ &\vdots \\ x_{n-1} + x_n &= 2a_{n-1} \\ x_n + x_1 &= 2a_n \end{cases}$$

Chương 10

Không gian vectơ Euclide (Nghiên cứu sơ bộ)

Thể được sử dụng là thể các số thực ; các kgv được xét là những $\mathbb{R}$ - kgv.

10.1 Tích vô hướng

Đề tài này sẽ được trình bày một cách sâu sắc hơn và trong một khung cảnh tổng quát hơn ($K = \mathbb{R}$ hoặc $K = \mathbb{C}$) trong Tập 3, 1.6.

10.1.1 Đại cương

♦ **Định nghĩa** Cho E là một $\mathbb{R}$ - kgv; **tích vô hướng** trên E là một ánh xạ $\varphi : E^2 \to \mathbb{R}$ sao cho:

(i) $\forall (x,y) \in E^2, \quad \varphi(y,x) = \varphi(x,y)$ (φ **đối xứng**)

(ii) $\forall \lambda \in \mathbb{R}, \forall (x,y,y') \in E^3, \quad \varphi(x,\lambda y + y') = \lambda\varphi(x,y) + \varphi(x,y')$

(φ **tuyến tính đối với vị trí thứ hai**)

(iii) $\forall x \in E, \quad \varphi(x,x) \geq 0$

(iv) $\forall x \in E, \quad (\varphi(x, x) = 0 \Leftrightarrow x = 0)$.

NHẬN XÉT:

Nếu φ là một tích vô hướng trên $\mathbb{R}$ - kgv E, thì:

$$\forall \lambda \in \mathbb{R}, \forall (x,x',y) \in E^3, \quad \varphi(\lambda x + x',y) = \lambda\varphi(x,y) + \varphi(x',y).$$

Ta nói rằng φ **tuyến tính đối với vị trí thứ nhất**.

Như vậy ta có thể thay (i) và (ii) bởi: "φ là một dạng song tuyến tính đối xứng".

Khi φ là một tích vô hướng, người ta thường ký hiệu $(x \mid y)$ hoặc $< x,y >$ hoặc $x \cdot y$ thay vì $\varphi(x,y)$.

VÍ DỤ:

1) Tích vô hướng thông thường trên $\mathbb{R}^n$, $n \in \mathbb{N}^*$

Ánh xạ $\varphi : (\mathbb{R}^n)^2 \to \mathbb{R}$ xác định bởi:

$$((x_1,\ldots,x_n),(y_1,\ldots,y_n)) = \sum_{k=1}^{n} x_k y_k$$

là một tích vô hướng trên $\mathbb{R}^n$, gọi là **tích vô hướng thông thường** (hoặc: **chính tắc**) **trên** $\mathbb{R}^n$.

2) Tích vô hướng chính tắc trên $\mathbf{M}_{n,p}(\mathbb{R})$, $(n, p) \in (\mathbb{N}^*)^2$

Xét ánh xạ $\varphi : (\mathbf{M}_{n,p}(\mathbb{R}))^2 \to \mathbb{R}$.

$$(A,B) \mapsto \operatorname{tr}({}^tAB)$$

(i) $\varphi(B, A) = \operatorname{tr}(BA) = \operatorname{tr}({}^t({}^tAB)) = \operatorname{tr}({}^tAB) = \varphi(A, B)$

(ii) $\varphi(A, \lambda B + B') = \operatorname{tr}({}^tA(\lambda B + B')) = \operatorname{tr}(\lambda {}^tAB + {}^tAB') = \lambda \operatorname{tr}({}^tAB) + \operatorname{tr}({}^tAB')$

$= \lambda\varphi(A,B) + \varphi(A,B')$

(iii) Đặt $A = (a_{ij})_{ij}$, ta có:

$$(A, A) = tr({}^tAA) = \sum_{i=1}^{n}\sum_{j=1}^{p} a_{ij}^2 = \sum_{\substack{1\le i\le n\\ 1\le j\le p}} a_{ij}^2 \ge 0$$

(iv) Tương tự: $\varphi(A, A) = 0 \Leftrightarrow \sum_{i,j} a_{ij}^2 = 0$.

$$\Leftrightarrow (\forall (i,j) \in \{1,\ldots,n\} \times \{1,\ldots,p\}, a_{ij} = 0) \Leftrightarrow A = 0.$$

Như vậy, φ là một tích vô hướng trên $\mathbf{M}_{n,p}(\mathbb{R})$, được gọi là **tích vô hướng chính tắc trên** $\mathbf{M}_{n,p}(\mathbb{R})$. Đặc biệt với $p = 1$, nếu đồng nhất $\mathbf{M}_{n,1}(\mathbb{R})$ với $\mathbb{R}^n$ thì ta trở lại tích vô hướng thông thường trên $\mathbb{R}^n$ (ví dụ 1) trên đây).

3) Cho $(a,b) \in \mathbb{R}^2$ sao cho $a < b$, và $E = C^0([a; b], \mathbb{R})$ là $\mathbb{R}$ - kgv các ánh xạ liên tục từ $[a; b]$ vào $\mathbb{R}$.

Xét ánh xạ $\varphi : E^2 \to \mathbb{R}$.

$$(f,g) \mapsto \int_a^b fg$$

(i) $\varphi(g,f) = \int_a^b gf = \int_a^b fg = \varphi(f,g)$

(ii) $\varphi(f, \lambda g_1 + g_2) = \int_a^b f(\lambda g_1 + g_2) = \lambda\int_a^b fg_1 + \int_a^b fg_2 = \lambda\varphi(f,g_1) + \varphi(f,g_2)$

(iii) $\varphi(f,f) = \int_a^b f^2 \ge 0$

(iv) $\varphi(f,f) = 0 \Leftrightarrow \int_a^b f^2 = 0 \Leftrightarrow f = 0$,

vì f liên tục (xem Tập 1, 6.2.5, Hệ quả 4).

Như vậy, φ là một tích vô hướng trên E.

♦ **Mệnh đề** Cho E là một $\mathbb{R}$ - kgv, φ là một tích vô hướng trên $\mathbb{R}$.

Ký hiệu $\phi : E \to \mathbb{R}$, $x \mapsto \varphi(x,x)$. Ta có:

1) $\forall (n, p) \in (\mathbb{N}^*)^2$, $\forall (\lambda_1,...,\lambda_n) \in \mathbb{R}^n$, $\forall (\mu_1,...,\mu_p) \in \mathbb{R}^p$,

$\forall (x_1,...,x_n) \in E^n$, $\forall (y_1,...,y_p) \in E^p$,

$$\varphi\left(\sum_{i=1}^{n} \lambda_i x_i, \sum_{j=1}^{p} \mu_j y_j\right) = \sum_{\substack{1\le i\le n\\ 1\le j\le p}} \lambda_i \mu_j \varphi(x_i, y_j)$$

2) $\forall (\lambda, \mu) \in \mathbb{R}^2$, $\forall (x, y) \in E^2$,

$$\phi(\lambda x + \mu y) = \lambda^2 \phi(x) + 2\lambda\mu\varphi(x, y) + \mu^2 \phi(y)$$

3) $\forall \lambda \in \mathbb{R}$, $\forall x \in E$, $\quad \phi(\lambda x) = \lambda^2 \phi(x)$

4) $\forall (x, y) \in E^2$, $\quad \phi(x + y) = \phi(x) + 2\varphi(x,y) + \phi(y)$

5) $\forall (x, y) \in E^2$, $\quad \phi(x + y) + \phi(x - y) = 2(\phi(x) + \phi(y))$.

Chứng minh:

1) Bằng quy nạp theo n, ta thấy rằng:

$$\forall Y \in E, \varphi\left(\sum_{i=1}^{n} \lambda_i x_i, Y\right) = \sum_{i=1}^{n} \lambda_i \varphi(x_i, Y).$$

từ đó:
$$\varphi\left(\sum_{i=1}^{n} \lambda_i x_i, \sum_{j=1}^{p} \mu_j y_j\right) = \sum_{i=1}^{n} \lambda_i \varphi\left(x_i, \sum_{j=1}^{p} \mu_j y_j\right)$$

$$= \sum_{i=1}^{n} \lambda_i \left(\sum_{j=1}^{n} \mu_j \varphi(x_i, y_j)\right) = \sum_{\substack{1\le i\le n\\ 1\le j\le p}} \lambda_i \mu_j \varphi(x_i, y_j).$$

2) Là trường hợp đặc biệt của 1).

3) và 4) Là những trường hợp đặc biệt của 2).

5) $\begin{cases} \phi(x + y) = \phi(x) + 2\phi(x, y) + \phi(y) \\ \phi(x - y) = \phi(x) - 2\phi(x, y) + \phi(y) \end{cases}$, sau đó cộng từng vế.

10.1.2 Các bất đẳng thức và chuẩn Euclide

Cho E là một $\mathbb{R}$ - kgv, φ là một tích vô hướng trên E, $\phi : E \to \mathbb{R}$.
$x \mapsto \varphi(x,x)$

♦ **Định lý 1 (Bất đẳng thức Cauchy -Schwarz)**

$$\forall (x,y) \in E^2, \quad (\varphi(x,y))^2 \le \phi(x)\phi(y).$$

Chứng minh:

Ta có: $\forall \lambda \in \mathbb{R}, \phi(x + \lambda y) \ge 0$, nên: $\forall \lambda \in \mathbb{R}, \phi(y)\lambda^2 + 2\varphi(x,y)\lambda + \phi(x) \ge 0$.

• Nếu $\phi(y) \ne 0$, tam thức $\lambda \mapsto \phi(y)\lambda^2 + 2\varphi(x,y)\lambda + \phi(x)$ là ≥ 0 trên $\mathbb{R}$, do vậy biệt thức ≤ 0:

$$(\varphi(x,y))^2 - \phi(x)\phi(y) \le 0.$$

• Nếu $\phi(y) = 0$, thì $y = 0$, bất đẳng thức cần chứng minh là hiển nhiên.

♦ **Mệnh đề 1 (Trường hợp đẳng thức trong bất đẳng thức Cauchy - Schwarz)**

$$\forall (x,y) \in E^2, (\varphi(x,y))^2 = \phi(x)\phi(y) \Leftrightarrow (x,y) \text{ phụ thuộc tuyến tính}).$$

Chứng minh:

1) Giả sử (x, y) phụ thuộc tuyến tính; chẳng hạn, tồn tại $\alpha \in \mathbb{R}$ sao cho $y = \alpha x$. Khi đó ta có:

$$\begin{cases} (\varphi(x,y))^2 = (\varphi(x,\alpha x))^2 = \alpha^2(\varphi(x,x))^2 = \alpha^2(\phi(x))^2 \\ \phi(x)\phi(y) = \phi(x)\alpha^2\phi(x) = \alpha^2(\phi(x))^2, \end{cases}$$

từ đó suy ra đẳng thức cần có.

2) Ngược lại, giả sử: $(\varphi(x,y))^2 = \phi(x)\phi(y)$.

Nếu $y = 0$, thì (x,y) phụ thuộc tuyến tính.

Giả sử $y \ne 0$ (do vậy $\phi(y) > 0$). Đặt $\lambda_0 = -\dfrac{\varphi(x,y)}{\phi(y)}$, ta có:

$$\phi(x + \lambda_0 y) = \left(\frac{\varphi(x,y)}{\phi(y)}\right)^2 \phi(y) - 2\frac{\varphi(x,y)}{\phi(y)}\varphi(x,y) + \phi(x)$$

$$= \frac{1}{\phi(y)}(-(\varphi(x,y))^2 + \phi(x)\phi(y)) = 0$$

nên $x + \lambda_0 y = 0$, (x,y) phụ thuộc tuyến tính.

Việc chọn λ_0 ứng với việc chọn không điểm duy nhất của đạo hàm của tam thức $\lambda \mapsto \phi(x + \lambda y)$, điều này cho phép ta nhận được giá trị cực tiểu của tam thức đó.

Ta có thể nhận xét rằng ở 1) thì α bằng $\dfrac{\varphi(x,y)}{\phi(x)}$ (nếu $x \ne 0$).

♦ **Định lý 2** **(Bất đẳng thức Minkowski)**

$$\forall (x,y)\in E^2,\quad (\phi(x+y))^{\frac{1}{2}} \le (\phi(x))^{\frac{1}{2}} + (\phi(y))^{\frac{1}{2}}$$

Chứng minh:

$$(\phi(x+y))^{\frac{1}{2}} \le (\phi(x))^{\frac{1}{2}} + (\phi(y))^{\frac{1}{2}} \Leftrightarrow \phi(x+y) \le \phi(x) + 2(\phi(x)\phi(y))^{\frac{1}{2}} + \phi(y)$$

$$\Leftrightarrow \varphi(x,y) \le (\phi(x)\phi(y))^{\frac{1}{2}},$$

mà bất đẳng thức cuối cùng trên là hệ quả của bất đẳng thức Cauchy - Schwarz.

♦ **Mệnh đề 2** **(Trường hợp đẳng thức trong bất đẳng thức Minkowski)**

Với mọi (x,y) thuộc E^2,

$$(\phi(x+y))^{\frac{1}{2}} = (\phi(x))^{\frac{1}{2}} + (\phi(y))^{\frac{1}{2}} \Leftrightarrow \begin{bmatrix} x=0 \\ \text{hoặc} \\ (\exists \alpha \in \mathbb{R}_+, y=\alpha x) \end{bmatrix}$$

Ta phát biểu điều đó bởi: (x,y) *phụ thuộc tuyến tính dương.*

Chứng minh:

1) Trường hợp $x = 0$ là hiển nhiên.

Nếu tồn tại $\alpha \in \mathbb{R}_+$ sao cho $y = \alpha x$, thì (xem 10.1, Mệnh đề *3*)):

$$\begin{cases} (\phi(x+y))^{\frac{1}{2}} = (\phi((1+\alpha)x))^{\frac{1}{2}} = (1+\alpha)(\phi(x))^{\frac{1}{2}} \\ (\phi(x))^{\frac{1}{2}} + (\phi(y))^{\frac{1}{2}} = (\phi(x))^{\frac{1}{2}} + \alpha(\phi(x))^{\frac{1}{2}}. \end{cases}$$

2) Ngược lại, giả sử $(\phi(x+y))^{\frac{1}{2}} = (\phi(x))^{\frac{1}{2}} + (\phi(y))^{\frac{1}{2}}$.

Lặp lại lược đồ tính toán trong phép chứng minh bất đẳng thức Minkowski, ta sẽ được:

$$\phi(x,y) = (\phi(x))^{\frac{1}{2}}(\phi(y))^{\frac{1}{2}}.$$

Khi đó ta có đẳng thức trong bất đẳng thức Cauchy - Schwarz, do vậy (xem Mệnh đề 1), (x,y) phụ thuộc tuyến tính. Vì trường hợp $x = 0$ là hiển nhiên, nên ta giả thiết $x \neq 0$. Tồn tại $\alpha \in \mathbb{R}$ sao cho $y = \alpha x$.

Khi đó ta có $|1 + \alpha|\,\phi(x) = (1 + |\alpha|)\phi(x))$, nên $(1 + \alpha)^2 = (1 + |\alpha|)^2$, $2\alpha = 2|\alpha|$, và cuối cùng $\alpha \in \mathbb{R}_+$.

♦ **Mệnh đề - Định nghĩa 3** Giả sử E là một $\mathbb{R}$ - kgv, φ là một tích vô hướng trên E. Ánh xạ $\|\cdot\| : E \to \mathbf{R}$, $x \mapsto (\varphi(x,x))^{\frac{1}{2}}$ là một chuẩn trên E, gọi là **chuẩn Euclide liên kết với** φ. Ánh xạ $d : E \times E \to \mathbf{R}$, $(x,y) \mapsto \|x-y\|$ được gọi là **khoảng cách Euclide liên kết với** φ.

Chứng minh:

Dễ dàng suy ra các điều kiện $\|\lambda x\| = |\lambda| \|x\|$ và $(\|x\| = 0 \Leftrightarrow x = 0)$.

Bất đẳng thức tam giác $\|x + y\| \le \|x\| + \|y\|$ là **bất đẳng thức Minkowski.**

NHẬN XÉT:

Theo 10.1.1, Mệnh đề *4), 5)*, ta có:

$$\forall (x, y) \in E^2, \quad \begin{cases} \varphi(x, y) = \dfrac{1}{2}(\|x + y\|^2 - \|x\|^2 - \|y\|^2) \\ \|x + y\|^2 + \|x - y\|^2 = 2(\|x\| + \|y\|)^2. \end{cases}$$

Đẳng thức cuối cùng được gọi là **đẳng thức hình bình hành** (hoặc: **đẳng thức đường trung tuyến**).

Bài tập

◊ **10.1.1** Giả sử E là một kgv, $\|\cdot\|$ là một chuẩn Euclide trên E. Chứng minh:

$$\|b - a\|^2 + \|c - b\|^2 + \|d - c\|^2 + \|a - d\|^2 = \|c - a\|^2 + \|d - b\|^2 + \|a - b + c - d\|^2.$$

◊ **10.1.2** Cho $n \in \mathbb{N}$, $A \in \mathbf{M}_n(\mathbb{R})$ phản đối xứng.

Chứng minh rằng $\mathbf{I}_n + A$ là khả nghịch.

◊ **10.1.3** Giả sử E là một kgv, $\langle \cdot, \cdot \rangle$ là một tích vô hướng trên E, $\|\cdot\|$ là chuẩn liên kết, $n \in \mathbb{N}^*$, $x_1, \ldots, x_n \in E$. Chứng minh

$$\left\| \sum_{k=1}^{n} x_k \right\|^2 \le n \sum_{k=1}^{n} \|x_k\|^2 .$$

◊ **10.1.4** Giả sử E là một kgv, $\langle \cdot, \cdot \rangle$ là một tích vô hướng trên E, $\|\cdot\|$ là chuẩn liên kết, $x, y, z \in E$.

Chứng minh : $\|x - z\|^2 \le 2(\|x - y\|^2 + \|y - z\|^2)$.

◊ **10.1.5** Giải phương trình $(1 - x)^2 + (x - y)^2 + (y - z)^2 + z^2 = \dfrac{1}{4}$, với ẩn $(x, y, z) \in \mathbb{R}^3$.

◊ **10.1.6** Giả sử $n \in \mathbb{N}^*$, $x_1, \ldots, x_n \in \mathbf{R}_+^*$ sao cho $\sum_{i=1}^{n} x_i = 1$.

Chứng minh : $\sum_{i=1}^{n} \dfrac{1}{x_i} \ge n^2$, và xét trường hợp đẳng thức.

◊ **10.1.7*** Giả sử $n \in \mathbb{N} - \{0, 1\}$, $(a_1, \ldots, a_n) \in (\mathbf{R}_+^*)^n$, $(b_1, \ldots, b_n) \in \mathbb{R}^n$. Chứng minh :

$$\sum_{i \ne j} a_i b_j = 0 \Rightarrow \sum_{i \ne j} b_i b_j \le 0 .$$

10.1.3 Tính trực giao

Cho E là một $\mathbb{R}$ - kgv. $<.\ ,\ .>$ là một tích vô hướng trên E, $\|\cdot\|$ là chuẩn Euclide liên kết với $<\cdot, \cdot>$.

♦ **Định nghĩa**

1) Cho $(x, y) \in E^2$; ta nói x **trực giao với** y, và ký hiệu $x \perp y$, khi và chỉ khi : $< x, y > = 0$.

2) Cho $x \in E$, $A \in \mathfrak{P}(E)$; ta nói x **trực giao với** A, và ký hiệu $x \perp A$, khi và chỉ khi:

$$\forall a \in A, < x, a > = 0.$$

3) Với mọi bộ phận A của E, ta định nghĩa **tập trực giao với** A, ký hiệu là $A^\perp$, là tập:

$$A^\perp = \{x \in E;\ \forall a \in A, < x, a > = 0\}.$$

4) Một họ phần tử $(x_i)_{i \in I}$ của E được gọi là **trực giao** khi và chỉ khi:

$$\forall (i, j) \in I^2,\ (i \neq j \Rightarrow < x_i, x_j > = 0).$$

5) Một họ phần tử $(x_i)_{i \in I}$ của E được gọi là **trực chuẩn** khi và chỉ khi:

$$\begin{cases} (x_i)_{i \in I} \text{ trực giao} \\ \forall i \in I,\ \| x_i \| = 1 \end{cases}$$

♦ **Mệnh đề 1**

1) Với mọi bộ phận A của E, $A^\perp$ là một kgvc của E.

2) $\forall (A, B) \in (\mathfrak{P}(E))^2, \quad (A \subset B \Rightarrow A^\perp \supset B^\perp)$.

3) $\forall A \in \mathfrak{P}(E), \quad A^\perp = (\text{Vect}(A))^\perp$.

4) $\forall A \in \mathfrak{P}(E), \quad A \subset A^{\perp\perp}$.

5) $E^\perp = \{0\}, \quad \{0\}^\perp = E$.

6) $\forall A \in \mathfrak{P}(E), \quad A \cap A^\perp \subset \{0\}$.

7) Với mọi kgvc F, G của E:

$$(F + G)^\perp = F^\perp \cap G^\perp, \quad (F \cap G)^\perp \supset F^\perp + G^\perp.$$

Chứng minh:

1) • $(\forall a \in A, < 0, a > = 0)$, nên $0 \in A^\perp$.

• Nếu $\lambda \in \mathbb{R}$ và $(x, y) \in (A^\perp)^2$, thì:

$$\forall a \in A, < \lambda x + y, a > = \lambda < x, a > + < y, a > = 0,$$

nên $\lambda x + y \in A^\perp$.

2) Giả sử $A \subset B$, và cho $y \in B^{\perp}$. Ta có: $\forall b \in B, < y, b > = 0$,
do vậy ta phải có: $\forall a \in A, < y, a > = 0$, nên $y \in A^{\perp}$.

3) • $A \subset \text{Vect}(A)$, nên $A^{\perp} \supset (\text{Vect}(A))^{\perp}$, xem 2).

• Tính chất là hiển nhiên nếu $A = \varnothing$. Ta giả thiết $A \neq \varnothing$. Cho $x \in A^{\perp}$; với mọi y thuộc $\text{Vect}(A)$, tồn tại $n \in \mathbb{N}^*$, $\lambda_1,...,\lambda_n \in \mathbb{R}$, $a_1,..., a_n \in A$ sao cho $y = \sum_{i=1}^{n} \lambda_i a_i$,

do đó :

$$< x, y > = < x, \sum_{i=1}^{n} \lambda_i a_i > = \sum_{i=1}^{n} \lambda_i < x, a_i > = 0,$$

và do vậy $x \in (\text{Vect}(A))^{\perp}$. Như vậy ta đã chứng minh: $A^{\perp} \subset (\text{Vect}(A))^{\perp}$.

4) Giả sử $a \in A$. Vì: $\forall x \in A^{\perp}, < a, x > = < x, a > = 0$, nên ta có: $a \in (A^{\perp})^{\perp}$.

5) Hiển nhiên.

6) Nếu $x \in A \cap A^{\perp}$, thì, đặc biệt, $<x,x> = 0$, nên $x = 0$.

7) a) • $\begin{cases} F \subset F+G \\ G \subset F+G \end{cases} \Rightarrow \begin{cases} F^{\perp} \supset (F+G)^{\perp} \\ G^{\perp} \supset (F+G)^{\perp} \end{cases} \Rightarrow F^{\perp} \cap G^{\perp} \supset (F+G)^{\perp}$.

• Ngược lại, giả sử $x \in F^{\perp} \cap G^{\perp}$. Ta có:

$$\begin{cases} \forall f \in F, \ < x, f > = 0 \\ \forall g \in G, < x, g > = 0 \end{cases}$$

Với mọi h thuộc $F + G$, tồn tại $(f, g) \in F \times G$ sao cho $h = f + g$, và do vậy:

$$< x, h > = < x, f > + < x, g > = 0, \text{ nên } x \in (F + G)^{\perp}.$$

b) $\begin{cases} F \cap G \subset F \\ F \cap G \subset G \end{cases} \Rightarrow \begin{cases} (F \cap G)^{\perp} \supset F^{\perp} \\ (F \cap G)^{\perp} \supset G^{\perp} \end{cases} \Rightarrow (F+G)^{\perp} \supset F^{\perp} + G^{\perp}$.

NHẬN XÉT:

Chúng ta sẽ thấy rằng (10.2.1, Hệ quả 3), nếu E là hữu hạn chiều, thì sẽ có đẳng thức trong công thức thứ hai của 7).

♦ **Mệnh đề 2** Cho $(x_i)_{i \in I}$ là một họ phần tử của E.

Nếu $\begin{cases} (x_i)_{i \in I} \text{ trực giao} \\ \forall i \in I, \ x_i \neq 0 \end{cases}$, thì $(x_i)_{i \in I}$ độc lập tuyến tính.

Chứng minh:

Giả sử $N \in \mathbb{N}^*$, $\lambda_1,..., \lambda_N \in \mathbb{R}$, $i_1,..., i_N \in I$ khác nhau từng đôi một, sao cho $\sum_{k=1}^{N} \lambda_k x_{i_k} = 0$.

Với mọi j thuộc $\{1,..., N\}$, ta có: $0 = < x_{i_j}, \sum_{k=1}^{N} \lambda_k x_{i_k} > = \sum_{k=1}^{N} \lambda_k < x_{i_j}, x_{i_k} > = \lambda_j \| x_{i_j} \|^2$,

do đó $\lambda_j = 0$.

◆ **Mệnh đề 3 (Định lý Pythagore)**

Với mọi (x, y) thuộc E^2 ta có:

$$x \perp y \Leftrightarrow \|x+y\|^2 = \|x\|^2 + \|y\|^2 \Leftrightarrow \|x-y\|^2 = \|x\|^2 + \|y\|^2.$$

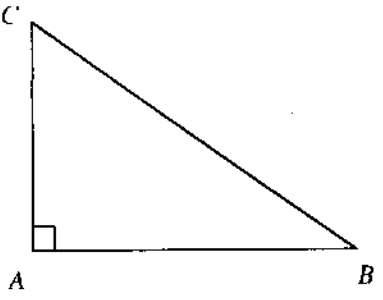
Chứng minh:

Dễ dàng suy ra bằng cách khai triển: $\|x+y\|^2 = \|x\|^2 + 2\langle x, y\rangle + \|y\|^2$.

NHẬN XÉT:

1) Với thuật ngữ của hình học afin, định lý Pythagore trở thành: để một tam giác ABC vuông ở A, thì cần và đủ là:

$$BC^2 = AB^2 + AC^2.$$



2) Đối với mọi họ hữu hạn trực giao $(x_i)_{1 \le i \le n}$ của E, ta có: $\left\|\sum_{i=1}^{n} x_i\right\|^2 = \sum_{i=1}^{n} \|x_i\|^2$

(xem 10.1.1, Mệnh đề *1*)).

Nhưng đảo lại là sai (nếu $n \geq 3$) ; chẳng hạn, trong $\mathbb{R}^2$ thông thường, họ (x_1, x_2, x_3) xác định bởi $x_1 = (1, 2)$, $x_2 = (0, 2)$, $x_3 = (0, -1)$, thoả mãn:

$$\|x_1 + x_2 + x_3\|^2 = \|x_1\|^2 + \|x_2\|^2 + \|x_3\|^2$$

và không trực giao.

10.2 Không gian vectơ Euclide

♦ **Định nghĩa** **Không gian vectơ Euclide** là mọi kgv hữu hạn chiều E, được trang bị một tích vô hướng.

Chẳng hạn, $\mathbb{R}^n$ với tích vô hướng thông thường là một không gian vectơ Euclide.

10.2.1 Thủ tục trực giao hóa Schmidt

Giả sử E là một không gian vectơ Euclide, $<\cdot,\cdot>$ là tích vô hướng, $n = \dim(E)$, $p \in \mathbb{N}^*$ sao cho $p \le n$, $(e_1,...,e_p)$ là một họ độc lập tuyến tính trong E.

Ta sẽ xây dựng một họ trực giao $(V_1,...V_p)$ những vectơ thuộc E, tất cả đều $\neq 0$, sao cho:

$$\forall k \in \{1,...,p\}, \quad \text{Vect}(e_1,...,e_k) = \text{Vect}(V_1,...,V_k).$$

- Đặt $V_1 = e_1 \neq 0$.
- Tìm V_2 dưới dạng $V_2 = e_2 + \lambda_{2,1} V_1$, trong đó cần tìm $\lambda_{2,1} \in \mathbb{R}$.

Ta có : $V_2 \perp V_1 \Leftrightarrow < V_1, e_2 + \lambda_{2,1} V_1 > = 0 \Leftrightarrow < V_1, e_2 > + \lambda_{2,1} \| V_1 \|^2 = 0$.

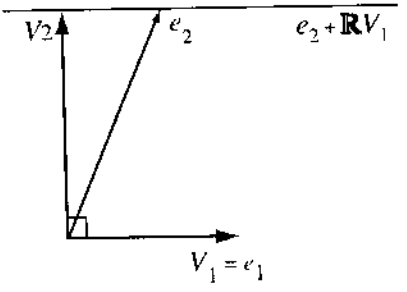
Vì $V_1 \neq 0$, tồn tại $\lambda_{2,1}$ thích hợp.

Nếu $V_2 = 0$, thì $e_2 \in \mathbb{R}V_1 = \mathbb{R}e_1$, mâu thuẫn với sự kiện (e_1, e_2) độc lập tuyến tính.

Vậy $V_2 \neq 0$.

Cuối cùng, hiển nhiên rằng:

$$\text{Vect}(e_1, e_2) = \text{Vect}(V_1, V_2).$$



- Giả sử đã xây dựng được $V_1,..., V_k$ (với $k \le p - 1$) sao cho:

$$\begin{cases} (V_1,..., V_k) \text{ trực giao và các vectơ thành phần đều } \neq 0. \\ \text{Vect}(e_1,..., e_k) = \text{Vect}(V_1,..., V_k). \end{cases}$$

Ta tìm V_{k+1} dưới dạng:

$$V_{k+1} = e_{k+1} + \sum_{i=1}^{k} \lambda_{k+1,i} V_i$$

trong đó cần tìm $(\lambda_{k+1,1}, ..., \lambda_{k+1,k}) \in \mathbb{R}^k$.

Ta có:

$$(\forall j \in \{1,..., k\}, V_{k+1} \perp V_j) \Leftrightarrow \forall\, j \in \{1,..., k\}, \quad < V_j, e_{k+1} + \sum_{i=1}^{k} \lambda_{k+1,i} V_i > = 0$$

$$\Leftrightarrow \left(\forall j \in \{1,...,k\}, < V_j, e_{k+1} > + \sum_{i=1}^{k} \lambda_{k+1,i} < V_j, V_i > = 0 \right)$$

$$\Leftrightarrow \left(\forall j \in \{1,...,k\}, \ < V_j, e_{k+1} > + \lambda_{k+1,j} \| V_j \|^2 = 0 \right)$$

Vì $V_1,\ldots, V_k$ đều $\neq 0$, hệ phương trình trên có nghiệm duy nhất:

$$\forall j \in \{1,\ldots,k\}, \quad \lambda_{k+1,j} = -\frac{< V_j, e_{k+1} >}{\| V_j \|^2}.$$

Xét vectơ V_{k+1} đã được xác định như trên.

Do cách xây dựng $(V_1,\ldots,V_{k+1})$ là một họ trực giao.

Nếu $V_{k+1} = 0$, thì:

$$e_{k+1} = -\sum_{i=1}^{k} \lambda_{k+1,i} V_i \in \text{Vect}(V_1,\ldots,V_k) = \text{Vect}(e_1,\ldots,e_k),$$

mâu thuẫn với sự kiện $(e_1,\ldots,e_{k+1})$ độc lập tuyến tính.

Như vậy : $V_{k+1} \neq 0$.

Vì $V_{k+1} \in \text{Vect}(e_{k+1}, V_1,\ldots,V_k)$ và $\text{Vect}(V_1,\ldots,V_k) = \text{Vect}(e_1,\ldots,e_k)$, nên ta có:

$$V_{k+1} \in \text{Vect}(e_1,\ldots,e_{k+1}),$$

và vì vậy : $\text{Vect}(V_1, \ldots, V_{k+1}) \subset \text{Vect}(e_1, \ldots, e_{k+1})$.

Tương tự, $e_{k+1} \in \text{Vect}(V_1,\ldots, V_k, V_{k+1})$ và $\text{Vect}(e_1,\ldots,e_k) = \text{Vect}(V_1,\ldots, V_k)$, nên :

$$\text{Vect}(e_1,\ldots,e_{k+1}) \subset \text{Vect}(V_1,\ldots, V_{k+1}).$$

Cuối cùng: $\text{Vect}(e_1,\ldots, e_{k+1}) = \text{Vect}(V_1,\ldots, V_{k+1})$.

Ta tóm tắt việc khảo sát trên:

♦ **Định lý (Thủ tục trực giao hóa Schmidt)**

Với mọi họ độc lập tuyến tính $(e_1,\ldots, e_p)$ của một không gian vectơ Euclide E, tồn tại một họ $(V_1,\ldots, V_p)$ trong E sao cho :

$$\begin{cases} (V_1,\ldots, V_p) \text{ trực giao} \\ \forall k \in \{1,\ldots, p\}, \text{Vect}(V_1,\ldots,V_k) = \text{Vect}(e_1,\ldots, e_k). \end{cases}$$

NHẬN XÉT:

1) Trong định lý trên, họ $(V_1,\ldots, V_p)$ sẽ là duy nhất nếu ta thêm điều kiện:

$$\forall k \in \{1,\ldots, p\}, \ < V_k, e_k > = 1.$$

2) Vì trong cách xây dựng, V_k được phân tích theo $e_k, V_1,\ldots, V_{k-1}$, nên ma trận chuyển từ $(e_1,\ldots, e_k)$ sang $(V_1,\ldots, V_k)$ là ma trận tam giác trên với các hạng tử chéo bằng 1. ■

Ta viết tắt cơ sở trực chuẩn là c.s.t.c.

♦ **Hệ quả 1 (Định lý về c.s.t.c không đầy đủ)**

Với mọi họ trực chuẩn $(e_1,..., e_p)$ của một không gian vectơ Euclide E, tồn tại $e_{p+1},..., e_n \in E$ (trong đó $n = \dim(E)$) sao cho $(e_1,..., e_n)$ là một c.s.t.c của E.

Chứng minh:

Theo định lý về cơ sở không đầy đủ, dạng yếu (6.4, Định lý 2), tồn tại $(x_{p+1},..., x_n)$ sao cho $(e_1,..., e_p, x_{p+1},..., x_n)$ là một cơ sở của E. Phương pháp trực giao hóa Schmidt bảo toàn $e_1,..., e_p$ và cho một họ trực giao $(e_1,..., e_p, V_{p+1},..., V_n)$, với các hạng tử đều $\neq 0$. Đặt $e_k = \frac{1}{\|V_k\|} V_k$ với $k \in \{p+1,..., n\}$, ta được một họ trực chuẩn $(e_1,..., e_n)$ và do vậy một c.s.t.c của E.

♦ **Hệ quả 2**

Mọi không gian vectơ Euclide có ít nhất một c.s.t.c.

Chứng minh:

Chỉ cần áp dụng Hệ quả 1 cho họ rỗng.

NHẬN XÉT:

Nếu $\mathcal{B} = (e_1,..., e_n)$ là một c.s.t.c của E thì:

$$\forall x \in E,\ x = \sum_{i=1}^{n} < e_i, x > e_i .$$

Thực vậy, với $x \in E$, tồn tại $(x_1,..., x_n) \in \mathbb{R}^n$ sao cho $x = \sum_{i=1}^{n} x_i e_i$ và với mọi i thuộc $\{1,..., n\}$:

$$< e_i, x > = < e_i, \sum_{j=1}^{n} x_j e_j > = \sum_{j=1}^{n} x_j < e_i, e_j > = x_i .$$

♦ **Mệnh đề 1** Giả sử E là một không gian vectơ Euclide, $\mathcal{B}$ là một c.s.t.c của E, $x, y \in E$, $X = \mathrm{Mat}_{\mathcal{B}}(x) = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, $y = \mathrm{Mat}_{\mathcal{B}}(y) = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$.

Khi đó ta có: $< x, y > = {}^{t}XY = \sum_{i=1}^{n} x_i y_i$.

Chứng minh:

Đặt $\mathcal{B} = (e_1,..., e_n)$, ta có:

$$< x, y > = < \sum_{i=1}^{n} x_i e_i, \sum_{j=1}^{n} y_j e_j > = \sum_{\substack{1 \le i \le n \\ 1 \le j \le n}} x_i y_j < e_i, e_j > = \sum_{i=1}^{n} x_i y_i .$$

vì rằng $< e_i, e_j > = \begin{cases} 1 & \text{nếu } i = j \\ 0 & \text{nếu } i \neq j \end{cases}$.

♦ **Mệnh đề - Định nghĩa 2** Cho E là một không gian vectơ Euclide.

Với mọi kgvc F của E, $F^\perp$ là một phần bù của F trong E, gọi là **phần bù trực giao của F trong E.**

Nói riêng: $\dim(F^\perp) = \dim(E) - \dim(F)$.

Chứng minh:

Theo Hệ quả 2, F có ít nhất một c.s.t.c $(e_1, ..., e_p)$, sau đó theo Hệ quả 1, tồn tại $e_{p+1}, ..., e_n \in E$ sao cho $(e_1, ..., e_n)$ là một c.s.t.c. của E.

Ta chứng minh rằng: $F^\perp = \text{Vect}(e_{p+1}, ..., e_n)$.

Giả sử $x \in E$, $x = \sum_{i=1}^{n} x_i e_i$ là phân tích của x trên cơ sở $(e_1,...,e_n)$ của E. Ta có:

$$x \in F^\perp \Leftrightarrow (\forall j \in \{1,..., p\}, \ < e_j, x > = 0)$$

$$\Leftrightarrow (\forall j \in \{1,..., p\}, \ \sum_{i=1}^{n} x_i < e_j, e_i > = 0)$$

$$\Leftrightarrow (\forall j \in \{1, ..., p\}, \ x_j = 0)$$

$$\Leftrightarrow x \in \text{Vect}(e_{p+1}, ..., e_n).$$

Như vậy, $F = \text{Vect}(e_1,..., e_p)$ và $F^\perp = \text{Vect}(e_{p+1},...,e_p)$ bù nhau trong E.

♦ **Hệ quả 3** Cho E là một không gian vectơ Euclide.

1) Với mọi kgvc F của E : $F^{\perp\perp} = F$.

2) Với mọi kgvc F, G của E : $(F \cap G)^\perp = F^\perp + G^\perp$.

Chứng minh:

1) Ta đã thấy: $F \subset F^{\perp\perp}$ (xem 10.1.3, Mệnh đề 1, *4*)).

Hơn nữa: $\dim(F^{\perp\perp}) = \dim(E) - (\dim(E) - \dim(F)) = \dim(F)$.

2) Ta đã thấy: $(F \cap G)^\perp \supset F^\perp + G^\perp$ (xem 10.1.3, Mệnh đề 1, *7*)). Hơn nữa:

$$\begin{aligned}\dim((F \cap G)^\perp) &= \dim(E) - \dim(F \cap G) \\ &= \dim(E) - (\dim(F) + \dim(G) - \dim(F+G)) \\ &= (\dim(E) - \dim(F)) + (\dim(E) - \dim(G)) - (\dim(E) - \dim(E+G)) \\ &= \dim(F^\perp) + \dim(G^\perp) - \dim((F+G)^\perp) \\ &= \dim(F^{\perp\perp}) + \dim(G^\perp) - \dim(F^{\perp\perp} \cap G^\perp), \text{ xem 10.1.3, Mệnh đề 1, } 7) \\ &= \dim(F^\perp + G^\perp).\end{aligned}$$

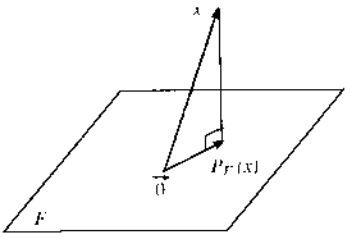
10.2.2 Phép chiếu trực giao, phép đối xứng trực giao

Cho E là một không gian Euclide, $<\cdot, \cdot>$ là tích vô hướng, $n = \dim(E)$.

♦ **Định nghĩa 1** Với mọi kgvc F của E, phép chiếu lên F song song với $F^\perp$ gọi là **phép chiếu trực giao lên** F.

Gọi p_F là phép chiếu trực giao lên F, ta có (xem 7.2.2, Mệnh đề 7):

$$\begin{cases} p_F \circ p_F = p_F, \quad \mathrm{Im}(p_F) = F, \quad \mathrm{Ker}(p_F) = F^\perp \\ \forall\, x \in E, \quad (p_F(x) \in F, \quad x - p_F(x) \in F^\perp). \end{cases}$$



♦ **Mệnh đề 1** Giả sử p là một phép chiếu của E (nghĩa là: $p \in \mathcal{L}(E)$ và $p \circ p = p$). Các tính chất sau là tương đương:

(i) p là một phép chiếu trực giao

(ii) $\forall\, (x, y) \in E^2, <p(x), y> = <x, p(y)>$.

Chứng minh:

(i) ⇒ (ii) :

Giả sử p là một phép chiếu trực giao, nghĩa là $p \circ p = p$ và $\mathrm{Ker}(p) = (\mathrm{Im}(p))^\perp$.

Giả sử $(x, y) \in E^2$. Ta có:

$$<p(x), y> = <p(x), y - p(y)> + <p(x), p(y)> = <p(x), p(y)>.$$

vì $p(x) \in \mathrm{Im}(p)$ và $y - p(y) \in \mathrm{Ker}(p)$.

Tương tự : $<x, p(y)> = <x - p(x), p(y)> + <p(x), p(y)> = <p(x), p(y)>$.

do đó: $<x, p(y)> = <p(x), y>$.

(ii) ⇒ (i)

Giả sử: $\forall (x, y) \in E^2, <x, p(y)> = <p(x), y>$.

Với mọi (x, y) thuộc $\mathrm{Ker}(p) \times \mathrm{Im}(p)$, ta có :

$$<x, y> = <x, p(y)> = <p(x), y> = <0, y> = 0.$$

và vì vậy p là một phép chiếu trực giao.

♦ **Định nghĩa 2** Giả sử F là một kgvc của E, $x \in E$. **Khoảng cách từ** x **tới** F, ký hiệu là $d(x, F)$, là số thực xác định bởi: $d(x, F) = \inf_{y \in F} \|x - y\|$.

Đây là một trường hợp đặc biệt của khoảng cách từ một điểm tới một bộ phận khác rỗng trong một kgv định chuẩn (xem Tập 3, 1.1.8, Định nghĩa1).

◆ **Mệnh đề 2** Giả sử F là một kgvc của E, $x \in E$. Ta có :

$$\begin{cases} \forall\, y \in F, \quad \|x - y\| \geq \|x - p_F(x)\| \\ \forall\, y \in F, \quad (\|x - y\| = \|x - p_F(x)\| \Leftrightarrow y = p_F(x)). \end{cases}$$

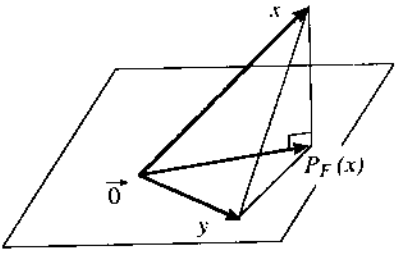
Nói cách khác, ánh xạ $F \to \mathbb{R}$, $y \mapsto \|x - y\|$ có biên dưới và chỉ đạt được biên dưới đó tại $p_F(x)$.

Chứng minh:

Chỉ cần nhận xét rằng với mọi $y \in F$ ta có:

$$\|x - y\|^2 = \|(x - p_F(x)) + (p_F(x) - y)\|^2$$
$$= \|x - p_F(x)\|^2 + \|p_F(x) - y\|^2,$$

vì $x - p_F(x) \in F^\perp$ và $p_F(x) - y \in F$.



◆ **Mệnh đề 3** Giả sử F là một kgvc của E. $(e_1,...,e_p)$ là một c.s.t.c của F. Khi đó ta có :

$$\forall x \in E, \quad p_F(x) = \sum_{i=1}^{p} < e_i, x > e_i \,.$$

Chứng minh :

Theo 10.2.1, Nhận xét, áp dụng cho $p_F(x)$ xem như một phần tử của F, ta có:

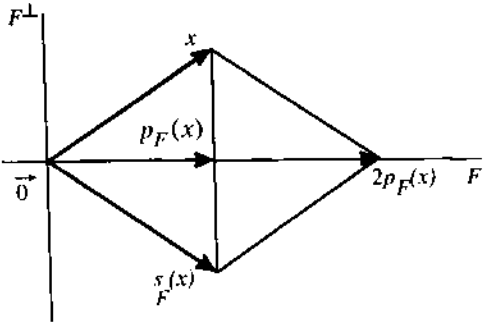
$$p_F(x) = \sum_{i=1}^{p} < e_i, p_F(x) > e_i = \sum_{i=1}^{p} < e_i, p_F(x) - x > e_i + \sum_{i=1}^{p} < e_i, x > e_i \,.$$

Mặt khác: $\forall\, i \in \{1,..., p\}$, $< e_i, p_F(x) - x > = 0$ vì $p_F(x) - x \in F^\perp$.

◆ **Định nghĩa 3** Với mọi kgvc F của E, **phép đối xứng trực giao qua** F là tự đồng cấu s_F của E xác định bởi: $s_F = 2p_F - e$, trong đó p_F là phép chiếu trực giao lên F, và $e = \mathrm{Id}_E$.

Hiển nhiên rằng:

$$\begin{cases} s_F \circ s_F = e. \\ \mathrm{Ker}(s_F - e) = F,\ \mathrm{Ker}(s_F + e) = F^\perp \\ p_F = \dfrac{1}{2}(e + s_F). \end{cases}$$



NHẬN XÉT: Giả sử F là một kgvc của E, $(e_1,...,e_p)$ là một c.s.t.c của F, mà ta bổ xung thành một c.s.t.c $\mathcal{B} = (e_1,...,e_n)$ của E (xem 10.2.1, Hệ quả 1). Khi đó:

$$\mathrm{Mat}_{\mathcal{B}}(s_F) = \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ & 0 & & 0 \\ & & & & \ddots \\ 0 & & & & & 0 \end{pmatrix}, \quad \mathrm{Mat}_{\mathcal{B}}(p_F) = \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ & & & -1 \\ & 0 & & & \ddots \\ 0 & & & & & -1 \end{pmatrix}$$

(dưới mỗi ma trận: p và $n - p$)

10.2.3 Siêu phẳng

Ta nhắc lại rằng trong một kgv n chiều E, siêu phẳng là các kgvc $n - 1$ chiều của E (xem 6.4, Định nghĩa 2).

Cho E là một không gian vectơ Euclide, $<\cdot, \cdot>$ là tích vô hướng, $n = \dim(E) \geq 1$.

Mệnh đề 1 Với mọi u thuộc E, ánh xạ $\varphi_u: E \to \mathbb{R}$, $x \mapsto <u, x>$ là một dạng tuyến tính trên E.

Chứng minh:

$\forall \alpha \in \mathbb{R}, \forall x, y \in E,$

$$\varphi_u(\alpha x + y) = <u, \alpha x + y> = \alpha <u, x> + <u, y> = \alpha\varphi_u(x) + \varphi_u(y).$$

Mệnh đề 2

Ánh xạ $\delta: E \to E^*$, $u \mapsto \varphi_u$ là một đẳng cấu kgv.

Ta nhắc lại rằng, $E^* = \mathcal{L}(E, \mathbb{R})$ là đối ngẫu của E (xem 7.1.1, Định nghĩa 3).

Chứng minh:

1) δ tuyến tính vì: $\forall \alpha \in \mathbb{R}, \forall u, v \in E. \forall x \in E,$

$$\begin{aligned}(\delta(\alpha u + v))(x) &= \varphi_{\alpha u + v}(x) = <\alpha u + v, x> \\ &= \alpha <u, x> + <v, x> = \alpha\varphi_u(x) + \varphi_v(x) \\ &= (\alpha\varphi_u + \varphi_v)(x) = (\alpha\delta(u) + \delta(v))(x).\end{aligned}$$

2) Giả sử $u \in \mathrm{Ker}(\delta)$. Ta có $\delta(u) = 0$, do vậy: $\forall x \in E, <u, x> = 0$.

Nói riêng: $||u||^2 = <u, u> = 0$, do vậy $u = 0$.

Như vậy, $\mathrm{Ker}(\delta) = \{0\}$, do đó δ là đơn ánh.

3) Theo 7.3.2, Mệnh đề, $\dim(E^*) = \dim(\mathcal{L}(E, \mathbb{R})) = \dim(E).\dim(\mathbb{R}) = \dim(E)$.

Từ đó suy ra (xem 7.3.1, Định lý 1) δ là một đẳng cấu kgv. ■

Cho H là một siêu phẳng của E.

Vì $\dim(H^\perp) = \dim(E) - \dim(H)$

$= n - (n - 1) = 1$,

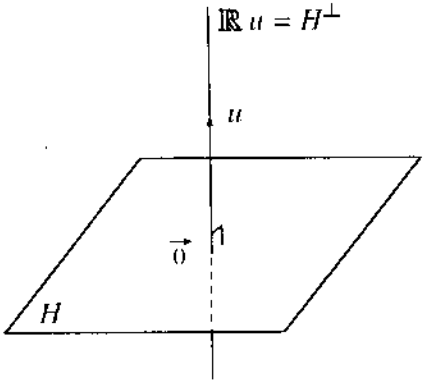
nên $H^\perp$ là một đường thẳng vectơ.

Do vậy tồn tại $u \in E$ sao cho $H^\perp = \mathbb{R}u$.

Khi đó hiển nhiên ta có:

$H = H^{\perp\perp} = (\mathbb{R}u)^\perp = \{u\}^\perp$.

Đường thẳng vectơ $\mathbb{R}u$ được gọi là **đường thẳng pháp với siêu phẳng** H.



Với các ký hiệu của hai Mệnh đề trên đây :

$$H = \mathrm{Ker}(\varphi_u) = \mathrm{Ker}(\delta(u)).$$

♦ **Định nghĩa** Mọi phép đối xứng trực giao qua một siêu phẳng của E gọi là một phép **phản chiếu** (của E).

Bài tập

◊ **10.2.1** * Cho E là một kgv Euclide, $\langle \cdot , \cdot \rangle$ là tích vô hướng, $x, y \in E$. Ta giả thiết $\dim(E) \geq 2$.

a) Chứng minh rằng, nếu $||x|| = ||y||$, thì tồn tại một siêu phẳng H của E sao cho $y = s_H(x)$.

b) Chứng minh rằng, nếu $\langle x, y \rangle = ||y||^2$, thì tồn tại một siêu phẳng H của E sao cho $y = p_H(x)$.

10.3 Nhóm trực giao

10.3.1 Tự đồng cấu trực giao

Cho $n \in \mathbb{N}^*$, E là một không gian vectơ Euclide n chiều, $<.\ ,\ .>$ là tích vô hướng.

♦ **Định nghĩa** Một tự đồng cấu f của E được gọi là **trực giao** khi và chỉ khi f bảo toàn tích vô hướng, nghĩa là:

$$\forall\ (x, y) \in E^2, \quad <f(x), f(y)> = <x, y>.$$

Ta ký hiệu $\mathcal{O}(E, <\cdot\ ,\ \cdot>)$ hoặc $\mathcal{O}(E)$ là tập hợp các tự đồng cấu trực giao của E.

NHẬN XÉT:

Do sự thiếu nhất quán của thuật ngữ, một phép chiếu trực giao của E (trừ Id_E) không phải là một tự đồng cấu trực giao. Trái lại, mọi phép đối xứng trực giao của E là một tự đồng cấu trực giao của E.

♦ **Mệnh đề 1** Giả sử $f \in \mathcal{L}(E)$. Hai tính chất sau là tương đương:

(i) $f \in \mathcal{O}(E)$.

(ii) $\forall\ x \in E,\ ||f(x)|| = ||x||$.

Chứng minh:

(i) ⇒ (ii)

Hiển nhiên khi thay y bằng x vào định nghĩa.

(ii) ⇒ (i)

Giả sử: $\forall\ x \in E,\ ||f(x)|| = ||x||$. Với mọi $(x, y) \in E^2$, ta có:

$$\begin{aligned} 2<f(x), f(y)> &= ||f(x) + f(y)||^2 - ||f(x)||^2 - ||f(y)||^2 \\ &= ||f(x + y)||^2 - ||f(x)||^2 - ||f(y)||^2 \\ &= ||x + y||^2 - ||x||^2 - ||y||^2 = 2<x, y>, \end{aligned}$$

và do vậy $f \in \mathcal{O}(E)$.

Các phần tử của $\mathcal{O}(E)$ cũng được gọi là những phép **đẳng cự vectơ**.

♦ **Mệnh đề 2** Cho $f \in \mathcal{L}(E)$. Các tính chất sau tương đương từng đôi một:

(i) $f \in \mathcal{O}(E)$

(ii) Với mọi c.s.t.c. $\mathcal{B}$ của E, $f(\mathcal{B})$ là một c.s.t.c của E

(iii) Tồn tại một c.s.t.c. $\mathcal{B}$ của E sao cho $f(\mathcal{B})$ là một c.s.t.c của E.

Chứng minh:

(i) ⇒ (ii):

Giả sử $f \in \mathcal{O}(E)$ và giả sử $\mathcal{B} = (e_1,...,e_n)$ là một c.s.t.c của E. Thế thì ta có:

$$\forall (i, j) \in \{1,..., n\}^2, \ < f(e_i), f(e_j) > = < e_i, e_j > = \delta_{ij},$$

do vậy $f(\mathcal{B})$ là một c.s.t.c của E.

(ii) ⇒ (iii):

Dễ dàng suy ra từ sự tồn tại của một c.s.t.c trong E (Xem 10.2.1, Hệ quả 2).

(iii) ⇒ (i):

Giả sử tồn tại một c.s.t.c. $\mathcal{B} = (e_1,..., e_n)$ của E sao cho $f(\mathcal{B}) = (f(e_1),..., f(e_n))$ là một c.s.t.c của E.

Giả sử $(x, y) \in E^2$, $(x_1,..., x_n)$ (tương ứng: $(y_1,..., y_n)$) là các thành phần của x (tương ứng: y) trong $\mathcal{B}$:

$$x = \sum_{i=1}^{n} x_i e_i, \qquad y = \sum_{j=1}^{n} y_j e_j .$$

Thế thì: $< f(x), f(y) > = < \sum_{i=1}^{n} x_i f(e_i), \ \sum_{j=1}^{n} y_j f(e_j) >$

$$= \sum_{1 \le i, j \le n} x_i y_j < f(e_i), f(e_j) > \ = \sum_{i=1}^{n} x_i y_i = < x, y >,$$

và do đó: $f \in \mathcal{O}(E)$.

♦ **Mệnh đề - Định nghĩa 3** Tập hợp $\mathcal{O}(E)$ các tự đồng cấu trực giao của E là một nhóm đối với luật $\circ$, gọi là **nhóm trực giao** của E.

Chứng minh:

Chúng ta sẽ chứng tỏ rằng $\mathcal{O}(E)$ là một nhóm con của $\mathcal{GL}(E)$ (xem 7.2.3, Mệnh đề - Định nghĩa).

1) Cho $f \in \mathcal{O}(E)$.

Giả sử $x \in E$ thỏa mãn $f(x) = 0$; thế thì ta có: $|| x || = || f(x) || = 0$, do vậy $x = 0$. Vậy $\mathrm{Ker}(f) = \{0\}$ nên f là đơn ánh. Vì $f \in \mathcal{L}(E)$ là đơn ánh và E hữu hạn chiều, nên f là một tự đẳng cấu của E (Xem 7.3.1, Định lý 2).

Điều đó chứng tỏ: $\mathcal{O}(E) \subset \mathcal{GL}(E)$.

2) Hiển nhiên là $\mathrm{Id}_E \in \mathcal{O}(E)$.

3) Nếu $f, g \in \mathcal{O}(E)$, thì:

$$\forall (x, y) \in E^2, < (g \circ f)(x), (g \circ f)(y) > = < f(x), f(y) > = < x, y >,$$

do đó: $g \circ f \in \mathcal{O}(E)$.

4) Giả sử $f \in \mathcal{O}(E)$. Ta có :

$$\forall (x, y) \in E^2, < f^{-1}(x), f^{-1}(y) > = < f(f^{-1}(x)), \ f(f^{-1}(y)) > = < x, y >,$$

và do đó $f^{-1} \in \mathcal{O}(E)$.

10.3.2 Ma trận trực giao

Cho $n \in \mathbb{N}^*$.

♦ **Định nghĩa 1** Một ma trận Ω thuộc $\mathbf{M}_n(\mathbb{R})$ được gọi là **trực giao** khi và chỉ khi tự đồng cấu của $\mathbb{R}^n$ được biểu diễn bởi Ω trong cơ sở chính tắc của $\mathbb{R}^n$ là một tự đồng cấu trực giao của $\mathbb{R}^n$ với tích vô hướng thông thường.

Ta ký hiệu tập hợp các ma trận trực giao của $\mathbf{M}_n(\mathbb{R})$ là $\mathbf{O}_n(\mathbb{R})$.

♦ **Mệnh đề 1** Cho $\Omega \in \mathbf{M}_n(\mathbb{R})$, E là một $\mathbb{R}$ - kgv n chiều, $< \cdot , \cdot >$ là một tích vô hướng trên E. Các tính chất sau từng đôi một tương đương :

1) $\Omega \in \mathbf{O}_n(\mathbb{R})$

2) ${}^t\Omega\Omega = \mathbf{I}_n$

3) $\Omega\, {}^t\Omega = \mathbf{I}_n$

4) Với mọi c.s.t.c B của E, tự đồng cấu của E được biểu diễn bởi Ω trong cơ sở $\mathcal{B}$ là trực giao.

5) Tồn tại một c.s.t.c của E, sao cho trong cơ sở đó tự đồng cấu được biểu diễn bởi Ω là trực giao.

6) Các cột của Ω tạo thành một c.s.t.c của $\mathbf{M}_{n,1}(\mathbb{R})$ đối với tích vô hướng thông thường.

7) Các dòng của Ω tạo thành một c.s.t.c của $\mathbf{M}_{1,n}(\mathbb{R})$ đối với tích vô hướng thông thường.

Chứng minh :

Gọi g là tự đồng cấu của $\mathbb{R}^n$ được biểu diễn bởi Ω trong cơ sở trực chuẩn $\mathcal{B}_0$ của $\mathbb{R}^n$.

1) ⇔ 2):

1) $\Leftrightarrow \forall (x, y) \in (\mathbb{R}^n)^2, < g(x), g(y) > = < x, y >$

$\Leftrightarrow \forall (X, Y) \in (\mathbf{M}_{n,1}(\mathbb{R}))^2, {}^t(\Omega X)\Omega Y = {}^t XY$

$\Leftrightarrow \forall (X, Y) \in (\mathbf{M}_{n,1}(\mathbb{R}))^2, {}^t X({}^t\Omega\Omega)Y = {}^t XY.$

• Áp dụng đẳng thức cuối cùng cho $X = \mathrm{E}_i$ và $Y = \mathrm{E}_j$, trong đó $(\mathrm{E}_1, ..., \mathrm{E}_n)$ là cơ sở chính tắc của $\mathbf{M}_{n,1}(\mathbb{R})$; vì ${}^t\mathrm{E}_i({}^t\Omega\Omega)\mathrm{E}_j$ là hạng tử thứ (i, j) của ${}^t\Omega\Omega$, nên ta suy ra ${}^t\Omega\Omega = \mathbf{I}_n$.

• Đảo lại là hiển nhiên.

2) ⇔ 3): Theo 8.1.5, Định lý.

2) ⇔ 4):

Giả sử $\mathcal{B}$ là một c.s.t.c của E, f là tự đồng cấu của E được biểu diễn bởi Ω trong cơ sở $\mathcal{B}$. Ta có:

$$\forall (x, y) \in E^2, < f(x), f(y) > = < x, y >$$
$$\Leftrightarrow \forall (X, Y) \in (\mathbf{M}_{n,1}(\mathbb{R}))^2, {}^t(\Omega X)\, \Omega Y = {}^t XY$$
$$\Leftrightarrow {}^t\Omega\Omega = \mathbf{I}_n,$$

như trên đây đối với tương đương thức 1) ⇔ 2).

2) ⇔ 5):

Do 2) ⇔ 4), vì theo Hệ quả 2 (xem 10.2.1) tồn tại một c.s.t.c.

1) ⇔ 6):

Thực vậy, các cột của Ω biểu diễn các thành phần của ảnh qua g của các vectơ thuộc $\mathcal{B}_0$.

1) ⇔ 7):

Suy ra từ 2) ⇔ 3), và 1) ⇔ 6) áp dụng cho ${}^t\Omega$. ■

♦ **Mệnh đề 2** $\mathbf{O}_n(R)$ là một nhóm đối với phép nhân, gọi là **nhóm trực giao (cấp n)**.

Chứng minh:

Chúng ta sẽ chứng tỏ rằng $\mathbf{O}_n(\mathbb{R})$ là một nhóm con của $\mathbf{GL}_n(\mathbb{R})$.

- $\mathbf{O}_n(\mathbb{R}) \subset \mathbf{GL}_n(\mathbb{R})$ vì mọi ma trận trực giao Ω là khả nghịch (nó có nghịch đảo là ${}^t\Omega$).
- $\mathrm{I}_n \in \mathbf{O}_n(\mathbb{R})$.
- Với mọi Ω_1, Ω_2 thuộc $\mathbf{O}_n(\mathbb{R})$:

$$ {}^t(\Omega_1\Omega_2)\,\Omega_1\Omega_2 = {}^t\Omega_2\,({}^t\Omega_1\,\Omega_1)\Omega_2 = {}^t\Omega_2\,\Omega_2 = \mathrm{I}_n, $$

do vậy $\Omega_1\Omega_2 \in \mathbf{O}_n(\mathbb{R})$.

Với mọi Ω thuộc $\mathbf{O}_n(\mathbb{R})$, $\Omega^{-1} = {}^t\Omega \in \mathbf{O}_n(\mathbb{R})$ *vì* ${}^t\Omega\Omega = \mathrm{I}_n$.

NHẬN XÉT:

Giả sử $\mathcal{B}$ là một c.s.t.c của E, $f \in \mathcal{L}(E)$, $\Omega = \mathrm{Mat}_{\mathcal{B}}(f)$.

Thế thì: $f \in \mathcal{O}(E) \Leftrightarrow \Omega \in \mathbf{O}_n(\mathbb{R})$.

Ánh xạ $\mathcal{O}(E) \to \mathbf{O}_n(\mathbb{R})$ là một đẳng cấu nhóm.

$$ f \mapsto \mathrm{Mat}_{\mathcal{B}}(f)\mathrm{p} $$

♦ **Mệnh đề 3** Giả sử $\mathcal{B}$ là một c.s.t.c, $\mathcal{B}'$ là một cơ sở của E, P là ma trận chuyển từ $\mathcal{B}$ sang $\mathcal{B}'$. Thế thì: $\mathcal{B}'$ là một c.s.t.c khi và chỉ khi P trực giao.

Chứng minh:

Giả sử $f \in \mathcal{L}(E)$ xác định bởi $\mathrm{Mat}_{\mathcal{B}}(f) = P$. Theo Mệnh đề 1, $\mathcal{B}'$ là một c.s.t.c khi và chỉ khi $f \in \mathcal{O}(E)$. Và theo Mệnh đề trên: $f \in \mathcal{O}(E) \Leftrightarrow P \in \mathbf{O}_n(\mathbb{R})$. ■

♦ **Mệnh đề 4**

1) $\forall\, \Omega \in \mathbf{O}_n(\mathbb{R})$, $\det(\Omega) \in \{-1,1\}$.

2) $\forall\, f \in \mathcal{O}(E)$, $\det(f) \in \{-1, 1\}$.

Chứng minh:

1) $\Omega \in \mathbf{O}_n(\mathbb{R}) \Leftrightarrow {}^t\Omega\Omega = \mathrm{I}_n \Rightarrow (\det(\Omega))^2 = \det({}^t\Omega\Omega) = 1$.

2) Suy từ 1).

♦ **Định nghĩa 2** Giả sử $f \in \mathcal{O}(E)$. Ta nói f là một tự đồng cấu trực giao **thuận** (tương ứng: **nghịch**) khi và chỉ khi $\det(f) = 1$ (tương ứng: $\det(f) = -1$).

Ta cũng nói: **phải** thay cho thuận.
trái thay cho nghịch.

NHẬN XÉT:

Với $f \in \mathcal{GL}(E)$, f là một tự đồng cấu trực giao thuận khi và chỉ khi f là một tự đồng cấu trực giao và một tự đồng cấu thuận (xem 9.7, Định nghĩa 3).

♦ **Mệnh đề - Định nghĩa 5** Tập hợp các tự đồng cấu trực giao thuận của E là một nhóm con của $\mathcal{O}(E)$, gọi là **nhóm trực giao đặc biệt của** E, ký hiệu là $\mathcal{SO}(E)$.

Chứng minh:

- $\mathcal{SO}(E) \subset \mathcal{O}(E)$
- $\det(\mathrm{Id}_E) = 1$
- $\forall f, g \in \mathcal{SO}(E)$, $\det(g \circ f) = \det(g)\det(f) = 1.1 = 1$
- $\forall f \in \mathcal{SO}(E)$, $\det(f^{-1}) = (\det(f))^{-1} = 1^{-1} = 1$. ■

Từ kết quả trên ta suy ra mệnh đề sau:

♦ **Mệnh đề - Định nghĩa 6** Cho $\Omega \in \mathbf{O}_n(\mathbb{R})$.
Ta nói Ω trực giao **phải** (tương ứng: **trái**) khi và chỉ khi $\det(\Omega) = 1$ (tương ứng: -1). Tập hợp các ma trận trực giao phải cấp n là một nhóm con của $\mathbf{O}_n(\mathbb{R})$, gọi là **nhóm trực giao đặc biệt**, ký hiệu là $\mathbf{SO}_n(\mathbb{R})$.

NHẬN XÉT:

Giả sử $\mathcal{B}$ là một c.s.t.c của E, $f \in \mathcal{L}(E)$, $\Omega = \mathrm{Mat}_{\mathcal{B}}(f)$.

Thế thì: $f \in \mathcal{SO}(E) \Leftrightarrow \Omega \in \mathbf{SO}_n(\mathbb{R})$.

Ánh xạ $\mathcal{SO}(E) \to \mathbf{SO}_n(\mathbb{R})$ là một đẳng cấu nhóm.
$f \mapsto \mathrm{Mat}_{\mathcal{B}}(f)$

♦ **Định nghĩa 3** Một không gian vectơ Euclide E được gọi là **định hướng** khi và chỉ khi kgv E là định hướng.

Nói cách khác, một không gian vectơ Euclide định hướng là một không gian vectơ Euclide trong đó ta đã chọn một cơ sở (trực giao hay không) làm cơ sở thuận.

Ta viết tắt cơ sở trực chuẩn thuận là c.s.t.c.t.

♦ **Mệnh đề - Định nghĩa 7** Giả sử E là một không gian vectơ Euclide định hướng, $(V_1, \ldots, V_n) \in E^n$. Định thức $\det_{\mathcal{B}}(V_1, \ldots, V_n)$ không phụ thuộc vào cách chọn c.s.t.c.t. $\mathcal{B}$, được gọi là **tích hỗn hợp** của $(V_1, \ldots, V_n)$ và được ký hiệu là $[V_1, \ldots, V_n]$.

Như vậy, với mọi c.s.t.c.t. $\mathcal{B}$ của E: $[V_1, \ldots, V_n] = \det_{\mathcal{B}}(V_1, \ldots, V_n)$.

Bài tập

◊ **10.3.1** Cho $A \in \mathbf{M}_n(\mathbb{R})$, $C_1, \ldots, C_n$ là các cột của A.

Chứng minh : $A \in \mathbf{O}_n(\mathbb{R}) \Leftrightarrow \sum_{j=1}^{n} C_j {}^tC_j = \mathbf{1}_n$.

◊ **10.3.2 Ma trận Householder**

Cho $C \in \mathbf{M}_{n,1}(\mathbb{R}) - \{0\}$, $S = \mathbf{I}_n - \frac{2}{{}^tCC} C^tC$ (gọi là *ma trận Householder*). Kiểm chứng rằng S là ma trận (trong cơ sở chính tắc) của phép phản chiếu qua siêu phẳng trực giao với C.

◊ **10.3.3** Chứng minh rằng : $\forall\, A = (a_{ij})_{ij} \in \mathbf{O}_n(\mathbb{R})$, $\left| \sum_{1 \le i,j \le n} a_{ij} \right| \le n$, và xét trường hợp đẳng thức.

◊ **10.3.4** Cho E là một kgv Euclide n chiều, $\mathcal{B}$ là một c.s.t.c của E, $V_1, \ldots, V_n \in E$.

a) Chứng minh: $|\det_{\mathcal{B}}(V_1, \ldots, V_n)| \le \prod_{i=1}^{n} \| V_i \|$.

b) Xét trường hợp đẳng thức.

◊ **10.3.5 Tự đồng cấu trực giao cảm sinh**

Cho E là một kgv Euclide, F là một kgvc của E, $f \in \mathrm{O}(E)$. Ta giả thiết là $f(E) \subset F$. Chứng minh :

$$\begin{cases} f(F) = F \\ f(F^\perp) = F^\perp \end{cases} \quad \text{và} \quad \begin{cases} f|_F \in \mathcal{O}(F) \\ f|_{F^\perp} \in \mathcal{O}(F^\perp) \end{cases}.$$

◊ **10.3.6 Dán những tự đồng cấu trực giao**

Giả sử E là một kgv Euclide, F là một kgvc của E, $u \in \mathcal{O}(F)$, $v \in \mathcal{O}(F^\perp)$, f là ánh xạ từ E vào F xác định bởi :

$$\forall x \in E,\ f(x) = u(p_F(x)) + v(p_{F^\perp}(x)).$$

Chứng minh rằng : $f \in \mathcal{O}(E)$.

◊ **10.3.7 Phân tích một tự đồng cấu trực giao thành tích những phép phản chiếu**

Cho E là một kgv Euclide, $n = \dim(E)$, $f \in \mathcal{O}(E)$. Chứng minh rằng tồn tại $s_1, \ldots, s_n \in \mathcal{L}(E)$ sao cho $f = s_1 \circ \ldots \circ s_n$ và mỗi s_i ($1 \le i \le n$) là một phép phản chiếu hoặc phép đồng nhất. (Sử dụng các bài tập 10.2.1 và 10.3.5, 10.3.6).

10.4 Hình học vectơ Euclide phẳng

Ta ký hiệu E_2 là một không gian vectơ Euclide 2 chiều, · là tích vô hướng trên E_2.
Chúng ta sẽ viết tường minh các phần tử của $\mathbf{O}_2(\mathbb{R})$ và do đó các phần tử của $\mathcal{O}(E_2)$.

Giả sử $\Omega = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{M}_2(\mathbb{R})$. Ta có (xem 10.3.2, Mệnh đề 1):

$$\Omega \in \mathbf{O}_2(\mathbb{R}) \Leftrightarrow \begin{cases} a^2 + c^2 = 1 \\ ab + cd = 0 \\ b^2 + d^2 = 1 \end{cases} \Leftrightarrow \left(\begin{cases} c = 0 \\ a^2 = 1 \\ b = 0 \\ d^2 = 1 \end{cases} \text{ hoặc } \begin{cases} c \neq 0 \\ d = -\dfrac{ab}{c} \\ a^2 + c^2 = 1 \\ b^2 = c^2 \end{cases} \right)$$

$$\Leftrightarrow \left(\begin{cases} c = 0 \\ a^2 = 1 \\ b = 0 \\ d^2 = 1 \end{cases} \text{ hoặc } \begin{cases} c \neq 0 \\ b = c \\ d = -a \\ a^2 + c^2 = 1 \end{cases} \text{ hoặc } \begin{cases} c \neq 0 \\ b = -c \\ d = a \\ a^2 + c^2 = 1 \end{cases} \right).$$

Như vậy:

$$\mathbf{O}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & -c \\ c & a \end{pmatrix};\ (a,c) \in \mathbb{R}^2,\ a^2 + c^2 = 1 \right\} \cup \left\{ \begin{pmatrix} a & c \\ c & -a \end{pmatrix};\ (a,c) \in \mathbb{R}^2, a^2 + c^2 = 1 \right\}$$

$$= \left\{ \begin{pmatrix} a & -\varepsilon c \\ c & \varepsilon a \end{pmatrix};\ (a,c,\varepsilon) \in \mathbb{R} \times \mathbb{R} \times \{-1,1\},\ a^2 + c^2 = 1 \right\}.$$

Ta tóm tắt kết quả khảo sát:

♦ **Mệnh đề 1**

- $\mathbf{O}_2(\mathbb{R}) = \{R_\theta;\ \theta \in \mathbb{R}\} \cup \{S_\varphi;\ \varphi \in \mathbb{R}\}$, trong đó:

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix},\quad S_\varphi = \begin{pmatrix} \cos\varphi & \sin\varphi \\ \sin\varphi & -\cos\varphi \end{pmatrix}$$

- $\mathbf{SO}_2(\mathbb{R}) = \{R_\theta;\ \theta \in \mathbb{R}\}$.

Từ đây trở đi, ta giả thiết là E_2 được định hướng.

Phép quay

♦ **Định nghĩa 1** Giả sử $\mathcal{B}$ là một c.s.t.c.t của E_2 và $\theta \in \mathbb{R}$.
Phép tự đồng cấu của E_2 có ma trận trong cơ sở $\mathcal{B}$ là $R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ được gọi là **phép quay góc** θ, và được ký hiệu là Rot_θ.

Khái niệm phép quay cho phép đưa ra một định nghĩa chặt chẽ cho khái niệm góc giữa hai vectơ $\neq 0$ thuộc E_2, tất nhiên tương ứng với khái niệm trực giác đã biết. Chúng ta sẽ phát triển quan điểm này bằng cách dùng các tính chất sơ cấp của các hàm cos và sin (xem Tập 2, 7.8).

Giả sử $u, v \in E_2 - \{0\}$, $U = \dfrac{1}{\|u\|}u$, $V = \dfrac{1}{\|v\|}v$.

Ta chứng minh rằng tồn tại $\theta \in \mathbb{R}$, duy nhất modulo 2π, sao cho $\mathrm{Rot}_\theta(U) = V$.

Ta ký hiệu (u_1, u_2) (tương ứng: (v_1, v_2)) là các thành phần của U (tương ứng: V) trong c.s.t.c.t. $\mathcal{B}$ của E_2.

Vì $u_1^2 + u_2^2 = 1$ và $v_1^2 + v_2^2 = 1$, nên tồn tại $(\alpha, \beta) \in \mathbb{R}^2$ sao cho:

$$\begin{cases} u_1 = \cos\alpha \\ u_2 = \sin\alpha \end{cases} \text{ và } \begin{cases} v_1 = \cos\beta \\ v_2 = \sin\beta \end{cases}.$$

Với mọi θ thuộc $\mathbb{R}$, ta có: $\mathrm{Rot}_\theta(U) = V \Leftrightarrow \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix} = \begin{pmatrix} \cos\beta \\ \sin\beta \end{pmatrix}$

$$\Leftrightarrow \begin{cases} \cos\theta\cos\alpha - \sin\theta\sin\alpha = \cos\beta \\ \sin\theta\cos\alpha + \cos\theta\sin\alpha = \sin\beta \end{cases}$$

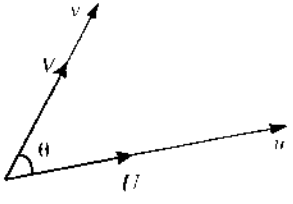
$$\Leftrightarrow \begin{cases} \cos(\theta+\alpha) = \cos\beta \\ \sin(\theta+\alpha) = \sin\beta \end{cases} \Leftrightarrow \theta \equiv \beta - \alpha\ |2\pi|.$$

Ta suy ra mệnh đề sau:

◆ **Mệnh đề - Định nghĩa 2** Giả sử $u, v \in E_2 - \{0\}$, $U = \dfrac{1}{\|u\|}u$, $V = \dfrac{1}{\|v\|}v$.

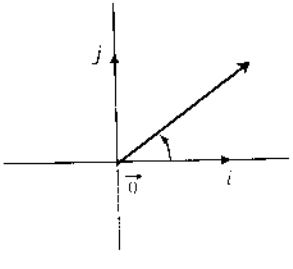
Tồn tại $\theta \in \mathbb{R}$, duy nhất modulo 2π, sao cho $\mathrm{Rot}_\theta(U) = V$; số thực θ này (hoặc lớp modulo 2π của nó) được gọi là **góc** của u và v, và ký hiệu là $(\widehat{u, v})$.

Như vậy ta có: $V = \mathrm{Rot}_{(\widehat{u,v})}(U)$

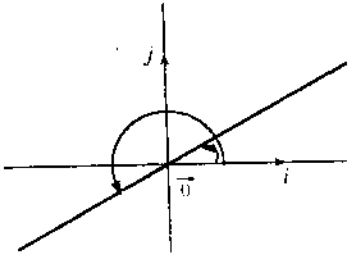


◆ **Định nghĩa 2** Giả sử $\mathcal{B} = (i, j)$ là một c.s.t.c.t của E_2.

- Với mọi $u \in E_2 - \{0\}$, **góc cực** của u (trong $\mathcal{B}$) là góc $(\widehat{i, u})$, xác định modulo 2π.
- **Góc cực** của một đường thẳng vectơ là góc cực của một vectơ chỉ phương của đường thẳng đó, xác định modulo π.



Góc cực của một vectơ



Góc cực của một đường thẳng

♦ Mệnh đề 3

$$\forall (u, v) \in (E_2 - \{0\})^2, \quad u.v = \|u\| \, \|v\| \cos(\widehat{u,v})$$

Chứng minh:

Với các ký hiệu trên đây:

$$u.v = \|u\| \, \|v\| \; U \bullet V = \|u\| \, \|v\| \, (\cos\alpha \cos B + \sin\alpha \sin\beta)$$

$$= \|u\| \, \|v\| \cos(\beta - \alpha) = \|u\| \, \|v\| \cos(\widehat{u,v}) .$$ ■

Ta nhắc lại rằng (xem 10.2.1, Nhận xét), nếu $B = (i, j)$ là một c.s.t.c của E_2, thì:

$$\forall\, u \in E_2, \quad u = (i \bullet u)\, i + (j \bullet u) j.$$ ■

♦ Mệnh đề 4

$$\forall (\theta, \theta') \in \mathbb{R}^2, \quad \mathrm{Rot}_\theta \circ \mathrm{Rot}_{\theta'} = \mathrm{Rot}_{\theta + \theta'}$$

Chứng minh:
$$R_\theta R_{\theta'} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \cos\theta' & -\sin\theta' \\ \sin\theta' & \cos\theta' \end{pmatrix}$$

$$= \begin{pmatrix} \cos\theta\cos\theta' - \sin\theta\sin\theta' & -\cos\theta\cos\theta' - \sin\theta\cos\theta' \\ \sin\theta\cos\theta' + \cos\theta\sin\theta' & -\sin\theta\sin\theta' + \cos\theta\cos\theta' \end{pmatrix}$$

$$= \begin{pmatrix} \cos(\theta+\theta') & -\sin(\theta+\theta') \\ \sin(\theta+\theta') & \cos(\theta+\theta') \end{pmatrix} = R_{\theta+\theta'} .$$

♦ Hệ quả (Hệ thức Chasles đối với góc)

$$\forall u, v, w \in E_2 - \{0\}, \qquad (\widehat{u,w}) \equiv (\widehat{u,v}) + (\widehat{v,w}) \quad [2\pi].$$

Chứng minh:

Đặt : $U = \dfrac{1}{\|u\|} u$, $V = \dfrac{1}{\|v\|} v$, $W = \dfrac{1}{\|w\|} w$.

Ta có: $W = \mathrm{Rot}_{(\widehat{v,w})}(V)$ và $V = \mathrm{Rot}_{(\widehat{u,v})}(U)$, nên:

$$W = \mathrm{Rot}_{(\widehat{v,w})} \circ \mathrm{Rot}_{(\widehat{u,v})}(U) = \mathrm{Rot}_{(\widehat{v,w})+(\widehat{u,v})}(U).$$

Mặt khác: $W = \mathrm{Rot}_{(\widehat{u,w})}(U)$.

Do đó: $(\widehat{u,v}) + (\widehat{v,w}) = (\widehat{u,w})\ [2\pi]$. ■

NHẬN XÉT: Vì $(\widehat{u,u}) = 0\ [2\pi]$, nên ta suy ra :

$$\forall u, v \in E_2 - \{0\}, \ (\widehat{v,u}) \equiv -(\widehat{u,v}) \quad [2\pi].$$

Phép phản chiếu

Giả sử $\varphi \in \mathbb{R}$, $S_\varphi = \begin{pmatrix} \cos\varphi & \sin\varphi \\ \sin\varphi & -\cos\varphi \end{pmatrix}$ (xem Mệnh đề 1), $\mathcal{B} = (i, j)$ là một c.s.t.c.t của E_2, s_φ là tự đồng cấu của E_2 có ma trận S_φ trong cơ sở $\mathcal{B}$.

Rõ ràng $s_\varphi \circ s_\varphi = \mathrm{Id}_{E_2}$, vì $S_\varphi^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$.

1) Ta xác định các bất biến của s_φ.

Với mọi $X = \begin{pmatrix} x \\ y \end{pmatrix}$ thuộc $\mathbf{M}_{2,1}(\mathbb{R})$, ta có:

$$S_\varphi X = X \Leftrightarrow \begin{cases} (1-\cos\varphi)x - \sin\varphi y = 0 \\ -\sin\varphi\, x + (1+\cos\varphi)y = 0 \end{cases} \Leftrightarrow \begin{cases} 2\sin\dfrac{\varphi}{2}\left(\sin\dfrac{\varphi}{2}x - \cos\dfrac{\varphi}{2}y\right) = 0 \\ 2\cos\dfrac{\varphi}{2}\left(-\sin\dfrac{\varphi}{2}x + \cos\dfrac{\varphi}{2}y\right) = 0 \end{cases}$$

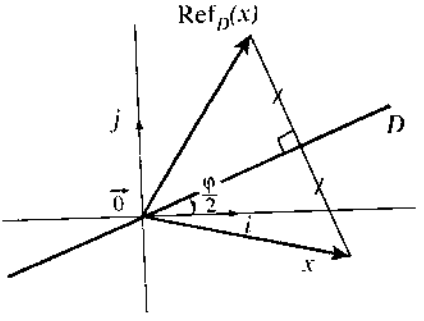
$$\Leftrightarrow x\sin\frac{\varphi}{2} - y\cos\frac{\varphi}{2} = 0.$$

Như vậy, tập hợp các bất biến của s_φ là đường thẳng vectơ $D_{\frac{\varphi}{2}}$ với góc cực $\dfrac{\varphi}{2}$, tức là đường thẳng sinh bởi $\cos\dfrac{\varphi}{2}i + \sin\dfrac{\varphi}{2}j$.

2) Một phép tính tương tự chứng tỏ rằng tập hợp các phản bất biến (nghĩa là tập hợp các u thuộc E_2 sao cho $s_\varphi(u) = -u$) là đường thẳng vectơ $D_{\frac{\varphi}{2}+\frac{\pi}{2}}$ có góc cực $\dfrac{\varphi}{2} + \dfrac{\pi}{2}$, tức là đường thẳng sinh bởi $-\sin\dfrac{\varphi}{2}i + \cos\dfrac{\varphi}{2}j$.

Ta tóm tắt kết quả khảo sát:

♦ **Mệnh đề 5** Giả sử $\mathcal{B} = (i, j)$ là một c.s.t.c.t của E_2, và $\varphi \in \mathbb{R}$. Tự đồng cấu của E_2 có ma trận theo cơ sở $\mathcal{B}$ là $S_\varphi = \begin{pmatrix} \cos\varphi & \sin\varphi \\ \sin\varphi & -\cos\varphi \end{pmatrix}$ là một phép phản chiếu qua đường thẳng vectơ D có góc cực $\dfrac{\varphi}{2}$, và được ký hiệu là Ref_D.



Từ sự khảo sát trên ta suy ra kết quả sau.

♦ **Mệnh đề 6**

- $SO(E_2) = \{\mathrm{Rot}_\theta\ ;\ \theta \in \mathbb{R}\}$
- $O(E_2) - SO(E_2) = \{\mathrm{Ref}_D\ ;\ D \in \mathcal{D}\}$,

trong đó $\mathcal{D}$ là tập hợp các đường thẳng vectơ của E_2. ■

♦ **Mệnh đề 7** Mọi phép quay của E_2 đều có thể phân tích được, ít nhất theo một cách, thành tích của hai phép phản chiếu.

Nói chính xác hơn, với mọi phép quay r của E_2 và mọi phép phản chiếu s của E_2, tồn tại một phép phản chiếu duy nhất t của E_2 sao cho $r = t \circ s$.

Chứng minh:

Đặt $t = r^{-1} \circ s$. t thuộc $O(E)$ và $\det(t) = (\det(r))^{-1} \det(s) = 1^{-1}.(-1) = -1$, vì vậy t là một phép phản chiếu.

Bài tập

◊ **10.4.1** Với $\varphi, \theta \in \mathbb{R}$, đặt $R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$, và $S_\varphi = \begin{pmatrix} \cos\varphi & \sin\varphi \\ \sin\varphi & -\cos\varphi \end{pmatrix}$ (xem 10.4, Mệnh đề 1).

Tính các tích $R_\theta R_{\theta'}$, $R_\theta S_\varphi$, $S_\varphi R_\theta$, $S_\varphi S_{\varphi'}$ với $\theta, \theta', \varphi, \varphi' \in \mathbb{R}$.

◊ **10.4.2** Giả sử r là một phép quay và s là một phép phản chiếu của E_2. Tính $s \circ r \circ s$ và $r \circ s \circ r$.

◊ **10.4.3** Trong $\mathbb{R}^2$, góc của $u = (-2, 1)$ và $v = (1, 3)$ là góc nào ?

◊ **10.4.4 Bó toàn phương trong E_2**

Cho $(a, b, c) \in \mathbb{R}^3 - \{0, 0, 0\}$.

a) Tìm điều kiện cần và đủ để phương trình $ax^2 + 2bxy + cy^2 = 0$ biểu diễn hợp của hai đường thẳng (có thể trùng nhau).

Từ lúc này, ta sẽ giả thiết $b^2 - ac \geq 0$, và ký hiệu D, D' là hai đường thẳng của E_2, mà hợp gọi là *bó toàn phương*, có phương trình $ax^2 + 2bxy + cy^2 = 0$.

b) Tính $\left|\widehat{(D, D')}\right|$ (thuộc $[0; \frac{\pi}{2}]$).

c) Viết phương trình của bó toàn phương các phân giác của D và D'.

10.5 Hình học vectơ Euclide 3 chiều

Ta ký hiệu E_3 là một không gian vectơ Euclide 3 chiều, $\cdot$ là tích vô hướng trên E_3.

10.5.1 Tự đồng cấu trực giao của E_3

Giả sử $f \in \mathcal{O}(E_3)$, $\mathcal{B} = (i, j, k)$ là một c.s.t.c.t của E_3, $\Omega = \mathrm{Mat}_{\mathcal{B}}(f)$.

• Trước hết, ta sẽ chứng minh rằng tồn tại $x \in E_3 - \{0\}$ sao cho $f(x) = x$ hoặc $f(x) = -x$ (nghĩa là, xem Tập 6, 2.1, Định nghĩa, 1 hoặc -1 là trị riêng của f).

Giả sử $\lambda \in \mathbb{R}$. Ta có:

$$(\exists x \in E_3 - \{0\}, f(x) = \lambda x) \Leftrightarrow (\exists x \in E_3 - \{0\}, x \in \mathrm{Ker}(f - \lambda\,\mathrm{Id}_{E_3}))$$

$$\Leftrightarrow (f - \lambda\,\mathrm{Id}_{E_3} \text{ không phải là đơn ánh}) \Leftrightarrow \det((f - \lambda\,\mathrm{Id}_{E_3}) = 0.$$

Ánh xạ $P : \underset{\lambda \mapsto \det(\Omega - \lambda I_n)}{\mathbb{R} \to \mathbb{R}}$ là một đa thức bậc 3, với hệ tử cao nhất -1. Vì P liên tục trên $\mathbb{R}$ và $\lim\limits_{-\infty} P = +\infty$, $\lim\limits_{+\infty} P = -\infty$, nên định lý các giá trị trung gian chứng tỏ rằng P có ít nhất một không điểm thực λ_0.

Như vậy, tồn tại $\lambda_0 \in \mathbb{R}$ và $x_0 \in E_3 - \{0\}$ sao cho $f(x_0) = \lambda_0 x_0$.

Nhưng, vì $f \in \mathcal{O}(E_3)$, ta có $\|f(x_0)\| = \|x_0\|$, nên $|\lambda_0| = 1$, nghĩa là $\lambda_0 \in \{-1, 1\}$.

Nói cách khác, ta đã chứng minh rằng 1 hoặc - 1 là trị riêng của f.

• Đặt $I = \dfrac{1}{\|x_0\|} x_0$ và $H = I^{\perp}$. Mặt phẳng vectơ H ổn định qua f vì, với mọi y thuộc H:

$$f(y) \cdot I = f(y) \cdot \left(\frac{1}{\lambda_0} f(I)\right) = \frac{1}{\lambda_0}(f(y) \cdot f(I)) = \frac{1}{\lambda_0}(y \cdot I) = 0.$$

Xét tự đồng cấu g của H cảm sinh bởi f là $g : \underset{y \mapsto f(y)}{H \to H}$, và trang bị cho H tích vô hướng thu hẹp của $\cdot$ trên $H \times H$, và một c.s.t.c. (J, K).

Vì $f \in \mathcal{O}(E_3)$ nên rõ ràng $g \in \mathcal{O}(H)$:

$$\forall (y, z) \in H^2, \quad g(y) \cdot g(z) = f(y) \cdot f(z) = y \cdot z.$$

Theo 10.4, Mệnh đề 6, g là một phép quay hoặc một phép phản chiếu.

Do đó có bốn trường hợp trong việc khảo sát f.

Trường hợp thứ nhất : $\lambda_0 = 1$ và g là một phép quay

Ma trận của f trong c.s.t.c. (I, J, K) của E_3 có dạng $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$, $\theta \in \mathbb{R}$.

Trường hợp thứ hai : $\lambda_0 = 1$ và g là một phép phản chiếu.

Gọi J' (tương ứng : K') là một vectơ chỉ phương chuẩn hóa của $\mathrm{Ker}(g - \mathrm{Id}_H)$ (tương ứng: của $\mathrm{Ker}(g + \mathrm{Id}_H)$).

Khi đó (I, J', K') là một c.s.t.c., trong cơ sở đó ma trận của f là: $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$,

như vậy f là một phép phản chiếu qua mặt phẳng vectơ sinh bởi (I, J').

Trường hợp thứ ba : $\lambda_0 = -1$ và g là một phép phản chiếu

Với các ký hiệu như ở trường hợp thứ hai, ma trận của f trong c.s.t.c. $(I, J' K')$ là :

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

Như vậy f là phép đối xứng trực giao qua đường thẳng vectơ sinh bởi J'.

Ma trận của f trong c.s.t.c. (J', I, K') là $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$; như vậy, f cũng là phép quay với trục định phương (và định hướng) bởi J' và với góc quay π.

Trường hợp thứ tư: $\lambda_0 = -1$ và g là một phép quay

Ma trận của f trong c.s.t.c. (I, J, K) có dạng $\begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$, $\theta \in \mathbb{R}$.

Ta chú ý rằng: $\begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$. ■

Từ đây về sau ta sẽ giả thiết E_3 được định hướng.

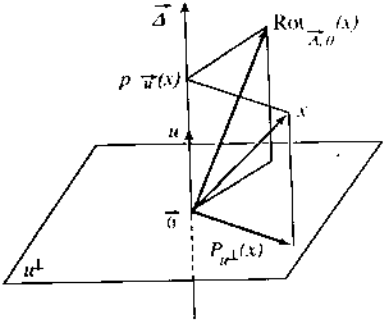
Việc mô tả hình học trường hợp thứ nhất dẫn tới định nghĩa sau.

♦ **Định nghĩa 1** Giả sử $u \in E_3$ thỏa mãn $\|u\| = 1$. $\vec{\Delta}$ là trục định phương và định hướng bởi u, và $\theta \in \mathbb{R}$. Tự đồng cấu của E_3 có ma trận là $\begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$ trong một c.s.t.c. (u, v, w), bắt đầu từ u, được gọi là **phép quay với trục** $\vec{\Delta}$ và với góc θ, ký hiệu là $\mathrm{Rot}_{\vec{\Delta},\theta}$.

Như vậy, với mọi $x \in E_3$ ta có:

$$\mathrm{Rot}_{\vec{\Delta},\theta}(x) = \mathrm{Rot}_{\theta}(p_{u^\perp}(x)) + p_{\mathbb{R}u}(x),$$

trong đó:
- $p_{u^\perp}(x)$ là hình chiếu trực giao của x lên mặt phẳng $u^\perp$
- $P_{\mathbb{R}u}(x)$ là hình chiếu trực giao của x lên đường thẳng $\mathbb{R}u$
- Rot_θ là phép quay với góc θ trong mặt phẳng $u^\perp$ được định hướng bởi cơ sở thuận (v, w).



NHẬN XÉT:

1) Cho $\vec{\Delta}$ là một trục, $\theta \in \mathbb{R} - 2\pi\mathbb{Z}$. Theo việc khảo sát trên, tồn tại một c.s.t.c. t. (u, v, w) sao cho u chỉ phương và chỉ hướng cho $\vec{\Delta}$, và trong cơ sở đó ma trận của $\mathrm{Rot}_{\vec{\Delta},\theta}$ là

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}.$$

Khi đó, rõ ràng là tập hợp các bất biến của $\mathrm{Rot}_{\vec{\Delta},\theta}$ là đường thẳng vectơ $\mathbb{R}.u$, vì phép quay $g : \begin{matrix} u^{\perp} \to u^{\perp} \\ y \mapsto f(y) \end{matrix}$ chỉ nhận $\vec{0}$ làm bất biến.

Điều đó chứng tỏ rằng một phép quay chỉ có hai trục, có cùng phương và có chiều ngược nhau.

2) Cho $\overrightarrow{\Delta_1}$, $\overrightarrow{\Delta_2}$ là hai trục, $\theta_1, \theta_2 \in \mathbb{R} - 2\pi\mathbb{Z}$. Từ 1) ta suy ra:

$$\mathrm{Rot}_{\vec{\Delta}_1,\theta_1} = \mathrm{Rot}_{\vec{\Delta}_2,\theta_2} \Leftrightarrow \left(\begin{cases} \overrightarrow{\Delta_2} = \overrightarrow{\Delta_1} \\ \theta_2 \equiv \theta_1 [2\pi] \end{cases} \text{ và } \begin{cases} \overrightarrow{\Delta_2} = -\overrightarrow{\Delta_1} \\ \theta_2 \equiv -\theta_1 [2\pi] \end{cases} \right),$$

trong đó $-\overrightarrow{\Delta_1}$ chỉ trục cùng phương và ngược chiều với $\overrightarrow{\Delta_1}$. ■

Việc mô tả hình học trường hợp thứ ba dẫn tới Định nghĩa sau.

♦ **Định nghĩa 2** Trong E_3 mọi phép quay với góc $\pi [2\pi]$ được gọi là phép **lật** (hay: **quay lại**) của E_3. ■

Việc khảo sát trên chứng tỏ rằng:

♦ **Định lý (Phân loại các tự đồng cấu trực giao của E_3)**

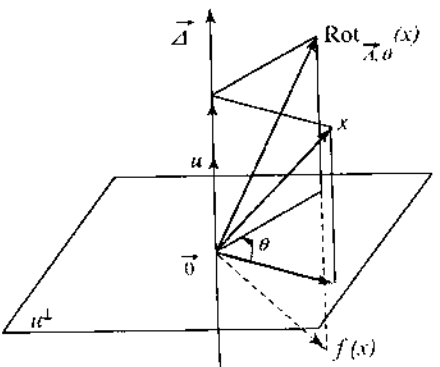
Giả sử $f \in \mathcal{O}(E_3) - \{\mathrm{Id}_{E_3}\}$.

1) Nếu $\det(f) = 1$, thì f là một phép quay của E_3.

2) Nếu $\det(f) = -1$, thì:

- Hoặc f là một phép phản chiếu của E_3
- Hoặc f là tích của một phép quay của E_3 và phép phản chiếu qua mặt phẳng vuông góc với trục của phép quay đó.

Trường hợp f là tích của một phép quay của E_3 và phép phản chiếu qua mặt phẳng vuông góc với trục của phép quay đó



Nhận dạng và xác định các phần tử đặc trưng của một tự đồng cấu trực giao của E_3

Giả sử $\Omega \in \mathbf{O}_3(\mathbb{R}) - \{I_3\}$, f là tự đồng cấu trực giao của E_3 biểu diễn bởi Ω trong một c.s.t.c.t. $\mathcal{B}$ của E_3.

1) Giả sử $\det(\Omega) = 1$.

Khi đó f là một phép quay của E_3.

Đường thẳng mang trục của f là tập hợp các bất biến của f, do vậy được xác định bằng việc giải phương trình $\Omega X = X$, với ẩn $X \in \mathbf{M}_{3,1}(\mathbb{R})$.

Theo kết quả khảo sát trên đây:

$$\text{tr}(\Omega) = \text{tr}(f) = \text{tr}\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix} = 1 + 2\cos\theta \ ,$$

điều đó cho phép xác định $\cos\theta$.

Gọi I là vectơ chỉ phương và chỉ hướng chuẩn hóa của trục của f, và (J, K) là một c.s.t.c. của $I^\perp$ sao cho (I, J, K) là một c.s.t.c.t. của E_3.

Giả sử $x \in E_3$, không đồng phương với I. Gọi (α, β, γ) là các thành phần của x trong c.s.t.c.t. (I, J, K).

Cột các thành phần của $f(x)$ trong (I, J, K) là:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta\cos\theta - \gamma\sin\theta \\ \beta\sin\theta + \gamma\cos\theta \end{pmatrix} \text{ và do vậy :}$$

$$[x, f(x), I] = \det_{(I,J,K)}(x, f(x), I) = \begin{vmatrix} \alpha & \alpha & 1 \\ \beta & \beta\cos\theta - \gamma\sin\theta & 0 \\ \gamma & \beta\sin\theta + \gamma\cos\theta & 0 \end{vmatrix} = (\beta^2 + \gamma^2)\sin\theta.$$

Như vậy, vì $\beta^2 + \gamma^2 > 0$ (do x không đồng phương với I), nên $\sin\theta$ cùng dấu với tích hỗn hợp $[x, f(x), I]$. Trong thực tế, ta tính tích hỗn hợp này bằng một định thức trong c.s.t.c.t. (i, j, k). Tóm lại:

1) Đường thẳng mang trục $\vec{\Delta}$ của f là tập hợp các bất biến của f, có được bằng cách giải $\Omega X = X$, với ẩn $X \in \mathbf{M}_{3,1}(\mathbb{R})$.

2) Ta xác định θ bằng :

- $\text{tr}(\Omega) = 1 + 2\cos\theta$
- $\sin\theta$ cùng dấu với tích hỗn hợp $[x, f(x), I]$ với bất kỳ vectơ x không đồng phương với I, trong đó I là vectơ chỉ phương và chỉ hướng đã chuẩn hóa của trục của f.

VÍ DỤ:

Nhận dạng tự đồng cấu f của $\mathbb{R}^3$ có ma trận trong cơ sở chính tắc là :

$$\Omega = \frac{1}{3}\begin{pmatrix} -2 & -1 & 2 \\ 2 & -2 & 1 \\ 1 & 2 & 2 \end{pmatrix}.$$

Rõ ràng $\Omega \in \mathbf{O}_3(\mathbb{R})$ (các cột của Ω được định chuẩn và từng đôi một trực giao với nhau). Hơn nữa : $\det(\Omega) = 1$.

Như vậy f là một phép quay.

Trục $\vec{\Delta}$ của f được định phương bởi $xi + yj + zk$, trong đó (x, y, z) được xác định bởi:

$$\frac{1}{3}\begin{pmatrix} -2 & -1 & 2 \\ 2 & -2 & 1 \\ 1 & 2 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \Leftrightarrow \begin{cases} -2x - y + 2z = 3x \\ 2x - 2y + z = 3y \\ x + 2y + 2z = 3z \end{cases}$$

$$\Leftrightarrow \begin{cases} 5x + y - 2z = 0 \\ 2x - 5y + z = 0 \\ x + 2y - z = 0 \end{cases} \Leftrightarrow \begin{cases} y = -5x + 2z \\ 27x - 9z = 0 \\ -9x + 3z = 0 \end{cases} \Leftrightarrow \begin{cases} y = x \\ z = 3x. \end{cases}$$

Một vectơ chỉ phương và chỉ hướng của trục $\vec{\Delta}$ của f là $u = i + j + 3k$, và một vectơ chỉ phương và chỉ hướng chuẩn hóa của $\vec{\Delta}$ là $I = \frac{1}{\sqrt{11}}(i + j + 3k)$.

Ký hiệu θ là góc của f.

Vì $1 + 2\cos\theta = \mathrm{tr}(\Omega) = -\frac{2}{3}$, nên ta suy ra $\cos\theta = -\frac{5}{6}$.

Cuối cùng, $\sin\theta$ cùng dấu với tích hỗn hợp :

$$[i, f(i), I] = \det_{(i,j,k)}(i, f(i), I) = \begin{vmatrix} 1 & -\frac{2}{3} & \frac{1}{\sqrt{11}} \\ 0 & \frac{2}{3} & \frac{1}{\sqrt{11}} \\ 0 & \frac{1}{3} & \frac{3}{\sqrt{11}} \end{vmatrix} = \frac{5}{3\sqrt{11}} > 0.$$

Ta kết luận : f là phép quay có trục định phương và định hướng bởi $I = \frac{1}{\sqrt{11}}(i+j+3k)$, và có góc $\theta = \mathrm{Arccos}\left(-\frac{5}{6}\right)$ $[2\pi]$.

2) Giả sử $\det(\Omega) = -1$.

Khi đó f hoặc là một phép phản chiếu, hoặc là tích của một phép quay và của một phép phản chiếu.

Ta chú ý rằng, với $\Omega \in \mathbf{O}_3(\mathbf{R})$, các hệ thức $\Omega^2 = \mathrm{I}_3$ và ${}^t\Omega = \Omega$ là tương đương, vì ${}^t\Omega\Omega = \mathrm{I}_3$.

a) Giả sử Ω đối xứng.

Vì $\Omega^2 = I_3$, nên f là một phép đối xứng trực giao.

Vì hơn nữa $\det(\Omega) = -1$, nếu $\Omega \neq -I_3$, nên f là một phép phản chiếu. Mặt phẳng của phép phản chiếu f là tập hợp các bất biến của f.

VÍ DỤ:

Nhận dạng tự đồng cấu f của $\mathbf{R}^3$ có ma trận trong cơ sở chính tắc là :

$$\Omega = -\frac{1}{9}\begin{pmatrix} -8 & 4 & 1 \\ 4 & 7 & 4 \\ 1 & 4 & -8 \end{pmatrix}.$$

Rõ ràng $\Omega \in \mathbf{O}_3(\mathbf{R})$, $\det(\Omega) = -1$, ${}^t\Omega = \Omega$. Do vậy f là một phép phản chiếu.

Mặt phẳng của phép phản chiếu f được xác định bởi : $\Omega X = X$. Với $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$:

$$\Omega X = X \Leftrightarrow \begin{cases} -8x + 4y + z = -9x \\ 4x + 7y + 4z = -9y \\ x + 4y - 8z = -9z \end{cases} \Leftrightarrow x + 4y + z = 0.$$

Kết luận : f là phép phản chiếu qua mặt phẳng vectơ có phương trình $x + 4y + z = 0$.
(Kiểm chứng : (1, 4, 1) đúng là một phần bất biến của f).

b) Giả sử Ω không đối xứng.

Khi đó f là hợp giao hoán của một phép quay $\mathrm{Rot}_{\vec{\Delta},\theta}$ với một phép phản chiếu Ref_P qua mặt phẳng P vuông góc với trục $\vec{\Delta}$.

Các phần tử của $\vec{\Delta}$ được đặc trưng bởi : $\Omega X = -X$.

Ta có :

$$\mathrm{tr}(\Omega) = \mathrm{tr}(f) = \mathrm{tr}\begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix} = -1 + 2\cos\theta.$$

điều đó cho phép xác định $\cos\theta$.

Cũng như ở 1) trên đây, $\sin\theta$ cùng dấu với tích hỗn hợp $[x, f(x), I]$ với bất kỳ vectơ x không đồng phương với I, trong đó I là vectơ chỉ phương và chỉ hướng đã chuẩn hóa của $\vec{\Delta}$.

Cuối cùng : $P = \Delta^{\perp}$.

VÍ DỤ:

Nhận dạng tự đồng cấu f của $\mathbf{R}^3$ có ma trận trong cơ sở chính tắc là :

$$\Omega = -\frac{1}{4}\begin{pmatrix} 3 & 1 & \sqrt{6} \\ 1 & 3 & -\sqrt{6} \\ -\sqrt{6} & \sqrt{6} & 2 \end{pmatrix}.$$

Rõ ràng $\Omega \in \mathbf{O}_3(\mathbb{R})$, Ω không đối xứng, và $\det(\Omega) = -1$. Do vậy, f là hợp giao hoán của một phép quay $\mathrm{Rot}_{\Delta,\theta}$ với phép phản chiếu Ref_P trong đó $P = \Delta^{\perp}$.

Các phần tử của Δ được xác định bởi : $\Omega X = -X$.

Với $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$, ta có :

$$\Omega X = -X \Leftrightarrow \begin{cases} 3x + y + \sqrt{6}z = 4x \\ x + 3y - \sqrt{6}z = 4y \\ -\sqrt{6}x + \sqrt{6}y + 2z = 4z \end{cases} \Leftrightarrow \begin{cases} -x + y + \sqrt{6} = 0 \\ \sqrt{6}x - \sqrt{6}y + 2z = 0 \end{cases} \Leftrightarrow \begin{cases} x = y \\ z = 0 \end{cases}.$$

Một vectơ chỉ phương và chỉ hướng chuẩn hóa của $\vec{\Delta}$ là $I = \dfrac{1}{\sqrt{2}}(i + j)$.

Vì $-1 + 2\cos\theta = \mathrm{tr}(\Omega) = -2$, nên ta suy ra $\cos\theta = -\dfrac{1}{2}$.

Cuối cùng, $\sin\theta$ cùng dấu với :

$$[i, f(i), I] = \begin{vmatrix} 1 & -\frac{3}{4} & \frac{1}{\sqrt{2}} \\ 0 & -\frac{1}{4} & \frac{1}{\sqrt{2}} \\ 0 & \frac{\sqrt{6}}{4} & 0 \end{vmatrix} = -\frac{\sqrt{3}}{4} < 0,$$

do đó $\theta = -\dfrac{2\pi}{3}$ $[2\pi]$.

Kết luận : f là tích $\mathrm{Rot}_{\Delta,\theta} \circ \mathrm{Ref}_P$, trong đó $\vec{\Delta}$ được định phương và định hướng bởi $I = \dfrac{1}{\sqrt{2}}(i+j)$, $\theta \equiv -\dfrac{2\pi}{3}$ $[2\pi]$, P là mặt phẳng vuông góc với Δ, có phương trình $x + y = 0$. ■

♦ Mệnh đề 1

Mọi tự đồng cấu trực giao của E_3 đều có thể phân tích thành tích của nhiều nhất ba phép phản chiếu.

Chứng minh:

Giả sử $f \in \mathcal{O}(E_3)$.

- Nếu $f = \mathrm{Id}_E$, rõ ràng f là hợp của hai phép phản chiếu (hai lần cùng một phép phản chiếu), hoặc f là một hợp rỗng.
- Kết quả là hiển nhiên nếu f là một phép phản chiếu.
- Trường hợp f là một phép quay

Với các ký hiệu ở 10.5.1, Định nghĩa 1, tồn tại hai đường thẳng vectơ D_1, D_2 thuộc $\Delta^{\perp}$ sao cho $g = \mathrm{Ref}_{D_2} \circ \mathrm{Ref}_{D_1}$, trong mặt phẳng $\Delta^{\perp}$.

Ký hiệu P_1 (tương ứng : P_2) là mặt phẳng vectơ sinh bởi $D_1 \cup \Delta$ (tương ứng: $D_2 \cup \Delta$), rõ ràng :

$$f = \mathrm{Ref}_{D_2} \circ \mathrm{Ref}_{D_1}.$$

• Nếu f là hợp của một phép quay và một phép phản chiếu, thì, theo trường hợp trên, f phân tích được thành tích của ba phép phản chiếu.

• Nếu $f = -\mathrm{Id}_{E_3}$, thì f là hợp của ba phép phản chiếu qua ba mặt phẳng tọa độ.■

♦ **Định nghĩa 3** Cho $u, v \in E_3 - \{0\}$. Ta định nghĩa góc của u và v, ký hiệu là (u, v), bởi :

$\widehat{(u, v)} = 0$ nếu $\exists \alpha \in \mathbb{R}_+^*, v = \alpha u$

$\widehat{(u, v)} = \pi$ nếu $\exists \alpha \in \mathbb{R}_-^*, v = \alpha u$

$\widehat{(u, v)}$ là giá trị tuyệt đối của góc (tính trong $]-\pi, \pi[$) của u và v trong mặt phẳng Euclide định hướng bởi u và v nếu (u, v) độc lập tuyến tính.

Như vậy, ta nhận thấy rằng một góc trong E_3 tự nó không định hướng. Một cách hình tượng, ta có thể nhìn mặt phẳng Vect(u, v) từ trên xuống hoặc từ dưới lên.

Từ 10.4, Mệnh đề 3, ta suy ra kết quả sau đây.

♦ **Mệnh đề 2**

$$\forall (u, v) \in E_3 - \{0\}, \quad u \cdot v = \|u\| \cdot \|v\| \cos(u, v).$$

Bài tập

◊ **10.5.1** Nhận dạng tự đồng cấu f của E_3 có ma trận Ω trong một c.s.t.c.t. (i, j, k) của E_3 được cho dưới đây, và chỉ rõ các phần tử đặc trưng của f :

a) $-\frac{1}{27}\begin{pmatrix} 2 & -26 & 7 \\ -23 & 2 & 14 \\ 14 & 7 & 22 \end{pmatrix}$ b) $\frac{1}{9}\begin{pmatrix} -7 & 4 & -4 \\ 4 & -1 & -8 \\ -4 & -8 & -1 \end{pmatrix}$

c) $\frac{1}{9}\begin{pmatrix} 7 & 4 & 4 \\ 4 & 1 & -8 \\ 4 & -8 & 1 \end{pmatrix}$ d) $\frac{1}{9}\begin{pmatrix} 7 & -4 & 4 \\ 4 & 8 & 1 \\ 4 & -1 & -8 \end{pmatrix}$

e) $\begin{pmatrix} a^2 & ab-c & ac+b \\ ab+c & b^2 & bc-a \\ ac-b & bc+a & c^2 \end{pmatrix}$, $(a, b, c) \in \mathbb{R}^3$, $a^2 + b^2 + c^2 = 1$.

◊ **10.5.2** Lập ma trận Ω, trong một c.s.t.c.t. (i, j, k) của E_3, của phép quay f có trục được định hướng bởi $i + j + k$ và có góc $\frac{\pi}{3}$ [2π].

◊ **10.5.3** Cho $f, g \in SO(E_3) - \{\mathrm{Id}_{E_3}\}$. Chứng tỏ rằng f và g là giao hoán được khi và chỉ khi :

hoặc f và g là hai phép quay có cùng trục
f và g là hai phép lật lại có các trục trực giao.

◊ **10.5.4** Chứng minh rằng mọi phép quay của E_3 có thể phân tích được, ít nhất theo một cách, thành hợp của nhiều nhất hai phép lật.

10.5.2 Tích vectơ

Ta nhắc lại (xem 10.3.2, Mệnh đề - Định nghĩa), rằng tích hỗn hợp $[u, v, w]$ của ba phần tử u, v, w của E_3 được xác định bởi : $[u, v, w] = \det_{\mathcal{B}}(u, v, w)$,

trong đó $\mathcal{B}$ là một c.s.t.c.t. bất kỳ của E_3.

Theo 9.2.2, Mệnh đề 2, ta có : $[u, v, w] = 0 \Leftrightarrow (u, v, w)$ phụ thuộc tuyến tính.

Vì, với (u, v) cố định, ánh xạ $\begin{array}{c} E_3 \to \mathbb{R} \\ w \mapsto [u,v,w] \end{array}$ là một dạng tuyến tính, nên Mệnh đề sau suy từ 10.2.3, Mệnh đề 2.

♦ **Mệnh đề - Định nghĩa 1** Cho $(u, v) \in E_3^2$. Tồn tại một phần tử duy nhất x của E_3 sao cho : $\forall w \in E_3, \quad [u, v, w] = x \bullet w$.
Phần tử x đó của E_3 được gọi là **tích vectơ** của u với v, và được ký hiệu là $u \wedge v$ (hoặc : $u \times v$).

Như vậy, theo định nghĩa ta có: $\forall u, v, w \in E_3, \quad [u, v, w] = (u \wedge v) \bullet w$,
điều này (hậu) lý giải cho cách diễn đạt "tích hỗn hợp" như là một sự "pha trộn" một tích vectơ và một tích vô hướng.

NHẬN XÉT:

1) Với mọi u, v, w thuộc E_3, ta có

$$\begin{cases} [u, v, w] = (u \wedge v) \bullet w \\ [u, v, w] = [v, w, u] = (v \wedge w) \bullet u \\ [u, v, w] = [w, u, v] = (w \wedge u) \bullet v. \end{cases}$$

2) Nếu $\mathcal{B} = (i, j, k)$ là một c.s.t.c.t. của E_3, thì : $i \wedge j = k, \quad j \wedge k = i, \quad k \wedge i = j$,
vì, chẳng hạn

$$\begin{aligned} i \wedge j &= ((i \wedge j) \bullet i)\, i + ((i \wedge j) \bullet j) j + ((i \wedge j) \bullet k) k \\ &= [i, j, i] i + [i, j, j] j + [i, j, k]\, k = k. \end{aligned}$$

♦ **Mệnh đề 2**
Ánh xạ $\begin{array}{c} E_3 \times E_3 \to E_3 \\ (u, v) \mapsto u \wedge v \end{array}$ là song tuyến tính thay phiên.

Chứng minh:

Giả sử $\alpha \in \mathbb{R}$, $u, v, v' \in E_3$.

• $\forall w \in E_3, (v \wedge u) \bullet w = [v, u, w] = -[u, v, w] = -(u \wedge v) \bullet w$,

do đó, từ tính duy nhất của $v \wedge u$ suy ra : $v \wedge u = -u \wedge v$.

• $\forall w \in E_3, (u \wedge (\alpha v + v')) \bullet w = [u, \alpha v + v', w] = \alpha [u, v, w] + [u, v', w]$

$$= \alpha (u \wedge v) \bullet w + (u \wedge v') \bullet w = (\alpha (u \wedge v) + (u \wedge v')) \bullet w,$$

do đó, từ tính duy nhất của $u \wedge (\alpha v + v')$ suy ra : $u \wedge (\alpha v + v') = \alpha (u \wedge v) + (u \wedge v')$.

Tính chất tuyến tính đối với vị trí thứ nhất suy từ tính chất tuyến tính đối với vị trí thứ hai và tính chất thay phiên.

♦ Mệnh đề 3

$$\forall u, v \in E_3, \quad (u \wedge v = 0 \Leftrightarrow (u, v) \text{ phụ thuộc tuyến tính}).$$

Chứng minh:

1) Nếu (u, v) phụ thuộc tuyến tính, thì $u \wedge v = 0$ (xem 9.1.2, Mệnh đề 2).

2) Ngược lại, giả sử $u \wedge v = 0$.

Nếu (u, v) độc lập tuyến tính, thì theo định lý về cơ sở không đầy đủ, dạng yếu (6.4, Định lý 2), tồn tại $w \in E_3$ sao cho (u, v, w) là một cơ sở của E_3, và khi đó $(u \wedge v) \cdot w = [u, v, w] \neq 0$ (xem 9.2.2, Mệnh đề 2), mâu thuẫn.

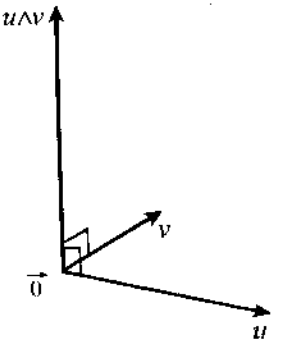
Do vậy (u, v) phụ thuộc tuyến tính.

♦ Hệ quả

Nếu (u, v) độc lập tuyến tính, thì $(u, v, u \wedge v)$ là một cơ sở thuận của E_3.

Chứng minh:

$$[u, v, u \wedge v] = (u \wedge v) \cdot (u \wedge v)$$
$$= \|u \wedge v\|^2 > 0.$$



♦ Mệnh đề 4

$$\forall u, v \in E_3, \quad (u \wedge v \perp u \text{ và } u \wedge v \perp v).$$

Chứng minh: $(u \wedge v) \cdot u = [u, v, u] = 0$, $(u \wedge v) \cdot v = [u, v, v] = 0$.

♦ Mệnh đề 5

Giả sử $\mathcal{B} = (i, j, k)$ là một c.s.t.c.t. của E_3, $u, v \in E_3$, (x, y, z) (tương ứng: (x', y', z')) là các thành phần của u (tương ứng : v) trong $\mathcal{B}$. Ta có:

$$u \wedge v = (yz' - zy')i + (zx' - xz')j + (xy' - yx')k.$$

Chứng minh:

Vì $\wedge$ là song tuyến tính thay phiên, và theo Mệnh đề trên, ta có:

$$u \wedge v = (xi + yj + zk) \wedge (x'i + y'j + z'k)$$
$$= (yz' - zy')i + (zx' - xz')j + (xy' - yx')k.$$

NHẬN XÉT:

Ta có thể ghi nhớ kết quả đó dưới dạng lược đồ:

$$u \wedge v = \begin{vmatrix} x & x' & i \\ y & y' & j \\ z & z' & k \end{vmatrix}$$

bằng cách khai triển "định thức giả" (vì i, j, k là những vectơ) này theo cột thứ ba.

♦ Mệnh đề 6 (Tích vectơ kép)

$$\forall u, v, w \in E_3, \quad u \wedge (v \wedge w) = (u \bullet w)v - (u \bullet v)w.$$

Chứng minh:

1) Nếu $v = 0$, tính chất trên là hiển nhiên.

2) Nếu $v \neq 0$ và nếu w đồng phương với v, thì tồn tại $\lambda \in \mathbb{R}$ sao cho $w = \lambda u$, từ đó suy ra:

$$(u \bullet w)v - (u \bullet v)w = \lambda(u \bullet v)v - \lambda(u \bullet v)v = 0 = u \wedge (v \wedge w).$$

3) Giả thiết (v, w) độc lập tuyến tính. Theo thủ tục trực giao hóa Schmidt, tồn tại một c.s.t.c.t (I, J, K) của E_3 và $\alpha, \beta, \gamma, a, b, c \in \mathbb{R}$ sao cho :

$$v = \alpha I, w = \beta I + \gamma J, u = a I + bJ + cK.$$

Khi đó ta có :

- $v \wedge w = \alpha\gamma K$, nên $u \wedge (v \wedge w) = -\alpha\gamma aJ + \alpha\gamma bI$
- $(u \bullet w)v - (u \bullet v)w = (a\beta + b\gamma)v - a\alpha w = b\gamma\alpha I - a\alpha\gamma J$,

từ đó suy ra công thức cần chứng minh.

♦ Mệnh đề 7

1) $\forall u, v \in E_3, \quad \|u \wedge v\|^2 + (u \bullet v)^2 = \|u\|^2\|v\|^2$

(hằng đẳng thức Lagrange)

2) $\forall u, v \in E_3 - \{0\}, \quad \|u \wedge v\| = \|u\| \|v\| |\sin(\widehat{u, v})|.$

Chứng minh: 1)

$$\|u \wedge v\|^2 = (u \wedge v) \bullet (u \wedge v) = [u, v, u \wedge v] = [v, u \wedge v, u] = (v \wedge (u \wedge v)) \bullet u$$
$$= ((v \bullet v)u - (v \bullet u)v) \bullet u = (v \bullet v)(u \bullet u) - (v \bullet u)(v \bullet u) = \|v\|^2 \|u\|^2 - (v \bullet u)^2.$$

2) Theo 10.5.1, Mệnh đề 2:

$$\|u \wedge v\|^2 = \|u\|^2 \|v\|^2 (1 - \cos^2(u, v)) = \|u\|^2 \|v\|^2 \sin^2(u, v).$$

NHẬN XÉT:

1) Nói riêng : $\forall u, v \in E_3, \quad (u \perp v \Leftrightarrow \|u \wedge v\| = \|u\| \|v\|)$.

2) Nếu u và v là những vectơ chuẩn hóa và trực giao, thì $(u, v, u \wedge v)$ là một c.s.t.c.t. của E_3.

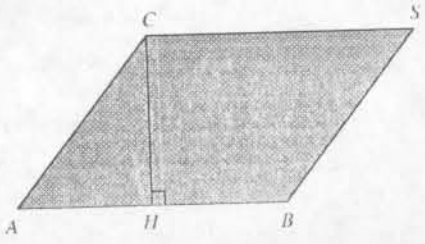
♦ Mệnh đề 8

1) Với mọi (u, v) thuộc E_3^2, $\|u \wedge v\|$ bằng diện tích hình bình hành dựng trên u, v.

2) Với mọi (u, v, w) thuộc E_3^2, $\|[u, v, w]\|$ bằng thể tích hình hộp dựng trên u, v, w.

Chứng minh :

1) Trong một mặt phẳng afin Euclide (định hướng) (xem Tập Hình học), giả sử A, B, C, S thỏa mãn $\overrightarrow{AB} = u$, $\overrightarrow{AC} = v$, $\overrightarrow{BS} = \overrightarrow{AC}$, và giả sử H là hình chiếu trực giao của C lên (AB) (trường hợp $u = 0$ là tầm thường).



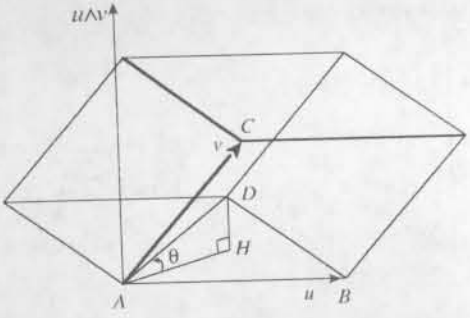
Diện tích $\mathcal{A}$ của hình bình hành $ABSC$ bằng $AB \times CH$.

Vì $AB = \|u\|$ và $CH = AC \sin \widehat{CAH} = \|v\| \, |\sin (\widehat{u, v})|$, nên ta kết luận :

$$\mathcal{A} = \|u\| \, \|v\| \, | \sin (\widehat{u, v}) | = \|u \wedge v\|.$$

Kết quả là diện tích tam giác ABC bằng $\dfrac{1}{2}\left\|\overrightarrow{AB} \wedge \overrightarrow{AC}\right\|$.

2) Trong (một) không gian afin Euclide (định hướng) 3 chiều, giả sử A, B, C, D thỏa mãn $\overrightarrow{AB} = u$, $\overrightarrow{AC} = v$, $\overrightarrow{AD} = w$, và giả sử H là hình chiếu trực giao của D lên mặt phẳng ABC (do trường hợp (u, v) phụ thuộc tuyến tính là tầm thường).



Thể tích $\mathcal{V}$ của hình hộp dựng trên A, B, C, D là $DH \times \mathcal{A}$, trong đó $\mathcal{A}$ là diện tích hình bình hành dựng trên ABC.

Đặt $\theta = \widehat{DAH}$, là góc giữa $\overrightarrow{AD}$ và mặt phẳng ABC.

Vì $u \wedge v \perp ABC$, ta có : $\left(\widehat{\overrightarrow{AD}, u \wedge v}\right) = \dfrac{\pi}{2} - \theta$,

do đó $DH = AD \, |\sin \theta| = AD \cdot \left|\cos(\widehat{\overrightarrow{AD}, u \wedge v})\right|$, rồi áp dụng 1) :

$$\mathcal{V} = \|u \wedge v\| \cdot AD \cdot \left|\cos(\widehat{\overrightarrow{AD}, u \wedge v})\right| = |(u \wedge v) \bullet w| = |[u, v, w]|.$$

Bài tập

◊ **10.5.5 Phép chia vectơ**

Với $(a, b) \in (E_3)^2$ cho trước, giải $a \wedge x = b$, với ẩn $x \in E_3$.

◊ **10.5.6** Giả sử $(a, b) \in (E_3)^2$ độc lập tuyến tính ; chứng minh rằng không tồn tại một c nào thuộc E_3 sao cho :

$$\forall x \in E_3, \quad a \wedge (b \wedge x) = c \wedge x.$$

◊ **10.5.7** Với $a \in E_3$ cho trước, giải $\begin{cases} a \wedge x + y = a \\ a \wedge y + x = a \end{cases}$, với ẩn $(x, y) \in (E_3)^2$.

◊ **10.5.8** Với $(a, b) \in (E_3)^2$ độc lập tuyến tính, giải $(a \wedge x) \wedge b = a \wedge (x \wedge b)$, với ẩn $x \in E_3$.

◊ **10.5.9** Với $(a, b) \in (E_3)^2$ độc lập tuyến tính, giải $(S) \begin{cases} a \wedge x = b \wedge y \\ a \wedge y = b \wedge x \\ x \wedge y = a \wedge b \end{cases}$, với ẩn $(x, y) \in (E_3)^2$.

◊ **10.5.10** Chứng minh, với mọi x, y, z, u, v, w thuộc E_3 :

$$[x \wedge u, y \wedge v, z \wedge w] + [x \wedge v, y \wedge w, z \wedge u] + [x \wedge w, y \wedge u, z \wedge v] = 0.$$

◊ **10.5.11** Giả sử $a \in E_3$, $f_a : (E_3)^2 \to E_3$ xác định bởi :

$$\forall (x, y) \in (E_3)^2, \quad f_a(x, y) = (a \wedge x) \wedge y + (a \wedge y) \wedge x.$$

a) Kiểm chứng rằng f_a là một ánh xạ song tuyến tính đối xứng, nghĩa là :

$$\begin{cases} \forall (x, y) \in (E_3)^2, \quad f_a(y, x) = f_a(x, y) \\ \forall \lambda \in \mathbb{R}, \forall (x, y, z) \in (E_3)^3, \quad f_a(x, y + \lambda z) = f_a(x, y) + \lambda f_a(x, z). \end{cases}$$

b) Chứng minh rằng, với mọi (x, y) thuộc $(E_3 - \{0\})^2$ sao cho $x \cdot y = 0$, ta có :

$$f_a(x, y) = 0 \Leftrightarrow a \in \mathbb{R}(x \wedge y).$$

◊ **10.5.12** Giả sử $u \in E_3$ chuẩn hóa, $f : E_3 \to E_3$, $x \mapsto x \wedge u$

Kiểm chứng : $f^3 = -f$.

◊ **10.5.13** Giả sử $u \in E_3$ chuẩn hóa, $(\alpha, \beta, \gamma) \in \mathbb{R}^3$, $f : E_3 \to E_3$ xác định bởi :

$$\forall x \in E_3, \quad f(x) = \alpha x + \beta(u \cdot x)\, u + \gamma\, u \wedge x.$$

Tìm điều kiện cần và đủ đối với (α, β, γ) để f là một phép quay, và trong trường hợp này hãy xác định các phần tử đặc trưng (trục, góc) của nó.

Bổ sung

◊ C 10.1 Đa thức Legendre

Gọi E là tập hợp các ánh xạ đa thức từ [-1, 1] vào $\mathbb{R}$ và, với mỗi n thuộc $\mathbb{N}$, E_n là tập hợp các ánh xạ đa thức từ [-1, 1] vào $\mathbb{R}$ với bậc $\leq n$. Ta có thể đồng nhất đa thức và ánh xạ đa thức từ [-1, 1] vào $\mathbb{R}$ (vì [-1, 1] vô hạn, xem 5.1.7, Mệnh đề 2). Dễ dàng suy ra rằng E là một $\mathbb{R}$-kgv đối với các luật thông thường.

Ta định nghĩa một ánh xạ $<\cdot, \cdot>$ từ E^2 vào $\mathbb{R}$ bởi :

$$\forall (P, Q) \in E^2, \quad <P, Q> = \int_{-1}^{1} P(x)Q(x)dx.$$

I Đa thức trực giao

1) Kiểm chứng rằng $<\cdot, \cdot>$ là một tích vô hướng trên E, và

$$\forall P, Q, R \in E, \ <PQ, R> = <P, QR>.$$

Ta ký hiệu $\|\cdot\|$ là chuẩn trên E liên kết với $<\cdot, \cdot>$.

2) Chứng minh rằng tồn tại một dãy duy nhất $(P_n)_{n \in \mathbb{N}}$ những phần tử của E sao cho :

$$\begin{cases} \forall (m, n) \in \mathbb{N}^2, \quad <P_m, P_n> = \begin{cases} 1 & \text{nếu } m = n \\ 0 & \text{nếu } m \neq n \end{cases} \\ \text{Với mọi } n \text{ thuộc } \mathbb{N}, P_n \text{ có bậc } n \text{ và có hệ số cao nhất} > 0. \end{cases}$$

3) Chứng minh rằng : $\forall n \in \mathbb{N}^*, P_n \in E_{n-1}^{\perp}$, trong đó $E_{n-1}^{\perp}$ là tập trực giao của E_{n-1} đối với tích vô hướng $<\cdot, \cdot>$.

II Với $n \in \mathbb{N}$, đặt $U_n = ((X^2 - 1)^n)^{(n)}$ (đạo hàm cấp n của $(X^2 - 1)^n$).

1) a) Cho $n \in \mathbb{N}$. Chứng minh rằng, nếu n chẵn (tương ứng : lẻ)) thì U_n chẵn (tương ứng : lẻ).

b) Chứng minh rằng, với mọi n thuộc $\mathbb{N}$, U_n có bậc n, và hãy tính hệ tử cao nhất của nó.

Với $n \in \mathbb{N}$, ta ký hiệu $L_n = \dfrac{1}{2^n n!} U_n$ và gọi là **đa thức Legendre** thứ n.

2) a) Chứng minh : $\forall (m, n) \in \mathbb{N}^2, (m \neq n \Rightarrow <U_m, U_n> = 0)$.

(Có thể tích phân từng phần một lần).

b) Tính $\|U_n\|$ với mọi $n \in \mathbb{N}$.

c) Chứng minh rằng : $\forall n \in \mathbb{N}, P_n = \dfrac{1}{2^n n!} \sqrt{\dfrac{2n+1}{2}} U_n$ (**công thức Rodrigues**).

d) Từ đó suy ra hệ số cao nhất của P_n với mọi $n \in \mathbb{N}$.

3) **Phương trình vi phân thỏa mãn bởi L_n**

Chứng minh : $\forall n \in \mathbb{N}, (1 - X^2) L_n'' - 2XL_n' + n(n+1)L_n = 0$.

(Có thể đặt $M_n = (X^2 - 1)^n$, nhận xét rằng $(X^2 - 1) M_n' = 2nXM_n$, sau đó lấy đạo hàm cấp $(n+1)$).

4) **Hệ thức truy hồi trên các L_n**

a) Chứng minh : $\forall n \in \mathbb{N}^*, (n+1)L_{n+1} = (2n+1)XL_n - nL_{n-1}$.

(Ký hiệu c_k là hệ tử cao nhất của L_k với $k \in \mathbb{N}$, và $D_n = c_n L_{n+1} - c_{n+1} XL_n$,

chứng tỏ rằng $\deg(D_n) \leq n$ và D_n trực giao với $L_0, \ldots, L_{n-2}, L_n$.

Sau đó đưa vào $R_{k-1} \in E$ sao cho (với $k = n-1, n$) $L_k = c_k X^k + R_{k-1}$ và $\deg(R_{k-1}) \leq k-1$).

b) Từ đó suy ra L_n với $n \in \{0, \ldots, 6\}$.

c) Tính $L_n(1)$ và $L_n'(1)$ với mọi n thuộc $\mathbb{N}$.

III Khảo sát các không điểm của L_n

1) Công thức Christoffel và Darboux

Chứng minh : $\forall n \in \mathbb{N}, \forall (x, y) \in \mathbb{R}^2$,

$$(x-y)\sum_{k=0}^{n}(2k+1)L_k(x)L_k(y) = (n+1)(L_{n+1}(x)L_n(y) - L_n(x)L_{n+1}(y)).$$

2) Chứng minh rằng, với mọi n thuộc $\mathbb{N}^*$, L_n là tách được trên $\mathbb{R}$ và có đúng n không điểm khác nhau từng đôi một và thuộc $]-1, 1[$.

(Câu hỏi này độc lập với 1)).

Ta ký hiệu $(\xi_{n,k})_{1 \leq k \leq n}$ là các không điểm của L_n, được sắp xếp sao cho :

$$-1 < \xi_{n,1} < \xi_{n,2} < \ldots < \xi_{n,n-1} < \xi_{n,n} < 1.$$

3) a) Suy từ 1) rằng: $\forall n \in \mathbb{N}, \forall x \in \mathbb{R}$,

$$\sum_{k=0}^{n}(2k+1)(L_k(x))^2 = (n+1)(L_{n+1}'(x)L_n(x) - L_n'(x)L_{n+1}(x)).$$

b) Với $n \in \mathbb{N}$, đặt $F_n = \dfrac{L_n}{L_{n+1}} \in \mathbb{R}[X]$.

Chứng tỏ rằng các hệ số của dạng phân tích thành các phần tử đơn giản của F_n (trong $\mathbb{R}[x]$) đều > 0. (Áp dụng 2) và 3) a)).

4) Sự lồng nhau của các không điểm của L_{n-1} và L_n.

Cho $n \in \mathbb{N} - \{0, 1\}$. Chứng minh :

$$\xi_{n,1} < \xi_{n-1,1} < \xi_{n,2} < \xi_{n-1,2} < \ldots < \xi_{n-1,n-2} < \xi_{n,n-1} < \xi_{n-1,n-1} < \xi_{n,n}.$$

5) Giả sử $n \in \mathbb{N}^*$, $c \in \mathbb{R}$. Chứng minh rằng $L_n + cL_{n-1}$ là tách được trên $\mathbb{R}$ và có tất cả các không điểm đơn.

Phần thứ hai

CHỈ DẪN VÀ TRẢ LỜI CÁC BÀI TẬP

Chỉ dẫn và trả lời
các bài tập chương 1

1.1.1 a) $(p \Leftrightarrow q) \Leftrightarrow \begin{cases} p \Rightarrow q \\ q \Rightarrow p \end{cases} \Leftrightarrow \begin{cases} q \Rightarrow p \\ p \Rightarrow q \end{cases} \Leftrightarrow (q \Leftrightarrow p)$.

b) $\begin{cases} \begin{cases} p \Rightarrow q \\ q \Rightarrow r \end{cases} \Rightarrow \begin{cases} p \Rightarrow r \\ r \Rightarrow p \end{cases} \Rightarrow (p \Leftrightarrow r), \ldots \\ r \Rightarrow p \end{cases}$

c) $(p \Rightarrow (q \Rightarrow r)) \Leftrightarrow (\neg p$ hoặc $(\neg q$ hoặc $r)) \Leftrightarrow ((\neg p$ hoặc $\neg q)$ hoặc $r) \Leftrightarrow (\neg(p$ và $q)$ hoặc $r)$
$\Leftrightarrow ((p$ và $q) \Leftrightarrow r)$

d) $((p$ hoặc $q) \Rightarrow r) \Leftrightarrow (\neg(p$ hoặc $q)$ hoặc $r) \Leftrightarrow ((\neg p$ và $\neg q)$ hoặc $r)$
$\Leftrightarrow ((\neg p$ hoặc $r)$ và $(\neg q$ hoặc $r)) \Leftrightarrow ((p \Rightarrow r)$ và $(q \Rightarrow r))$.

1.1.2 a) Dễ dàng.

b) $A \cap B = (A \cap B \cap (C \cup \overline{C})) = (A \cap B \cap C) \cup (A \cap B \cap \overline{C}) \subset (A \cap C) \cup (B \cap \overline{C})$.

c) $\Rightarrow$: $B \subset A \cup B = A \cap C \subset A$ và $A \subset A \cup B = A \cap C \subset C$

$\Leftarrow$: Dễ dàng.

d) $\Rightarrow$: $B = (A \cup B) \cap B = (A \cup C) \cap B = (A \cap B) \cup (C \cap B) = (A \cap C) \cup (C \cap B)$

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

$\Leftarrow$: Hiển nhiên.

e) $(A - B) \cup (A - C) = (A \cap \overline{B}) \cup (A \cap \overline{C}) = A \cap (\overline{B} \cup \overline{C}) = A \cap (\overline{B \cap C}) = A - (B \cap C)$.

f) $(A - B) - (A - C) = (A \cap \overline{B}) \cap \overline{A \cap \overline{C}} = A \cap \overline{B} \cap (\overline{A} \cup C) = (A \cap B \cap \overline{A}) \cup (A \cap \overline{B} \cap C)$

$= A \cap \overline{B} \cap C = (A - B) \cap C = (A \cap C) - B$.

g) $\Rightarrow$: $A = A \cap (C \cup \overline{C}) = (A \cap C) \cup (A \cap \overline{C}) \subset (B \cap C) \cup (B \cap \overline{C}) = B \cap (C \cup \overline{C}) = B$

$\Leftarrow$: Hiển nhiên.

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

i) Tương tự như h).

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

k) $A = A \cap (C \cup D) \subset A \cap (C \cup B) = (A \cap C) \cup (A \cap B) = C \cup (C \cap D) = C$.

1.1.3 $X' = X' \cap E = X' \cap (X \cup Y \cup Z) = (X' \cap X) \cup (X' \cap Y) \cup (X' \cap Z) \subset X \cup (X' \cap Y') \cup (X' \cap Z')$

$= X \cup (X \cap Y) \cup (X \cap Z) = X$

1.1.4 ◇ **Trả lời :** •

a) $\varnothing$ nếu $A \not\subset B$, $\{(B - A) \cup Y ; Y \in \mathfrak{P}(A)\}$ nếu $A \subset B$

b) $\varnothing$ nếu $B \not\subset A$, $\{B \cup Y ; Y \in \mathfrak{P}(\complement_E(A))\}$ nếu $B \subset A$

c) $\varnothing$ nếu $A \cap B \neq \varnothing$, $\{B \cup Y ; Y \in \mathfrak{P}(A)\}$ nếu $A \cap B = \varnothing$

d) $\{A \Delta B\}$.

1.1.5 a) • Giả sử $A \in \mathcal{A}$. Với mọi x thuộc A, ta có $x \in F$ (theo định nghĩa của F), vậy $A \in \mathfrak{P}(F)$. Điều này chứng tỏ : $\mathcal{A} \subset \mathfrak{P}(F)$.

- $(\forall A \in \mathcal{A}, A \neq \varnothing)$ vì $\mathcal{P}$ là một phân hoạch của E.
- $(\forall (A, B) \in \mathcal{A}^2, (A \neq B \Rightarrow A \cap B = \varnothing))$ vì $\mathcal{P}$ là một phân hoạch của E.
- $(\forall x \in F, \exists A \in \mathcal{A}, x \in A)$ theo định nghĩa của F.

Điều này chứng tỏ rằng $\mathcal{A}$ là một phân hoạch của F. Hoán vị $(\mathcal{A}, F)$ và $(\mathcal{B}, G)$, ta kết luận $\mathcal{B}$ là một phân hoạch của G.

b) • Giả sử $x \in F \cap G$. Tồn tại $A \in \mathcal{A}$, $B \in \mathcal{B}$ sao cho $x \in A$ và $x \in B$. Vì $\mathcal{P}$ là một phân hoạch của E, nên ta có $A = B$, do đó $\mathcal{A} \cap \mathcal{B} \neq \varnothing$, mâu thuẫn. Vậy $F \cap G = \varnothing$.

• Giả sử $x \in E$. Tồn tại $P \in \mathcal{P}$ sao cho $x \in P$. Vì $\mathcal{P} = \mathcal{A} \cup \mathcal{B}$, ta có ($P \in \mathcal{A}$ hoặc $P \in \mathcal{B}$), do đó theo định nghĩa của F và G : $x \in F$ hoặc $x \in G$. Điều này chứng tỏ : $F \cup G = E$.

1.1.6 • $\forall i \in \{1, ..., n\}, B_i \neq \varnothing$.

• Giả sử $i, j \in \{1, ..., n\}$ sao cho $i < j$. Ta có : $B_i \subset A_i$ và $B_j = A_j - A_{j-1} \subset A_j - A_i$, vậy $B_i \cap B_j = \varnothing$.

• Giả sử $x \in E$. Tồn tại $i \in \{1, ..., n\}$ sao cho $x \in A_i$ và $x \notin A_{i-1}$, từ đây $x \in B_i$.

1.2.1 • $x \mathcal{R} y \Rightarrow \begin{cases} x \mathcal{R} y \\ y \mathcal{R} y \end{cases} \Rightarrow y \mathcal{R} x$.

• $\begin{cases} x \mathcal{R} y \\ y \mathcal{R} z \end{cases} \Rightarrow z \mathcal{R} x \Rightarrow x \mathcal{R} z$.

1.2.1 • $\mathcal{S}$ phản xạ vì $\mathcal{R}$ phản xạ.

• $\mathcal{S}$ hiển nhiên đối xứng.

• $\begin{cases} x \mathcal{S} y \\ y \mathcal{S} z \end{cases} \Rightarrow \begin{cases} x \mathcal{R} y \text{ và } y \mathcal{R} x \\ y \mathcal{R} z \text{ và } z \mathcal{R} y \end{cases} \Rightarrow \begin{cases} x \mathcal{R} z \\ z \mathcal{R} x \end{cases} \Rightarrow x \mathcal{S} z$.

1.2.3 a) Chú ý : $\forall (x, y) \in \mathbb{R}^2, (x \mathcal{R} y \Leftrightarrow f(x) = f(y))$, trong đó $f : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x^2 - x \end{array}$.

b) ◇ **Trả lời :** $\mathrm{cl}_{\mathcal{R}}(x) = \begin{cases} \{x, 1 - x\} & \text{nếu } x \neq \dfrac{1}{2} \\ \dfrac{1}{2} & \text{nếu } x = \dfrac{1}{2} \end{cases}$.

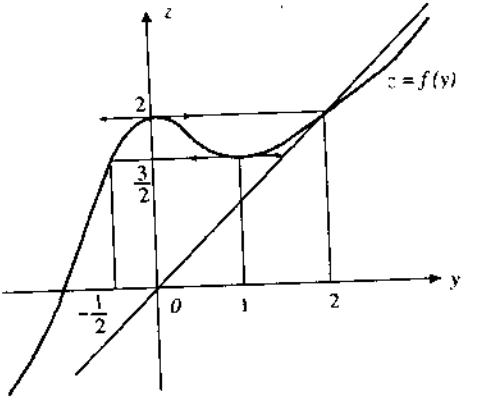
1.2.4 a) Chú ý rằng : $\forall (x, y) \in \mathbb{R}^2, (x \mathcal{K} y \Leftrightarrow f(x) = f(x))$, trong đó $f : \mathbf{R} \to \mathbf{R}$, $x \mapsto \frac{x^3+2}{x^2+1}$

b) Khảo sát sự biến thiên của f :

f khả vi trên $\mathbb{R}$ và :

$$\forall y \in \mathbb{R}, f'(y) = \frac{y(y-1)(y^2+y+4)}{(y^2+1)^2}$$

y	$-\infty$		0		1		$+\infty$
$f'(y)$		$+$	0	$-$	0	$+$	
$f(y)$	$-\infty$	↗	2	↘	$\frac{3}{2}$	↗	$+\infty$



Với mọi x thuộc $\mathbb{R}$, ta có : $\mathrm{cl}_{\mathcal{K}}(x) = \{y \in \mathbb{R} ; f(y) = f(x)\}$; khảo sát giao điểm của đường cong biểu diễn f với đường thẳng nằm ngang có tung độ $f(x)$.

◇ **Trả lời :** Số các phần tử của $\mathrm{cl}_{\mathcal{K}}(x)$ là :

$$\begin{cases} 1 \text{ nếu } x \in \left]-\infty; \frac{1}{2}\right[\cup \left]2; +\infty\right[\\ 2 \text{ nếu } x \in \left\{-\frac{1}{2}, 0, 1, 2\right\} \\ 3 \text{ nếu } x \in \left]-\frac{1}{2}; 0\right[\cup \left]0; 1\right[\cup \left]1; 2\right[\end{cases}$$

1.2.5 ◇ **Trả lời :**

	Tập hợp các chặn trên trong E	Tập hợp các phần tử cực đại	Biên trên (Cận trên đúng)	Phần tử lớn nhất
A	$\{5\}$	$\{2, 3\}$	5	không tồn tại
B	$\varnothing$	$\{2, 4\}$	không tồn tại	không tồn tại
C	$\{5\}$	$\{5\}$	5	5

1.2.6 a) $\mathrm{Sup}_E(B)$ là một chặn trên của B, như vậy cũng là một chặn trên của A (trong E) và $\mathrm{Sup}_E(A)$ là chặn trên nhỏ nhất của A trong E, do đó : $\mathrm{Sup}_E(A) \leq \mathrm{Sup}_E(B)$.

b) ◇ **Trả lời :**

1) $E = \mathbb{R}$, $\leq$ thông thường, $A = \mathbb{R}_-$, $B = \mathbb{R}$

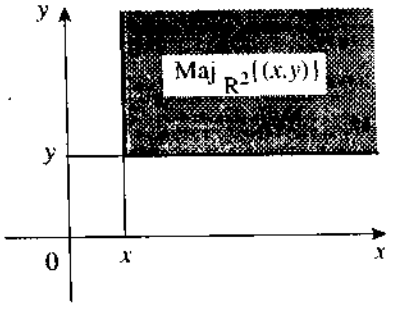
2) $E = \mathbb{Q}$, $\leq$ thông thường, $A = \{x \in \mathbb{Q} ; x^2 < 2\}$, $B = \{x \in \mathbb{Q} ; x \leq 2\}$

3) $E = \mathbb{R}$, $\leq$ thông thường, $A = \{x \in \mathbb{Q} ; x^2 < 2\}$, $B = A \cup \{2\}$.

1.2.7 a) Dễ dàng.

b) α) ◇ **Trả lời :**

$\text{Maj}_{\mathbf{R}^2}\{(x, y)\} = [x ; \infty[\times [y ; +\infty[$.



β) $\mathcal{P}$ không toàn phần trong $\mathbb{R}$ vì (1, 0) và (0, 1) là không so sánh được.

γ) ◇ **Trả lời :** $\{(x, y) \in \mathbb{R}^2 ; x + y = 0\}$.

δ) $\text{Maj}_{\mathbf{R}^2}(\mathbf{R}_-^*)^2 = (\mathbf{R}_+)^2$ và $(\mathbf{R}_+^2)$ có (0, 0) là phần tử nhỏ nhất.

◇ **Trả lời :** $(\mathbf{R}_-^*)^2$ có biên trên trong $\mathbb{R}^2$, đó là (0, 0).

1.2.8 a) • Tính phản xạ là hiển nhiên.

• Cho $(x, y), (x', y') \in E \times F$ sao cho $\begin{cases}(x,y)\angle(x',y')\\(x',y')\angle(x,y)\end{cases}$, tức là :

$$\left|\begin{array}{ll} x \prec x' & (1)\\ \text{hoặc} & \\ (x = x' \text{ và } y \preccurlyeq y') & (2)\end{array}\right. \quad \text{và} \quad \left|\begin{array}{ll} x \prec x' & (3)\\ \text{hoặc} & \\ (x = x' \text{ và } y \preccurlyeq y') & (4)\end{array}\right.$$

Chỉ có các trường hợp (2) và (4) là không mâu thuẫn. Do đó $(x, y) = (x', y')$.

Điều này chứng tỏ $\angle$ phản đối xứng.

• Cho $(x, y), (x', y'), (x'', y'') \in E \times F$ sao cho : $\begin{cases}(x,y)\angle(x',y')\\(x',y')\angle(x'',y'')\end{cases}$. Thế thì ta có :

$$\left|\begin{array}{ll} x \prec x' & (1)\\ \text{hoặc} & \\ (x = x' \text{ và } y \preccurlyeq y') & (2)\end{array}\right. \quad \text{và} \quad \left|\begin{array}{ll} x' \prec x''; & (3)\\ \text{hoặc} & \\ (x' = x'' \text{ và } y' \preccurlyeq y'') & (4)\end{array}\right.$$

Các điều kiện ((1) và (3)), ((1) và (4)), ((2) và (3)) kéo theo $x \prec x''$, vậy $(x, y) \angle (x'', y'')$.

Cuối cùng : $\begin{cases}(2)\\(4)\end{cases} \Rightarrow \begin{cases}x = x''\\ y \preccurlyeq y'\end{cases} \Rightarrow (x, y) \angle (x'', y'')$. Như vậy, $\angle$ có tính bắc cầu.

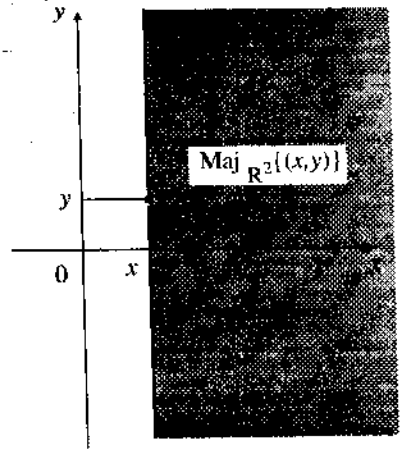
b) Cho $(x, y), (x', y') \in E \times F$.

Vì $\preccurlyeq$ là thứ tự toàn phần trong E, ta có : $x \prec x'$ hoặc $x = x'$ hoặc $x' \prec x$.

Nếu $x \prec x'$, thì $(x, y) \angle (x', y')$.

Nếu $x' \prec x$, thì $(x', y') \angle (x, y)$.

Nếu $x = x'$, vì $\preccurlyeq$ là toàn phần trong F, nên ta có $y \preccurlyeq y'$ hoặc $y' \preccurlyeq y$, từ đó $(x, y) \angle (x', y')$ hoặc $(x', y') \angle (x, y)$.



c) α) ◇ **Trả lời :** $\text{Maj}_{\mathbf{R}^2}\{x, y\} =$

$(\{x\} \times [y ; +\infty[) \cup (]x ; \infty) \times \mathbb{R})$.

β) $\text{Maj}_{\mathbf{R}^2}(\mathbf{R}_-^* \times \mathbb{R}) = \mathbb{R}_+ \times \mathbb{R}$, và $\mathbb{R}_+ \times \mathbb{R}$ không có phần tử nhỏ nhất đối với $\mathcal{P}$.

◇ **Trả lời :** $\mathbf{R}_-^* \times \mathbb{R}$ không có biên trên trong $\mathbb{R}^2$ đối với $\angle$.

1.3.1 Các phép chứng minh là dễ dàng. Chẳng hạn, đối với 6) :

$$\varphi_{A\cdot B} = 1 - \varphi_{\overline{A\cdot B}} = 1 - \varphi_{\overline{A}\cdot\overline{B}} = 1 - (1 - \varphi_A)(1 - \varphi_B) = \varphi_A + \varphi_B - \varphi_A\varphi_B.$$

1.3.2 a) Việc chứng minh các tính phản xạ, phản đối xứng, bắc cầu là dễ dàng.

b) ◇ **Trả lời :** • Các phần tử cực đại của $\mathcal{U}$ đối với $\mathcal{R}$ là các (E, f) trong đó $f \in F^E$.

• Các phần tử cực tiểu của $\mathcal{U}$ đối với $\mathcal{R}$ là các $(\{x\}, f)$ trong đó $x \in E$ và $f \in F^{\{x\}}$.

1.3.3 $(g' \circ f') \circ u = g' \circ (f' \circ u) = g' \circ (v \circ f) = (g' \circ v) \circ f = (w \circ g) \circ f = w \circ (g \circ f)$.

1.3.4 a) 1) Giả sử tồn tại $h : F \to G$ sao cho $h \circ f = g$. Ta có, với mọi (x, x') thuộc E^2 :

$$f(x) = f(x') \Rightarrow h(f(x)) = h(f(x')) \Rightarrow g(x) = g(x').$$

2) Ngược lại, giả sử : $\forall (x, x') \in E^2, \quad (f(x) = f(x') \Rightarrow g(x) = g(x')$.

Cho $y \in F$.

• Nếu y không có tạo ảnh qua f, ta đặt $h(y) = e$, trong đó e là một phần tử cố định bất kỳ của G.

• Nếu y có ít nhất một tạo ảnh x qua f, ta đặt $h(y) = g(x)$, điều này là đúng đắn vì nếu y có ít nhất hai tạo ảnh x, x' qua f, thì $g(x) = g(x')$.

Như vậy ta đã xác định ánh xạ $h : F \to G$ thỏa mãn : $\forall x \in E, h(f(x)) = g(x)$, tức là $h \circ f = g$.

b) 1) Giả sử tồn tại $f : E \to F$ sao cho $h \circ f = g$. Khi đó ta có : $\forall x \in E, g(x) = h(f(x))$, vậy $\forall x \in E, \exists y \in F, g(x) = h(y)$.

2) Ngược lại, giả sử : $\forall x \in E, \exists y \in F, g(x) = h(y)$. Cho $x \in E$.

Theo giả thiết, tồn tại $y \in F$ sao cho $g(x) = h(y)$. Ta khảo sát ánh xạ $f : E \xrightarrow[x \mapsto y]{} F$, trong đó y là một phần tử thỏa mãn $g(x) = h(y)$. (Việc xây dựng này sử dụng "tiên đề chọn").

Vậy ta đã xác định một ánh xạ $f : E \to F$ thỏa mãn : $\forall x \in E, g(x) = h(f(x))$, tức là $h \circ f = g$.

1.3.5 • $f \circ g \circ f$ song ánh $\Rightarrow \begin{cases} f \circ g \circ f \text{ đơn ánh} \\ f \circ g \circ f \text{ toàn ánh} \end{cases} \Rightarrow \begin{cases} f \text{ đơn ánh} \\ f \text{ toàn ánh} \end{cases} \Rightarrow f$ song ánh

(xem 1.3.2, Mệnh đề 2).

• Rồi thì: $g = f^{-1} \circ (f \circ g \circ f) \circ f^{-1}$.

1.3.6 a) $\begin{cases} g \circ f & \text{đơn ánh} \\ f & \text{toàn ánh} \end{cases} \Rightarrow \begin{cases} g & \text{đơn ánh} \\ g & \text{toàn ánh} \end{cases} \Rightarrow f$ song ánh, rồi $g = (g \circ f) \circ f^{-1}$ là đơn ánh.

b) $\begin{cases} g \circ f & \text{toàn ánh} \\ f & \text{đơn ánh} \end{cases} \Rightarrow \begin{cases} f & \text{toàn ánh} \\ f & \text{đơn ánh} \end{cases} \Rightarrow g$ song ánh, rồi $f = g^{-1} \circ (g \circ f)$ là toàn ánh.

1.3.7 a) Áp dụng bài tập 1.3.4 *a*), vào $E, F, E, f, \mathrm{Id}_E$ thay vì E, F, G, f, g ta được : f là đơn ánh khi và chỉ khi tồn tại $h : F \to E$ sao cho $h \circ f = \mathrm{Id}_E$. Hơn nữa, nếu $h \circ f = \mathrm{Id}_E$ thì h là toàn ánh (xem 1.3.2, Mệnh đề 2).

b) Áp dụng bài tập 1.3.4, *b*), vào $F, E, F, \mathrm{Id}_F, f$ thay vì E, F, G, g, h, ta được : f là toàn ánh khi và chỉ khi tồn tại $g : F \to E$ sao cho $f \circ g = \mathrm{Id}_F$. Hơn nữa, nếu $f \circ g = \mathrm{Id}_F$, thì g là đơn ánh (xem 1.3.2, Mệnh đề 2).

1.3.8 Kết quả suy ra từ bài tập 1.3.7.

1.3.9 a) ◇ **Trả lời :** • f là đơn ánh, không toàn ánh.
• g là toàn ánh, không đơn ánh.

b) ◇ **Trả lời :** $g \circ f = \mathrm{Id}_{\mathbf{N}}$, $f \circ g : \mathbf{N} \to \mathbf{N}$, $x \mapsto \begin{cases} x & \text{nếu } x \text{ chẵn} \\ x-1 & \text{nếu } x \text{ lẻ} \end{cases}$

1.3.10 a) Dễ dàng.

b) Các ánh xạ : $\varphi : E/\mathcal{R} \times F/\mathcal{S} \to (E \times F)/\mathcal{T}$, $(\mathrm{cl}_{\mathcal{R}}(x), \mathrm{cl}_{\mathcal{S}}(y)) \mapsto \mathrm{cl}_{\mathcal{T}}(x, y)$ và $\psi : (E \times F)/\mathcal{T} \to E/\mathcal{R} \times F/\mathcal{S}$, $\mathrm{cl}_{\mathcal{T}}(x, y) \mapsto (\mathrm{cl}_{\mathcal{R}}(x), \mathrm{cl}_{\mathcal{S}}(y))$ đều được

định nghĩa đúng đắn, bởi vì với mọi (x, y), (x', y') thuộc $E \times F$:

$$(\mathrm{cl}_{\mathcal{R}}(x), \mathrm{cl}_{\mathcal{S}}(y)) = (\mathrm{cl}_{\mathcal{R}}(x'), \mathrm{cl}_{\mathcal{S}}(y')) \Leftrightarrow \begin{cases} \mathrm{cl}_{\mathcal{R}}(x) = \mathrm{cl}_{\mathcal{R}}(x') \\ \mathrm{cl}_{\mathcal{S}}(y) = \mathrm{cl}_{\mathcal{S}}(y') \end{cases} \Leftrightarrow \begin{cases} x \mathcal{R} x' \\ y \mathcal{S} y' \end{cases} \Leftrightarrow (x, y)\, \mathcal{T}(x', y')$$

$$\Leftrightarrow \mathrm{cl}_{\mathcal{T}}(x, y) = \mathrm{cl}_{\mathcal{T}}(x', y').$$

Rõ ràng : $\psi \circ \varphi = \mathrm{Id}_{E/\mathcal{R} \times F/\mathcal{S}}$ và $\varphi \circ \psi = \mathrm{Id}_{(E \times F)/\mathcal{T}}$. Theo 1.3.2, Mệnh đề 5, ta kết luận rằng φ và ψ là các song ánh thuận ngược lẫn nhau.

1.3.11 a) 1) Với mọi f thuộc E, $f \mathcal{R} f$ bởi vì $\mathrm{Id}_{\mathbf{R}} \circ f = f \circ \mathrm{Id}_{\mathbf{R}}$.

2) Giả sử $(f, g) \in E^2$ sao cho $f \mathcal{R} g$; tồn tại song ánh $\varphi \in E$ sao cho $\varphi \circ f = g \circ \varphi$. Thế thì $\varphi^{-1} \in E$, φ^{-1} là song ánh, và :

$$\varphi^{-1} \circ g = \varphi^{-1} \circ (g \circ \varphi) \circ \varphi^{-1} = \varphi^{-1} \circ (\varphi \circ f) \circ \varphi^{-1} = f \circ \varphi^{-1}, \text{ vậy } g \mathcal{R} f.$$

3) Giả sử $(f, g, h) \in E^3$ sao cho $f \mathcal{R} g$ và $g \mathcal{R} h$; tồn tại φ, $\psi \in E$, đều song ánh, sao cho :

$$\varphi \circ f = g \circ \varphi \text{ và } \psi \circ g = h \circ \psi.$$

Thế thì $\psi \circ \varphi \in E$, $\psi \circ \varphi$ là song ánh, và :

$$(\psi \circ \varphi) \circ f = \psi \circ (\varphi \circ f) = \psi \circ (g \circ \varphi) = (\psi \circ g) \circ \varphi = (h \circ \psi) \circ \varphi = h \circ (\psi \circ \varphi),$$

từ đó $f \mathcal{R} h$.

b) 1) Nếu ch $\mathcal{R}$ sh, thì tồn tại $\varphi \in E$ song ánh sao cho $\varphi \circ \mathrm{ch} = \mathrm{sh} \circ \varphi$; thế thì $\mathrm{ch} = \varphi^{-1} \circ \mathrm{sh} \circ \varphi$, vậy ch là song ánh, mâu thuẫn.

2) Giả sử cos $\mathcal{R}$ sin. Tồn tại một song ánh $\varphi : \mathbb{R} \to \mathbb{R}$ sao cho $\varphi \circ \cos = \sin \circ \varphi$, tức là :

$\forall x \in \mathbb{R}$, $\varphi(\cos x) = \sin(\varphi(x))$. Ta có : $\begin{cases} \varphi(1) = \varphi(\cos 0) = \sin(\varphi(0)) \in [-1;1] \\ \varphi(-1) = \varphi(\cos \pi) = \sin(\varphi(\pi)) \in [-1;1] \\ \sin(\varphi(1)) = \varphi(\cos 1) = \varphi(\cos(-1)) = \sin(\varphi(-1)), \end{cases}$

từ đó $\varphi(1) = \varphi(-1)$, mâu thuẫn với tính song ánh của φ.

◇ **Trả lời :** ch $\not\mathcal{R}$ sh và cos $\not\mathcal{R}$ sin.

c) 1) Giả sử $f \mathcal{R} g$. Tồn tại $\varphi : \mathbb{R} \to \mathbb{R}$ song ánh sao cho $\varphi \circ f = g \circ \varphi$.

Xét $\psi : \mathbb{R} \to \mathbb{R}$, $x \mapsto \varphi(x) + \dfrac{p}{2}$, hiển nhiên ψ là song ánh. Ta có, với mọi x thuộc $\mathbb{R}$:

$$\psi(x^2) = \varphi(f(x)) + \frac{p}{2} = g(\varphi(x)) + \frac{p}{2} = (\varphi(x))^2 + p\varphi(x) + q + \frac{p}{2} = (\psi(x))^2 + C,$$

trong đó $C = \dfrac{p}{2} - \dfrac{p^2}{4} + q$.

Vậy ta có : $\forall x \in \mathbb{R}, (\psi(-x))^2 = \psi(x^2) - C = (\psi(x))^2$, từ đó : $\forall x \in \mathbb{R}, \psi(-x) = \begin{vmatrix} \psi(x) \\ \text{hoặc} \\ -\psi(x) \end{vmatrix}$

Giả sử $x \in \mathbb{R}^*$; vì $x \neq -x$ và ψ là song ánh, nên ta có $\psi(-x) = -\psi(x)$ và $\psi(x) \neq 0$. Kết quả là $\psi(0) = 0$ và $C = \psi(0^2) - (\psi(0))^2 = 0$.

2) Ngược lại nếu $\frac{p}{2} - \frac{p^2}{4} + q = 0$, thì ánh xạ $\varphi : \underset{x \mapsto -\frac{p}{2}}{\mathbf{R} \to \mathbf{R}}$ là song ánh và thỏa mãn $\varphi \circ f = g \circ \varphi$.

◇ **Trả lời** : $f : \underset{x \mapsto x^2}{\mathbf{R} \to \mathbf{R}}$ và $g : \underset{x \mapsto x^2 + px + q}{\mathbf{R} \to \mathbf{R}}$ tương đương khi và chỉ khi $\frac{p}{2} - \frac{p^2}{4} + q = 0$.

1.3.12 • Tính phản xạ là hiển nhiên.

• $\begin{cases} x \mathcal{R} y \\ y \mathcal{R} x \end{cases} \Rightarrow \begin{cases} f(x) \preccurlyeq f(y) \\ f(y) \preccurlyeq f(x) \end{cases} \Rightarrow f(x) = f(y) \Rightarrow x = y.$

• $\begin{cases} x \mathcal{R} y \\ y \mathcal{R} x \end{cases} \Rightarrow \begin{cases} f(x) \preccurlyeq f(y) \\ f(y) \preccurlyeq f(z) \end{cases} \Rightarrow f(x) \preccurlyeq f(z) \Rightarrow x \mathcal{R} z.$

1.3.13 a) ◇ **Trả lời :**

↗ có nghĩa là : tang

↘ có nghĩa là : giảm

↗↗ có nghĩa là :
tăng nghiêm ngặt

↘↘ có nghĩa là :
giảm nghiêm ngặt

g \ f	↗	↘
↗	↗	↘
↘	↘	↗

g \ f	↗↗	↘↘
↗↗	↗↗	↘↘
↘↘	↘↘	↗↗

b) ◇ **Trả lời** : $E = F = \{0, 1\}$, = trong E, $\leq$ thông thường trong F, $f = \mathrm{Id}_E$.

c) Giả sử $(x, x') \in E^2$ sao cho $x \prec x'$. Vì f tăng và đơn ánh : $f(x) \preccurlyeq f(x')$ và $f(x) \neq f(x')$ nên $f(x) \prec f(x')$.

d) Giả sử $(x, x') \in E^2$ sao cho $f(x) = f(x')$. Vì $\preccurlyeq$ là toàn phần trong E, ta có : $x \prec x'$ hoặc $x' \prec x$ hoặc $x = x'$. Nếu $x \prec x'$ (tương ứng : $x' \prec x$), thì, vì f tăng nghiêm ngặt, $f(x) \prec f(x')$ (tương ứng : $f(x') \prec f(x)$), mâu thuẫn. Vậy $x = x'$.

1.3.14 1) (i) $\Rightarrow$ (ii) :

• Thay Y bởi X : $f(X) \supset f(f(X)) \cup f(X) \cup X$, từ đó $f(X) \supset X$ và $f(X) \supset f(f(X))$. Thay X bởi $f(X)$ trong $f(X) \supset X$, ta được $f(f(X)) \supset f(X)$, vậy $f(f(X)) = f(X)$.

• Nếu $X \subset Y$, thì : $f(Y) = f(X \cup Y) \supset f(f(X)) \cup f(Y) \cup Y \supset f(f(X)) = f(X)$.

2) (ii) $\Rightarrow$ (i) :

$\begin{cases} X \subset X \cup Y \\ Y \subset X \cup Y \end{cases}$ từ đó $\begin{cases} f(X) \subset f(X \cup Y) \\ f(Y) \subset f(X \cup Y) \end{cases}$, và $f(X \cup Y) \supset f(X) \cup f(Y) = f(f(X)) \cup f(Y) \cup Y$.

1.3.15 a) $\forall x \in A, (f \circ g)(f(x)) = f((g \circ f)(x)) = f(x)$, vậy : $\forall x \in A, f(x) \in B$.

Tương tự : $\forall y \in B, g(y) \in A$.

Điều này cho phép định nghĩa các ánh xạ $f' : \underset{x \mapsto f(x)}{A \to B}$ và $g' : \underset{y \mapsto g(y)}{B \to A}$.

b) 1) Giả sử $(a, a') \in A^2$ sao cho $a \prec a'$.

Vì f tang : $f(a) \preccurlyeq f(a')$, vậy $f'(a) \preccurlyeq f'(a')$.

Nếu $f'(a) = f'(a')$, thì : $a = (g \circ f)(a) = g(f'(a)) = g(f'(a')) = (g \circ f)(a') = a'$, mâu thuẫn.

Điều này chứng tỏ : $\forall (a, a') \in A^2, (a \prec a' \Rightarrow f'(a) \prec f'(a')$, tức là : f' tang nghiêm ngặt.

Tương tự, g' tăng nghiêm ngặt.

2) $\forall a \in A, (g' \circ f')(a) = g'(f'(a)) = g(f(a)) = (g \circ f)(a) = a$, vậy $g' \circ f' = \mathrm{Id}_A$.

Tương tự, $f' \circ g' = \mathrm{Id}_B$.

Theo 1.3.2, Mệnh đề 5, f' và g' là những song ánh thuận ngược lẫn nhau.

1.3.16 Vì $f \circ g = \mathrm{Id}_F$, f là toàn ánh (xem 1.3.2, Mệnh đề 2), từ đó $f(E) = F$ rồi thì $(g \circ f)(E) = g(f(E)) = g(F)$.

1.3.17 1) Giả sử $y \in f(f^{-1}(A'))$; tồn tại $x \in f^{-1}(A')$ sao cho $y = f(x)$. Thế thì $y \in A'$ và $y \in f(E)$, từ đó $y \in A' \cap f(E)$.

2) Ngược lại, giả sử $y \in A' \cap f(E)$. Vì $y \in f(E)$, tồn tại $x \in E$ sao cho $y = f(x)$. Vì $y = f(x) \in A'$, nên ta có : $x \in f^{-1}(A')$, vậy $y = f(x) \in f(f^{-1}(A'))$.

1.3.18 1) Giả sử f là song ánh.

• Giả sử $y \in f(\complement_E(A))$; vậy tồn tại $x \in \complement_E(A)$ sao cho $y = f(x)$.

Nếu $y \in f(A)$, thì tồn tại $a \in A$ sao cho $y = f(a)$, từ đó $f(x) = f(a)$ với $x \neq a$, mâu thuẫn (f là song ánh). Vậy $y \in \complement_{E'}(f(A))$.

Điều này chứng minh : $f(\complement_E(A)) \subset \complement_{E'}(f(A))$.

• Giả sử $y \in \complement_{E'}(f(A))$. Vì f là song ánh, nên tồn tại $x \in E$ sao cho $y = f(x)$.

Nếu $x \in A$, thì $y = f(x) \in f(A)$, mâu thuẫn. Vậy $x \in \complement_E(A)$, rồi thì $y = f(x) \in f(\complement_E(A))$.

Điều này chứng tỏ : $\complement_{E'}(f(A)) \subset f(\complement_E(A))$.

2) Ngược lại, giả sử : $\forall A \in \mathfrak{P}(E), f(\complement_E(A)) = \complement_{E'}(f(A))$.

• Đặc biệt : $f(E) = f(\complement_E(\varnothing)) = \complement_{E'}(\varnothing) = E'$, vậy f là toàn ánh.

• Giả sử $(x, y) \in E^2$ sao cho $f(x) = f(y)$. Nếu $y \neq x$, thì $f(x) = f(y) \in f(\complement_E\{x\}) = \complement_{E'}(f\{x\})) = \complement_{E'}\{f(x)\}$, mâu thuẫn, vậy $x = y$. Điều này chứng tỏ f là đơn ánh.

1.3.19 (i) $\Rightarrow$ (ii) :

• Giả sử $y \in E'$. Tồn tại $x \in E$ sao cho $y = f(x)$, từ đó $x \in f^{-1}(\{y\})$, rồi thì $y = f(x) \in f(f^{-1}(\{y\}))$.

Điều này chứng tỏ : $\{y\} \subset f(f^{-1}(\{y\}))$.

• Bao hàm thức $f(f^{-1}(\{y\})) \subset \{y\}$ đã có (xem 1.3.5, Mệnh đề 3)).

(ii) $\Rightarrow$ (iii) :

Giả sử $A' \in \mathfrak{P}(E)$.

• Bao hàm thức $f(f^{-1}(A')) \subset A'$ đã có (xem 1.3.5, Mệnh đề 3)).

• Giả sử $y \in A'$. Vì $f(f^{-1}(\{y\})) = \{y\}$, tồn tại $x \in f^{-1}(\{y\})$ sao cho $y = f(x)$. Thế thì $y = f(x)$ và $x \in f^{-1}(A')$, vậy $y \in f(f^{-1}(A'))$, điều này chứng tỏ $A' \subset f(f^{-1}(A'))$.

(iii) $\Rightarrow$ (iv) :

Giả sử $A' \in \mathfrak{P}(E')$ sao cho $f^{-1}(A') = \varnothing$. Thế thì : $A' = f(f^{-1}(A')) = f(\varnothing) = \varnothing$.

(iv) $\Rightarrow$ (i) :

Giả sử $y \in F$: vì $\{y\} \neq \varnothing$, ta có $f^{-1}(\{y\}) \neq \varnothing$, vậy tồn tại $x \in E$ sao cho $y = f(x)$.

1.3.20 . a) Theo 1.3.5, Mệnh đề, ta có :

$$f^{-1}(A' \,\Delta\, B') = f^{-1}((A' \cap \complement B') \cup (\complement A' \cap B')) = (f^{-1}(A') \cap \overline{f^{-1}(B')}) \cup (\overline{f^{-1}(A')} \cap f^{-1}(B'))$$
$$= f^{-1}(A') \,\Delta\, f^{-1}(B').$$

b) 1) Giả sử f là đơn ánh và giả sử $(A, B) \in (\mathfrak{P}(E))^2$.

α) $f(A \,\Delta\, B) = f((A \cap \complement B) \cup (\complement A \cap B)) = f(A \cap \complement B) \cup f(\complement A \cap B) \subset (f(A) \cap f(\complement B)) \cup (f(\complement A) \cap f(B))$.

Ta chứng minh $f(\complement B) \subset \overline{f(B)}$.

Cho $y \in f(\complement B)$. Nếu $y \in f(B)$ thì tồn tại $b \in B$ và $c \in \complement B$ sao cho $y = f(b) = f(c)$, mâu thuẫn với giả thiết f đơn ánh. Vậy $y \in \overline{f(B)}$.

Chứng minh tương tự : $f(\complement A) \subset \overline{f(A)}$.

Thế thì : $f(A \,\Delta\, B) \subset (f(A) \cap \overline{f(B)}) \cup (\overline{f(A)} \cap f(B)) = f(A) \,\Delta\, f(B)$.

β) Giả sử $y \in f(A) \cap \overline{f(B)}$.

Tồn tại $a \in A$ sao cho $y = f(a)$.

Nếu $a \in B$, thì $y = f(a) \in f(B)$, mâu thuẫn. Vậy $a \notin B$, $y = f(a) \in f(A \cap \complement B)$.

Điều này chứng tỏ : $f(A) \cap \overline{f(B)} \subset f(A \cap \complement B)$.

Tương tự : $\overline{f(A)} \cap f(B) \subset f(\complement A \cap B)$. Từ đó :

$$f(A) \,\Delta\, f(B) = (f(A) \cap \overline{f(B)}) \cup (\overline{f(A)} \cap f(B)) \subset f(A \cap \complement B) \cup f(\complement A \cap B)$$
$$= f((A \cap \complement B) \cup (\complement A \cap B)) = f(A \,\Delta\, B).$$

2) Ngược lại, giả sử : $\forall (A, B) \in (\mathfrak{P}(E))^2$, $f(A \,\Delta\, B) = f(A) \,\Delta\, f(B)$.

Giả sử $(x, y) \in E^2$ sao cho $f(x) = f(y)$.

Nếu $x \neq y$, thì : $\begin{cases} f(\{x\} \,\Delta\, \{y\}) = f(\{x, y\}) = \{f(x)\} = \varnothing \\ f(\{x\}) \,\Delta\, f(\{y\}) = \{f(x)\} \,\Delta\, \{f(y)\} = \varnothing \end{cases}$, mâu thuẫn. Vậy $x = y$.

Điều này chứng tỏ f là đơn ánh.

1.3.21 ◇ **Trả lời** : Mọi bộ phận khác rỗng $\mathcal{G}$ của $\mathcal{J}$ có biên trên và biên dưới trong $\mathcal{J}$ đối với quan hệ bao hàm, chúng tương ứng là $\{x \in E ; \exists X \in \mathcal{G}, x \in X\}$ và $\{x \in E ; \forall X \in \mathcal{G}, x \in X\}$, tức là, với các ký hiệu ở 1.3.6, $\bigcup_{X \in \mathcal{G}} X$ và $\bigcap_{X \in \mathcal{G}} X$.

1.3.22 a) • $x \in \complement_E \left(\bigcup_{i \in I} A_i \right) \Leftrightarrow$ không $(\exists i \in I, x \in A_i) \Leftrightarrow (\forall i \in I, x \in \complement_E(A_i))$

$\Leftrightarrow x \in \bigcap_{i \in I} \complement_E(A_i)$.

• Chứng minh tương tự đối với quan hệ thứ hai.

b) • $x \in \left(\bigcup_{i\in I} A_i\right) \cap B \Leftrightarrow \begin{cases} \exists i \in I, x \in A_i \\ x \in B \end{cases} \Leftrightarrow (\exists i \in I, x \in A_i \cap B) \Leftrightarrow x \in \bigcup_{i\in I}(A_i \cap B)$.

• Tương tự đối với quan hệ kia.

c) • $x \in \left(\bigcup_{i\in I} A_i\right) \cap \left(\bigcup_{j\in J} B_j\right) \Leftrightarrow \begin{cases} \exists i \in I, x \in A_i \\ \exists j \in J, x \in B_j \end{cases} \Leftrightarrow (\exists (i,j) \in I \times J, x \in A_i \cap B_j)$

$$\Leftrightarrow x \in \bigcup_{(i,j)\in I\times J} A_i \cap B_j .$$

• $x \in \left(\bigcap_{i\in I} A_i\right) \cup \left(\bigcap_{j\in J} B_j\right) \Leftrightarrow \left|\begin{array}{l} \forall i \in I, x \in A_i \\ \text{hoặc} \\ \forall j \in J, x \in B_j \end{array}\right. \Leftrightarrow (\forall (i,j) \in I \times J, x \in A_i \cup B_j)$

$$\Leftrightarrow x \in \bigcap_{(i,j)\in I\times J} (A_i \cup B_j) .$$

Câu hỏi c) là một dạng tổng quát hóa của b).

d) Dễ dàng.

e) $\bigcap_{i\in I}(A_i - B_i) = \bigcap_{i\in I}(A_i \cap \complement_E(B_i)) = \left(\bigcap_{i\in I} A_i\right) \cap \left(\bigcap_{i\in I} \complement_E(B_i)\right) = \left(\bigcap_{i\in I} A_i\right) \cap \complement_E\left(\bigcup_{i\in I} B_i\right)$

$= \left(\bigcap_{i\in I} A_i\right) - \left(\bigcup_{i\in I} B_i\right)$.

1.3.23 a) • Với mọi x thuộc E :

$$x \in f^{-1}\left(\bigcup_{i\in I} A'_i\right) \Leftrightarrow \left(f(x) \in \bigcup_{i\in I} A'_i\right) \Leftrightarrow (\exists i \in I, f(x) \in A'_i) \Leftrightarrow (\exists i \in I, x \in f^{-1}(A'_i))$$

$$\Leftrightarrow x \in \bigcup_{i\in I} f^{-1}(A'_i) .$$

• Tương tự đối với quan hệ kia.

b) Với mọi y thuộc E' :

• $y \in f\left(\bigcup_{i\in I} A_i\right) \Leftrightarrow \left(\exists x \in \bigcup_{i\in I} A_i, y = f(x)\right) \Leftrightarrow (\exists i \in I, \exists x \in A_i, y = f(x))$

$$\Leftrightarrow (\exists i \in I, y \in f(A_i)) \Leftrightarrow y \in \bigcup_{i\in I} f(A_i) .$$

• $y \in f\left(\bigcap_{i\in I} A_i\right) \Leftrightarrow \left(\exists x \in \bigcap_{i\in I} A_i, y = f(x)\right) \Leftrightarrow \left(\exists x \in E, \begin{cases} y = f(x) \\ \forall i \in I, x \in A_i \end{cases}\right)$

$\Rightarrow (\forall i \in I, \exists x \in A_i, y = f(x)) \Leftrightarrow (\forall i \in I, y \in f(A_i)) \Leftrightarrow y \in \bigcap_{i\in I} f(A_i)$.

Các câu hỏi a) b) tổng quát hóa các kết quả đã thấy ở 1.3.5.

c) Giả sử f là đơn ánh.

Cho $y \in \bigcap_{i\in I} f(A_i)$. Với mọi i thuộc I, tồn tại $a_i \in A_i$ sao cho $y = f(a_i)$.

Vì f là đơn ánh, nên ta có : $\forall (i,j) \in I^2, a_i = a_j$.

Vậy tồn tại $a \in E$ sao cho : $\forall i \in I, a_i = a$. Do đó $y = f(x) \in f\bigcap_{i\in I} A_i$.

1.3.24 a) α) $(g \circ f)(A) = g(f(A)) \subset g(A) \subset A$.

β) Suy ra dễ dàng từ α).

γ) $A \supset f(A) \supset f^2(A) \supset \ldots \supset f^n(A) = A$,

vậy $A = f(A) = f^2(A = \ldots = f^n(A)$.

b) Theo bài tập 1.3.23, b) : $\begin{cases} f\left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I} f(A_i) \subset \bigcup_{i\in I} A_i \\ f\left(\bigcap_{i\in I} A_i\right) \subset \bigcap_{i\in I} f(A_i) \subset \bigcap_{i\in I} A_i \end{cases}$.

1.3.25 a) • Giả sử $i \in I$. Vì $A'_i \neq \varnothing$ và f là toàn ánh, ta có $f^{-1}(A'_i) \neq \varnothing$.

• Giả sử $(i, j) \in I^2$ sao cho $f^{-1}(A'_i) \cap f^{-1}(A'_j) \neq \varnothing$.

Thế thì $f^{-1}(A'_i \cap A'_j) = f^{-1}(A'_i) \cap f^{-1}(A'_j) \neq \varnothing$, vậy $A'_i \cap A'_j \neq \varnothing$, $i = j$.

• Cho $x \in E$. Tồn tại $i \in I$ sao cho $f(x) \in A'_i$, từ đó $x \in f^{-1}(A'_i)$.

Điều này chứng tỏ rằng $(f^{-1}(A'_i))_{i\in I}$ là một phân hoạch của E.

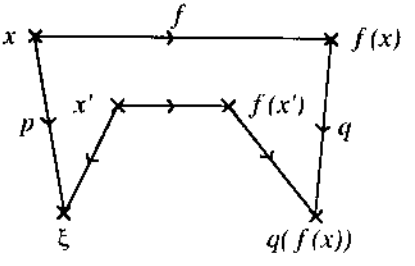
b) ◇ **Trả lời** : $E = \{0, 1\}, E' = \{0\}, f : \begin{array}{c} E \to E', (A_i)_{i\in I} = (\{0\}, \{1\}). \\ x \mapsto 0 \end{array}$

C.1.1 **A** 1) α) Giả sử f tương thích với $\mathcal{R}$ và $\mathcal{S}$.

Tồn tại

Giả sử $\xi \in E / \mathcal{R}$; tồn tại $x \in E$ sao cho $\xi = p(x)$. Ta định nghĩa $\varphi(\xi)$ bởi : $\varphi(\xi) = q(f(x))$, điều này là đúng đắn, vì nếu x' là một phần tử (khác) của E sao cho $\xi = p(x')$, thì $x \mathcal{R} x'$, do đó $f(x) \mathcal{S} f(x')$, tức là $q(f(x)) = q(f(x'))$.

Nói khác đi, tất cả các phần tử của ξ có cùng một ảnh qua $q \circ f$.



Theo cách xây dựng : $\forall x \in E$, $\varphi(p(x)) = q(f(x))$, tức là : $\varphi \circ p = q \circ f$.

Duy nhất

Giả sử $\varphi, \psi : E / \mathcal{R} \to F / \mathcal{S}$ sao cho $\varphi \circ p = q \circ f$ và $\psi \circ p = q \circ f$.

Thế thì ta có : $\forall x \in E$, $\varphi(p(x)) = \psi(p(x))$, từ đó vì p là toàn ánh ; $\forall \xi \in E / \mathcal{R}$, $\varphi(\xi) = \psi(\xi)$.

β) Ngược lại, giả sử tồn tại $\varphi : E / \mathcal{R} \to F / \mathcal{S}$ sao cho $\varphi \circ p = q \circ f$.

Ta có, với mọi $(x; x')$ thuộc E^2 :

$x \mathcal{R} x' \Leftrightarrow p(x) = p(x') \Rightarrow \varphi(p(x) = \varphi(p(x')) \Leftrightarrow q(f(x)) = q(f(x')) \Leftrightarrow f(x) \mathcal{S} f(x')$.

Như vậy f tương thích với $\mathcal{R}$ và $\mathcal{S}$.

Chỉ dẫn và trả lời
các bài tập chương 2

2.1.1 a) Tính giao hoán là hiển nhiên.

Vì $(-1 * 0) * 2 = 0 * 2 = -3$ và $(-1) * (0 * 2) = (-1) * (-3) = 3$, nên * không có tính kết hợp. Rõ ràng 1 là phần tử trung hòa.

b) ◇ **Trả lời:** 1) $\left\{-2, \frac{4}{3}\right\}$ 2) $\{-1, 0, 1\}$.

2.1.2 $a * (b * c) = (0 * (-a)) * (b * c) = (0 * (0 * a)) * (b * c) = a * (0 * 0) * (b * c)$

$= (a * 0) * (b * c) = c * (b * (a * 0)) = c * (0 * (a * b)) = (a * b) * (0 * c) = (a * b) * (-c)$.

Một ví dụ: * = -

2.1.3 $(x \top y) \top z = (x * a * y) * a * z = x * a * (y * a * z) = x \top (y \top z)$.

2.1.4 1) Ta chứng minh bằng quy nạp theo n: $\forall n \in \mathbb{N}^*, x^n y = y x^n$.

- $n = 1$: $xy = yx$ theo giả thiết.
- nếu $x^n y = y x^n$, thì: $x^{n+1} y = x(x^n y) = x(y x^n) = (yx)x^n = y x^{n+1}$

2) Áp dụng kết quả trên vào (p, y, x^n) thay cho (n, x, y), ta kết luận: $y^p x^n = x^n y^p$.

2.1.5 1) Nếu $x \in E$ là khả đối xứng đối với * thì với mọi (y, z) thuộc E^2:

$$x * y = x * z \Rightarrow x^{-1} * (x * y) = x^{-1} * (x * z) \Rightarrow (x^{-1} * x) * y = (x^{-1} * x) * z \Rightarrow y = z$$

vậy x là phần tử chính quy trái. Tương tự, x là phần tử chính quy phải.

2) Trong $(\mathbb{N}, +)$, 1 là phần tử chính quy nhưng không khả đối xứng.

2.1.6 a) γ_a là đơn ánh khi và chỉ khi: $\forall (x, y) \in E^2, (a * x = a * y \Rightarrow x = y)$, tức là khi và chỉ khi a là phần tử chính quy trái.

b) $(\forall (a, b, c) \in E^3, \quad (a * x) * b = a * (x * b))$.

$\Leftrightarrow \forall (a, b) \in E^2, \forall x \in E, \delta_b(\gamma_a(x)) = \gamma_a(\delta_b(x)) \Leftrightarrow \forall (a, b) \in E^2, \delta_b \circ \gamma_a = \gamma_a \circ \delta_b$.

2.1.7 Ta ký hiệu $\gamma_x : E \to E$ và $\delta_x : E \to E$.
$\quad y \mapsto x * y \qquad\qquad y \mapsto y * x$

Vì x chính quy, nên γ_x và δ_x đều là đơn ánh (xem bài tập 2.1.6 a)). Vì E hữu hạn, ta suy ra rằng (xem dưới đây 3.2.2, Mệnh đề 6), γ_x và δ_x đều là song ánh.

• Vậy tồn tại $(a, b) \in E^2$ sao cho $\gamma_x(a) = x$ và $\delta_x(b) = x$, tức là: $x * a = x$ và $b * x = x$.

Ta có: $\forall y \in E,\ x * (a * y) = (x * a) * y = x * y$, vậy vì x chính quy: $\forall y \in E, \quad a * y = y$.

Tương tự: $\forall y \in E, \quad y * b = y$.

Như thế, a là phần tử trung hòa trái và b là phần tử trung hòa phải; thế thì: $a * b = b$ và $a * b = a$, vậy với ký hiệu $e = a = b$ thì e là trung hòa .

• Tồn tại $(x', x'') \in E^2$ sao cho $\gamma_x(x') = e$ và $\delta_x(x'') = e$, tức là: $x * x' = e$ và $x'' * x = e$.

Ta có: $x' = (x'' * x) * x' = x'' * (x * x') = x''$, vậy x là khả đối xứng.

2.1.8 a) $(x * y) * (x * y) = (x * (y * x)) * y = (x * (x * y)) * y = (x * x) * (y * y) = x * y$.

b) $x^{-1} * x^{-1} = (x * x)^{-1} = x^{-1}$ (xem 2.1, Mệnh đề 4).

Vả lại: $x = x * (x * x^{-1}) = (x * x) * x^{-1} = x * x^{-1} = e$.

2.1.9 a) $(x * y)\mathrm{T}(x' * y') = (x\mathrm{T}(x' * y')) * (y\mathrm{T}(x' * y')) = (x\mathrm{T}x') * (x\mathrm{T}y') * (y\mathrm{T}x') * (y\mathrm{T}y')$

và $(x * y)\mathrm{T}(x' * y') = ((x * y)\mathrm{T}x') * ((x * y)\mathrm{T}y') = (x\mathrm{T}x') * (y\mathrm{T}x') * (x\mathrm{T}y') * (y\mathrm{T}y')$,

do đó, vì $x\mathrm{T}x'$ và $y\mathrm{T}y'$ đều chính quy đối với * :

$$(x\mathrm{T}y') * (y\mathrm{T}x') = (y\mathrm{T}x') * (x\mathrm{T}y').$$

b) Ký hiệu ε là phần tử trung hòa của T, kết quả của a) áp dụng vào $(x, y, \varepsilon, \varepsilon)$ thay cho (x, y, x', y') chứng tỏ rằng $x\mathrm{T}\varepsilon$ và $y\mathrm{T}\varepsilon$ đều giao hoán được đối với *, tức là: $x * y = y * x$.

c) Hệ quả hiển nhiên của b).

2.1.10 a) Ánh xạ $f :]0; +\infty[\to]0; +\infty[$ là một đẳng cấu phổng nhóm từ $(]0; +\infty[, *)$ lên
$\qquad x \mapsto x^2$

$(]0; +\infty[, +)$.

◇ **Trả lời**: * có tính kết hợp, giáo hoán và không có phần tử trung hòa.

b) $f(a * \ldots * a) = f(a) + \ldots + f(a) = na^2$, vậy $a * \ldots * a = f^{-1}(na^2) = \sqrt{n}a$.

◇ **Trả lời**: $\sqrt{n}a$.

2.1.11 a) Ánh xạ $f : \mathbb{R} \to \mathbb{R}$ là một đẳng cấu phổng nhóm từ $(\mathbb{R}, *)$ lên $(\mathbb{R}, .)$.
$\qquad x \mapsto 1 - x$

◇ **Trả lời**: * có tính kết hợp, giao hoán, nhận 0 là phần tử trung hòa. Mọi phần tử x thuộc $\mathbb{R} - \{1\}$ có phần tử đối xứng đối với *, đó là $\dfrac{x}{x-1}$; 1 không có phần tử đối xứng đối với *.

b) ◇ **Trả lời**: $1 - (1 - a)^n$.

2.1.12 a) $\forall (a, a') \in A^2, f(a) \top f(a') = f(a * a') \in f(A)$.

b) $\forall (x, x') \in (f^{-1}(B))^2, f(x * x') = f(x) \top f(x') \in B$.

2.1.13 1) Với mọi x thuộc X : $((f * g) * h)(x) = (f * g)(x) * h(x) = (f(x) * g(x)) * h(x)$
$= f(x) * (g(x) * h(x)) = f(x) * (g*h)(x) = (f * (g * h))(x)$.

2) Với mọi x thuộc X : $(g * f)(x) = g(x) * f(x) = f(x) * g(x) = (f * g)(x)$.

3) Ký hiệu e là phần tử trung hòa của E đối với $*$, ánh xạ hằng $e : X \to E$, $x \mapsto e$ là phần tử trung hòa của $*$ trong E^X.

4) Với $f \in E^X$, ánh xạ $X \to E$, $x \mapsto (f(x))^{-1}$ là đối xứng của f đối với $*$.

2.1.14 a) 1) Hiển nhiên.

2) • Giả sử $x \in (A * B) * C$. Tồn tại $(a, b, c) \in E^3$ sao cho $x = (a * b) * c$. Thế thì: $x = a * (b * c) \in A * (B*C)$. Điều này chứng minh bao hàm thức $(A * B) * C \subset A * (B * C)$. Bao hàm thức kia được chứng minh một cách tương tự.

• Phương pháp tiến hành tương tự như đối với tính giao hoán.

3) Hiển nhiên:

b) Ta lấy $E = R$, $* = +$, $A = \{0, 1\}$. Không tồn tại bộ phận B của $\mathbb{R}$ sao cho $A + B = \{0\}$.

◇ **Trả lời**: Không.

2.1.15
- $(a * x) * (a * y) = a * (x * a * y) \in \{a\} * E$.
- $(x * b) * (y * b) = (x * b * y) * b \in E * \{b\}$.
- $(a * x * b) * (a * y * b) = a * (x * b * a * y) * b \in \{a\} * E * \{b\}$.
- $(x * a * y) * (x' * a * y') = x * a * (y * x' * a * y') \in E * \{a\} * E$.

2.1.16 a) 1) $B \subset B \cup C$ và $C \subset B \cup C$ vậy (xem bài tập 2.1.14, *a*) *1*)):

$$A * B \subset A * (B \cup C) \quad \text{và} \quad A * C \subset A * (B \cup C),$$

từ đó: $(A * B) \cup (A * C) \subset A * (B \cup C)$.

2) Giả sử $x \in A * (B \cup C)$. Tồn tại $(a, y) \in A \times (B \cup C)$ sao cho $x = a * y$.

Nếu $y \in B$ (tương ứng : C) thì $x \in A * B$ (tương ứng : $A * C$). Vậy $x \in (A * B) \cup (A * C)$.

◇ **Trả lời**: $A * (B \cup C) = (A * B) \cup (A * C)$.

b) 1) $B \cap C \subset B$ và $B \cap C \subset C$ vậy (xem bài tập 2.1.14, *a*), *1*)):

$$A * (B \cap C) \subset (A * B) \text{ và } A * (B \cap C) \subset A * C,$$

suy ra : $A * (B \cap C) \subset (A * B) \cap (A * C)$.

2) Bao hàm thức ngược có thể sai, chẳng hạn như trong ví dụ sau:

$$E = \mathbb{Z}, \quad * = +, \quad A = \mathbb{Z}_+, \quad B = \mathbb{R}_+, \quad C = \mathbb{R}_+^*,$$

trong đó ta có: $A * (B \cap C) = \varnothing$ và $(A * B) \cap (A * C) = \mathbb{Z}_+$.

◇ **Trả lời**: $A * (B \cap C) \subset (A * B) \cap (A * C)$.

2.1.17 Giả sử $(x, a) \in E \times A$; ta giả thiết $x * a \notin A$ (tức là: $x * a$ chính quy đối với $*$). Với mọi (y, z) thuộc E^2:

$$a * y = a * z \Rightarrow x * (a * y) = x * (a * z) \Rightarrow (x * a) * y = (x * a) * z \Rightarrow y = z,$$

vậy a chính quy trái.

Tương tự, a chính quy phải, vậy a chính quy, mâu thuẫn.

2.1.18 a) $\forall (a, b, c, d) \in A^4, (a * b) * (c * d) \in A * A$.

b) Giả sử $(x, y) \in (A^c)^2$, ta có:

$$\forall a \in A, (x * y) * a = x * (y * a) = x * (a * y) = (x * a) * y = (a * x) * y = a * (x * y),$$

vậy $x * y \in A^c$.

2.1.19 a) Giả sử $(a, a') \in A^2$; ta có, với mọi (y, z) thuộc E^2:

$$((a * a') * y) * z = (a * (a' * y)) * z = a * ((a' * y) * z) = a * (a' * (y * z)) = (a * a') * (y * z),$$

vậy $a * a' \in A$.

b) $\forall (x, y, z) \in A^3, (x * y) * z = x * (y * z)$ bởi vì $x \in A$ và $(y, z) \in E^2$.

2.1.20 a) Giả sử $(a, a') \in C^2$; ta có:

$$(a * a') * x = a * (a' * x) = a * (x * a') = (a * x) * a' = (x * a) * a' = x * (a * a'),$$

với mọi x thuộc E. Vậy $a * a' \in C$.

Ta cũng có thể chú ý rằng $C = E^C$ (xem bài tập 2.1.18).

b) $\forall (a, b) \in C^2, a * b = b * a$ (vì $a \in C$ và $b \in E$).

2.1.21 1) $((x, y) * (x, y')) * (x'', y'') = (x \mathsf{T} x', y \perp y') * (x'', y'') = ((x \mathsf{T} x') \mathsf{T} x'', (y \perp y') \perp y'')$
$= (x \mathsf{T} (x' \mathsf{T} x''), y \perp (y' \perp y'')) = (x, y) * (x' \mathsf{T} x'', y' \perp y'') = (x, y) * ((x', y') * (x'', y''))$.

2) $(x', y') * (x, y) = (x' \mathsf{T} x, y' \perp y) = (x \mathsf{T} x', y \perp y') = (x, y) * (x', y')$.

3) Nếu e (tương ứng : ε) là phần tử trung hòa đối với T (tương ứng : $\perp$), thì (e, ε) là phần tử trung hòa đối với $*$ vì:

$$\forall (x, y) \in E \times F, \begin{cases} (x, y) * (e, \varepsilon) = (x \mathsf{T} e, y \perp \varepsilon) = (x, y) \\ (e, \varepsilon) * (x, y) = (e \mathsf{T} x, \varepsilon \perp y) = (x, y) \end{cases}$$

4) Nếu x (tương ứng : y) có phần tử đối xứng x' (tương ứng : y') đối với T (tương ứng : $\perp$), thì (x, y) có (x', y') là đối xứng đối với $*$ vì:

$$\begin{cases} (x, y) * (x', y') = (x \mathsf{T} x', y \perp y') = (e, \varepsilon) \\ (x', y') * (x, y) = (x' \mathsf{T} x, y' \perp y) = (e, \varepsilon). \end{cases}$$

2.1.22 a) 1) Giả sử f là đơn ánh. Với mọi (g, h) thuộc E^2, ta có:

$$f \circ g = f \circ h \Rightarrow (\forall x \in X, f(g(x)) = f(h(x))) \Rightarrow (\forall x \in X, g(x) = h(x)) \Rightarrow g = h,$$

vậy f chính quy trái đối với $\circ$ trong E.

2) Ngược lại, giả sử f chính quy trái đối với $\circ$ trong E. Giả sử $(x, x') \in X^2$ sao cho $f(x) = f(x')$. Nếu $x \neq x'$, ta xét $g: X \to X$, xác định bởi: $\begin{cases} g(x) = x', \ g(x') = x \\ \forall t \in X - \{x, x'\}, \ g(t) = t \end{cases}$. Thế thì ta có $f \circ g = f = f \circ \mathrm{Id}_X$, vậy $g = \mathrm{Id}_X$, $x = x'$, mâu thuẫn.

Vậy $x = x'$.

b) 1) Giả sử f là toàn ánh. Cho $(g, h) \in E^2$ sao cho $g \circ f = h \circ f$, và $y \in X$. Tồn tại $x \in X$ sao cho $y = f(x)$; ta có: $g(y) = g(f(x)) = h(f(x)) = h(y)$.

Điều này chứng tỏ $g = h$, vậy f chính quy phải đối với $\circ$ trong E.

2) Ngược lại, giả sử f chính quy phải đối với $\circ$ trong E. Ta lập luận phản chứng: Giả sử f không là toàn ánh. Thế thì tồn tại $\beta \in X$ sao cho $\beta \notin f(X)$. Ta xét $g : X \to X$, xác định bởi:

$$g(t) = \begin{cases} t & \text{nếu } t \in f(X) \\ f(\beta) & \text{nếu } t \notin f(X) \end{cases}.$$

Ta có: $\forall x \in X$, $(g \circ f)(x) = g(f(x)) = f(x)$.

Vậy: $g \circ f = f = \mathrm{Id}_Y \circ f$,

từ đó: $g = \mathrm{Id}_X$.

Đặc biệt: $\beta = g(\beta)$.

Nhưng $\beta \notin f(X)$, vậy $g(\beta) = f(\beta)$.

Như thế: $\beta = f(\beta) \in f(X)$, mâu thuẫn.

2.1.23 a) • $\begin{cases} a * b \leq b \\ a * b \leq a \end{cases}$, vậy $a * b \leq b * a$

• $\begin{cases} b * a \leq a \\ b * a \leq b \end{cases}$, vậy $b * a \leq a * b$.

b) • $a * a \leq a$

• $\begin{cases} a \leq a \\ a \leq a \end{cases}$, vậy $a \leq a * a$.

c) $\begin{cases} a * c \leq a \leq b \\ a * c \leq c \end{cases} \Rightarrow a * c \leq b * c$.

d) $\begin{cases} a \leq b \\ c \leq d \end{cases} \Rightarrow \begin{cases} a * c \leq b * c \\ c * b \leq d * b \end{cases} \Rightarrow a * c \leq b * d$.

e) • $\begin{cases} b * c \leq b \Rightarrow a * (b * c) \leq a * b \\ a * (b * c) \leq b * c \leq c \end{cases}$, vậy $a * (b * c) \leq (a * b) * c$.

• $\begin{cases} a * b \leq b \Rightarrow (a * b) * c \leq b * c \\ (a * b) * c \leq a * b \leq a \end{cases}$, vậy $(a * b) * c \leq a * (b * c)$.

2.2.1 Giả sử $(x, y) \in G^2$. Ta có: $\begin{cases} (xy^2) = (xy)(xy) = x(yx)y \\ (xy)^2 = e = x^2 y^2 = x(xy)y \end{cases}$, do đó vì x và y đều chính quy: $yx = xy$.

2.2.2 Giả sử $x \in G$; để chứng minh rằng tồn tại $(a, b) \in A \times B$ sao cho $x = ab$, tức là $a^{-1}x = b$, ta sẽ chứng minh rằng các bộ phận của $xA^{-1}x$ (xác định bởi $A^{-1}x = \{a^{-1}x;\ a \in A\}$ và B, đều không rời nhau.

Vì $a \mapsto a^{-1}x$ là một song ánh từ A lên $A^{-1}x$, ta có $\mathrm{Card}(A^{-1}x) = \mathrm{Card}(A)$, và do vậy: $\mathrm{Card}(A^{-1}x) + \mathrm{Card}(B) = \mathrm{Card}(A) + \mathrm{Card}(B) > \mathrm{Card}(G)$. Suy ra: $(A^{-1}x) \cap B \neq \varnothing$. Vậy tồn tại $y \in (A^{-1}x) \cap B$, và $a \in A$ sao cho $y = a^{-1}x$. Vậy: $x = ay \in AB$.

2.2.3 a) Tính phản xạ và tính đối xứng là hiển nhiên. Nếu $x\mathcal{R}y$ và $y\mathcal{R}z$, thì $(y = x$ và $z = y)$ hoặc $(y = x$ và $z = y^{-1})$ hoặc $(y = x^{-1}$ và $z = y)$ hoặc $(y = x^{-1}$ và $z = y^{-1})$, từ đó: $z = x$ hoặc $z = x^{-1}$.

b) $G/\mathcal{R}$ gồm $\{e\}$, các đơn tử $\{x\}$ $(x \in S)$ và các tập có hai phần tử $\{x, x^{-1}\}$ $(x \in G - (S \cup \{e\}))$. Ta ký hiệu $\alpha = \mathrm{Card}(S)$, $\beta = \mathrm{Card}(g - (S \cup \{e\}))$.

Ta có: $1 + \alpha + 2\beta = \mathrm{Card}(G)$, vậy α và $\mathrm{Card}(G)$ có tính chẵn lẻ trái nhau.

2.2.4 1) Giả sử $(a, b), (c, d) \in (\mathbb{R}^* \times \mathbb{R})$; ta có: $\forall x \in \mathbb{R}$, $(f_{a,b} \circ f_{c,d})(x) = a(cx + d) + b = f_{ac,ad+b}(x)$, vậy $f_{a,b} \circ f_{c,d} = f_{ac,ad+b}$, điều này chứng tỏ rằng $\circ$ là một luật hợp thành trong $\mathcal{A}$.

2) $f_{1,0} = \mathrm{Id}_{\mathbb{R}}$ là phần tử trung hòa đối với $\circ$.

3) $\circ$ có tính kết hợp trong $\mathbb{R}^*$, do đó trong $\mathcal{A}$.

4) mỗi phần tử $f_{a,b}$ của $\mathcal{A}$ có đối xứng đối với $\circ$, đó là $f_{\frac{1}{a}, -\frac{b}{a}}$.

5) $f_{1,1} \circ f_{2,0} = f_{2,1}$, $f_{2,0} \circ f_{1,1} = f_{2,2}$ và $f_{2,1} \neq f_{2,2}$.

Xem thêm ví dụ 2.2.6.

◇ **Trả lời**: $(\mathcal{A}, \circ)$ là một nhóm không giao hoán.

2.2.5 1) Chiều $\Leftarrow$ là hiển nhiên.

2) Giả sử $H \cup K = G$.

Ta lập luận phản chứng: Giả sử $H \neq G$ và $K \neq G$. Tồn tại $x \in G$ sao cho $x \notin H$ và tồn tại $y \in G$ sao cho $y \notin K$. Vì $H \cup K = G$, nên ta có $x \in K$ và $y \in H$.

Xét phần tử xy của G.

Vì $xy \in G = H \cup K$ nên ta có : $xy \in H$ hoặc $xy \in K$.

Nếu $xy \in H$, thì $x = (xy)y^{-1} \in H$, mâu thuẫn.

Nếu $xy \in K$ thì $y = x^{-1}(xy) \in K$, mẫu thuẫn.

2.2.6 a) 1) Rõ ràng rằng * là luật hợp thành trong G.

2) $((x, y) * (x', y')) * (x'', y'') = (xx', xy' + y) * (x'', y'') = (xx'x'', xx'y'' + xy' + y)$

và $(x, y) * ((x', y') * (x'', y'')) = (x, y) * (x'x'', x'y'' + y') = (xx'x'', xx'y'' + xy' + y)$,

vậy * có tính kết hợp.

3) $(1, 0)$ là phần tử trung hòa đối với *.

4) Việc giải $(x, y) * (x', y') = (x', y') * (x, y) = (1, 0)$ chứng tỏ rằng mọi phần tử (x, y) của $\mathbb{R}^* \times \mathbb{R}$ có đối xứng đối xứng đối với *, đó là $\left(\frac{1}{x}, -\frac{y}{x}\right)$.

5) $(1, 1) * (2, 0) = (2, 1)$ và $(2, 0) * (1, 1) = (2, 2)$, vậy * không giáo hoán.

Nhận xét : Ta cũng có thể sử dụng một sự chuyển cấu trúc nhóm (xem 2.2.3, Mệnh đề 3), chú ý rằng ánh xạ $(x, y) \mapsto f_{x,y}$ (xác định trong bài tập 2.2.4) là một đẳng cấu phóng nhóm và $\mathcal{A} = \{f_{x,y} ; (x, y) \in \mathbb{R}^* \times \mathbb{R}\}$ là một nhóm.

b) Ký hiệu $H = \mathbb{R}^{*+} \times \mathbb{R}$ ($H \subset G$).

1) $(1, 0) \in H$.

2) $\forall ((x, y), (x', y')) \in H^2$, $(x, y) * (x', y') = (xx', xy' + y) \in H$ (vì $xx' > 0$).

3) $\forall (x, y) \in H$, $(x, y)^{-1} = \left(\frac{1}{x}, -\frac{y}{x}\right) \in H$ (vì $\frac{1}{x} > 0$).

2.2.7 1) $e \in C$.

2) Giả sử $(x, x') \in C^2$; ta có: $\forall y \in G$, $(xx')y = x(x'y) = x(yx') = (xy)x' = (yx)x' = y(xx')$, vậy $xx' \in C$ (xem thêm bài tập 2.1.20, *a*)).

Giả sử $x \in C$; ta có, với mọi y thuộc G : $xy = yx \Rightarrow x^{-1}(xy)x^{-1} = x^{-1}(yx)x^{-1} \Rightarrow yx^{-1} = x^{-1}y$, và do vậy $x^{-1} \in C$.

2.2.8 a) Tương tự như bài tập 2.2.6 *a*).

b) Giả sử $(a, b) \in G$, ta có, với mọi (x, y) thuộc G:

$$(a,b)*(x,y) = (x,y)*(a,b) \Leftrightarrow ay + \frac{b}{x} = xb + \frac{y}{a} \Leftrightarrow (a^2 - 1)xy + ab(1 - x^2) = 0.$$

Vậy:

$$(\forall (x, y) \in G, (a, b) * (x, y) = (x, y) * (a, b)) \Leftrightarrow (\forall (x, y) \in \mathbb{R}^{*+} \times \mathbb{R}, (a^2 - 1)xy + ab(1 - x^2) = 0).$$

$$\Leftrightarrow \begin{cases} a^2 - 1 = 0 \\ ab = 0 \end{cases} \Leftrightarrow \left(\begin{cases} a = 1 \\ b = 0 \end{cases} \text{ hoặc } \begin{cases} a = -1 \\ b = 0 \end{cases} \right).$$

◇ **Trả lời:** $\{(1, 0), (-1, 0)\}$.

c) Kiểm chứng dễ dàng.

d) Tương tự như c), ta chứng minh dễ dàng rằng H_k là một nhóm con của G. Hơn nữa, với mọi (x, x') thuộc $(\mathbb{R}^*)^2$:

$$\left(x, k\left(x - \frac{1}{x}\right)\right) * \left(x', k\left(x' - \frac{1}{x'}\right)\right) = \left(xx', k\left(xx' - \frac{1}{xx'}\right)\right) = \left(x', k\left(x' - \frac{1}{x'}\right)\right) * \left(x, k\left(x - \frac{1}{x}\right)\right).$$

2.2.9 *Suy luận phản chứng*

Giả sử $H \neq G$. Tồn tại $x \in G$ sao cho $x \notin H$. Ánh xạ $h \mapsto hx$ là một song ánh từ H lên Hx (vì x là khả đối xứng). Vậy ta có:

$$\text{Card}(Hx) + \text{Card}(H) = 2\text{Card}(H) > \text{Card}(G).$$

Kết quả là $(Hx) \cap H \neq \emptyset$. Vậy tồn tại $y \in (Hx) \cap H$, rồi $z \in H$ sao cho $y = zx$. Thế thì ta có $x = yz^{-1} \in H$, mâu thuẫn.

So sánh với bài tập 2.2.2.

2.2.10 Các phép kiểm chứng là dễ dàng.

2.2.11 1) Ta có, với mọi x thuộc $[0; 1]$:

$$\left\{\begin{array}{r} x+\mathrm{i}x^2 \in G \\ (1-x)+\mathrm{i}(1-x)^2 \in G \end{array}\right| \Rightarrow (x+\mathrm{i}x^2 - (1-x) - \mathrm{i}(1-x)^2 \in G \Rightarrow (2x-1)(1+\mathrm{i}) \in G.$$

Vì $x \mapsto 2x - 1$ là một toàn ánh từ $[0; 1]$ lên $[-1;1]$, nên nói riêng ta có:

$$\forall t \in [0; 1], \quad t + \mathrm{i}t = t(1 + \mathrm{i}) \in G$$

2) Giả sử $x \in [0 ; 1]$; ta có $x + \mathrm{i}x^2 \in G$ và $x^2 + \mathrm{i}x^2 \in G$ (xem 1)), vậy $x - x^2 \in G$.

Vì $x \mapsto x - x^2$ là một toàn ánh từ $[0;1]$ lên $\left[0;\frac{1}{4}\right]$ nên, ta suy ra $\left[0;\frac{1}{4}\right] \subset G$.

Rõ ràng ràng: $\forall x \in \mathbb{R}$, $\exists n \in \mathbb{Z}$, $\exists u \in \left[0;\frac{1}{4}\right]$, $x = nu$ từ đó $\mathbb{R} \subset G$.

3) Giả sử $x \in [0;1]$; ta có $x + \mathrm{i}x^2 \in G$ và $x + \mathrm{i}x \in G$ (xem 1)), từ đó $\mathrm{i}(x - x^2) \in G$. Như ở 2), ta suy ra $\mathrm{i}\mathbb{R} \subset G$.

Cuối cùng, vì G là một nhóm con của $\mathbb{C}$, ta kết luận $\mathbb{C} = \mathbb{R} + \mathrm{i}\mathbb{R} \subset G$.

2.2.12 a) • $e' = f(e) \in f(H)$.

• Nếu $(x',y') \in (f(H))^2$ thì, tồn tại $(x,y) \in H^2$ sao cho $x' = f(x)$, $y' = f(y)$, từ đó: $x' \perp y' = f(x) \perp f(y) = f(x \top y) \in f(H)$, vì $x \top y \in H$.

• Nếu $x' \in f(H)$ thì tồn tại $x \in H$ sao cho $x' = f(x)$, từ đó:

$x'^{-1} = (f(x))^{-1} = f(x^{-1}) \in f(H)$, vì $x^{-1} \in H$.

b) • $f(e) = e' \in H'$, vậy $e \in f^{-1}(H')$.

• Nếu $(x, y) \in (f^{-1}(H'))^2$, thì $f(x), f(y) \in H'$, từ đó: $f(x \top y) = f(x) \perp f(y) \in H'$, vậy $x \top y \in f^{-1}(H')$.

• Nếu $x \in f^{-1}(H')$, thì $f(x) \in H'$, từ đó: $f(x^{-1}) = (f(x))^{-1} \in H'$, vậy $x^{-1} \in f^{-1}(H')$.

2.2.13 Suy ra từ 2.1, Mệnh đề 5.

2.2.14 1) Giả sử f là đơn ánh.

Bao hàm thức $\{e\} \subset \mathrm{Ker}(f)$ là tầm thường.

Giả sử $x \in \mathrm{Ker}(f)$; ta có $f(x) = e' = f(e)$, vậy $x = e$, và như thế $\mathrm{Ker}(f) \subset \{e\}$.

2) Ngược lại, giả sử $\mathrm{Ker}(f) = \{e\}$. Giả sử $(x_1, x_2) \in G^2$ sao cho $f(x_1) = f(x_2)$. Ta có:

$$f(x_1x_2^{-1}) = f(x_1)(f(x_2))^{-1} = f(x_1)(f(x_1))^{-1} = e',$$

vậy $x_1x_2^{-1} \in \mathrm{Ker}(f) = \{e\}$, từ đó $x_1x_2^{-1} = e$, rồi $x_1 = x_2$. Điều này chứng tỏ f là đơn ánh.

2.2.15 Suy luận phản chứng.

Giả sử $f^2 \neq \mathrm{Id}_G$, và ký hiệu $A = \{x \in G ; f(x) = x^{-1}\}$.

Tồn tại $x \in G$ sao cho $f^2(x) \neq x$.

Nếu $x \in A$, thì $f^2(x) = f(f(x)) = f(x^{-1}) = (f(x))^{-1} = (x^{-1})^{-1} = x$, mâu thuẫn, vậy $x \notin A$.

Ta chứng minh $xA \cap A = \emptyset$. Giả sử tồn tại $y \in xA \cap A$. Thế thì tồn tại $a \in A$ sao cho $y = xa$, và: $f(x) = f(x)f(a), f(y) = y^{-1}, f(a) = a^{-1}$, vậy $f(x) = y^{-1}a$, rồi thì $f^2(x) = f(y^{-1}a) = (f(y))^{-1}f(a) = ya^{-1} = (xa)a^{-1} = x$, mâu thuẫn.

Điều này chứng minh: $xA \cap A = \emptyset$.

Mặt khác, $a \mapsto xa$ là một song ánh từ A lên xA.

Ta suy ra: $\mathrm{Card}(G) \geq \mathrm{Card}(A) + \mathrm{Card}(xA) = 2\mathrm{Card}(A)$, mâu thuẫn.

Ta cũng có thể quy về bài tập 2.2.9, bằng cách chứng minh rằng bộ phận B của G xác định bởi $B = \{x \in G ; f^2(x) = x\}$ là một nhóm con chứa A của G.

2.2.16 Giả sử $f : H \times K \to HK$, $(h,k) \mapsto hk$, đó rõ ràng là một toàn ánh.

Giả sử $(h,k) \in H \times K$, ta sẽ chứng minh: $\mathrm{Card}(f^{-1}(\{hk\})) = \mathrm{Card}(H \cap K)$.

1) Giả sử $(h', k') \in H \times K$ sao cho $f(h, k) = f(h', k')$. Ta có $kk'^{-1} = h^{-1}h'$, vậy $h^{-1}h' \in H \cap K$, $h' \in h(H \cap K)$. Tồn tại $z \in H \cap K$ sao cho $h' = hz$; rồi thì $k' = h'^{-1}hk = z^{-1}k$.

2) Ngược lại, với mọi z thuộc $H \cap K$: $hz \in H$, $z^{-1}k \in K$, và $f(hz, z^{-1}k) = (hz)(z^{-1}k) = hk$.

Như vậy, $H \cap K \to f^{-1}(\{h,k\})$, $z \mapsto (hz, z^{-1}k)$ là một song ánh.

Ký hiệu $\alpha \in \mathrm{Card}(H \cap K)$, mỗi phần tử của HK có đúng α tạo ảnh qua f, từ đó:

$$\mathrm{Card}(H)\,\mathrm{Card}(K) = \mathrm{Card}(H \times K) = \mathrm{Card}(HK)\mathrm{Card}(H \cap K).$$

Nhận xét : H, K, $H \cap K$ đều là những nhóm con của G, nhưng HK có thể không phải là một nhóm con của G.

2.2.17 1) Giả sử $y \in G$. Vì f là toàn ánh, nên tồn tại $z \in G$ sao cho $y = z^3$.

Giả sử $x \in G$. Vì f là một đồng cấu, ta có: $(xzx^{-1})^3 = x^3z^3x^{-3}$, từ đó:

$$xyx^{-1} = xz^3x^{-1} = (xzx^{-1})^3 = x^3z^3x^{-3} = x^3yx^{-3}, \text{ vậy } yx^3 = x^3y.$$

2) $x(yx)^2 y = (xy)^3 = x^3y^3 = x(x^2y^2)y$, vậy $(yx)^2 = x^2y^2 = (x^2y)y = (yx^2)y = (yx)(xy)$, từ đó $yx = xy$.

2.2.18 Tương tự như trong lời giải của bài tập 2.2.17, 1).

2.2.19 Tồn tại $a \in G$ sao cho $G = < a >$.

Giả sử $x' \in G'$. Tồn tại $x \in G$ sao cho $x' = f(x)$, rồi tồn tại $n \in \mathbb{Z}$ sao cho $x = a^n$. Thế thì ta có: $x' = f(x) = f(a^n) = (f(a))^n$, điều này chứng tỏ : $G' = < f(a) >$.

Hơn nữa, nếu G hữu hạn, thì G hữu hạn vì f là toàn ánh.

2.2.20 Giả thiết tồn tại một đẳng cấu nhóm f: $(\mathbb{Q}, +) \to (\mathbb{Q}_+^*, \times)$.

Vì $2 \in \mathbb{Q}_+^*$, ký hiệu $\alpha = f^{-1}(2)$ và $\beta = \dfrac{\alpha}{2}$, ta có: $2 = f(\alpha) = f(\beta + \beta) = (f(\beta))^2$.

Nhưng ta biết rằng phương trình $x^2 = 2$ không có nghiệm trong $\mathbb{Q}$ (Xem Tập 1, bài tập 1.1.1), mâu thuẫn.

2.2.21 Giả thiết tồn tại một đẳng cấu nhóm $f: (\mathbb{R}^*, \times) \to (\mathbb{C}^*, \times)$.

Vì $i \in \mathbb{C}^*$, ký hiệu $\alpha = f^{-1}(i)$, ta có:

$$f(\alpha^2) = (f(\alpha))^2 = i^2 = -1 = f(-1)$$

(vì $(f(-1))^2 = f((-1)^2) = f(1) = 1$, $f(1) = 1$ và $f(-1) \neq f(1)$), vậy $\alpha^2 = -1$, mâu thuẫn ($\alpha \in \mathbb{R}$).

2.3.1 a) $x^2 = x$, $x^2 = (-x)^2 = -x$, từ đó $2x = 0$.

b) $x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$, từ đó $xy + yx = 0$, rồi thì $xy = xy + 2yx = (xy + yx) + yx = yx$.

c) 1) Nếu $(x + y)z = 0$, thì $yz = -xz = xz$, từ đó: $x(y + 1)z = xyz + xz = x^2z + xz = xz + xz = 0$ và $(x + 1)yz = xyz + yz = x^2z + xz = 0$.

2) Ngược lại, nếu $x(y + 1)z = (x + 1)yz = 0$, thì $xyz + xz = xyz + yz$, vậy $xz = yz$, $(x + y)z = xz + yz = 2xz = 0$.

2.3.2 a) Trước tiên chứng minh rằng C là một nhóm con của $(A, +)$.

Giả sử $(x, y) \in A^2$; ta có:

$$(x + y)^2 - (x + y) = (x^2 - x) + (y^2 - y) + (xy + yx),$$

từ đó $xy + yx \in C$.

b) Theo a) $x(xy + yx) = (xy + yx)x$, từ đó $x^2y = yx^2$.

Nhưng cũng có $(x^2 - x)y = y(x^2 - x)$ (vì $x^2 - x \in C$) do đó $xy = yx$.

2.3.3 a) Tồn tại $(n, p) \in (\mathbb{N}^*)^2$ sao cho $x^n = y^p = 0$. Theo công thức nhị thức Newton:

$$(x+y)^{n+p-1} = \sum_{k=0}^{n+p-1} C_{n+p-1}^k x^k y^{n+p-1-k}$$

$$= \left(\sum_{k=0}^{n-1} C_{n+p-1}^k x^k y^{n-1-k}\right) y^p - x^n \left(\sum_{k=n}^{n+p-1} C_{n+p-1}^k x^{k-n} y^{n+p-1-k}\right) = 0$$

và do vậy $(x + y)$ là lũy linh.

b) Nếu $x^n = 0$, thì $(xy)^n = x^n y^n = 0$.

c) Nếu $x^n = 0$, ký hiệu $y = \sum_{k=0}^{n-1} x^k$, ta có: $(1 - x)y = y(1 - x) = 1 - x^n = 1$.

◇ **Trả lời**: Nếu $x^n = 0$, thì $1 - x$ là khả nghịch, và $(1 - x)^{-1} = \sum_{k=0}^{n-1} x^k$.

2.3.4 ◇ **Trả lời**: Đặc số của $\mathbb{Z}$ (tương ứng : $\mathbb{Z}/n\mathbb{Z}$) là 0 (tương ứng : n).

2.3.5 Theo giả thiết, tồn tại $b \in A$ sao cho $ba = 1$.

Ta xét, với $n \in \mathbb{N}$, $c_n = b + a^n(1 - ab)$ (trong đó, theo quy ước, $a^0 = 1$).

Với mọi n thuộc $\mathbb{N}$, c_n là nghịch đảo trái của a vì:

$$c_n a = ba + a^{n+1} - a^{n+1}ba = 1 + a^{n+1} - a^{n+1} = 1.$$

Ta chứng minh rằng các c_n ($n \in \mathbb{N}$) từng đôi khác nhau. Giả sử $(n, p) \in \mathbb{N}^2$ sao cho, chẳng hạn $n > p$, và giả thiết $c_n = c_p$.

Ta có: $c_n = c_p \Leftrightarrow a^n(1 - ab) = a^p(1 - ab) \Rightarrow b^n a^n(1 - ab) = b^n a^p(1 - ab)$.

Vì $ba = 1$, một phép quy nạp đơn giản chứng tỏ rằng: $\forall k \in \mathbb{N}$, $b^k a^k = 1$.

Vậy ta được: $1 - ab = b^{n-p}(1 - ab) = b^{n-p} - b^{n-p-1}(ba)b = b^{n-p} - b^{n-p-1}b = 0$, từ đó $ab = 1$, mâu thuẫn.

2.3.6 a) Các phép kiểm chứng là dễ dàng (xem thêm bài tập 2.1.13).

b) • Ánh xạ $\psi: (\mathbb{Z}/2\mathbb{Z})^X \to \mathfrak{P}(X)$ xác định bởi: $\forall f \in (\mathbb{Z}/2\mathbb{Z})^X$, $\psi(f) = \{x \in X; f(x) = \hat{1}\}$ rõ ràng thỏa mãn: $\psi \circ \theta = \mathrm{Id}_{\mathfrak{P}(X)}$ và $\theta \circ \psi = \mathrm{Id}_{(\mathbb{Z}/2\mathbb{Z})^X}$ điều này chứng tỏ rằng θ là song ánh.

• Với mọi (A, B) thuộc $(\mathfrak{P}(X))^2$, $\theta(A \Delta B) = \theta_{A \Delta B} = \theta_A + \theta_B - 2\theta_A\theta_B = \theta_A + \theta_B = \theta(A) + \theta(B)$, (xem bài tập 1.3.1) và $\theta(A \cap B) = \theta_{A \cap B} = \theta_A\theta_B = \theta(A)\theta(B)$.

2.4.1

• $xy = x(x^{-1} + y^{-1})y = y + x = -1$, và tương tự $yx = -1$; như vậy $xy = yx = -1$.

• $1 = (x + y)^2 = x^2 + 2xy + y^2$, từ đây $x^2 + y^2 = 3$.

• $9 = (x^2 + y^2)^2 = x^4 + 2x^2y^2 + y^4$, từ đây $x^4 + y^4 = 7$.

2.4.2 Giả thiết rằng đặc số n của K là $\neq 0$. Nếu n không nguyên tố thì tồn tại $(a, b) \in (\mathbb{N}^*)^2$ sao cho $n = ab$, $a < n$, $b < n$, từ đó $a1_K \neq 0$, $b1_K \neq 0$ và $(a1_K)(b1_K) = n1_K = 0$, mâu thuẫn.

Chú ý: Suy luận trên chứng tỏ một cách tổng quát rằng đặc số của một vành nguyên thì bằng 0 hoặc bằng một số nguyên tố.

2.4.3 Ta ký hiệu $f: K \to K$ và $E = f(K)$.
$x \mapsto x^2$

Mỗi phần tử của $K - \{0\}$ có nhiều nhất hai tạo ảnh qua f, vì:

$$f(x) = f(y) \Leftrightarrow x^2 = y^2 \Leftrightarrow (x - y)(x + y) = 0 \Leftrightarrow (y = x \text{ hoặc } y = -x),$$

và 0 chỉ có một tạo ảnh là 0.

Vậy: $\mathrm{Card}(E) \geq \dfrac{\mathrm{Card}(K) - 1}{2} + 1$, tức là: $\mathrm{Card}(E) > \dfrac{1}{2}\mathrm{Card}(K)$.

Theo bài tập 2.2.2, ta kết luận $K = E + E$, tức là: $\forall x \in K$, $\exists (a, b) \in K^2$, $x = a^2 + b^2$

Người ta chứng minh (định lý Wedderburn) rằng mọi thể hữu hạn đều giao hoán.

2.4.4 Giả thiết tồn tại một thể K sao cho tồn tại một đẳng cấu nhóm $f: (K, +) \to (K - \{0\}, \times)$.

Trường hợp thứ 1: $1_K + 1_K = 0_K$.

Giả sử $x \in K$. Ta có lần lượt:

$$x + x = x(1_K + 1_K) = x0_K = 0_K,$$
$$(f(x))^2 = f(x + x) = f(0_K) = 1_K,$$
$$f(x) = 1_K \text{ hoặc } f(x) = -1_K = 1_K.$$

Như vậy $f(K) = \{1_K\}$, K hữu hạn. Nhưng thế thì K và $K - \{0\}$ không có cùng một bản số, mâu thuẫn.

Trường hợp thứ 2: $1_K + 1_K \neq 0_K$.

Ta ký hiệu $\alpha = f^{-1}(1_K)$, $\beta = f^{-1}(-1_K)$. Ta có: $\begin{cases} f(2\alpha) = f(\alpha + \alpha) = (f(\alpha))^2 = 1_K^2 = 1_K \\ f(2\beta) = f(\beta + \beta) = (f(\beta))^2 = (-1_K)^2 = 1_K \end{cases}$,

từ đó $2\alpha = 2\beta$, vì f là song ánh.

Vì $2.1_K \neq 0$ và $(2.1_K)(\alpha - \beta) = 0$, ta suy ra $\alpha - \beta = 0$, rồi $1_K = -1_K$, mâu thuẫn.

◇ **Trả lời**: Không.

C 2.1 1) a) • $\overline{e} \neq \emptyset$ vì $e \in \overline{e}$

• $(x, y) \in (\overline{e})^2 \Leftrightarrow \begin{cases} x\mathcal{R}e \\ y\mathcal{R}e \end{cases} \Leftrightarrow \begin{cases} x\mathcal{R}e \\ xy\mathcal{R}xe \end{cases} \Rightarrow xy\mathcal{R}e \Rightarrow xy \in \overline{e}$

• $x \in \overline{e} \Leftrightarrow x\mathcal{R}e \Rightarrow x^{-1}x\mathcal{R}x^{-1}e \Leftrightarrow e\mathcal{R}x^{-1} \Leftrightarrow x^{-1} \in \overline{e}$

b) • $x\mathcal{R}x' \Rightarrow x^{-1}x\mathcal{R}x^{-1}x' \Leftrightarrow x^{-1}x' \in \overline{e}$

• $x^{-1}x' \in \overline{e} \Leftrightarrow x^{-1}x'\mathcal{R}e \Rightarrow x(x^{-1}x')\mathcal{R}xe \Leftrightarrow x'\mathcal{R}x$

• $x\mathcal{R}x' \Leftrightarrow x^{-1}x' \in \overline{e} \Leftrightarrow x' \in x\overline{e}$.

2) a) 1) • Giả sử $x \in g$; vì $x^{-1}x = e \in H$, ta có: xR_Hx, từ đó được tính phản xạ.

• Giả sử $(x, x') \in G^2$. Ta có:

$x\mathcal{R}_Hx' \Leftrightarrow x^{-1}x' \in H \Rightarrow x'^{-1}x = (x^{-1}x')^{-1} \in H \Leftrightarrow x'\mathcal{R}_Hx$, từ đó được tính đối xứng.

• $\begin{cases} x\mathcal{R}_H x' \\ x'\mathcal{R}_H x'' \end{cases} \Leftrightarrow \begin{cases} x^{-1}x' \in H \\ x'^{-1}x'' \in H \end{cases} \Rightarrow x^{-1}x'' = (x^{-1}x')(x'^{-1}x'') \in H \Leftrightarrow x\mathcal{R}_Hx''$, từ đó được tính bắc cầu.

Vậy ta đã chứng minh R_H là một quan hệ tương trong G.

2) Giả sử $(x, x', y) \in G^3$. Vì $(yx)^{-1}(yx') = x^{-1}x'$, nên ta có: $x\mathcal{R}_Hx' \Rightarrow yx\mathcal{R}yx'$.

Như vậy R_H tương thích trái với luật của G.

3) $x \in H \Leftrightarrow e^{-1}x \in H \Leftrightarrow eR_Hx \Leftrightarrow x \in \overline{e}$, từ đó $H = \overline{e}$.

b) Vì $\overline{x} = xH = x\overline{e}$, rõ ràng rằng: $\forall y \in H$, $xy \in \overline{x}$. ta ký hiệu $\varphi : \overline{e} \to \overline{x}$, $y \mapsto xy$.

• Giả sử $z \in \overline{x}$. Ký hiệu $y = x^{-1}z$, ta có: $y \in \overline{e}$ và $\varphi(y) = z$. Điều này chứng minh tính toàn ánh của φ.

• Nếu $(y_1, y_2) \in (\overline{e})^2$ sao cho $\varphi(y_1) = \varphi(y_2)$, thì $y_1 = x^{-1}(xy_1) = x^{-1}(xy_2) = y_2$, điều này chứng minh tính đơn ánh của φ.

Tổng quát hơn, với mọi (x, x') thuộc G^2, ánh xạ $y \mapsto x'x^{-1}y$ là một song ánh từ $\overline{x}$ lên $\overline{x'}$.

3) • Vì R_H là một quan hệ tương đương trong G, nên G/R_H là một phân hoạch của G, vậy:

$$\mathrm{Card}(G) = \sum_{\xi \in G/\mathcal{R}_H} \mathrm{Card}(\xi)$$

Hơn nữa, tất cả các lớp modulo R_H có cùng một bản số, theo 2) b): vậy:

$$\forall \xi \in G/R_H, \quad \mathrm{Card}(\xi) = \mathrm{Card}(\overline{e}) = \mathrm{Card}(H).$$

Như thế ta được: $\mathrm{Card}(G) = \mathrm{Card}(G/\mathcal{R}_H)\,\mathrm{Card}(H)$ (đẳng thức này thường được gọi là **phương trình lớp**). Đặc biệt: $\mathrm{Card}(H) \mid \mathrm{Card}(G)$.

4) a) 10 không chia hết 24.

◇ **Trả lời**: Không.

b) Vì $H \cap K$ là một nhóm con của H và của K, nên theo định lý Lagrange, $\mathrm{Card}(H \cap K)$ chia hết $\mathrm{Card}(H)$ và chia hết $\mathrm{Card}(K)$. Vì $\mathrm{UCLN}(\mathrm{Card}(H), \mathrm{Card}(K)) = 1$, nên suy ra $\mathrm{Card}(H \cap K) = 1$, vậy $H \cap K = \{e\}$.

C 2.2 **I** 1) • Theo C 2.1 1) *a*), $\overline{e}$ là một nhóm con của G.

• $y \in \overline{e} \Leftrightarrow y\mathcal{R}e \Rightarrow xyx^{-1}\mathcal{R}xex^{-1} = e \Leftrightarrow xyx^{-1} \in \overline{e}$.

2) • Theo C 2.1 2) *a*), $\mathcal{R}_H$ là một quan hệ tương đương trong G, tương thích trái với luật của G, và $H = \overline{e}$.

• Giả sử $(x, x', y) \in G^3$. Ta có:

$x\mathcal{R}_H x' \Leftrightarrow x^{-1}x' \in H \Rightarrow y^{-1}(x^{-1}x')y \in H \Leftrightarrow (xy)^{-1}(x'y) \in H \Leftrightarrow x'y\mathcal{R}_H xy$, điều này chứng minh rằng $\mathcal{R}_H$ tương thích phải với luật của G.

Nhận xét : Một nhóm con H của G là chuẩn tắc trong G khi và chỉ khi: $\forall x \in G, xH = Hx$.

3) a) Hiển nhiên

b) ◇ **Trả lời**: $G = \mathfrak{S}_3$, $H = \{e, \tau_{1,2}\}$ (xem 3.4.2, Ví dụ) ; $\tau_{13} \circ \tau_{12} \circ \tau_{13}^{-1} = \tau_{23} \notin H$.

4) a) • Theo bài tập 2.2.12 b), $f^{-1}(H')$ là một nhóm - con của G.

• Giả sử $x \in f^{-1}(H')$, $y \in G$.

Ta có: $f(yxy^{-1}) = f(y)\,f(x)\,(f(y))^{-1} \in H'$, *vì* $f(x) \in H'$ và $H' \lhd G'$.

Như vậy $yxy^{-1} \in f^{-1}(H')$, và cuối cùng $f^{-1}(H') \lhd G$. Đặc biệt: $\mathrm{Ker}(f) \lhd G$.

b) ◇ **Trả lời**: $G = \mathfrak{S}_2$, $G' = \mathfrak{S}_3$, $H = \mathfrak{S}_2$, $f : \mathfrak{S}_2 \to \mathfrak{S}_3$ xác định bởi $f(\mathrm{Id}) = \mathrm{Id}$ và $f(\tau_{12}) = \tau_{12}$ (xem 3.4.2, Ví dụ và 3) b) trên đây).

c) • Theo bài tập 2.2.12 *a*), $f(H)$ là một nhóm - con của G'.

• Giả sử $x' \in f(H)$, $y' \in G'$. Tồn tại $x \in H$ sao cho $x' = f(x)$ và vì f là toàn ánh, nên tồn tại $y \in G$ sao cho $y' = f(y)$. Ta có: $y'x'y'^{-1} = f(y)\,f(x)\,(f(y))^{-1} = f(xyy^{-1}) \in f(H)$ vì $x \in H$ và $H \lhd G$.

Cuối cùng: $f(H) \lhd G'$.

5) a) • $e \in C(G)$: hiển nhiên.

• Giả sử $(a, b) \in (C(G))^2$. Ta có: $\forall x \in G$, $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$, từ đó: $ab \in C(G)$.

• Giả sử $a \in C(G)$. Ta có: $\forall x \in G$, $a^{-1}x = a^{-1}(xa)a^{-1} = a^{-1}(ax)a^{-1} = xa^{-1}$, từ đó: $a^{-1} \in C(G)$.

• Giả sử $a \in C(G)$, $y \in G$. Ta có: $yay^{-1} = yy^{-1}a = a \in C(G)$.

b) Giả sử H là một nhóm con của G sao cho $\text{Card}(H) = n$.

1) Giả sử $x \in G$.

• Nếu $x \in H$, thì $xH = H = Hx$.

• Nếu $x \notin H$, thì $(xH) \cap H = \varnothing$ và $(Hx) \cap H = \varnothing$, từ đó, vì $\text{Card}(xH) = \text{Card}(Hx) = \text{Card}(H) = n$, $xH = Hx$.

Như vậy ta đã chứng minh: $\forall x \in G,\ xH = Hx$.

2) Giả sử $(h, x) \in H \times G$. Vì $xh \in xH = Hx$, nên tồn tại $k \in h$ sao cho $xh = kx$, từ đó: $xhx^{-1} = (kx)x^{-1} = k \in H$.

Cuối cùng: $H \lhd G$.

II 1) $\begin{cases} x\mathcal{R}x' \\ y\mathcal{R}y' \end{cases} \Rightarrow \begin{cases} xy\mathcal{R}x'y \\ x'y\mathcal{R}x'y' \end{cases} \Rightarrow xy\mathcal{R}x'y'$.

2) Giả sử $(\xi, \zeta) \in (G/H)^2$.

Nếu $(x, y, x', y') \in G^4$ sao cho $\xi = \overline{x} = \overline{x'}$ và $\zeta = \overline{y} = \overline{y'}$, thì theo 1), $\overline{xy} = \overline{x'y'}$, vậy ta có thể định nghĩa $\xi\zeta$ bởi: $\xi\zeta = \overline{xy}$.

3) • $\forall x \in G$, $\begin{cases} \overline{xe} = \overline{x}\overline{e} = \overline{x} \\ \overline{e}\,\overline{x} = \overline{ex} = \overline{x} \end{cases}$, vậy $\overline{e}$ là phần tử trung hòa trong G/H.

• $\forall (x, y, z) \in G^3$, $(\overline{x}\,\overline{y})\overline{z} = \overline{xy}\,\overline{z} = \overline{(xy)z} = \overline{x(yz)} = \overline{x}\,\overline{yz} = \overline{x}(\overline{y}\,\overline{z})$, vậy $\cdot$ có tính kết hợp trong G/H

• $\forall x \in G$, $\begin{cases} \overline{x}\,\overline{x^{-1}} = \overline{xx^{-1}} = \overline{e} \\ x^{-1}\overline{x} = x^{-1}x = \overline{e} \end{cases}$, vậy mọi phần tử của G/H có một đối xứng đối với $\cdot$.

Cuối cùng, G/H là một nhóm.

4) a) • Ta có, với mọi (x, y) thuộc G^2:

$$x\mathcal{R}_H y \Leftrightarrow x^{-1}y \in H \Rightarrow f(x^{-1}y) \in H' \Leftrightarrow (f(x))^{-1} f(y) \in H' \Leftrightarrow f(x)\mathcal{R}_{H'} f(y),$$

điều này chứng minh rằng f tương thích với $\mathcal{R}_H$ và $\mathcal{R}_{H'}$.

• Với mọi (x, y) thuộc G^2:

$$\begin{aligned} \tilde{f}(\overline{x}\,\overline{y}) = \tilde{f}(\overline{xy}) &= (\tilde{f} \circ p)(xy) = (p' \circ f)(x)(p' \circ f)(y) \\ &= (\tilde{f} \circ p)(x)(\tilde{f} \circ p)(y) = \tilde{f}(\overline{x})\tilde{f}(\overline{y}), \end{aligned}$$

vậy $\tilde{f}$ là một đồng cấu nhóm.

b) Ta đã thấy (I, 4) *a*)): $\text{Ker}(f) \lhd G$. Quan hệ $\mathcal{R}$ xác định trong G bởi:

$$x\mathcal{R}y \Leftrightarrow x^{-1}y \in \text{Ker}(f),$$

là một quan hệ tương đương, tương thích với luật của G.

Theo C 1.1 *B 1) b*), tồn tại một ánh xạ duy nhất $\hat{f} : G/R \to \text{Im}(f)$ sao cho $f = i \circ \hat{f} \circ p$ và $\hat{f}$ là song ánh.

Cuối cùng, $\hat{f}$ là một đồng cấu nhóm vì, với mọi (x, y) thuộc G^2:

$$\begin{aligned} \hat{f}(p(x)p(y)) = \hat{f}(p(xy)) &= (i \circ \hat{f} \circ p)(xy) = f(xy) = f(x)f(y) \\ &= (i \circ \hat{f} \circ p)(x)(i \circ \hat{f} \circ p)(y) = \hat{f}(p(x))\,\hat{f}(p(y)). \end{aligned}$$

Trong ví dụ, $\text{Ker}(f) = n\mathbb{Z}$, $\text{Im}(f) = \mathbb{Z}/_{n\mathbb{Z}}$, $\begin{array}{ccc} \mathbf{Z} & \xrightarrow{f} & \mathbf{Z}/_{n\mathbf{Z}} \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ \mathbf{Z}/_{n\mathbf{Z}} & \xrightarrow[\hat{f}]{} & \mathbf{Z}/_{n\mathbf{Z}} \end{array}$ f là toàn ánh, và $\hat{f} = \mathbf{Id}_{\mathbf{Z}/_{n\mathbf{Z}}}$.

C 2.3 I 1) a) Vì $(\mathbb{Z}/_{2\mathbb{Z}}, +, .)$ là một vành, nên $((\mathbb{Z}/_{2\mathbb{Z}})^E, +, .)$ cũng là một vành (xem bài tập 2.3.6, hoặc 2.1.13). Giả sử $\varphi \in (\mathbb{Z}/_{2\mathbb{Z}})^E$, $x \in E$; ta có: $\varphi^2(x) = (\varphi(x))^2 = \varphi(x)$, vì $\varphi(x) \in \{\hat{0}, \hat{1}\}$. Như thế: $\forall \varphi \in (\mathbb{Z}/_{2\mathbb{Z}})^E$, $\varphi^2 = \varphi$, vậy $((\mathbb{Z}/_{2\mathbb{Z}})^E, +, \cdot)$ là một vành Boole.

b) Ta biết rằng $(\mathfrak{P}(E), \Delta, \cap)$ là một vành đẳng cấu với $((\mathbb{Z}/_{2\mathbb{Z}})^E, +, \cdot)$ (xem bài tập 2.3.6, khái niệm về hàm đặc trưng). Hơn nữa: $\forall A \in \mathfrak{P}(E)$, $A \cap A = A$, vậy $(\mathfrak{P}(E), \Delta, \cap)$ là một vành Boole.

Tổng quát hơn ta có thể chú ý rằng, nếu A là một vành Boole và $\theta: A \to B$ là một đẳng cấu vành, thì B là vành Boole vì:

$$\forall b \in B,\ b^2 = (\theta(\theta^{-1}(b)))^2 = \theta((\theta^{-1}(b))^2) = \theta(\theta^{-1}(b)) = b.$$

2) a) $x + x = (x + x)^2 = x^2 + x^2 + x^2 + x^2 = x + x + x + x$, từ đó $x + x = 0$.

Nói khác đi: $\forall x \in A$, $x = -x$.

b) $x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$, từ đó $xy + yx = 0$, rồi thì, vì $yx + yx = 0$ (xem a)), $xy - yx = (xy + yx) - (yx + yx) = 0$, và cuối cùng: $xy = yx$.

c) $xy(x + y) = xyx + xy^2 = x^2y + xy^2 = xy + xy = 0$.

d) Giả thiết $A \neq \{0\}$.

Giả sử $x \in A$. Theo c) (áp dụng cho $y = 1$), $x(x + 1) = 0$. Vì A là vành nguyên, ta suy ra $x = 0$ hoặc $x = -1 = 1$. Như thế, $A \subset \{0, 1\}$. Cuối cùng: $A = \{0\}$ hoặc $A = \{0, 1\}$.

II 1) *Tính phản xạ:* Với mọi x thuộc A, $x \leq x$, vì $x^2 = x$.

Tính phản đối xứng: $\begin{cases} x \leq y \\ y \leq x \end{cases} \Leftrightarrow \begin{cases} xy = x \\ yx = y \end{cases} \Rightarrow x = y$

Tính bắc cầu: $\begin{cases} x \leq y \\ y \leq z \end{cases} \Leftrightarrow \begin{cases} xy = x \\ yz = y \end{cases} \Rightarrow xz = (xy)z = x(yz) = xy = x \Rightarrow x \leq z$

2) a) 1) • $(xy)x = x^2y = xy$, vậy $xy \leq x$; tương tự, $xy \leq y$.

• Cho $z \in A$ sao cho $\begin{cases} z \leq x \\ z \leq y \end{cases}$. Thế thì $\begin{cases} zx = z \\ zy = z \end{cases}$, từ đây $z(xy) = (zx)y = zy = z$, vậy $z \leq xy$. Điều này chứng tỏ xy là phần tử lớn nhất trong các chặn (cận) dưới (trong A) của tập hợp tạo thành bởi x và y, vậy $\mathrm{Inf}(x, y)$ tồn tại và bằng xy.

2) • $(x + y + xy)x = x^2 + yx + xyx = x + xy + xy = x$, vậy $x \leq x + y + xy$; tương tự $y \leq x + y + xy$.

• Cho $z \in A$ sao cho $\begin{cases} x \leq z \\ y \leq z \end{cases}$. Thế thì $\begin{cases} zx = z \\ zy = z \end{cases}$, từ đó $(x + y + xy)z = xz + yz + xyz = x + y + xy$, vậy $x + y + xy \leq z$.

Điều này chứng tỏ $x + y + xy$ là phần tử bé nhất trong các chặn (cận) trên (trong A) của tập hợp tạo thành bởi x và y, vậy $\mathrm{Sup}(x, y)$ tồn tại và bằng $x + y + xy$.

b) • $\wedge$ có tính giao hoán: $x \wedge y = xy = yx = y \wedge x$.

• $\vee$ có tính giao hoán: $x \vee y = x + y + xy = y + x + yx = y \vee x$.

• $\wedge$ có tính kết hợp : $(x \wedge y) \wedge z = (xy)z = x(yz) = x \wedge (y \wedge z)$.

• $\vee$ có tính kết hợp : $(x \vee y) \vee z = (x + y + xy) + z + (x + y + xy)z = x + y + z + xy + xz + yz + xyz = x + (y + z + yz) + x(y + z + yz) = x \vee (y \vee z)$.

• $\wedge$ có tính phân phối đối với $\vee$:

$$\begin{cases} x \wedge (y \vee z) = x(y + z + yz) = xy + xz + xyz \\ (x \wedge y) \vee (x \wedge z) = xy + xz + (xy)(xz) = xy + xz + xyz. \end{cases}$$

• $\vee$ có tính phân phối đối với $\wedge$:

$$\begin{cases} x \vee (y \wedge z) = x + yz + xyz \\ (x \vee y) \wedge (x \vee z) = (x + y + xy)(x + z + xz) \\ \qquad\qquad = x + (xy + xy) + (xz + xz) + yz + (xyz + xyz) + xyz \\ \qquad\qquad = x + yz + xyz. \end{cases}$$

Nhận xét : Nhờ $x \mapsto x^* = 1 + x$ (Xem dưới đây, 3)), ta có thể suy ra tính phân phối của luật kia

3) a) $\forall x \in A$, $0 \le x$ (vì $0x = 0$)

b) Cho $x \in A$.

• Nếu tồn tại $y \in A$ sao cho $\begin{cases} x \wedge y = 0 \\ x \vee y = 0 \end{cases}$, thì $\begin{cases} xy = 0 \\ x + y + xy = 1 \end{cases}$, suy ra $y = 1 - x = 1 + x$ và tính duy nhất của y.

• Ngược lại ta có:

$$\begin{cases} x \wedge (1 + x) = x(1 + x) = x + x^2 = x + x = 0 \\ x \vee (1 + x) = x + (1 + x) + x(1 + x) = x + (1 + x) = 1. \end{cases}$$

Như thế với mọi x thuộc A, tồn tại một và chỉ một phần tử x^* thuộc A sao cho $\begin{cases} x \wedge x^* = 0 \\ x \vee x^* = 1 \end{cases}$ và ta có : $x^* = 1 - x$.

c) 1) $0^* = 1 + 0 = 1$, $\quad 1^* = 1 + 1 = 0$.

2) $x^{**} = 1 + (1 + x) = (1 + 1) + x = x$.

3) • $(x \vee y)^* = 1 + (x + y + xy) = (1 + x)(1 + y) = x^* \wedge y^*$.

• $(x \wedge y)^* = (x^{**} \wedge y^{**})^* = ((x^* \vee y^*)^*)^* = x^* \vee y^*$.

4) $x \le y \Leftrightarrow xy = x \Leftrightarrow 1 + x + y + xy = 1 + x + y + x \Leftrightarrow (1 + x)(1 + y) = 1 + y$
$\Leftrightarrow y^* \le x^*$.

5) $x \le y \Leftrightarrow xy = x \Leftrightarrow xy + x = 0 \Leftrightarrow x(1 + y) = 0 \Leftrightarrow x \wedge y^* = 0 \Leftrightarrow (x \wedge y^*)^* = 1$
$\Leftrightarrow x^* \vee y = 1$.

4) a) Giả sử $(x, m) \in A \times M$. ta có: $mx = x \Leftrightarrow x \le m \Leftrightarrow \mathrm{Sup}(x, m) = m$.

Mặt khác, vì m là cực đại trong $A - \{1\}$ và $m \le \mathrm{Sup}(x, m)$, ta có: $\mathrm{Sup}(x, m) \in \{m, 1\}$. Vậy:

$$(\text{không } (x \le m)) \Leftrightarrow mx \ne m \Leftrightarrow \mathrm{Sup}(x, m) \ne m \Leftrightarrow x \vee m = 1 \Leftrightarrow x^* \le m$$
$$\Leftrightarrow x^* \wedge m^* = 0 \Leftrightarrow (1 + x)(1 + m) = 0.$$

b) Giả sử $(x, y, m) \in A \times A \times M$. Sử dụng a):

$$\left(\text{Không} \begin{vmatrix} x \le m \\ \text{hoặc} \\ y \le m \end{vmatrix}\right) \Leftrightarrow \begin{cases} x^* \le m \\ y^* \le m \end{cases} \Leftrightarrow x^* \vee y^* \le m \Leftrightarrow (x \wedge y)^* \le m \Leftrightarrow \text{không } (x \wedge y \le m).$$

c) 1) • Ta có: $(\forall m \in M, 0 \le m)$, vậy $\phi(0) = \varnothing$.

• Ngược lại, cho $x \in A$ sao cho $\phi(x) = \varnothing$. Giả thiết $x \ne 0$, tức là $1 + x \ne 1$. Vì A hữu hạn, tồn tại $m_0 \in M$ sao cho $1 + x \le m_0$ (chứng minh rằng, trong mọi tập được sắp thứ tự hữu hạn $(E, \le)$, với mọi a thuộc E, tồn tại ít nhất một phần tử cực đại m của E sao cho $a \le m$).

Thế thì ta có $x \le m_0$ (vì $m_0 \notin \phi(x)$) và $x^* = 1 + x \le m_0$, từ đó: $1 = x \vee x^* \le m_0$, mâu thuẫn.

Điều này chứng tỏ: $x = 0$.

2) Cho $x \in A$. Ta có, với mọi m thuộc M: $m \in \phi(x^*) \Leftrightarrow (x^*)^* \leq m \Leftrightarrow x \leq m$ $\Leftrightarrow m \notin \phi(x)$, điều này chứng tỏ: $\phi(x^*) = \complement_M(\phi(x))$.

3) Giả sử $(x, y) \in A^2$.

• Ta có, với mọi m thuộc M:

$$m \in \phi(x \wedge y) \Leftrightarrow (x \wedge y)^* \leq m \Leftrightarrow x^* \vee y^* \leq m \Leftrightarrow \begin{cases} x^* \leq m \\ y^* \leq m \end{cases} \Leftrightarrow \begin{cases} m \in \phi(x) \\ m \in \phi(y) \end{cases},$$

từ đó: $\phi(x \wedge y) = \phi(x) \cap \phi(y)$.

4) $\phi(x \vee y) = \phi((x^* \wedge y^*)^*) = \complement_M(\phi(x^*) \cap \phi(y^*)) = \complement_M(\complement_M(\phi(x)) \cap (\complement_M(\phi(y))))$

$= \phi(x) \cup \phi(y)$.

d) 1) **ϕ là một đồng cấu vành**

Giả sử $(x, y) \in A^2$. Ta có, sử dụng b):

• $\phi(xy) = \phi(x \wedge y) = \phi(x) \cap \phi(y)$.

• $\phi(x + y) = \phi(x(1 + y) + y(1 + x) + x(1 + y)y(1 + x)) = \phi((xy^*) \vee (x^*y))$

$= \phi(xy^*) \cup \phi(x^*y) = (\phi(x) \cap \complement_M(\phi(y))) \cup ((\complement_M(\phi(x))) \cap \phi(y)) = \phi(x)_\Delta\phi(y)$.

• $\phi(I) = \{m \in M; 0 \leq m\} = M$, là phần tử trung hòa đối với $\cap$ trong $\mathfrak{P}(M)$.

2) **ϕ là đơn ánh**

Cho $(x, y) \in A^2$ sao cho $\phi(x) = \phi(y)$. Ta có, sử dụng b):

$$\phi(x \wedge y^*) = \phi(x) \cap \complement_M(\phi(y)) = \varnothing.$$

vậy $x \wedge y^* = 0$, và tương tự, $x^* \wedge y = 0$.

Thế thì (xem 3) c)) : $\begin{cases} x \leq y \\ y \leq x \end{cases}$, vậy $x = y$.

3) **ϕ là toàn ánh**

Giả sử $F \in \mathfrak{P}(M)$.

Nếu $F = \varnothing$ thì $F = \phi(0)$.

Vậy giả thiết $F \neq \varnothing$, và ký hiệu $N = \text{Card}(F)$, $F = \{m_1, \ldots, m_N\}$, $p = m_1 \wedge \ldots \wedge m_N$. Ta chứng minh: $F = \phi(p^*)$.

Theo a) và b) ta có, với mọi m thuộc M:

$$m \in \phi(p^*) \Leftrightarrow p \leq m \Leftrightarrow m_1 \wedge \ldots \wedge m_N \leq m$$

$$\Leftrightarrow \left| \begin{array}{l} m_1 \leq m \\ \text{hoặc} \\ \vdots \\ \text{hoặc} \\ m_N \leq m \end{array} \right. \Leftrightarrow \left| \begin{array}{l} m_1 = m \\ \text{hoặc} \\ \vdots \\ \text{hoặc} \\ m_N = m \end{array} \right. ,$$

vì $m_1, \ldots, m_N$ đều là các cực đại trong $A - \{1\}$ và $m \in A - \{1\}$.

Như thế, $\phi(p^*) = \{m_1, \ldots, m_N\} = F$, từ đó ϕ là toàn ánh.

Cuối cùng, ϕ là một đẳng cấu vành.

Chỉ dẫn và trả lời
các bài tập chương 3

3.1.1 Kỹ hiệu $\alpha = a - 1 \in \mathbb{N}$, $\beta = b - 1 \in \mathbb{N}$, $\gamma = c - 1 \in \mathbb{N}$, ta có:

$$ab < c \Leftrightarrow \alpha\beta + \alpha + \beta < \gamma \Rightarrow \alpha + \beta < \gamma \Leftrightarrow \alpha + \beta + 2 \le \gamma + 1 \Leftrightarrow a + b \le c.$$

3.1.2 Nếu (x, y, z) là nghiệm, thì y lẻ: $y = 2Y + 1$, $Y \in \mathbb{N}$. Phương trình quy về:

$$5x + 15Y + 3z = 59. \qquad (2)$$

Nếu (x, Y, z) là nghiệm của (2), thì $3 \mid 2x - 2$, $3 \mid x - 1$, vậy $x = 3X + 1$, $X \in \mathbb{N}$. Rồi (2) quy về:

$$5X + 5Y + z = 18. \qquad (3)$$

Nếu (X, Y, z) là nghiệm của (3) thì $5 \mid z - 3$, vậy $z = 5Z + 3$, $Z \in \mathbb{N}$. Rồi (3) quy về: $X + Y + Z = 3$.

◇ **Trả lời**:

{(10, 1, 3), (7, 3, 3), (7, 1, 8), (4, 5, 3), (4, 3, 8), (4, 1, 13), (1, 7, 3), (1, 5, 8), (1, 3, 13), (1, 1, 18)}.

3.1.3 (i) Với $n = 0, 1, 2$ công thức được kiểm chứng dễ dàng. Với $n \ge 3$:

$1^{2n} + 2^{2n} + 3^{2n} > 3^{2n} \ge 2.\ 7^n$ vì $\left(\frac{9}{7}\right)^n \ge \left(\frac{9}{7}\right)^2 \ge 2$ (ta đi trước việc khảo sát các phân số).

(ii) Với $n = 0, 1, 2$, công thức được kiểm chứng dễ dàng. Với $n \ge 3$.

$1^{2n+1} + 2^{2n+1} + 3^{2n+1} > 3.9^n \ge 6^{n+1}$ vì $\left(\frac{3}{2}\right)^n \ge \left(\frac{3}{2}\right)^3 \ge 2$.

◇ **Trả lời**: Có đẳng thức trong (i) (tương ứng : (ii)) nếu và chỉ nếu $n \in \{1, 2\}$ (tương ứng : $n \in \{0, 1\}$).

3.1.4 a) Với $n = 2$ công thức được kiểm chứng dễ dàng. Ta giả thiết công thức đúng với một n thuộc $\mathbb{N} - \{0, 1\}$. Thế thì: $\sum_{k=1}^{n+1} \frac{1}{k^2} > \frac{3n}{2n+1} + \frac{1}{(n+1)^2}$, và ta có :

$$\frac{3n}{2n+1} + \frac{1}{(n+1)^2} \ge \frac{3(n+1)}{2(n+1)+1}$$

$$\Leftrightarrow (3n(n+1)^2 + (2n+1))(2n+3) \ge 3(n+1)^3(2n+1) \Leftrightarrow n^2 + 2n \ge 0.$$

Từ đó: $\sum_{k=1}^{n+1} \frac{1}{k^2} > \frac{3(n+1)}{2(n+1)+1}$.

b) Công thức là hiển nhiên với $n = 1$. Ta giả thiết công thức đúng với một n thuộc $\mathbb{N}$. Thế thì:

$$4^{n+1}((n+1)!)^3 = (4^n(n!)^3).\ 4(n+1)^3 < (n+1)^{3n}\ 4(n+1)^3 = 4(n+1)^{3n+3}.$$

Theo công thức nhị thức Newton:

$$\left(1+\frac{1}{n+1}\right)^{3n+3} \geq 1+C_{3n+3}^{1}\frac{1}{n+1}=4,$$

từ đó: $4(n+1)^{3n+3} \leq (n+2)^{3n+3}$, vậy: $4^{n+1}((n+1)!)^3 < (n+2)^{3(n+1)}$.

c) Công thức hiển nhiên với $n = 1$. Ta giả thiết công thức đúng với một n thuộc $\mathbb{N}^*$. Thế thì:

$$1!\,3!\ldots(2n+3)! = (1!\,3!\ldots(2n+1)!)((2n+3)!) \geq ((n+1)!)^{n+1}(2n+3)!.$$

Ta có:

$$((n+1)!)^{n+1}(2n+3)! \geq ((n+2)!)^{n+2} \Leftrightarrow (2n+3)! \geq (n+1)!\,(n+2)^{n+2}$$

$$\Leftrightarrow (n+2)(n+3)\ldots(2n+3) \geq (n+2)^{n+2},$$

và bất đẳng thức cuối cùng này đúng, vì $n+2, n+3, \ldots, 2n+3$ đều $\geq n+2$.

d) Với $n = 1$, công thức được kiểm chứng dễ dàng. Ta giả thiết công thức đúng với một n thuộc $\mathbb{N}$. Thế thì chỉ cần chứng minh:

$$\frac{4n+5}{4n+7}\sqrt{\frac{3}{4n+3}} > \sqrt{\frac{3}{4n+7}} \qquad (1)$$

và

$$\frac{4n+5}{4n+7}\sqrt{\frac{5}{4n+5}} < \sqrt{\frac{5}{4n+9}}. \qquad (2)$$

Cuối cùng thì :

$$(1) \Leftrightarrow (4n+5)^2 > (4n+7)(4n+3) \Leftrightarrow 25 > 21.$$

$$(2) \Leftrightarrow (4n+5)(4n+9) < (4n+7)^2 \Leftrightarrow 45 < 49.$$

3.1.5 Tính chất đúng với $n = 2$, theo định nghĩa của Δ. Ta giả thiết tính chất đúng với một n thuộc $\mathbb{N} - \{0, 1\}$, và giả sử $A_1, \ldots A_{n-1}$ là những bộ phận của E.

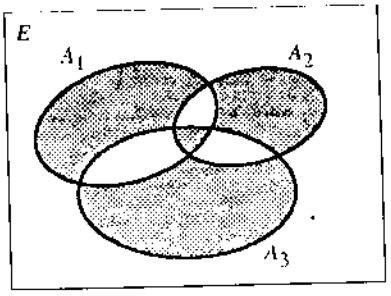
Vì Δ có tính kết hợp (bài tập 2.3.6), ta có:

$$\mathop{\Delta}_{i=1}^{n+1} A_i = \left(\mathop{\Delta}_{i=1}^{n} A_i\right)\Delta A_{n+1} = \left\{ x \in E : \begin{array}{l} x \in \mathop{\Delta}_{i=1}^{n} A_i \text{ và } x \notin A_{n+1} \\ \text{hoặc} \\ x \notin \mathop{\Delta}_{i=1}^{n} A_i \text{ và } x \in A_{n+1} \end{array} \right\}.$$

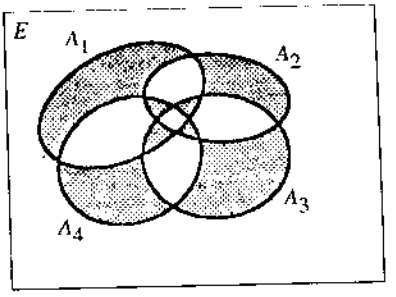
Như thế: $\mathop{\Delta}_{i=1}^{n+1} A_i$ là tập hợp các x thuộc E sao cho:

$$\left| \begin{array}{l} x \text{ thuộc một số lẻ các } A_i\ (1 \leq i \leq n) \text{ và } x \notin A_{n+1} \\ \text{hoặc} \\ x \text{ thuộc một số chẵn các } A_i\ (1 \leq i \leq n) \text{ và } x \in A_{n+1} \end{array} \right.$$

Vậy $\mathop{\Delta}_{i=1}^{n+1} A_i$ là tập hợp các x của E thuộc một số chẵn các A_i $(1 \leq i \leq n+1)$.



$n = 3$



$n = 4$

3.1.6 Giả sử $(x, y), (u, v) \in \mathbb{N} \times \mathbb{N}^*$ sao cho $f(x, y) = f(u, v)$.

Nếu $x + y < u + v$, thì:

$$f(u, v) = (u + v)^2 + v \geq (x + y + 1)^2 + v = (x + y)^2 + y + (2x + y + 1 + v) > f(x,y).$$

Vậy $x + y \geq u + v$, và tương tự $u + v \geq x + y$, vậy $u + v = x + y$.

Thế thì, vì $(x + y)^2 + y = (u + v)^2 + v$, ta suy ra $v = y$, $u = x$.

Xem thêm bài tập 3.2.6.

3.1.7 • Giả sử (f, g) thích hợp.

Với $x = y = 1$, ta được $f(1) = 1$.

Với $x = 2$, $y = 1$, ta được $(f(2))^{g(1)} = 2$, vậy $g(1) = 1$ (và $f(2) = 2$).

Với $x \in \mathbb{N}^*$ và $y = 1$, ta được: $f(x) = x$.

Với $x = y \geq 2$, ta được: $g(x) = 1$.

• Khẳng định đảo là tầm thường.

◇ **Trả lời:** $\left\{\begin{pmatrix} f: \mathbb{N}^* \to \mathbb{N}^*, & \mathbb{N}^* \to \mathbb{N}^* \\ x \mapsto x & x \mapsto 1 \end{pmatrix}\right\}$

3.1.8 Giả sử (f, g, h) thích hợp:

Với $x = y = z = 1$, ta được $f(1) = g(1) = h(1) = 1$.

Với $x \in \mathbb{N}^*$, $y = z = 1$, ta được $f(x) = x$. Sau đó tương tự, $g = h = \mathrm{Id}_{\mathbb{N}^*}$.

Nhưng thế thì, thay (x, y, z) bởi $(2, 2, 1)$, ta gặp một mâu thuẫn.

◇ **Trả lời**: $\mathcal{S} = \varnothing$.

3.1.9 Giả sử f thích hợp. Ta sẽ chứng minh bằng quy nạp mạnh theo n: $\forall n \in \mathbb{N}, f(n) = n$.

• Vì $f: \mathbb{N} \to \mathbb{N}$ tăng nghiêm ngặt và $f(2) = 2$, nên ta có: $f(0) = 0, f(1) = 1$.

• Giả sử $n \in \mathbb{N} - \{0, 1\}$; giả thiết: $\forall k \in \{0, \ldots, n\}, f(k) = k$.

1) Nếu $n + 1$ chẵn, tồn tại $p \in \mathbb{N}^*$ sao cho $n + 1 = 2p$, từ đó:

$$f(n + 1) = f(2p) = f(2)f(p) = 2p = n + 1,$$

vì $p \leq n$.

2) Giả thiết $n+1$ lẻ; tồn tại $q \in \mathbb{N}^*$ sao cho $n+2 = 2q$. Vì $n \geq 2$, ta có $q \leq n$, từ đó:

$$f(n+2) = f(2q) = f(2)\,f(q) = 2q = n+2.$$

Thế thì: $f(n) = n$, $f(n+2) = n+2$, từ đó $f(n+1) = n+1$ vì f tăng nghiêm ngặt.

3.1.10 $$\sum_{k=1}^{n} k(n+1-k) = (n+1)\sum_{k=1}^{n} k - \sum_{k=1}^{n} k^2 = (n+1)\frac{n(n+1)}{2} - \frac{n(n+1)(2n+1)}{6}$$

◇ **Trả lời:** $\dfrac{n(n+1)(n+2)}{6}$.

3.1.11 1) Với $p \in \mathbb{N}$ cố định, ta xác định phần chính của $S_p(n)$ khi n tiến ra vô tận. Ta có:

$$S_p(n) = n^{p-1}\frac{1}{n}\sum_{k=1}^{n}\left(\frac{k}{n}\right)^p \quad \text{và} \quad \frac{1}{n}\sum_{k=1}^{n}\left(\frac{k}{n}\right)^p \xrightarrow[n\infty]{} \int_0^1 x^p\,dx = \frac{1}{p+1}$$

Từ đó $S_p(n) \underset{n\infty}{\sim} \dfrac{n^{p+1}}{p+1}$.

2) Giả sử (p, q, r) thích hợp. Theo 1) ta có: $\dfrac{n^{p+1}}{p+1} \underset{n\infty}{\sim} \left(\dfrac{n^{q+1}}{q+1}\right)^r$, từ đó, do tính duy nhất của phần chính:

$$p+1 = (q+1)r \text{ và } p+1 = (q+1)^r.$$

Ta suy ra: $(q+1)^{r-1} = r$.

Chứng minh bằng quy nạp: $\forall r \geq 3, \quad 2^{r-1} > r$.

Vậy, nếu $r \geq 3$ thì:

$$(q+1)^{r-1} = r < 2^{r-1} \leq (q+1)^{r-1}, \text{ mâu thuẫn.}$$

Từ đó $r = 2$, rồi $q = 1$, $p = 3$.

◇ **Trả lời:** $\{(3, 1, 2)\}$.

3.2.1 *Phương pháp thứ 1:*

Quy nạp theo $n = \#(E)$.

Tính chất là tầm thường với $n = 0$, vì lúc đó: $E = \varnothing$ và $\mathfrak{P}(E) = \{\varnothing\}$.

Giả thiết tính chất đúng với một n thuộc $\mathbb{N}$, và giả sử E là một tập hợp hữu hạn có bản số $n+1$. Ta xét một phần tử ω cố định của E. Ta có: $\mathfrak{P}(E) = \mathcal{A} \cup \mathcal{B}$, trong đó $\mathcal{A} = \{X \in \mathfrak{P}(E);\ \omega \notin X\} = \mathfrak{P}(E - \{\omega\})$ và $\mathcal{B} = \{X \in \mathfrak{P}(E);\ \omega \in X\}$.

Rõ ràng rằng $\mathfrak{P}(E - \{\omega\}) \to \mathcal{B}$ là một song ánh, từ đó $\#(\mathcal{B}) = \#\,\mathfrak{P}(E - \{\omega\}) = 2^n$.
$Y \mapsto Y \cup \{\omega\}$

Vì $\mathcal{A} \cap \mathcal{B} = \varnothing$, ta được:

$$\#(\mathfrak{P}(E)) = \#(\mathcal{A}) + \#(\mathcal{B}) = 2^n + 2^n = 2^{n+1}.$$

Phương pháp thứ 2: Ánh xạ $A \mapsto \chi_A$ (trong đó χ_A là hàm đặc trưng của A, (xem 1.3.1, Ví dụ 5), là một song ánh từ $\mathfrak{P}(E)$ lên $\{0, 1\}^E$, vậy: $\#\,\mathfrak{P}(E) = \#(\{0, 1\}^E) = 2^{\#(E)}$.

3.2.2 Áp dụng 3.2.2, Mệnh đề 3 1), chú ý rằng $E \to \mathfrak{P}(E)$ là đơn ánh.
$x \mapsto \{x\}$

3.2.3 Giả sử $(u_n)_{n\in\mathbb{N}}$ là một dãy giảm lấy các hạng tử trong $\mathbb{N}$. Giả thiết $(u_n)_{n\in\mathbb{N}}$ không dừng; thế thì: $\forall n \in \mathbb{N}, \exists k \in \mathbb{N}, (k > n$ và $u_k < u_n)$.

Tồn tại một ánh xạ $\sigma: \mathbb{N} \to \mathbb{N}$ sao cho: $\begin{cases}\sigma(0) = 0\\ \forall n \in N, (\sigma(n+1) > \delta(n) \text{ và } u_{\sigma(n+1)} < u_{\sigma(n)}\}.\end{cases}$

Thế thì ta có: $u_0 \geq u_{\sigma(0)} \geq u_{\sigma(1)} + 1 \geq u_{\sigma(2)} + 2 \geq \ldots$, vậy: $\forall\, n \in \mathbb{N}, u_0 \geq u_{\sigma(n)} + n \geq n$, mâu thuẫn (chọn $n = u_0 + 1$).

3.2.4 a) Ánh xạ cảm sinh $A \to f(A)$ là toàn ánh và A là hữu hạn, vậy (xem 3.2.2, Mệnh đề 3 2)
$x \mapsto f(x)$

$f(A)$ hữu hạn và $\#(f(A)) \leq \#(A)$.

b) • $f^{-1}(B)$ có thể không hữu hạn, như trong ví dụ $f: \mathbf{N} \to \mathbf{N}$ thì $B = \{0\}, f^{-1}(B) = \mathbb{N}$.
$x \mapsto 0$

• Nếu f là đơn ánh thì ánh xạ cảm sinh $f^{-1}(B) \to B$ là đơn ánh, vậy (xem 3.2.2, Mệnh đề 3 *1*)),
$x \mapsto f(x)$

$f^{-1}(B)$ hữu hạn và $\#(f^{-1}(B)) \leq \#(B)$.

3.2.5 Bằng cách sử dụng $f^2 = \mathrm{Id}_E$, ta chứng minh rằng quan hệ R xác định trong E bởi:

$$xRy \Leftrightarrow (y = x \text{ hoặc } y = f(x))$$

là một quan hệ tương đương.

Ta ký hiệu $\mathcal{R}_A$ là quan hệ tương đương trên A cảm sinh bởi R: $\forall (x, y) \in A^2, (x\mathcal{R}_A y \Leftrightarrow xRy)$.

Vì $(\forall x \in A, x \neq f(x))$, nên mỗi lớp modulo $\mathcal{R}_A$ là hữu hạn và có đúng hai phần tử.

Kết quả là Card(A) chẵn.

3.2.6 1) **Đơn ánh:** Tương tự như lời giải của bài tập 3.1.6.

2) **Toàn ánh**

Giả sử $n \in \mathbb{N}$. Tồn tại $n \in \mathbb{N}$ sao cho:

$$\frac{n(n+1)}{2} \leq N \leq \frac{(n+1)(n+2)}{2}$$

Đặt $x = N - \dfrac{n(n+1)}{2}$, $y = n - x$.

Ta có: $x \in \mathbb{N}$ và :

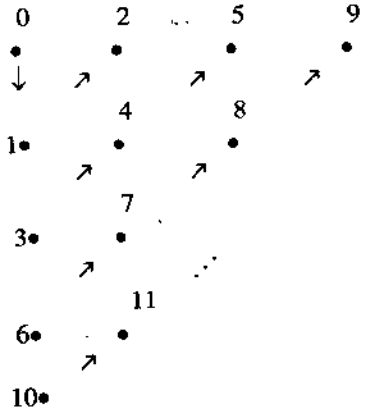
$$x < \frac{(n+1)(n+2)}{2} - \frac{n(n+1)}{2} = n+1$$

vậy $x \leq n$, từ đó $y \in \mathbb{N}$.

Theo cách xây dựng n, x, y:

$$f(x, y) = \frac{(x+y)(x+y+1)}{2} + x$$

$$= \frac{n(n+1)}{2} + x = N.$$



3.2.7 Quy nạp theo n.
Công thức là tầm thường với $n = 1$, và đã biết với $n = 2$ (xem 3.2.2, Mệnh đề 5).
Ta giả thiết công thức đúng với một n thuộc $\mathbb{N}^*$, và giả sử $E_1,\dots,E_{n+1}$ là những tập hợp hữu hạn.
Ta có:

$$\#\left(\bigcup_{i=1}^{n+1}E_i\right)=\#\left(\left(\bigcup_{i=1}^{n}E_i\right)\cup E_{n+1}\right)=\#\left(\bigcup_{i=1}^{n}E_i\right)+\#(E_{n+1})-\left(\#\left(\bigcup_{i=1}^{n}E_i\right)\cap E_{n+1}\right)$$

$$=\#\left(\bigcup_{i=1}^{n}E_i\right)+\#(E_{n+1})-\#\bigcup_{i=1}^{n}\left(E_i\cap E_{n+1}\right)$$

$$=\sum_{k=1}^{n}(-1)^{k-1}\sum_{I\in\mathfrak{P}_k(\{1,\dots,n\})}\#\left(\bigcap_{i\in I}E_i\right)+\#(E_{n+1})-\sum_{k=1}^{n}(-1)^{k-1}\sum_{I\in\mathfrak{P}_k(\{1,\dots,n\})}\#\left(\left(\bigcap_{i\in I}E_i\right)\cap E_{n+1}\right)$$

$$=\sum_{k=1}^{n+1}(-1)^{k-1}\sum_{\substack{I\in\mathfrak{P}_k(\{1,\dots,n+1\})\\ n+1\notin I}}\#\left(\bigcap_{i\in I}E_i\right)+\sum_{l=1}^{n+1}(-1)^{l-1}\sum_{J\in\mathfrak{P}_l(\{1,\dots,n+1\})}\#\left(\bigcap_{j\in J}E_j\right)$$

$$=\sum_{k=1}^{n+1}(-1)^{k-1}\sum_{I\in\mathfrak{P}_k(\{1,\dots,n+1\})}\#\left(\bigcap_{i\in I}E_i\right).$$

3.2.8 a) Vì $\{(x,y)\in E^2;\ x\mathcal{R}y\}=\bigcup_{i=1}^{N}E_i^2$ và các E_i^2 đều từng đôi rời nhau, ta có:

$$\nu=\sum_{i=1}^{N}\#(E_i^2)=\sum_{i=1}^{N}(\#(E_i))^2\ .$$

b) Áp dụng bất đẳng thức Cauchy – Schwarz (Tập 1, 1.2.2), ta có:

$$\left(\sum_{i=1}^{N}1.\#(E_i)\right)^2\le\left(\sum_{i=1}^{N}1^2\right)\left(\sum_{i=1}^{N}(\#(E_i))^2\right),$$

tức là: $n^2\le N\nu$.

3.2.9 Nếu tồn tại (p,q) sao cho $p\neq q$ và $a_p=a_q$, thì (p,q) hoặc (q,p) thích hợp.
Vậy giả thiết $\mathbb{N}\to\mathbb{N}$ là đơn ánh.
$n\mapsto a_n$
Tập hợp $\{b_n;\ n\in\mathbb{N}\}$ có một phần tử bé nhất; vậy tồn tại $p\in\mathbb{N}$ sao cho: $\forall n\in\mathbb{N},\quad b_p\le b_n$.
Vì $\mathbb{N}\to\mathbb{N}$ là đơn ánh, tồn tại $q\in\mathbb{N}$ sao cho: $q>p$ và $a_p\le a_q$.
$n\mapsto a_n$
Thế thì ta có: $p\neq q$, $a_p\le a_q$, $b_p\le b_q$, vậy (p,q) thích hợp.

3.2.10 Quan hệ $\mathcal{R}$ xác định trong $\{1,\dots,n\}$ bởi: $i\mathcal{R}j\Leftrightarrow x_i=x_j$ là một quan hệ tương đương. Ta ký hiệu $N=\#(\{1,\dots,n\}/\mathcal{R})$, và $X_1,\dots,X_N$ là các lớp modulo $\mathcal{R}$, vậy ta có:

$$\sum_{i=1}^{N}\#(X_i)=\#(\{1,\dots,n\})=n\ .$$

Nếu $\begin{cases}N\le p\\ \forall i\in\{1,\dots,N\},\#(X_i)\le p\end{cases}$, thì $n\le p^2$, mâu thuẫn.

Vậy: (1) $N\ge p$
hoặc
(2) $\exists i\in\{1,\dots,N\},\#(X_i)>p$.

Trong trường hợp (1) ít nhất $p+1$ số $x_1,...,x_n$ từng đôi khác nhau.

Trong trường hợp (2), ít nhất $p+1$ số $x_1,...,x_n$ đều bằng nhau.

3.2.11 1) Giả sử $(X, \leq)$ là một tập hợp được sắp thứ tự. Ta chứng minh rằng mọi bộ phận hữu hạn khác rỗng Y của X có ít nhất một phần tử cực đại.

Vì $Y \neq \emptyset$, Y có ít nhất một phần tử y_1. Nếu y_1 không phải cực đại (trong Y), tồn tại $y_2 \in Y$ sao cho $y_1 < y_2$. Nếu y_2 không phải cực đại, tồn tại $y_3 \in Y$ sao cho $y_2 < y_3$,...

Nếu Y không có một phần tử cực đại nào, ta xây dựng một dãy $(y_n)_{n\geq 1}$ tăng nghiêm ngặt. Thế thì Y sẽ là vô hạn, mâu thuẫn.

Nếu E hữu hạn, áp dụng kết quả trên vào $(\mathfrak{P}(E), \subset)$, ta kết luận: Mọi bộ phận khác rỗng của $\mathfrak{P}(E)$ có ít nhất một phần tử cực đại.

2) Ngược lại, giả thiết E vô hạn. Tập hợp $\mathfrak{J}(E)$ các bộ phận hữu hạn của E là một bộ phận khác rỗng của $\mathfrak{J}(E)$; ta chứng minh $\mathfrak{J}(E)$ không có một phần tử cực đại nào.

Cho $F \in \mathfrak{J}(E)$. Vì F hữu hạn, được bao hàm trong E vô hạn nên tồn tại $x \in E - F$. Thế thì $F \subset F \cup \{x\}$ và $F \cup \{x\} \in \mathfrak{J}(E)$. Điều này chứng tỏ rằng F không phải là cực đại trong $\mathfrak{J}(E)$.

3.3.1 $C_{C_n^2}^2 = \dfrac{C_n^2(C_n^2-1)}{2} = \dfrac{n(n-1)(n^2-n-2)}{8}$ và $3C_{n+1}^4 = \dfrac{(n+1)n(n-1)(n-2)}{8}$

3.3.2 $C_n^p - C_{n-1}^p = C_{n-1}^{p-1} = \dfrac{(n-1)!}{(p-1)!(n-p)!}$,

vậy $C_n^p = C_{n-1}^p + C_{n-1}^{p-1} \Leftrightarrow \begin{cases} 0 \leq x \leq p \\ \dfrac{(n-x)!}{(p-x)!} = \dfrac{(n-1)!}{(p-1)!} \end{cases}$

Nếu $x \geq 2$, thì $\forall k \in \{1,...,n-p\}$, $1 \leq p-x+k < p-1+k$,

từ đó $(n-x)(n-x-1)...(p-x+1) < (n-1)(n-2)...p$, vậy $\dfrac{(n-x)!}{(p-x)!} < \dfrac{(n-1)!}{(p-1)!}$

◇ **Trả lời :** $\{1\}$.

3.3.3 $(k+1)\dfrac{C_n^{k+1}}{C_n^k} = n-k$

◇ **Trả lời:** $\dfrac{n(n+1)}{2}$.

3.3.4 $P_n = \prod_{k=0}^{n} \dfrac{n!}{k!(n-k)!} = \dfrac{(n!)^{n+1}}{\left(\prod_{k=0}^{n} k!\right)^2}$, từ đó $\dfrac{P_n}{P_{n-1}} = \dfrac{n^{n+1}(n-1)!}{(n!)^2} = \dfrac{n^n}{n!}$.

3.3.5 $\sum_{k=0}^{q} \dfrac{p}{p+q-k} \cdot \dfrac{C_q^k}{C_{p+q}^k} = \sum_{k=0}^{q} \dfrac{p \cdot q!(p+q-k-1)!}{(q-k)!(p+q)!} = \dfrac{p \cdot q!}{(p+q)!} \sum_{k=0}^{q} \dfrac{(p+q-k-1)!}{(q-k)!}$

$= \dfrac{1}{C_{p+q}^p} \sum_{k=0}^{q} C_{p+q-k-1}^{p-1} = \dfrac{1}{C_{p+q}^p} \sum_{j=0}^{q} C_{p+j-1}^{p-1}$.

Chứng minh, bằng quy nạp theo q : $\sum_{j=0}^{q} C_{p-j-1}^{p-1} = C_{p+q}^p$.

3.3.6 Phương pháp tiến hành như với bài tập 3.3.5.

3.3.7 $(n!)!=\prod_{i=1}^{n!} i = \prod_{k=1}^{(n-1)!} u_{n,k}$, trong đó

$$u_{n,k} = \prod_{i=kn-n+1}^{kn} i = (kn-n+1)(kn-n+2)\dots(kn) = \frac{(kn)!}{(kn-n)!} = A_{kn}^{n} = n!\,C_{kn}^{n},$$

vậy $(n!)!=(n!)^{(n-1)!}\left(\prod_{k=1}^{(n-1)!} C_{kn}^{n}\right)$.

3.3.8 Quy nạp theo q (với p cố định).

Tính chất là tầm thường với $q = 1$.

Ta giả thiết tính chất đúng với một q thuộc $\mathbb{N}^*$. Ta có:

$$\sum_{k=0}^{q}(p-2k)C_p^k = \sum_{k=0}^{q-1}(p-2k)C_p^k + (p-2q)C_p^q = qC_p^q + (p-2q)C_p^q =$$

$$= (p-q)C_p^q = \frac{p!}{q!(p-q-1)!} = (q+1)C_p^{q+1}$$

3.3.9 Quy nạp theo n.

Tính chất là tầm thường với $q = 1$.

Nếu tính chất đúng với một n thuộc $\mathbb{N}^*$, thì:

$$\sum_{k=0}^{n+1} C_{p-k}^{q} = \sum_{k=0}^{n} C_{p-k}^{q} + C_{p-n-1}^{q} = C_{p+1}^{q+1} - C_{p-n}^{q+1} + C_{p-n-1}^{q} = C_{p+1}^{q+1} - C_{p-n-1}^{q+1}$$

3.3.10 $$\sum_{i=1}^{n}\prod_{j=1}^{p-1}(i+j) = \sum_{i=1}^{n}\frac{(i+p-1)!}{(i-1)!} = \sum_{i=0}^{n-1}\frac{(i+p)!}{i!} = p!\sum_{i=0}^{n-1} C_{p+i}^{p}$$

Ta chứng minh, bằng quy nạp theo n: $\forall n \in \mathbb{N}^*$, $\sum_{i=0}^{n} C_{p+i}^{p} = C_{p+n}^{p+1}$.

Tính chất là tầm thường với $n = 1$.

Nếu tính chất đúng với một n thuộc $\mathbb{N}^*$, thì: $\sum_{i=0}^{n} C_{p+i}^{p} = \left(\sum_{i=0}^{n-1} C_{p+i}^{p}\right) + C_{p+n}^{p} = C_{p+n}^{p+1} + C_{p+n}^{p} = C_{p+n+1}^{p+1}$

◇ **Trả lời**: $\dfrac{(p+n)!}{(p+1)\cdot(n-1)!}$.

3.3.11 Ký hiệu $A = \sum_{k=0}^{E(\frac{n}{2})} C_n^{2k}$ và $B = \sum_{k=0}^{E(\frac{n}{2})} C_n^{2k-1}$, công thức nhị thức Newton cho:

$$A + B = \sum_{k=0}^{n} C_n^k = 2^n \text{ và } A - B = \sum_{k=0}^{n}(-1)^k C_n^k = 0.$$

◇ **Trả lời** : $\sum_{k=0}^{E(\frac{n}{2})} C_n^{2k} = \sum_{k=0}^{E(\frac{n}{2})} C_n^{2k+1} = 2^{n-1}$.

3.3.12 Việc xét các hệ tử của X^{2p} trong $(1 + X)^n(1 + X)^n$ và $(1 + X)^{2n}$ cho ta: $\sum_{k=0}^{2p} C_n^k C_n^{2p-k} = C_{2n}^{2p}$.

Tiếp theo, ta chú ý rằng: $\sum_{k=0}^{2p} C_n^k C_n^{2p-k} = 2\sum_{k=0}^{p} C_n^{p-k} C_n^{p+k} - \left(C_n^p\right)^2$

◇ **Trả lời:** $\frac{1}{2}\left(C_{2n}^{2p} + \left(C_n^p\right)^2\right)$.

3.3.13 Áp dụng công thức nhị thức Newton, hệ tử của X^k trong $(X + 1)^q$ là C_q^k, và hệ tử của X^{n-k-1} trong $p(X + 1)^{p-1}$ (đạo hàm của $(X + 1)^p$) là $(n - k) C_p^{n-k}$. Như thế, $\sum_{k=0}^{n} (n-k) C_p^{n-k} C_q^k$ là hệ tử của X^{n-1} trong $p(X + 1)^{p+q-1}$, đó cũng là:

$$p\, C_{p+q-1}^{n-1} = p\frac{(p+q-1)!}{(n-1)!(p+q-n)!} = \frac{pn}{p+q}\cdot\frac{(p+q)!}{n!(p+q-n)!} = \frac{pn}{p+q} C_{p+q}^n.$$

3.3.14 a) Theo công thức nhị thức Newton: $(X-1)^n = \sum_{k=0}^{n} C_n^k (-1)^{n-k} X^k$.

Đạo hàm p lần, ta suy ra: $\frac{n!}{(n-p)!}(X-1)^{n-p} = \sum_{k=p}^{n} C_n^k (-1)^{n-k} \frac{k!}{(k-p)!} X^{k-p}$.

Thay X bởi 1, ta được, nếu $n > p$:

$$0 = \sum_{k=p}^{n} C_n^k (-1)^{n-k} \frac{k!}{(k-p)!} = p! \sum_{k=p}^{n} C_n^k (-1)^{n-k} C_k^p = p! \sum_{k=0}^{n} (-1)^{n-k} C_n^k C_k^p.$$

Mặt khác, nếu $n = p$: $\sum_{k=0}^{n} (-1)^{n-k} C_n^k C_k^p = \left(C_n^n\right)^2 = 1$.

b) $\sum_{k=0}^{n} (-1)^{n-k} C_n^k y_k = \sum_{k=0}^{n} (-1)^{n-k} C_n^k \sum_{p=0}^{k} C_k^p x_p = \sum_{k=0}^{n} (-1)^{n-k} C_n^k \sum_{p=0}^{n} C_k^p x_p = \sum_{p=0}^{n} \left(\sum_{k=0}^{n} (-1)^{n-k} C_n^k C_k^p \right) x_p$

$= x_n$.

3.3.15 a) Xem §3.3.3.

b) $2\sum_{k=0}^{E\left(\frac{n-1}{2}\right)} \left(\frac{n-2k}{n} C_n^k\right)^2 = \sum_{k=0}^{n} \left(\frac{n-2k}{n} C_n^k\right)^2 = \sum_{k=0}^{n} \left(C_n^k - 2\frac{k}{n} C_n^k\right)^2 = \sum_{k=0}^{n} \left(C_n^k - 2C_{n-1}^{k-1}\right)^2$

$= \sum_{k=0}^{n} \left(C_n^k\right)^2 - 4\sum_{k=0}^{n} C_n^k C_{n-1}^{k-1} + 4\sum_{k=0}^{n} \left(C_{n-1}^{k-1}\right)^2 = \sum_{k=0}^{n} C_n^k C_n^{k-1} - 4\sum_{k=0}^{n} C_n^k C_{n-1}^{k-1} + 4\sum_{k=0}^{n-1} C_{n-1}^{k-1} C_{n-1}^{n-k}$

$= C_{2n}^n - 4C_{2n-1}^n + 4C_{2n-2}^{n-1} =$

$= \frac{(2n-2)!}{(n!)^2}(2n(2n-1) - 4(2n-1)n + 4n^2) = \frac{(2n-2)!2n}{(n!)^2} = \frac{2}{n} C_{2n-2}^{n-1}$.

3.3.16 a) Bất đẳng thức mong muốn là tầm thường với $i = k$. Giả thiết $i < k$; ta có:

$$C_n^i = C_n^k \frac{k(k-1)\dots(i+1)}{(n-i)(n-i-1)\dots(n-k+1)} \le C_n^k \left(\frac{k}{n-k+1}\right)^{k-i}.$$

và $0 \le \frac{k}{n-k+1} \le \frac{1}{2}$ vì $3k \le n+1$.

b) $\sum_{i=0}^{k} C_n^i \le \left(\sum_{i=0}^{k} \frac{2}{2^{k-i}}\right) C_n^k = 2\left(1 - \frac{1}{2^{k+1}}\right) C_n^k \le 2C_n^k$.

3.3.17 Tồn tại $m \in \mathbb{N}^*$ và $(p_1,\dots,p_m) \in \mathbb{N}^*$ sao cho: $n = 2^{p_1} + 2^{p_2} + \dots + 2^{p_m}$ và $0 \le p_1 < p_2 < \dots < p_m$.

Chẳng hạn: $13 = 2^0 + 2^2 + 2^3$ và trong cơ sở 2: $13 = \overline{1101}$.

Chứng minh rằng (bằng quy nạp hoặc bằng công thức nhị thức Newton) rằng, với mọi p thuộc $\mathbb{N}$, tồn tại A_p trong $\mathbb{Z}[X]$ sao cho: $(X+1)^{2^p} = X^{2^p} + 1 + 2A_p$.

Thế thì: $(X+1)^n = \prod_{i=1}^{m} (X+1)^{2^{p_i}} = \prod_{i=1}^{m} ((X^{2^{p_i}} + 1) + 2A_{p_i})$.

Vậy tồn tại $A \in \mathbb{Z}[X]$ sao cho : $(X+1)^n = \prod_{i=1}^{m} (X^{2^{p_i}} + 1) + 2A$.

Mặt khác, khai triển $\prod_{i=1}^{m} (X^{2^{p_i}} + 1)$, ta được 2^m đơn thức có bậc từng đôi khác nhau và có hệ tử 1. Suy ra rằng số các số nguyên lẻ trong các C_n^k $(0 \le k \le n)$ là 2^m.

◇ **Trả lời**: 2^m trong đó m là số các số 1 trong biểu diễn n trong cơ sở 2. Chẳng hạn với $n = 13 = \overline{1101}$, có đúng 8 (= 2^3) hệ tử C_n^k $(0 \le k \le n)$ lẻ, vậy có 5 hệ tử chẵn.

3.3.18 Với mọi ánh xạ f: $\{1, \dots, n\} \to \{1, \dots, p\}$, ánh xạ

$\{1, \dots, n\} \to f(\{1, \dots, n\})$ là toàn ánh, và với mọi k thuộc $\{0, 1, \dots, p\}$, có C_p^k

$i \mapsto f(i)$

bộ phận có k phần tử lấy trong $\{1, \dots, p\}$. Ta suy ra:

$$p^n = \mathrm{Card}\left(\{1,\dots,p\}^{\{1,\dots,n\}}\right) = \sum_{k=1}^{p} C_p^k S_n^k.$$

◇ **Trả lời**:

p	1	2	3	4	5
S_5^p	1	30	150	240	120

3.3.19 a) $S_{p+1}(n+1)=\sum_{k=0}^{n+1}k^{p+1}=\sum_{k=1}^{n+1}k^{p+1}=\sum_{q=0}^{n}(q+1)^{p+1}=\sum_{q=0}^{n}\left(\sum_{k=0}^{p+1}C_{p+1}^{k}q^{k}\right)$

$=\sum_{k=0}^{p+1}\left(\sum_{q=0}^{n}C_{p+1}^{k}q^{k}\right)=\sum_{k=0}^{p+1}C_{p+1}^{k}S_k(n)$

b) $(n+1)^{p+1}=S_{p+1}(n+1)\ldots S_{p+1}(n)=\sum_{k=0}^{p}C_{p+1}^{k}S_k(n)$.

c) • $n+1=C_1^0S_0(n)$, từ đó $S_0(n)=n+1$. Vả lại: $S_0(n)=0^0+1^0+\ldots+n^0=n+1$.

Chú ý ở đây $0^0=1$.

• Từ $(n+1)^2=C_2^0S_0(n)+C_2^1S_1(n)$, ta suy ra $S_1(n)=\frac{n(n+1)}{2}$.

Chú ý, với $p\geq 1$: $S_p(n)=\sum_{k=0}^{n}k^p=\sum_{k=1}^{n}k^p$ vì $0^p=0$.

• Từ $(n+1)^3=C_3^0S_0(n)+C_3^1S_1(n)+C_3^2S_2(n)$, ta suy ra $S_2(n)=\frac{n(n+1)(2n+1)}{6}$.

• Tương tự ta được: $S_3(n)=\left(\frac{n(n+1)}{2}\right)^2$.

3.3.20 a) Việc cho một phần tử của A_k quy về:

• Việc cho $x_1,\ldots,x_{p+k}$ sao cho có đúng p trong chúng có trị 1 (vậy có C_{p+k}^{p} cách chọn).

• Việc cho $x_{p+k+2},\ldots,x_{p+q+1}$ bất kỳ thuộc $\{0,1\}$ (vậy có 2^{q-k} cách chọn).

Ta suy ra: $\text{Card}(A_k)=C_{p+k}^{p}2^{q-k}$.

b) • A là hợp các A_k $(0\leq k\leq q)$ và các A_k là rời nhau từng đôi, vậy:

$$\text{Card}(A)=\sum_{k=0}^{q}\text{Card}(A_k)=\sum_{k=0}^{q}C_{p+k}^{p}2^{q-k}.$$

• Trao đổi các vai trò của 0 và 1, ta được: $\text{Card}(B)=\sum_{k=0}^{p}C_{q+k}^{q}2^{q-k}$.

◇ **Trả lời:** $\text{Card}(A)=\sum_{k=0}^{q}C_{p+k}^{p}2^{q-k}$, $\text{Card}(B)=\sum_{k=0}^{q}C_{q+k}^{q}2^{p-k}$.

c) Vì $B=\complement_E(A)$, *ta có:* $\text{Card}(E)=\text{Card}(A)+\text{Card}(B)$,

$$2^{p+q+1}=\sum_{k=0}^{q}C_{p+k}^{p}2^{q-k}+\sum_{k=0}^{p}C_{q+k}^{q}2^{p-k},$$

từ đó được hệ thức mong muốn.

d) Áp dụng c) với $q=p$.

3.3.21 Ta ký hiệu, với $n \in \mathbb{N}$: $S_n = \sum_{k=0}^{n} \frac{1}{C_n^k}$.

Ta có với mọi n thuộc $\mathbb{N}^*$:

$$\frac{2^{n+1}}{n+1} S_n - \frac{2^n}{n} S_{n-1} = \frac{2^{n+1}}{n+1} + T_n,$$

trong đó: $T_n = \sum_{k=0}^{n-1} \left(\frac{2^{n+1}}{(n+1)C_n^k} - \frac{2^n}{nC_{n-1}^k} \right)$.

Và $T_n = 2^n \sum_{k=0}^{n-1} \left(\frac{2 \cdot k!(n-k)!}{(n+1)!} - \frac{k!(n-1-k)!}{n!} \right) =$

$$= \frac{2^n}{(n+1)!} \sum_{k=0}^{n-1} \left(2k!(n-k)! - (n+1)k!(n-1-k)! \right)$$

$$= \frac{2^n}{(n+1)!} \sum_{k=0}^{n-1} k!(n-1-k)!(n-2k-1) \underset{[i=n-1-k]}{=} \frac{2^n}{(n+1)!} \sum_{i=0}^{n-1} (n-1-i)!i!(-n+2i+1) = -T_n,$$

từ đó $T_n = 0$.

Như thế: $\forall n \in \mathbb{N}^*$, $\frac{2^{n+1}}{n+1} S_n = \frac{2^n}{n} S_{n-1} + \frac{2^{n+1}}{n+1}$,

từ đó lấy tổng: $\forall n \in \mathbb{N}^*$, $\frac{2^{n+1}}{n+1} S_n = \sum_{k=0}^{n+1} \frac{2^k}{k} + 2S_n = \sum_{k=1}^{n+1} \frac{2^k}{k}$.

3.4.1 $\tau_{13} \circ \tau_{12}(2) = 3$ và $\tau_{12} \circ \tau_{13}(2) = 1$, vậy $\tau_{13} \circ \tau_{12} \neq \tau_{12} \circ \tau_{13}$.

3.4.2 Phương pháp thứ 1

Số các nghịch thế của $\sigma = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ n & n-1 & \dots & 2 & 1 \end{pmatrix}$ là: $(n-1) + (n-2) + \dots + 1$, từ đó:

$$\varepsilon(\sigma) = (-1)^{\frac{(n-1)n}{2}}.$$

Phương pháp thứ 2

Ta phân tích σ thành những chuyển vị:

- n chẵn, $n = 2p$ ($p \in \mathbb{N}^*$) $\sigma = \tau_{1,2p} \circ \tau_{2,2p-1} \circ \dots \circ \tau_{p,p+1}$ từ đó $\varepsilon(\sigma) = (-1)^p$,
- n lẻ, $n = 2p+1 (p \in \mathbb{N}^*)$, $\sigma = \tau_{1,2p+1} \circ \tau_{2,2p} \circ \dots \circ \tau_{p,p+2}$, từ đó $\varepsilon(\sigma) = (-1)^p$.

◇ **Trả lời**: $\varepsilon(\sigma) = (-1)^{\frac{(n-1)n}{2}} = (-1)^{E\left(\frac{n}{2}\right)}$, hoặc $\varepsilon(\sigma) = \begin{cases} 1 & \text{nếu } n \equiv 0 \text{ hoặc } 1 \ [4] \\ -1 & \text{nếu } n \equiv 2 \text{ hoặc } 3 \ [4] \end{cases}$

3.4.3 Ta đếm các nghịch thế của σ: đó là các cặp: (2, 1), (4, 1), (4, 3), (6, 1), (6, 3), (6, 5),…,(2n, 1), (2n, 3), … ,(2n, 2n-1). Vậy có cả thảy $1 + 2 + 3 + \dots + n$.

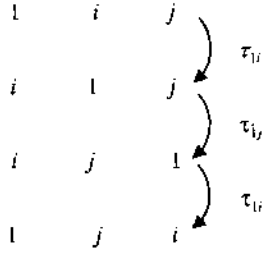
◇ **Trả lời**: $\varepsilon(\delta) = (-1)^{\frac{n(n+1)}{2}}$.

3.4.4 a) ◇ **Trả lời**: $I(\sigma) = 27$, σ lẻ.

b) ◇ **Trả lời**: $\sigma = \tau_{10,12} \circ \tau_{8,11} \circ \tau_{8,10} \circ \tau_{2,9} \circ \tau_{4,8} \circ \tau_{2,7} \circ \tau_{3,6} \circ \tau_{3,5} \circ \tau_{1,2}$.

c) ◇ **Trả lời**: $\sigma = (1, 7, 9, 2) \circ (3, 5, 6) \circ (4, 12, 10, 11, 8)$, $\varepsilon(\sigma) = (-1)^{4-1}(-1)^{3-1}(-1)^{5-1} = -1$.

3.4.5 a)



Vì các chuyển vị sinh ra $\mathfrak{S}_n$ và mỗi chuyển vị phân tích thành những τ_{1i} $(2 \le i \le n)$, ta suy ra rằng $\{\tau_{1i};\ 2 \le i \le n\}$ sinh $\mathfrak{S}_n$.

b)

từ đó $\tau_{1j} \circ \tau_{1i} = (1, i, j)$.

Cho $\sigma \in \mathcal{A}_n$. Theo a), tồn tại $N \in \mathbb{N}^*$, $i_1, \ldots, i_N \in \{2, \ldots, n\}$ sao cho $\sigma = \tau_{1i_1} \circ \ldots \circ \tau_{1i_N}$. Vì σ chẵn và mọi chuyển vị là lẻ, nên N là chẵn. Nhóm các τ_{1i_k} $(1 \le k \le N)$ từng đôi một, ta kết luận rằng σ được phân tích trên chu trình 3 : $(1, i, j)$, $(i, j) \in \{2, \ldots, n\}^2$, $i \ne j$.

c) Theo b) $\tau_{1k} \circ \tau_{12} = (1, 2, k$ và $\tau_{12} \circ \tau_{1k} = (1, k, 2) = (1, 2, k)^2$.

Từ đó: $\gamma_i \circ \gamma^2_j = (\tau_{1i} \circ \tau_{12})\, 0\ (\tau_{12} \circ \tau_{1j}) = \tau_{1i} \circ \tau_{1j}$.

Vậy ta suy ra từ b) rằng mọi σ thuộc $\mathcal{A}_n$ được phân tích thành những γ_i $(3 \le i \le n)$.

3.5.1 Tồn tại một đối tượng ω không thuộc F. Ta ký hiệu $G = F \cup \{\omega\}$, $\mathcal{F}(E, F)$ là tập hợp các hàm từ E đến F. Với mọi f thuộc $\mathcal{F}(E, F)$, ánh xạ

$E \to G$ là một song ánh

$$x \mapsto \begin{cases} f(x) & \text{nếu } x \text{ có một ảnh qua } f. \\ \omega & \text{nếu } x \text{ không có ảnh qua } f. \end{cases}$$

Vậy: $\#(\mathcal{F}(E, F)) = \#(G^E) = (\#G)^{\#(E)}$.

◇ **Trả lời**: $(p+1)^n$.

3.5.2 Giả sử a là một phần tử cố định của $\{1, \ldots, n+1\}$ (chẳng hạn $a = n+1$). Việc cho một phân hoạch của $\{1, \ldots, n+1\}$ được xác định bởi:

- Cho một bộ phận A của $\{1, \ldots, n+1\}$ sao cho $a \in A$ (có C_n^k khả năng, trong đó $k = \#(A) - 1$).
- Tiếp theo cho một phân hoạch của $\{1, \ldots, n+1\} - A$.

Suy ra: $P_{n+1} = \sum_{k=0}^{n} C_n^k P_k$.

◇ **Trả lời**:

n	0	1	2	3	4	5
P_n	1	1	2	5	15	52

3.5.3 a) Các phân hoạch của $\{1, ..., n+1\}$ thành $p+1$ bộ phận là :

• một mặt, các phân hoạch có chứa đơn tử $\{n+1\}$ (có $P_{n,p}$ phân hoạch)

• mặt khác, các phân hoạch không chứa đơn tử $\{n+1\}$ (có $(p+1)P_{n,p+1}$ phân hoạch).

b) ◇ **Trả lời :**

n \ p	1	2	3	4	5
1	1	0	0	0	0
2	1	1	0	0	0
3	1	3	1	0	0
4	1	7	6	1	0
5	1	15	25	10	1

c) • Việc cho một phân hoạch của $\{1, ..., n+1\}$ thành n bộ phận (vậy khác rỗng) quy về việc cho một cạp thuộc $\{1, ..., n+1\}$, từ đó $P_{n+1,n} = C_{n+1}^2 = \dfrac{n(n+1)}{2}$.

• Việc cho một phân hoạch của $\{1, ..., n+1\}$ thành 2 bộ phận (vậy khác rỗng) quy về việc cho một cạp $(A, \complement_{\{1,...,n\}}(A))$ trong đó $A \neq \varnothing$, từ đó suy ra $P_{n+1,2} = \dfrac{1}{2}(2^{n+1} - 2) = 2^n - 1$.

• *Quy nạp theo n*

Công thức $P_{n+1,3} = \dfrac{3^n - 2^{n+1} + 1}{2}$ là hiển nhiên với $n = 2$.

Nếu công thức đúng với một n ($n \geq 2$), thì :

$$P_{n+2,3} = P_{n+1,2} + 3P_{n+1,3} = 2^n - 1 + \frac{3}{2}(3^n - 2^{n+1} + 1)$$

$$= \frac{3^{n+1}}{2} - 2^{n+1} + \frac{1}{2} = \frac{3^{n+1} - 2^{n+2} + 1}{2}.$$

3.5.4 a) 1) Cho $x_1 \in E$ cố định. Ta có :

$$b_{n,k} = \#(\{f : E \to \mathbb{N};\ \sum_{x \in E} f(x) = k\}) = \#(\{g : E - \{x_1\} \to \mathbb{N};\ \sum_{x \in E - \{x_1\}} g(x) \leq k\}) = a_{n-1,k}.$$

2) Tập hợp $A_{n,k}$ là hợp rời nhau của $B_{n,k}$ và $A_{n,k-1}$, từ đó $a_{n,k} = b_{n,k} + a_{n,k-1}$.

b) 1) Quy nạp theo $n + k$, để chứng minh $a_{n,k} = C_{n-k}^k$.

• Nếu $n + k = 0$, thì $n = k = 0$, và $a_{0,0} = 1 = C_0^0$.

• Cho $p \in \mathbb{N}$, và giả thiết $a_{n,k} = C_{n+k}^k$ với một cạp (n, k) thuộc $\mathbb{N}^2$ sao cho $n + k = p$. Giả sử $(n, k) \in \mathbb{N}^2$ sao cho $n + k = p + 1$.

Nếu $n \geq 1$ và $k \geq 1$, thì $(n - 1, k) \in \mathbb{N}^2$, $(n, k - 1) \in \mathbb{N}^2$, và $(n - 1) + k = n + (k - 1) = p$, từ đó, theo giả thiết quy nạp :

$$a_{n,k} = a_{n-1,k} + a_{n,k-1} = C_{n-1+k}^k + C_{n+k-1}^{k-1} = C_{n+k}^k.$$

Hơn nữa : $a_{0,k} = a_{n,0} = 1$.

Chỉ dẫn và trả lời
các bài tập chương 4

4.1.1 • Nếu $n = 2p$ ($p \in \mathbb{Z}$), thì $n^2 = 4p^2$, vậy $n^2 \equiv 0[4]$, từ đó $n^2 \equiv 0$ hoặc $4[8]$.

• Nếu $n = 2p + 1$ ($p \in \mathbb{Z}$), thì $n^2 = 4p(p + 1) + 1$, vậy $n^2 \equiv 1[8]$, vì $p(p + 1)$ chẵn, do p hoặc $p + 1$ chẵn.

4.1.2 Chú ý rằng : $5^{2^{n-2}} - 1 = \prod_{k=0}^{n-3}\left(5^{2^k} + 1\right)$ (nếu $n \geq 3$), và mỗi thừa số $5^{2^k} + 1$ ($k \in \mathbb{N}$) chẵn, nhưng đồng dư modulo 4 với 2.

4.1.3 $$\sum_{k=1}^{2n}\frac{(2n)!}{k} = \sum_{k=1}^{n}\frac{(2n)!}{k} + \sum_{k=n+1}^{2n}\frac{(2n)!}{k} = \sum_{k=1}^{n}\frac{(2n)!}{k} + \sum_{l=1}^{n}\frac{(2n)!}{2n+1-l}$$

$$= \sum_{k=1}^{n}(2n)!\left(\frac{1}{k} + \frac{1}{2n+1-k}\right) = (2n+1)\sum_{k=1}^{n}\frac{(2n)!}{k(2n+1-k)}.$$

Vì, với mọi k thuộc $\{1,\ldots, n\}$, k và $2n + 1 - k$ khác nhau và nhỏ hơn $2n$, nên số hữu tỷ $\dfrac{(2n)!}{k(2n+1-k)}$ là một số nguyên.

4.1.4 Quy nạp theo n.

Tính chất là hiển nhiên với $n = 1$.

Giả thiết tính chất đúng với một n thuộc $\mathbb{N}^*$. Vì

$$(5(n + 1))! = (5n)! \cdot (5n + 1)(5n + 2)(5n + 3)(5n + 4)(5n + 5)$$

và $40^{n+1}(n + 1)! = (40^n n!)40(n + 1)$, nên chỉ cần chứng minh: $8 \mid (5n + 1)(5n + 2)(5n + 3)(5n + 4)$.

Trong 4 số liên tiếp $5n + 1$, $5n + 2$, $5n + 3$, $5n + 4$, có 2 số chẵn, và một trong hai số này là bội của 4. Ta cũng có thể chú ý rằng: $C_{5n+4}^{4} \in \mathbb{N}$.

4.1.5 Ký hiệu $\alpha = 2n - 1$ và $u_n = (3n^2 - 3n + 1)(3n^2 - 3n + 2)$, ta có $u_n = \dfrac{1}{16}(3\alpha^2 + 1)(3\alpha^2 + 5)$,

từ đó:

$$2n - 1 \mid u_n \Rightarrow \alpha \mid (3\alpha^2 + 1)(3\alpha^2 + 5) \Rightarrow \alpha \mid 15 \Rightarrow \alpha \in \{1, 5\} \Rightarrow n = 3.$$

Ngược lại, $u_3 = 380$ chia hết cho 5.

4.1.6 Ký hiệu $E_n = \{k \in \mathbb{N}^*;\ n! < k < (n + 1)!\}$. Để tồn tại $k \in E_n$ sao cho $n^3 \mid k$, chỉ cần E_n chứa ít nhất n^3 số liên tiếp (trong chúng sẽ có một bội của n^3). Vì $\mathrm{Card}(E_n) = (n + 1)! - n! - 1 = n \cdot n! - 1$, chỉ cần: $\forall n \geq 4$, $n \cdot n! > n^3 + 1$, điều này có thể chứng minh dễ dàng (bằng quy nạp theo n).

4.1.7 Ký hiệu $m = ad + bc$, tồn tại $(\alpha, \beta, \gamma, \delta) \in \mathbb{Z}^4$ sao cho $a = m\alpha, \ldots, d = m\delta$. Thế thì: $m = ad + bc = m^2(\alpha\delta + \beta\gamma)$, từ đó $m^2 \mid m$, $m \in \{-1, 0, 1\}$.

4.1.8 Ký hiệu $r_1 = \dfrac{3-\sqrt{5}}{2}, r_2 = \dfrac{3+\sqrt{5}}{2}$ và $u_n = r_1^n + r_2^n$, $(n \in \mathbb{N})$, $(u_n)_{n \in \mathbb{N}}$ là một dãy truy hồi tuyến tính cấp hai với hệ tử hằng (Xem Tập 1, 3.4.2, 2)), và ta có:

$$\forall n \in \mathbb{N}, \quad u_{n+2} - (r_1 + r_2)u_{n+1} + r_1 r_2 u_n = 0,$$

tức là: $\forall n \in \mathbb{N}$, $u_{n+2} = 3u_{n+1} - u_n$.

Vì $u_0 = 2$ và $u_1 = 3$, nên rõ ràng (bằng quy nạp hai bước theo n) là: $\forall n \in \mathbb{N}$, $u_n \in \mathbb{Z}$, và hơn nữa, do $r_1 \geq 0$ và $r_2 \geq 0$ nên: $\forall n \in \mathbb{N}$, $u_n \in \mathbb{N}$.

Như thế, với mọi n thuộc $\mathbb{N}$, $(3 + \sqrt{5})^n + (3 - \sqrt{5})^n = 2^n u_n$, vậy nó là một số nguyên chia hết cho 2^n.

4.1.9 a) Chú ý trước tiên: $\forall n \in \mathbb{Z}$, $3n + 4 \neq 0$.

Ký hiệu $m = n + 1$, ta có: $\dfrac{11n+8}{3n+4} = \dfrac{11m-3}{3m+1} \underset{|m|\to\infty}{\to} \dfrac{11}{3} < 4$.

Ký hiệu: $k = \dfrac{11m-3}{3m+1} \in \mathbb{Q}$.

• Nếu $k \in \mathbb{Z}$ và $|k| \geq 4$, thì: $11|m| + 3 \geq |11m + 3| = |k||3m + 1| \geq 4(3|m| - 1)$, từ đó: $|m| \leq 7$.

Thử các trị $-7, -6, \ldots, 7$ của m.

• Thử các trị $-3, -2, \ldots, 3$ của k.

Chú ý: Vấn đề quy về việc xác định các điểm có toạ độ nguyên trên đường hypebol có phương trình: $y = \dfrac{11x+8}{3x+4}$.

◇ **Trả lời**: $\{-8, -3, -2, -1, 0, 2\}$.

b) Trước tiên chứng minh: $\forall n \in \mathbb{Z}$, $\begin{cases} n^2 - 6 \neq 0, \ n^2 + 3n - 2 \neq 0 \\ \dfrac{n^2-6}{n^2+3n-2} \neq 1 \text{ và } \neq -1 \end{cases}$.

Thế thì, nếu $\dfrac{n^2-6}{n^2+3n-2} \in \mathbb{Z}$:

$$n^2 + 6 \geq |n^2 - 6| \geq 2|n^2 - 3n - 2| \geq 2(n^2 - 3|n| - 2),$$

từ đó: $n^2 - 6|n| - 10 \leq 0$, vậy $|n| \leq 3 + \sqrt{19} < 8$.

Thử các trị $-7, -6, \ldots, 7$ của n.

◇ **Trả lời**: $\{-4, 0\}$.

4.1.10 Chú ý là: $a^3 + b^3 + c^3 - 3abc = (a + b + c)(a^2 + b^2 + c^2 - ab - ac - bc)$.

4.1.11 • Ta có: $\forall k \in \mathbb{N}^*$, $(k \mid n \Rightarrow a^k - 1 \mid a^n - 1)$.

Thật vậy, nếu $n = km$, $(k, m) \in (\mathbb{N}^*)^2$, thì: $a^n - 1 = (a^k)^m - 1 = (a^k - 1)\sum_{i=0}^{m-1} (a^k)^i$.

• Vì ánh xạ $\mathbb{N}^* \to \mathbb{N}^*$ là đơn ánh (vì $a \geq 2$), ta kết luận $d(a^n - 1) \geq d(n)$.

$k \mapsto a^k - 1$

4.1.12 **Trường hợp thứ nhất:** k lẻ, $k = 2l + 1$, $l \in \mathbb{N}$.

Thế thì: $m = d_1 d_{2l+1} = d_2 d_{2l} = \ldots = d_l d_{l+2} = d_{l+1}^2$, từ đó: $\left(\prod_{i=1}^{k} d_i\right)^2 = \prod_{i=1}^{k} d_i d_{2l+2-i} = n^k$.

Trường hợp thứ 2: k **chẵn**, tương tự.

4.1.13 a) $xy = 2x + 3y \Leftrightarrow (x - 3)(y - 2) = 6$.

◇ **Trả lời:** {(-3, 1), (0, 0), (1, -1), (2, -4), (4, 8), (5, 5), (6, 4), (9, 3) }.

b) $x^2 - y^2 - x + 3y = 30 \Leftrightarrow \left(x - \frac{1}{2}\right)^2 - \left(x - \frac{3}{2}\right)^2 = 28 \Leftrightarrow (x + y - 2)(x - y + 1) = 28$.

◇ **Trả lời:** {(-14, -12), (-5, 0), (-5, 3), (-14, 15), (15, -12), (6, 0), (6, 3), (15, 15) }.

c) $\frac{1}{x} + \frac{1}{y} = \frac{1}{5} \Leftrightarrow xy = 5(x + y) \Leftrightarrow (x - 5)(y - 5) = 25$.

◇ **Trả lời:** {(-20, 4), (4, -20), (6, 30), (10, 10), (30, 6)}.

d) $x^2 - 3xy + 2y^2 - x - 3y - 6 = 0 \Leftrightarrow (x - y + 2)(x - 2y - 1) = 4$.

◇ **Trả lời:** {(-12, -6), (-7, -3), (-3, 0), (-7, -6), (-3, -3), (2, 0)}.

e) $2x^3 + xy - 7 = 0 \Leftrightarrow x(2x^2 + y) = 7$.

◇ **Trả lời:** {(-7, -99), (-1, -9), (1, 5), (7, -97)}.

f) Chú ý trước tiên đến các vai trò đối xứng của x và y, cho phép ta quy về $x \le y$.

Nếu $x^3 + xy + y^3 = 209$ thì:

- $y^3 \le 209$, vậy $y \le 5$.
- $209 \le y^3 + y^2 + y^3 \le 3y^3$, vậy $y \ge 5$.

◇ **Trả lời:** {(4, 5), (5, 4)}.

g) Ký hiệu $t = x + 4$, phương trình quy về: $(t^2 - 9)(t^2 - 16) = y^2$, và ta có $t^2 \le 9$ hoặc $t^2 \ge 16$.

- Thử các trị -3, -2,..., 3 của t.
- Nếu $t^2 \ge 16$, thì $(t^2 - 16)^2 \le y^2 \le (t^2 - 9)^2$; giải mỗi phương trình: $(t^2 - k)^2 = (t^2 - 9)(t^2 - 16)$, với $k \in \{9,\ldots,16\}$.

◇ **Trả lời:** {(-9, 12), (-8, 0), (-7, 0), (-4, -12), (-4, 12), (-1, 0), (0, 0), (1, 12)}.

h) $x^2 = 9y^2 - 39y + 40 \Leftrightarrow (2x - 6y + 13)(2x + 6y - 13) = -9$.

◇ **Trả lời:** {(-2, 3), (2, 3)}.

i) Giả sử (x, y, z) thích hợp. Ta có: $x^3 = y^3 + z^3 + 3xyz \ge y^3$, vậy $x \ge y$, và cả $x \ge z$.

Rồi thì $x^2 = 2(y + z) \le 4x$ và x chẵn, vậy $x \in \{0, 2, 4\}$.

◇ **Trả lời:** {(0, 0, 0), (2, 0, 2), (2, 1, 1), (2, 2, 0)}.

j) Nếu (x, y, z) thích hợp, thì: $4(x^2 + y^2) = 4z^2 = (xy - 2(x + y))^2$, từ đó $xy(xy - 4(x + y) + 8) = 0$, và do vậy $(x - 4)(y - 4) = 8$.

◇ **Trả lời:** {(5, 12, 13), (6, 8, 10), (8, 6, 10), (12, 5, 13).

k) Giả sử (x, y) thích hợp.

Vì 3^x lẻ nên y chẵn, vậy (xem bài tập 4.1.1), $y^2 \equiv 1$ [8].

Mặt khác, nếu x lẻ thì $3^x \equiv 3$[8], mâu thuẫn. Vậy x chẵn, $x = 2X$, $X \in \mathbb{N}$. Thế thì $(3^X - y)(3^X + y) = 8$, từ đó $3^X \leq 8$, $X \in \{0, 1\}$.

◇ **Trả lời:** $\{(2, 1)\}$.

4.1.14 1) Trong các ví dụ chỉ chứa n ở số mũ, ta thường có thể sử dụng các đồng dư. Chẳng hạn, với a):

$$2^{2n+1} + 3^{2n+1} = 4^n \cdot 2 + 9^n \cdot 3 \underset{[5]}{\equiv} 4^n(2 + 3) \underset{[5]}{\equiv} 0.$$

Như thế ta có thể giải các ví dụ: a), c), e), f), h), l), m), o), p), q), r).

2) Trong các ví dụ hỗn hợp các hàm mũ và các đa thức, phép quy nạp thường sẽ cho phép ta kết luận. Chẳng hạn, với b), ký hiệu $u_n = 4^n - 1 - 3n$, ta có: $u_0 = 0$ và nếu $u_n = 0$ [9], thì:

$$u_{n+1} = 4^{n+1} - 1 - 3(n + 1) = 4(u_n + 1 + 3n) - 3n - 4 = 4u_n + 9n \equiv 0 \ [9].$$

Ta có thể giải các ví dụ: b), d), g), i), j), k), n), s), t) theo cách này.

u) Ký hiệu $u_n = 3.\,81^{n+1} + (16n - 54)9^{n+1} - 320n^2 - 144n + 243$.

Ta có: $u_n = (3.\,9^{n+1} + (40n - 27))(9^{n+1} + (-8n - 9)) = 64\alpha_n \beta_n$,

trong đó: $\alpha_n = \dfrac{1}{8}(27(9^n - 1) + 40n) = 27\sum_{k=0}^{n-1} 9^k + 5n$ và $\beta_n = \dfrac{1}{8}(9(9^n - 1) - 8n) = 9\sum_{k=0}^{n-1} 9^k - n$

Vì $9 \equiv 1$[8], ta có: $\alpha_n \underset{[8]}{\equiv} 27\sum_{k=0}^{n-1} 1 + 5n = 32n \underset{[8]}{\equiv} 0$ và $\beta_n \underset{[8]}{\equiv} 9\sum_{k=0}^{n-1} 1 - n = 8n \underset{[8]}{\equiv} 0$.

Như thế: $8 \mid \alpha_n$ và $8 \mid \beta_n$, từ đó $2^{12} = 64^2 \mid u_n$.

4.1.15 Quy nạp theo n (với $a \in \mathbb{Z}$ lẻ cố định).

- $n = 3$: $a^{2^{n-2}} = a^2 \equiv 1$ [8] (xem bài tập 4.1.1).
- Giả sử $a^{2^{n-2}} \equiv 1$ [2^n]; tồn tại $\lambda \in \mathbb{Z}$ sao cho: $a^{2^{n-2}} = 1 + \lambda 2^n$. Thế thì ta có:

$$a^{2^{n-1}} = (a^{2^{n-2}})^2 = (1 + \lambda 2^n)^2 = 1 + \lambda 2^{n+1} + \lambda^2 2^{2n} \equiv 1 \ [2^{n+1}], \text{ vì } 2n \geq n + 1.$$

4.1.16 • Trong $\mathbb{Z}/7\mathbb{Z}$:

$\hat{x}$	$\widehat{-3}$	$\widehat{-2}$	$\widehat{-1}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$
$\widehat{x^2}$	$\hat{1}$	$\widehat{-1}$	$\widehat{-1}$	$\hat{0}$	$\hat{1}$	$\hat{1}$	$\widehat{-1}$

- Giả sử $(a, b, c) \in \mathbb{Z}^3$ sao cho $7 \nmid abc$. Thế thì $\hat{a} \neq \hat{0}$, $\hat{b} \neq \hat{0}$, $\hat{c} \neq \hat{0}$, vậy: $(\hat{a}^3, \hat{b}^3, \hat{c}^3) \in \{\widehat{-1}, \hat{1}\}^3$, từ đó $\hat{a}^3 + \hat{b}^3 + \hat{c}^3 \in \{-3, -\hat{1}, \hat{1}, \hat{3}\}$, vậy $7 \nmid a^3 + b^3 + c^3$.

4.1.17 $n^2 + (n+1)^2 + (n+3)^2 = 3n^2 + 8n + 10 \underset{[10]}{\equiv} 3n^2 - 2n$.

Modulo 10 :

n	-4	-3	-2	-1	0	1	2	3	4	5
$3n^2 - 2n$	-4	3	-4	5	0	1	-2	1	0	5

◇ **Trả lời**: $n \equiv 0$ hoặc 4 [10].

4.1.18 • Nếu n chẵn, $n = 2k$ ($k \in \mathbb{N}$), thì:

$$3^n + 4n + 1 = 9^k + 8k + 1 \underset{[8]}{\equiv} 1 + 8k + 1 \underset{[8]}{\equiv} 2.$$

• Nếu n lẻ, $n = 2k + 1$ ($k \in \mathbb{N}$), thì:

$$3^n + 4n + 1 = 3.9^k + 8k + 5 \underset{[8]}{\equiv} 3 + 8k + 5 \underset{[8]}{\equiv} 0.$$

◇ **Trả lời**: n lẻ.

4.1.19 a) Vì $2^6 = 64 \equiv 1$ [21] nên lớp modulo 21 của 2^n phụ thuộc vào lớp modulo 6 của n:

n mod. 6	0	1	2	3	4	5
2^n mod. 21	1	2	4	8	-5	-10
2^{2n} mod. 21	1	4	-5	1	4	-5
$2^{2n}+2^n+1$ mod. 21	3	7	0	10	0	-14

◇ **Trả lời**: $n \equiv 2$ hoặc 4 [6].

b) Vì $2^3 = 8 \equiv 1$ [7], nên lớp modulo 7 của 2^n phụ thuộc vào lớp modulo 3 của n. Mặt khác, vì $2^2 = 4 \equiv 1$ [3], nên lớp modulo 3 của 2^n phụ thuộc vào lớp modulo 2 của n. Từ đó có bảng:

n mod. 6	0	1	2	3	4	5
2^n mod. 7	1	2	4	1	2	4
2^n mod. 3	1	2	1	2	1	2
2^{2n} mod. 7	2	4	2	4	2	4
$2^{2n}+2^n+1$ mod. 7	4	0	0	6	5	2

◇ **Trả lời**: $n \equiv 1$ hoặc 2[6].

4.1.20 Vì $3^2 \equiv 1$ [8], ta có: $3^n \equiv 1$ hoặc 3 [8], vậy $3^n + 1 \equiv 2$ hoặc 4 [8]. Điều này chứng minh: $8 \nmid 3^n + 1$. Vả lại, việc khảo sát trường hợp $n = 2$ là dễ dàng.

4.1.21 Tính các lớp modulo 23 của 2^k và 3^k với $k = 0, 1, 2, \ldots$ Ta chú ý: $2^{11} \equiv 1$ [23] và $3^{11} \equiv 1$ [23]. Như thế, các lớp modulo 23 của 2^k và 3^k phụ thuộc vào lớp modulo của k.

k mod. 11	0	1	2	3	4	5	6	7	8	9	10
2^k mod. 23	1	2	4	8	-7	9	-5	-10	3	6	12
3^k mod. 23	1	3	9	4	12	-10	-7	2	6	-5	8

Ký hiệu: $A = \{\hat{1}, \hat{2}, \hat{4}, \hat{8}, -\hat{7}, \hat{9}, -\hat{5}, -\widehat{10}, \hat{3}, \hat{6}, -\widehat{11}\}$ và $B = \{-\hat{1}, -\hat{3}, -\hat{9}, -\hat{4}, \hat{1}, \widehat{10}, \hat{7}, -\hat{2}, -\hat{6}, \hat{5}, -\hat{8}\}$,

ta có: $\begin{cases} \forall a \in \mathbb{N}, \quad \widehat{2^a} \in A \\ \forall b \in \mathbb{N}, \quad -\widehat{3^b} \in B. \\ A \cap B = \varnothing \end{cases}$

Ta kết luận: $\forall (a, b) \in \mathbb{N}^2$, $23 \nmid 2^a + 3^b$.

4.1.22 a) Nếu (x, y) là nghiệm thì $5y^2 \leq 3$, từ đó $y^2 < 1$, $y = 0$, rồi $x^2 = 3$, mâu thuẫn.

b) Chuyển qua modulo 5:

x mod. 5	0	1	2
x^2 mod. 5	0	1	-1

Như thế: $\forall x \in \mathbb{Z}$, $x^2 \equiv -1, 0$ hoặc 1 [5].

Nhưng, nếu $x^2 - 5y^2 = 3$, thì $x^2 \equiv 3$ [5], mâu thuẫn.

c) Giả sử (x, y) là một nghiệm. Thế thì $3 \mid 7y^2$, vậy $3 \mid y$ (vì 3 là nguyên tố, hoặc tách ra các trường hợp: $y \equiv -1, 0, 1$ [3]). Vậy tồn tại $Y \in \mathbb{Z}$ sao cho $y = 3Y$, và: $5x^2 - 21Y^2 = 3$. Tương tự, $3 \mid 5x^2$, $3 \mid x$. Vậy tồn tại $X \in \mathbb{Z}$ sao cho $x = 3X$, và: $15X^2 - 7Y^2 = 1$.

Chuyển qua modulo 3, ta suy ra $Y^2 \equiv -1$ [3]. Nhưng ta có: $\forall Y \in \mathbb{Z}$, $Y^2 \equiv 0$ hoặc 1 [3], từ đó gặp mâu thuẫn.

d) Chuyển qua modulo 8 và sử dụng bài tập 4.1.1.

e) Nếu (x, y) là nghiệm, chuyển qua modulo 3, ta suy ra $x^3 - x - 1 \equiv 0$ [3].

Nhưng mặt khác: $\forall x \in \mathbb{Z}$, $x^3 - x - 1 \equiv -1$ [3], như ta thấy rõ khi tách ra các trường hợp $x \equiv -1, 0, 1$ [3].

f) Giả thiết tồn tại một nghiệm (x, y).

1) $x^3 + 11^3 \geq 12^3 \Rightarrow x^3 \geq 397 \Rightarrow x \geq 8$.

2) • $y^3 = x^3 + 11^3 > x^3 \Rightarrow y > x \Rightarrow y \geq x + 1$.

- Modulo 2: $x^3 \equiv x$, $y^3 \equiv y$, $11^3 \equiv 1$, vậy $y \equiv x + 1$ [2]. Đặc biệt $y \neq x + 2$.
- Modulo 3: $x^3 \equiv x$, $y^3 \equiv y$, $11^3 \equiv -1$, vậy $y \equiv x - 1$ [3]. Đặc biệt $y \neq x + 1$.

Vậy ta có: $y \geq x + 3$, rồi thì:

$$11^3 = y^3 - x^3 \geq (x + 3)^3 - x^3 = 9x^2 + 27x + 27,$$

từ đó: $9x^2 + 27x - 1304 \leq 0$, vậy $x \leq 10$.

Thử các trị 8, 9, 10 của x.

Cuối cùng, phương trình đã cho vô nghiệm.

4.1.23 α) Giả sử (x, y, z) thích hợp. Vì các vai trò của x, y, z đối xứng, nên ta có thể quy về trường hợp: $1 \leq x \leq y \leq z$.

Thế thì: $\begin{cases} 1 \leq x + y - 1 \leq 2z - 1 \\ z \mid x + y - 1 \end{cases}$, vậy $z = x + y - 1$.

Rồi $\begin{cases} 1 \leq z + x - 1 = 2x + y - 2 \leq 3y - 2 \\ y \mid 2x + y - 2 \end{cases}$, vậy $2x + y - 2 \in \{y, 2y\}$.

1) Nếu $2x + y - 2 = y$, thì $x = 1$ và $z = y$.

2) Giả thiết $2x + y - 2 = 2y$; thế thì $y = 2x - 2$ và $z = 3x - 3$. Trong trường hợp này, ta có:

$$\begin{cases} x + y \equiv 1 \ [z] \\ y + z \equiv 1 \ [x] \\ z + x \equiv 1 \ [y] \end{cases} \Leftrightarrow \begin{cases} 3x - 3 \equiv 0 \ [3x - 3] \\ 5x - 6 \equiv 0 \ [x] \\ 4x - 4 \equiv 0 \ [2x - 2] \end{cases} \Leftrightarrow 5x \equiv 6 [x] \Leftrightarrow x \mid 6 \Leftrightarrow x \in \{1, 2, 3, 6\}$$

β) Kiểm chứng rằng các bộ ba nhận được là thích hợp:

◇ **Trả lời**: $\{(1, y, y); y \in \mathbb{N}^*\} \cup \{(2, 2, 3), (3, 4, 6), (6, 10, 15)\}$.

4.1.24 Theo bài tập 4.1.1: $n^2 \equiv 1 \ [8]$. Vậy tồn tại $\lambda \in \mathbb{N}$ sao cho $n^2 = 1 + 8\lambda$, từ đó: $n^4 = 1 + 16\lambda + 64\lambda^2 \equiv 1 \ [16]$.

4.1.25 Modulo 10:

- $2^{100} = (2^5)^{20} \equiv 2^{20} = (2^5)^4 \equiv 2^4 \equiv 6$
- $3^{100} = (3^4)^{25} \equiv 1^{25} = 1$
- $4^{100} = (2^{100})^2 \equiv 6^2 \equiv 6$
- $5^{100} \equiv 5$
- $6^{100} \equiv (-4)^{100} = 4^{100} \equiv 6$, ... khi chuyển qua các đối.

◇ **Trả lời**: 3.

4.1.26 Vì $2^4 \equiv 1 \ [5]$, $3^4 \equiv 1 \ [5]$, $4^4 \equiv 1 \ [5]$, nên các lớp modulo 5 của 2^n, 3^n, 4^n, 5^n phụ thuộc vào lớp modul 4 của n:

n mod. 4	1	2	3	4
2^n mod. 5	2	-1	-2	1
3^n mod. 5	-2	-1	2	1
4^n mod. 5	-1	1	-1	1
$1^n + 2^n + 3^n + 4^n$ mod. 5	0	0	0	4

Như thế: $5 \mid 1^n + 2^n + 3^n + 4^n \Leftrightarrow n \equiv 1$ hoặc 2 hoặc 3 $[4] \Leftrightarrow 4 \nmid n$.

4.1.27 $3^4 = 81 \equiv 1 \ [10]$, vậy, modulo 10: $3^{n+4b} = 3^n.(3^4)^b \equiv 3^n \equiv -1$, 3^{a-4b}, $3^{4b} = 3^n \equiv -1$ và $3^{a-4b}.3^{4b} \equiv 3^{a-4b}$.

Bài tập hiển nhiên này cũng quy về: $\forall n \in \mathbb{N}$, $3^{2+4n} \equiv -1 \ [10]$.

4.1.28 Giả sử $k \in \mathbb{N} - \{0, 1\}$. Nếu tồn tại $N \in \mathbb{N}^*$ sao cho ($\phi_n = \phi_0$ và $\phi_{N+1} = \phi_1$), thì bằng lập luận quy nạp, ta thấy rằng dãy $(\phi_n \text{ mod. } k)_{n \in \mathbb{N}}$ là N- tuần hoàn (tức là tuần hoàn chu kỳ N), vậy ϕ_n mod. k chỉ phụ thuộc và lớp modulo N của n.

a)

n	0	1	2	3	4
ϕ_n mod. 2	0	1	1	0	1

Dãy $(\phi_n \bmod 2)_{n\in\mathbb{N}}$ là 3- tuần hoàn và lập lại bộ ba (0, 1, 1).

Vậy: $2 \mid \phi_n \Leftrightarrow n \equiv 0\ [3] \Leftrightarrow 3 \mid n$.

b)

n	0	1	2	3	4	5	6	7	8	9
$\phi_n \bmod 3$	0	1	1	-1	0	-1	-1	1	0	1

Dãy $(\phi_n \bmod 3)_{n\in\mathbb{N}}$ là 8- tuần hoàn và: $3 \mid \phi_n \Leftrightarrow n \equiv 0$ hoặc $4\ [8] \Leftrightarrow n \equiv 0\ [4] \Leftrightarrow 4 \mid n$.

c)

n	0	1	2	3	4	5	6	7
$\phi_n \bmod 4$	0	1	1	2	-1	1	0	1

Dãy $(\phi_n \bmod 4)_{n\in\mathbb{N}}$ là 6- tuần hoàn và: $4 \mid \phi_n \Leftrightarrow n \equiv 0[6] \Leftrightarrow 6 \mid n$.

4.1.29 $2^{2^n} \equiv -1\left[F_n\right]$, từ đó: $2^{F_n} = 2.2^{2^{2^n}} = 2\left(2^{2^n}\right)^{2^{2^n}-n} \underset{[F_n]}{\equiv} 2(-1)^{2^{2^n}-n} \equiv 2$, vì $2^{2^n}-n$, chẵn, do $2^n - n \geq 1$.

4.1.30 Trước tiên, rõ ràng rằng các $k\mathbb{Z}$ $(k \in \mathbb{N})$ đều là những nhóm con của $(\mathbb{Z}, +)$.

Cho G là một nhóm con của $\mathbb{Z}$; giả thiết $G \neq \{0\}$. Tồn tại $a \in G$ sao cho $a \neq 0$.

Nếu $a > 0$, thì $G \cap \mathbb{N}^* \neq \varnothing$.

Nếu $a < 0$, thì $-a \in G$, vậy $G \cap \mathbb{N}^* \neq \varnothing$.

Như thế, $G \cap \mathbb{N}^*$ là một bộ phận khác rỗng của $\mathbb{N}^*$, vậy có một phần tử bé nhất, ký hiệu là k.

Ta chứng minh rằng $G = k\mathbb{Z}$.

1) Vì $k \in G$, một phép luận quy nạp chứng tỏ: $\forall n \in \mathbb{N}$, $kn \in G$, rồi thì, chuyển qua các phần tử đối: $\forall n \in \mathbb{N}$, $kn \in G$. Ta kết luận: $k\mathbb{Z} \subset G$.

2) Ngược lại, giả sử $x \in G$. Theo phép chia Euclide x cho k, tồn tại $(q, r) \in \mathbb{Z}^2$ sao cho:

$$x = kq + r \text{ và } 0 \leq r < k.$$

Vì $x \in G$, $kq \in G$ và G là một nhóm con của $\mathbb{Z}$, ta được $r \in G$, rồi theo định nghĩa của k, $r = 0$.

Như thế: $x = kq \in k\mathbb{Z}$.

4.1.31 Giả sử H là một nhóm con của $(\mathbb{Z}/n\mathbb{Z}, +)$. Vì toàn ánh chính tắc $s : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ là một đồng cấu nhóm, nên $s^{-1}(H)$ là một nhóm con của $\mathbb{Z}$ (xem bài tập 2.2.12, *b*)). Theo bài tập 4.1.30, tồn tại $k \in \mathbb{Z}$ sao cho $s^{-1}(H) = k\mathbb{Z}$.

Vì s là toàn ánh, ta có: $H = s(s^{-1}(H)) = s(k\mathbb{Z}) = \hat{k}\ \mathbb{Z}/n\mathbb{Z}$.

◇ **Trả lời**: Các nhóm con của $(\mathbb{Z}/n\mathbb{Z}, +)$ là các $\hat{k}\ \mathbb{Z}/n\mathbb{Z}$, $k \in \mathbb{Z}$.

4.1.32 Ký hiệu a là một phần tử sinh của nhóm đơn G : $G = <\{a\}>$. Ánh xạ $\varphi : \mathbb{Z} \to G$, $n \mapsto a^n$ là một đồng cấu nhóm vì:

$$\forall (m, n) \in \mathbb{Z}^2, \quad \varphi(m + n) = a^{m+n} = a^m a^n = \varphi(m)\varphi(n).$$

Hơn nữa, φ là toàn ánh, vì $G = \{a^n ; n \in \mathbb{Z}\}$.

Trường hợp thứ 1

Nếu φ là đơn ánh, thì φ là một đẳng cấu nhóm, vậy $G \cong \mathbb{Z}$. Đặc biệt, G vô hạn.

Trường hợp thứ 2

Giả thiết φ không là đơn ánh. Vì $\mathrm{Ker}(\varphi)$ là một nhóm con của $\mathbb{Z}$ (xem 2.2, Mệnh đề 2), theo bài tập 4.1.30, tồn tại $n \in \mathbb{N}$ sao cho $\mathrm{Ker}(\varphi) = n\mathbb{Z}$.

Vì $\mathrm{Ker}(\varphi) \neq \{0\}$, ta có: $n \in \mathbb{N}^*$.

Các phần tử $e, a, a^2, \ldots, a^{n-1}$ của G khác nhau từng đôi vì, nếu $(k, l) \in \{0, \ldots, n-1\}^2$ nghiệm đúng $a^k = a^l$, thì $l - k \in \mathrm{Ker}(\varphi)$, $n \mid l - k$, vậy $l = k$.

Như thế: $G = \{e, a, a^2, \ldots, a^{n-1}\}$.

Kiểm chứng rằng ánh xạ $\psi : \begin{array}{ccc} G & \to & \mathbb{Z}/n\mathbb{Z} \\ a^k & \mapsto & \hat{k} \end{array}$ $(0 \leq k \leq n-1)$ là một đẳng cấu nhóm.

4.1.33 Trong $\mathbb{Z}/17\mathbb{Z}$:

- $\widehat{2x+3y} = \hat{0} \Leftrightarrow \hat{3}\hat{y} = -\hat{2}\hat{x} \Leftrightarrow \hat{y} = \hat{6}(-\hat{2}\hat{x}) = \hat{5}\hat{x}$, vì $\hat{6}.\hat{3} = \hat{1}$
- $\widehat{9x+5y} = \hat{0} \Leftrightarrow \hat{5}\hat{y} = -\widehat{9}\hat{x} \Leftrightarrow \hat{y} = \hat{7}(-\widehat{9}\hat{x}) = \hat{5}\hat{x}$, vì $\hat{7}.\hat{5} = \hat{1}$.

4.1.34 a) $x^2 + x + \hat{7} = 0 \Leftrightarrow x^2 + \widehat{14}x + \hat{7} = 0 \Leftrightarrow (x+\hat{7})^2 - \widehat{42} = 0 \Leftrightarrow (x+\hat{7})^2 = \hat{3}$. Ta chú ý rằng $\hat{3} = \widehat{4^2}$. Từ đó:

$$(x+\hat{7})^2 = \hat{3} \Leftrightarrow (x+\hat{7}-\hat{4})(x+\hat{7}+\hat{4}) = \hat{0} \Leftrightarrow (\hat{x} = -3 \text{ hoặc } \hat{x} = -11),$$

vì $\mathbb{Z}/13\mathbb{Z}$ là một thể (13 là số nguyên tố).

◇ **Trả lời**: $\{-\hat{3}, \hat{2}\}$.

b) $x^2 - \hat{4}x + \hat{3} = \hat{0} \Leftrightarrow (x-\hat{2})^2 = \hat{1}$.

Ta tính các bình phương trong $\mathbb{Z}/12\mathbb{Z}$:

t	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$	$\hat{6}$
t^2	$\hat{0}$	$\hat{1}$	$\hat{4}$	-3	$\hat{4}$	$\hat{1}$	$\hat{0}$

Như thế: $\forall t \in \mathbb{Z}/12\mathbb{Z}, (t^2 = \hat{1} \Leftrightarrow t \in \{-\hat{5}, -\hat{1}, \hat{1}, \hat{5}\})$.

◇ **Trả lời**: $\{-\hat{5}, -\hat{3}, \hat{1}, \hat{3}\}$.

4.1.35 Giả sử $x_1, \ldots, x_5 \in \mathbb{Z}$.

- Nếu $\hat{1}, \hat{0}, \hat{1}$ (trong $\mathbb{Z}/3\mathbb{Z}$) có mặt trong $\hat{x}_1, \ldots, \hat{x}_5$, thì ít nhất một trong các tổng của ba hạng tử là $\hat{0}$.
- Nếu không, ít nhất một trong các phần tử $-\hat{1}$, $\hat{0}$, $\hat{1}$ được lặp lại ba lần, và một trong các tổng của ba hạng tử bằng $\hat{0}$.

4.1.36 Cho $n \in \mathbb{N}^*$, $(a, b, c, d) \in \mathbb{N}^4$ sao cho $2^n = a^2 + b^2 + c^2 + d^2$. Vì a, b, c, d đóng những vai trò đối xứng, nếu cần có thể hoán vị a, b, c, d, nên tồn tại $\alpha \in \mathbb{N}$ sao cho: $2^\alpha \mid a$, $2^\alpha \mid b$, $2^\alpha \mid c$, $2^\alpha \mid d$, $2^{\alpha+1} \nmid a$, rồi tồn tại $a', b', c', d') \in \mathbb{N}^4$ sao cho: $a = 2^\alpha a'$, $b = 2^\alpha b'$, $c = 2^\alpha c'$, $d = 2^\alpha d'$.

Thế thì: $a'^2 + b'^2 + c'^2 + d'^2 = 2^{n-2\alpha}$, vậy $n - 2\alpha \geq 0$.

Trường hợp thứ 1: a', b', c', d' đều lẻ.

Thế thì (xem bài tập 4.1.1): $a'^2 \equiv 1\ [8], \ldots, d'^2 \equiv 1\ [8]$, từ đó $2^{n-2\alpha} \equiv 4\ [8]$, vậy $n - 2\alpha = 2$, rồi $a' = b' = c' = d' = 1$, $a = b = c = d = 2^\alpha$.

Trường hợp thứ 2: a', b' lẻ, c', d' chẵn (sai khác về thứ tự). Thế thì $a'^2 \underset{[4]}{\equiv} 1, b'^2 \underset{[4]}{\equiv} 1, c'^2 \underset{[4]}{\equiv} 0, d'^2 \underset{[4]}{\equiv} 0$, từ đó $2^{n-2\alpha} \equiv 2\ [4]$, $n - 2\alpha = 1$, rồi $a' = b' = 1$, $c' = d' = 0$, $a = b = 2^\alpha$, $c = d = 0$.

Trường hợp thứ 3: a' lẻ, b', c', d' chẵn. Thế thì $n - 2\alpha = 0$, $a' = 1$, $b' = c' = d' = 0$, $a = 2^\alpha$, $b = c = d = 0$.

◇ **Trả lời**:

	Các nghiệm (a, b, c, d)	Số các nghiệm
n chẵn, $n = 2\alpha + 2$, $\alpha \in \mathbb{N}$	$(2^\alpha, 2^\alpha, 2^\alpha, 2^\alpha)$, $(2^{\alpha+1}, 0, 0, 0)$ và các hoán vị của nó	5
n lẻ, $n = 2\alpha + 1$, $\alpha \in \mathbb{N}$	$(2^\alpha, 2^\alpha, 0, 0)$ và các hoán vị của nó	6

4.1.37 Chú ý rằng mọi số nguyên ≥ 1 được viết một cách duy nhất, dưới dạng $2^\alpha(2\beta + 1)$, $(\alpha, \beta) \in \mathbb{N}^2$. Vậy với mỗi i thuộc $\{0,\ldots,n\}$, tồn tại $(\alpha_i, \beta_i) \in \mathbb{N}^2$ sao cho $a_i = 2^{\alpha_i}(2\beta_i + 1)$. $n + 1$ số nguyên $\beta_0,\ldots,\beta_n$ thuộc $\{0,\ldots, n-1\}$, vốn có bản số n; vậy tồn tại $(i, j) \in \{0,\ldots, n\}^2$ sao cho $i \neq j$ và $\beta_i = \beta_j$. Thế thì ta có $(\alpha_i \leq \alpha_j$ hoặc $\alpha_j \leq \alpha_i)$, từ đó $(a_i \mid a_j$ hoặc $a_j \mid a_i)$.

4.1.38 a) Hiển nhiên.

b) • $S(2n+1) = \sum_{k=1}^{2n} \frac{\delta(k)}{k} + \frac{\delta(2n+1)}{2n+1} = S(2n) + 1$

• Tách các hạng tử có chỉ số chẵn hoặc lẻ:

$$S(2n) = \sum_{\substack{k=1 \\ k \text{ chẵn}}}^{2n} \frac{\delta(k)}{k} + \sum_{\substack{k=1 \\ k \text{ lẻ}}}^{2n} \frac{\delta(k)}{k} = \sum_{p=1}^{n} \frac{\delta(2p)}{2p} + n = \frac{1}{2}\sum_{p=1}^{n} \frac{\delta(2p)}{p} + n = \frac{1}{2}S(n) + n.$$

c) • $S(2n+1) = S(2n) + 1 \Leftrightarrow F(2n+1) + \frac{2(2n+1)}{3} = F(2n) + \frac{4n}{3} + 1$, từ đó $F(2n+1) = F(2n) + \frac{1}{3}$

• $S(2n) = \frac{1}{2}S(n) + n \Leftrightarrow F(2n) + \frac{4n}{3} = \frac{1}{2}F(n) + \frac{n}{3} + n$, từ đó $F(2n) = \frac{1}{2}F(n)$.

• $F(1) = S(1) - \frac{2}{3} = \frac{1}{3}$.

• Ta chứng minh bằng quy nạp theo n, tính chất $\mathcal{P}_n$: $\forall k \in \{1,\ldots, n\}$, $\begin{cases} 0 < F(2k) < \frac{1}{3} \\ 0 < F(2k+1) < \frac{2}{3} \end{cases}$

1) $\mathcal{P}_1$ đúng, vì $F(2) = \frac{1}{2}F(1) = \frac{1}{6}$ và $F(3) = F(2) + \frac{1}{3} = \frac{1}{2}$.

2) Nếu $\mathcal{P}_n$ đúng, thì: $\begin{cases} 0 < F(2(n+1)) = \frac{1}{2}F(n+1) < \frac{1}{2}\cdot\frac{2}{3} = \frac{1}{3} \\ 0 < F(2(n+1)) = F(2n+2) + \frac{1}{3} < \frac{1}{3} + \frac{1}{3} = \frac{2}{3}. \end{cases}$

4.2.1 a) $\forall d \in \mathbb{N}^*$, $\left(\begin{cases} d \mid n^2 + n \\ d \mid 2n+1 \end{cases} \Rightarrow d \mid (2n+1)^2 - 4(n^2+n) = 1 \Rightarrow d = 1 \right)$.

b) Bảng thuật toán Euclide:

	n	n	n
n^4+3n^2+1	n^3+2n	n^2+1	n
n^2+1	n	1	

c) $\forall d \in \mathbb{N}^*$, $\left(\begin{cases} d \mid n^2+1 \\ d \mid (n+1)^2+1 \end{cases} \Rightarrow \begin{cases} d \mid n^2+1 \\ d \mid 2n+1 \end{cases} \Rightarrow \begin{cases} d \mid (2n+1)^2-4(n^2+1)=4n-3 \\ d \mid 2n+1 \end{cases} \right.$

$\left. \Rightarrow d \mid 2(2n+1)-(4n-3)=5 \right).$

4.2.2 Ta ký hiệu, với $n \in \mathbb{N}^*$, $u_n = 16^n + 10^n - 1$, $v_n = u_n + 1 = 16^n + 10^n$, và $\delta = \text{UCLN}\{u_n ; n \in \mathbb{N}^*\}$.

1) Dãy $(v_n)_{n\in\mathbb{N}^*}$ là một dãy truy hồi tuyến tính cấp hai với hệ tử hằng (xem Tập 1, 3.4.2) mà phương trình đặc trưng có nghiệm là 16 và 10; vậy ta có:

$$\forall n \in \mathbb{N}^*, \quad v_{n+2} - (16+10)v_{n+1} + 16.10v_n = 0,$$

từ đó: $\forall n \in \mathbb{N}^*$, $u_{n+2} = 26u_{n+1} - 160u_n - 135$.

Vì $(\delta \mid u_n, \delta \mid u_{n+1}, \delta \mid u_{n+2})$, ta suy ra $\delta \mid 135$. Mặt khác, $\delta + u_1 = 25$.

Từ đó: $\delta \mid 135 \wedge 25 = 5$.

2) $\forall n \in \mathbb{N}^*$, $u_n \underset{[5]}{\equiv} 1^n + 0^n - 1 = 0$.

◇ **Trả lời**: 5.

4.2.3 a) Cộng vế với vế $\begin{cases} r_0 = r_1 q_1 + r_2 \\ \vdots \\ r_{n-2} = r_{n-1} q_{n-1} + r_n \\ r_{n-1} = r_n q_n \end{cases}$, ta được $\sum_{i=0}^{n-1} r_i = \sum_{i=1}^{n} r_i q_i + \sum_{i=2}^{n} r_i$,

từ đó: $\sum_{i=1}^{n} r_i q_i = r_0 + r_1 - r_n = a + b - a \wedge b$.

b) Cộng vế với vế $\begin{cases} r_0 r_1 = r_1^2 q_1 + r_1 r_2 \\ \vdots \\ r_{n-2} r_{n-1} = r_{n-1}^2 q_{n-1} + r_{n-1} r_n \\ r_{n-1} r_n = r_n^2 q_n \end{cases}$, ta được $\sum_{i=0}^{n-1} r_i r_{i+1} = \sum_{i=1}^{n} r_i^2 q_i + \sum_{i=2}^{n-1} r_i r_{i+1}$,

từ đó: $\sum_{i=1}^{n} r_i^2 q_i = r_0 r_1 = ab$.

4.2.4 a) Tập hợp $\{n \in \mathbb{N}^* ; x^n = e\}$ là một bộ phận khác rỗng của $\mathbb{N}^*$, vậy có một phần tử bé nhất, ký hiệu $\omega(x)$.

b) α) • Vì G hữu hạn, nên các phần tử x^n ($n \in \mathbb{N}$) không khác nhau từng đôi. Vậy tồn tại $(k, l) \in \mathbb{N}^*$ sao cho: $k < l$ và $x^k = x^l$.

Ký hiệu $n = l - k$, ta có: $n \in \mathbb{N}^*$ và $x^n = e$, vậy x có cấp hữu hạn.

• Cho $p \in \mathbb{N}$; theo phép chia Euclide p cho $\omega(x)$, tồn tại $(q, r) \in \mathbb{N}^2$ sao cho: $p = q\omega(x) + r$ và $0 \leq r < \omega(x)$, từ đó $x^n = (x^{\omega(x)})^q x^r = x^r$.

Mặt khác, theo định nghĩa của $\omega(x)$, ta suy ra rằng $e, x, x^2, ..., x^{\omega(x)-1}$ khác nhau từng đôi.

Như thế: $< x > = \{e, x, ..., x^{\omega(x)-1}\}$.

Theo định lý Lagrange (C 2.1), $\text{Card}(< x >) \mid \text{Card}(G)$, vậy $\omega(x) \mid \text{Card}(G)$.

β) ◇ **Trả lời**: Tồn tại các nhóm vô hạn mà mọi phần tử đều có cấp hữu hạn, chẳng hạn $((\mathbb{Z}/_{2\mathbb{Z}})[X], +)$, nhóm cộng các đa thức một ẩn và lấy các hệ tử trong thể $\mathbb{Z}/_{2\mathbb{Z}}$ (xem dưới đây, chương 5).

c) Cũng phương pháp như trong lời giải *b)* α).

d) α) • Ta ký hiệu $\mu = \omega(x) \vee \omega(y)$. Vì $\omega(x) \mid \mu$, ta có $x^\mu = y^\mu = 1$ (xem *c)*), từ đó $(xy)^\mu = x^\mu y^\mu = e$, vì x và y giao hoán.

Như thế, xy có cấp hữu hạn và $\omega(xy) \mid \mu$ (xem c)).

• Chọn $G = (\mathbb{Z}/2\mathbb{Z}, +)$, $x = y = \hat{1}$, ta có: $\omega(x) = 2$, $\omega(y) = 2$, $x + y = y + x$, $\omega(x + y) = 1 \neq \omega(x) \vee \omega(y)$.

◇ **Trả lời**: Không.

β) ◇ **Trả lời**: Ta có thể chọn G là nhóm các đẳng cự vectơ của mặt phẳng Euclide (luật là ∘), x và y là hai phần tử đối xứng đối với hai đường thẳng vectơ D, Δ sao cho $(\widehat{D, \Delta}) = \alpha$, trong đó $\alpha \in \mathbb{R}$ sao cho $\alpha \notin \pi\mathbb{Q}$, chẳng hạn $\alpha = 1$ (biết rằng π vô tỷ), hoặc $\alpha = \pi\sqrt{2}$ (biết rằng $\sqrt{2}$ vô tỷ).

4.2.5 1) Rõ ràng rằng, với mọi chu trình c thuộc $\mathfrak{S}_n$, khi ký hiệu $\gamma(c)$ là bản số của giá của c, ta có:

• c có cấp $\gamma(c)$

• $\varepsilon(c) = (-1)^{\gamma(c)-1}$.

2) **Phương pháp thứ 1**: $(\varepsilon(\sigma))^N = \varepsilon(\sigma^N) = \varepsilon(c) = 1$ và N lẻ, vậy $\varepsilon(\sigma) = 1$.

Phương pháp thứ 2: Theo 3.4.3, Định lý, σ có một dạng phân tích $\sigma = c_1 \circ ... \circ c_\nu$ thành tích các chu trình với giá rời nhau từng đôi. Vì $c_1, ..., c_\nu$ giao hoán từng đôi, ta có: $\sigma^N = c_1^N \circ ... \circ c_\nu^N$, từ đó, theo tính duy nhất của phép phân tích e thành tích những chu trình với giá rời nhau từng đôi:

$$\forall k \in \{1, ..., \nu\},\ c_k^N = e.$$

Thế thì ta có (xem bài tập 4.2.4 *c)*): $\forall k \in \{1, ..., \nu\},\ \gamma(c_k) \mid N$.

Vì N lẻ, kết quả là các $\gamma(c_k)$ đều lẻ, rồi thì các c_k đều chẵn.

Cuối cùng, $\sigma = c_1 \circ ... \circ c_N$ chẵn.

4.2.6 Vì $c_1, ..., c_\nu$ giao hoán từng đôi: $\forall p \in \mathbb{N}^*,\ \sigma^p = c_1^p \circ ... \circ c_\nu^p$.

Do tính duy nhất của phép phân tích e thành tích những chu trình với giá rời nhau từng đôi, ta có, với mọi p thuộc $\mathbb{N}^*$:

$$\sigma^p = e \Leftrightarrow c_1^p = ... = c_\nu^p = e \Leftrightarrow (\forall k \in \{1, ..., \nu\},\ \omega(c_k) \mid p) \Leftrightarrow \text{BCNN}((\omega(c_k))_{1 \leq k \leq \nu}) \mid p).$$

Ví dụ: $\sigma = (1, 7, 3) \circ (2, 8, 10, 11) \circ (4, 6, 12)$, $\omega(\sigma) = \text{BCNN}(3, 4, 3) = 12$.

◇ **Trả lời**: 12.

4.3.1 Theo bài tập 4.1.1 : $n^2 \equiv 1\ [8]$.

Mặt khác: $n \not\equiv 0\ [3] \Rightarrow n \equiv -1$ hoặc $1\ [3] \Rightarrow n^2 \equiv 1\ [3]$.

Vì $3 \wedge 8 = 1$: $\begin{cases} 3 \mid n^2 - 1 \\ 8 \mid n^2 - 1 \end{cases} \Rightarrow 24 \mid n^2 - 1$.

4.3.2 Giả sử $(x, y) \in (\mathbb{N}^*)^2$, $\delta = x \wedge y$; tồn tại $(x', y') \in (\mathbb{N}^*)^2$ sao cho $x = \delta x'$, $y = \delta y'$, $x' \wedge y' = 1$; ta có: $x \vee y = \delta x'y'$ (xem 4.3.3, Mệnh đề 4).

a) $\begin{cases} x \wedge y = 18 \\ x \vee y = 540 \end{cases} \Rightarrow \begin{cases} \delta = 18 \\ x'y' = 30 \end{cases}$

◇ **Trả lời**: {(18, 540), (36, 270), (54, 180), (90, 108) và các cặp đảo ngược}.

b) $\begin{cases} x \vee y - x \wedge y = 534 \\ x \vee y - 5(x \wedge y) = 510 \end{cases} \Rightarrow \begin{cases} x \wedge y = 6 \\ x \vee y = 540 \end{cases}$ và kết thúc như ở a).

◇ **Trả lời**: {(6, 540), (12, 270), (30, 108), (54, 60) và các cặp đảo ngược}.

c) $x \vee y - 3(x \wedge y) = 135 \Leftrightarrow \delta(x'y' - 3) = 135$. Do các vai trò đối xứng của x' và y', ta có thể giả thiết $x' \leq y'$. Các ước của 135 (trong $\mathbb{N}^*$) là: 1, 3, 5, 9, 15, 27, 45, 135.

	$\begin{cases}\delta = 1 \\ x'y' = 138\end{cases}$	$\begin{cases}\delta = 3 \\ x'y' = 48\end{cases}$	$\begin{cases}\delta = 5 \\ x'y' = 30\end{cases}$	$\begin{cases}\delta = 9 \\ x'y' = 18\end{cases}$	$\begin{cases}\delta = 15 \\ x'y' = 12\end{cases}$	$\begin{cases}\delta = 27 \\ x'y' = 8\end{cases}$	$\begin{cases}\delta = 45 \\ x'y' = 6\end{cases}$	$\begin{cases}\delta = 135 \\ x'y' = 4\end{cases}$
x'	1 2 3 6	1 3	1 2 3 5	1 2	1 3	1	1 2	1
y'	138 69 46 23	48 16	30 15 10 6	18 9	12 4	8	6 3	4

◇ **Trả lời**: {(1, 138), (2, 69), (3, 46), (3, 144), (5, 150), (6, 23), (9, 48), (9, 162), (10, 75), (15, 50), (15, 180), (18, 81), (25, 30), (27, 216), (45, 60), (45, 270), (90, 135), (135, 540), và các cặp đảo ngược}.

d) $\begin{cases} x + y = 1008 \\ x \wedge y = 24 \end{cases} \Rightarrow \begin{cases} \delta = 24 \\ x' + y' = 42 \end{cases}$

x'	1	5	11	13	17	19
y'	41	37	31	29	25	23

◇ **Trả lời**: {(24, 984), (120, 888), (264, 744), (312, 696), (408, 600), (456, 552), và các cặp đảo ngược}.

e) $\delta^2 \mid 19476 \Rightarrow \delta \in \{1, 2, 3, 6\}$.

Với mỗi trị của δ, giải $\begin{cases} x'^2 + y'^2 = \dfrac{19476}{\delta^2} \\ x'y' = \dfrac{1260}{\delta} \end{cases}$, bằng cách tính $(x' + y')^2$.

◇ **Trả lời**: {(60, 126), (126, 60)}.

f) $x \wedge y + x \vee y = 9 + y \Leftrightarrow \delta(1 + x'y' - y') = 9 \Rightarrow \delta \mid 9 \Rightarrow \delta \in \{1, 3, 9\}$.

Với mỗi trị của δ, giải $(x' - 1)y' = \dfrac{9}{\delta} - 1$.

◇ **Trả lời**: $\{(3, 4), (5, 2), (9, 1), (9, 3)\} \cup \{(9, 9\lambda);\ \lambda \in \mathbb{N}^*\}$.

4.3.3 a) Áp dụng, chẳng hạn, thuật toán Euclide.

b) Như ở 4.3.2, ta tính một cặp (u_0, v_0) thích hợp: (28, -25).

• Nếu (u, v) thích hợp, thì $442u + 495v = 1 = 442u_0 + 495v_0$, từ đó $442(u - u_0) = -495(v - v_0)$.

Vì $442 \wedge 495 = 1$, định lý Gauss chứng tỏ: $442 \mid v - v_0$. Tồn tại $k \in \mathbb{Z}$ sao cho $v = 442k + v_0$, rồi $u = -495k + u_0$.

• Khẳng định đảo là hiển nhiên.

◇ **Trả lời**: $\{(28 - 495k, -25 + 442k);\ k \in \mathbb{Z}\}$.

c) $\hat{1} = \widehat{442} \cdot \widehat{28} + \widehat{495} \cdot (\widehat{-25}) = \widehat{442} \cdot \widehat{28}$ vậy 442 khả nghịch và có nghịch đảo là $\widehat{28}$.
Thế thì: $\widehat{442}x = \widehat{314} \Leftrightarrow x = \widehat{28} \cdot \widehat{314}$.
◇ **Trả lời:** $\{\widehat{377}\}$.

4.3.4 Trước tiên, phép giải trong $\mathbb{Z}$ cho:

$$\{(x, y) \in \mathbb{Z}^2;\ 2x + 3y = n\} = \{(-n + 3z, n - 2z);\ z \in \mathbb{Z}\}.$$

Giả sử $z \in \mathbb{Z}$; ta có: $\begin{cases} -n+3z \geq 0 \\ n-2z \geq 0 \end{cases} \Leftrightarrow \frac{n}{3} \leq z \leq \frac{n}{2}$.

Vì ánh xạ $z \mapsto (-n + 3z, n - 2z)$ là đơn ánh, ta suy ra:

$$\text{Card}\{(x, y) \in \mathbb{N}^2;\ 2x + 3y = n\} = \text{Card}\left\{z \in \mathbf{Z};\ \frac{n}{3} \leq z \leq \frac{n}{2}\right\}.$$

Tách thành những trường hợp modulo 6 của n.

◇ **Trả lời:** $\mathrm{E}\left(\frac{n}{6}\right)$ nếu $n \equiv 1\,[6]$, $1 + \mathrm{E}\left(\frac{n}{6}\right)$ nếu trái lại.

4.3.5 Giả sử $\delta = a \wedge b$; tồn tại $(a', b') \in (\mathbb{Z}^*)^2$ sao cho: $a = \delta a'$, $b = \delta b'$, $a' \wedge b' = 1$.

Ta ký hiệu $S = \{(x, y) \in (\mathbb{Z}^*)^2;\ ax + by = c\}$.

Nếu $\delta \nmid c$, thì $S = \varnothing$.

Giả thiết $\delta \mid c$; tồn tại $c' \in \mathbb{Z}$ sao cho $c = \delta c'$.

• Cho $(x, y) \in \mathbb{Z}^2$ sao cho $ax + by = c$. Thế thì ta có: $a'x + b'y = c'$. Theo định lý Bezout vì $a' \wedge b' = 1$ nên tồn tại $(u, v) \in \mathbb{Z}^2$ sao cho $a'u + b'v = 1$. Từ đó: $a'(x - c'u) = b'(c'v - y)$.

Vì $a' \wedge b' = 1$, định lý Gauss chứng tỏ rằng $a' \mid c'v - y$. Vậy tồn tại $k \in \mathbb{Z}$ sao cho $c'v - y = ka'$, rồi thì $x - c'u = kb'$.

• Ngược lại, ta chứng minh dễ dàng rằng, với mọi k thuộc $\mathbb{Z}$, cặp $(c'u + kb', c'v - ka')$ thích hợp.

◇ **Trả lời:** • $\varnothing$ nếu $a \wedge b \nmid c$

• $\{(c'u + kb', c'v - ka');\ k \in \mathbb{Z}\}$ nếu $a \wedge b \mid c$, trong đó a', b', c' được xác định bởi: $\delta = a \wedge b$, $a = \delta a'$, $b = \delta b'$, $c = \delta c'$, và $(u, v) \in \mathbb{Z}^2$ sao cho $a'u + b'v = 1$.

Ví dụ: a) $\varnothing$; b) $\{5k + 12, -3k - 6);\ k \in \mathbb{Z}\}$.

4.3.6 1) **Tồn tại**

Theo 4.3.2, Mệnh đề, tồn tại $(u, v) \in \mathbb{Z}^2$ sao cho: $au + bv = 1$, $|u| < b$, $v \neq a$.

Trước tiên rõ ràng rằng u và v đều khác không, và $|v| \neq a$.

Nếu $u < 0$, ta ký hiệu $(u', v') = (u + b, v - a)$; ta có:

$$\begin{cases} au'+bv' = au+bv = 1 \\ 1 \leq u' < b \\ |bv'| = |1 - au'| \leq 1 + au' \leq 1 + ab < (a+1)b, \text{ vậy } |v'| \leq a. \end{cases}$$

Điều này chứng tỏ rằng, nếu cần thiết thì ta thay (u, v) bởi $(u + b, v - a)$, ta có thể quy về:

$$au + bv = 1,\ 1 \leq u \leq b - 1,\ 1 \leq -v \leq a - 1.$$

a) Trường hợp $0 \leq u \leq \mathrm{E}\left(\frac{b}{2}\right)$.

Khi đó $b(-v) = au - 1 < au < a\frac{b}{2}$, vậy $-v < \frac{a}{2}$, và cặp $(x,y) = (u,v)$ thích hợp.

b) Trường hợp $E\left(\frac{b}{2}\right)+1 \le u \le b-1$

Ta ký hiệu $x = u - b$, $y = v + a$. Thế thì:

- $ax + by = au + bv = 1$
- $|x| = -x = b - E\left(\frac{b}{2}\right) - 1 < \frac{b}{2}$
- $by = 1 - ax = 1 + a(-x) \le 1 + \frac{ab}{2}$, vậy $y < \frac{1}{b} + \frac{a}{2} < 1 + \frac{a}{2}$. Nếu $y = \frac{a}{2}$, thì $a(2x + y) = 2$, mâu thuẫn (vì $a \ge 3$); từ đó $y < \frac{a}{2}$.

2) Duy nhất

Giả sử (x, y), (x', y') thích hợp. Thế thì ta có $a(x - x') = b(y' - y)$, từ đó, vì $a \wedge b = 1$, $a \mid y' - y$.

Nhưng mặt khác: $|y' - y| \le |y'| + |y| < \frac{a}{2} + \frac{a}{2} = a$. Ta suy ra $y' - y = 0$, rồi $x' - x = 0$.

4.3.7 Cùng kiểu suy luận như đối với bài tập 4.3.6.

4.3.8 Ta ký hiệu $u_n = (n^2 - 1)(n^2 - 9)(n^2 - 49)$, và chú ý rằng: $23040 = 2^9.3^2.5$.

1) Modulo 5

$n^2 \equiv 1$ hoặc -1 [5], vậy $5 \mid n^2 - 1$ hoặc $5 \mid n^2 - 9$, từ đó $5 \mid u_n$.

2) Modulo 9

n	0	1	2	3	4
n^2	0	1	4	0	-2

Nếu $n^2 \equiv 0$ hoặc 1 hoặc 4, thì $9 \mid n^2 - 9$ hoặc $9 \mid n^2 - 1$ hoặc $9 \mid n^2 - 49$, vậy $9 \mid u_n$.

Nếu $n^2 \equiv -2$ [9], thì $n^2 - 1 \equiv 0$ [3] và $n^2 - 49 \equiv 0$ [3], vậy $9 \mid u_n$.

3) Modulo 2^9

Theo bài tập 4.1.1, $n^2 \equiv 1$ [8], vậy $8 \mid n^2 - 1$, $8 \mid n^2 - 9$, $8 \mid n^2 - 49$, từ đó $2^9 = 8^3 \mid u_n$.

Cuối cùng, vì 5, 9, 2^9 nguyên tố cùng nhau đôi một, ta kết luận: $23040 \mid u_n$.

4.3.9 Giả thiết tồn tại $(x, y, z, t) \in \mathbb{Z}^4$ thích hợp.

Ký hiệu δ = ƯCLN(x, y, z, t), tồn tại $(X, Y, Z, T) \in (\mathbb{Z}^*)^4$ sao cho: $x = \delta X$,..., $t = \delta T$, ƯCLN$(X, Y, Z, T) = 1$, và $X^2 + 10Y^2 = Z^2$, $10X^2 + Y^2 = T^2$.

Trường hợp thứ 1: X lẻ

Thế thì Z lẻ, $Z - X$ và $Z + X$ đều chẵn, $4 \mid Z^2 - X^2 = 10Y^2$, $2 \mid Y$; rồi thì T^2 chẵn, T chẵn. Nhưng thế thì, modulo 4: $X^2 \equiv 1$, $Y^2 \equiv 0$, $T^2 \equiv 0$; điều này mâu thuẫn với : $10X^2 + Y^2 = T^2$.

Trương hợp thứ 2: X chẵn

Khi đó Z chẵn. Nếu Y chẵn, thì T chẵn, mâu thuẫn. Vậy Y và T đều lẻ. Nhưng khi đó, modulo 4: $X^2 \equiv 0$, $Y^2 \equiv 1$, $T^2 \equiv 1$; điều này mâu thuẫn với $X^2 + 10Y^2 = Z^2$.

4.3.10 $(n+1)C_{2n}^{n+1} = nC_{2n}^{n}$ và $(n+1) \wedge n = 1$, vậy $(n+1) \mid C_{2n}^{n}$.

4.3.11 a) Ta ký hiệu $\delta = a \wedge b$, $(a', b') \in (\mathbb{Z}^*)^2$ sao cho: $a = \delta a'$, $b = \delta b'$, $a' \wedge b' = 1$. Ta có: $a^2 \wedge b^2 = \delta^2(a'^2 \wedge b'^2) = \delta^2$. Nếu $a^2 \mid b^2$, thì $a^2 \wedge b^2 = a^2$, từ đó $\delta^2 = a^2$, $\delta = |a|$, $a \mid b$.

b) Cho $\alpha \in \mathbb{Q}^*$; tồn tại $(a, b) \in (\mathbb{Z}^*)^2$ sao cho $\alpha = \dfrac{b}{a}$. Theo a):

$$\alpha^2 \in \mathbb{Z} \Leftrightarrow a^2 \mid b^2 \Rightarrow a \mid b \Leftrightarrow \alpha \in \mathbb{Z}.$$

c) Bằng cách khai triển, ta quy về (nếu $y \neq 0$) : $\quad 2y^2 + (x^2 - 3x)y + 3x^2 + x = 0 \qquad (1)$

Chứng minh: $(1) \Leftrightarrow (4y + (x^2 - 3x))^2 = x(x + 1)^2(x - 8)$. Khảo sát các trường hợp $x = -1, 0, 8$.

Bây giờ ta giả thiết $x \neq -1, 0, 8$. Theo a), $x + 1$ chia hết $4y + (x^2 - 3x)$.

Suy ra tồn tại $\lambda \in \mathbb{N}^*$ sao cho $x(x - 8) = \lambda^2$.

Thế thì: $(x - 4)^2 = 16 + \lambda^2$, vậy $|x - 4| \geq \lambda + 1$, rồi: $16 + \lambda^2 \geq (\lambda + 1)^2$, suy ra $\lambda \leq 7$.

Thử các trị 0,..., 7 của λ trong hệ thức $(x - 4)^2 = 16 + \lambda^2$. Ta suy ra $x = 9$.

◇ **Trả lời**: $(\mathbb{Z} \times \{0\}) \cup \{(-1, -1), (8, -10), (9, -6), (9, -21)\}$.

4.3.12 Ta ký hiệu $d = a \wedge c$, $\delta = b \wedge c$; tồn tại $a', c', b'', c'' \in \mathbb{Z}^*$ sao cho:

$$\begin{cases} a = da', c = dc', a' \wedge c' = 1 \\ b = \delta b'', c = \delta c'', b'' \wedge c'' = 1 \end{cases}$$

Ta có $dc' \mid da'\delta b''$, từ đó $c' \mid a'\delta b''$. Vì $c' \wedge a' = 1$, ta suy ra (định lý Gauss): $c' \mid \delta b''$. Rồi: $\delta c'' = c = dc' \mid d\delta b''$, từ đó $c'' \mid db''$. Vì $c'' \wedge b'' = 1$, ta suy ra $c'' \mid d$, và cuối cùng: $c = \delta c'' \mid \delta d$.

4.3.13 Vì $\dfrac{a^n - b^n}{a - b} = \sum_{k=0}^{n-1} a^k b^{n-1-k} \equiv na^{n-1} [a - b]$,

ta có: $\left(\dfrac{a^n - b^n}{a - b}\right) \wedge (a - b) = (na^{n-1}) \wedge (a - b)$.

Ta ký hiệu $\delta = a \wedge b$.

1) Với ước d bất kỳ của $(n\delta^{n-1}) \wedge (a - b)$, vì $\delta \mid a$, ta suy ra: $d \mid (na^{n-1}) \wedge (a - b)$.

2) Ngược lại, giả sử $d \in \mathbb{N}^*$ sao cho $d \mid (na^{n-1}) \wedge (a - b)$. Vậy ta có: $a \equiv b\ [d]$ và $na^{n-1} \equiv 0\ [d]$.

Mặt khác, tồn tại $(u, v) \in \mathbb{Z}^2$ sao cho $\delta = ua + vb$. Ta suy ra $\delta \equiv (u + v)a\ [d]$, rồi $n\delta^{n-1} \equiv n(u + v)^{n-1}a^{n-1} \equiv 0\ [d]$. Vậy $d \mid (n\delta^{n-1}) \wedge (a - b)$.

Cuối cùng: $(na^{n-1}) \wedge a - b = (n\delta^{n-1}) \wedge (a - b)$.

4.3.14 1) Các không điểm thực của tam thức $6X^2 + 5X + 1$ là $-\dfrac{1}{2}$ và $-\dfrac{1}{3}$. Vậy phương trình $6x^2 + 5x + 1 = 0$ không có nghiệm trong $\mathbb{Z}$.

2) Cho $n \in \mathbb{N}^*$; tồn tại $(k, m) \in \mathbb{N}^2$ sao cho $n = 2^k(2m + 1)$.

Vì $3 \wedge 2^k = 1$, nên 3 có một nghịch đảo modulo 2^k, ký hiệu α: $\quad 3\alpha \equiv 1[2^k]$. Thế thì:

$$\forall x \in \mathbb{Z},\ (3x + 1 \equiv 0\ [2^k] \Leftrightarrow x \equiv -\alpha\ [2^k]).$$

Tương tự, vì $2 \wedge (2m + 1) = 1$, nên 2 có một nghịch đảo modulo $2m + 1$, ký hiệu β: $2\beta \equiv 1\ [2m + 1]$

Thế thì: $\quad \forall x \in \mathbb{Z},\quad (2x + 1 \equiv 0\ [2m + 1] \Leftrightarrow x \equiv -\beta\ [2m + 1])$.

Mặt khác, $2^k \wedge (2m + 1) = 1$, vậy tồn tại $(u, v) \in \mathbb{Z}^2$ sao cho $2^k u + (2m + 1)v = 1$. Thế thì ta có: $\alpha - \beta = (\alpha - \beta)(2^k u + (2m + 1)v)$, từ đó, với ký hiệu $\xi = -\alpha + (\alpha - \beta)2^k u = -\beta + (\beta - \alpha)(2m + 1)v$, ta có :

$$\begin{cases} \xi \equiv -\alpha\ [2^k] \\ \xi \equiv -\beta\ [2m + 1] \end{cases}, \text{ từ đó } \begin{cases} 3\xi + 1 \equiv 0[2^k] \\ 2\xi + 1 \equiv 0[2m + 1] \end{cases},$$

vậy $\quad 6\xi^2 + 5\xi + 1 \equiv 0\ [n]$.

Ta có thể chú ý rằng, theo định lý (cổ) Trung Hoa (bài tập 4.3.16), hệ đồng dư thức $\begin{cases} x \equiv -\alpha\,[2^k] \\ x \equiv -\beta\,[2m+1] \end{cases}$ có ít nhất một nghiệm, vì $2^k \wedge (2m+1) = 1$.

4.3.15 Ký hiệu $E_i = \{1,..., n\} - \{i\}$, với $i \in \{1,..., n\}$, ta có:

$$\text{ƯCLN}(A_1,...,A_n) = \prod_{k \in \bigcap_{i=1}^{n} E_i} a_k = \prod_{k \in \varnothing} a_k = 1.$$

4.3.16 a) Ta ký hiệu với $i \in \{1,..., n\}$, $A_i = \dfrac{a}{a_i}$. Giả sử $i \in \{1,..., n\}$; vì $A_i \wedge a_i = 1$, theo định lý Bezout tồn tại $c_i \in \mathbb{Z}$ sao cho: $A_i c_i \equiv 1\ [a_i]$.

Ta ký hiệu $x = \sum_{i=1}^{n} A_i b_i c_i$. Ta có: $\forall i \in \{1,... , n\}, x \equiv A_i b_i c_i \equiv b_i\,[a_i]$.

Ví dụ

Trên một ví dụ tương tự ta sẽ không áp dụng phép chứng minh trên.

Giả thiết x thích hợp.

Vì $x \equiv 4\ [5]$, tồn tại $\lambda \in \mathbb{Z}$ sao cho: $x = 5\lambda + 4$.

Ta có: $x \equiv 3\ [6] \Leftrightarrow 5\lambda \equiv -1\ [6] \Leftrightarrow -\lambda \equiv -1\ [6] \Leftrightarrow \lambda \equiv 1\ [6]$.

Vậy tồn tại $\mu \in \mathbb{Z}$ sao cho $\lambda = 6\mu + 1$, từ đó $x = 30\mu + 9$. Thế thì:

$$x \equiv 2\ [7] \Leftrightarrow 30\mu \equiv -7\ [7] \Leftrightarrow 2\mu \equiv 0\ [7] \Leftrightarrow \mu \equiv 0\ [7],$$

vì 2 khả nghịch modulo 7.

Vậy tồn tại $\nu \in \mathbb{Z}$ sao cho $\mu = 7\nu$; từ đó $x = 210\nu + 9$.

Khẳng định đảo thấy ngay.

◇ **Trả lời**: $\{210\nu + 9;\ \nu = \in \mathbb{Z}\}$.

b) Giả sử $\xi \in \mathbb{Z}/_{a\mathbb{Z}}$. Tồn tại $x \in \mathbb{Z}$ sao cho $\xi = \text{cl}_a(x)$; ta đặt $\theta(\xi) = (\text{cl}_{a_1}(x),...,\text{cl}_{a_n}(x))$.

Định nghĩa này là đúng đắn bởi vì, với mọi (x, y) thuộc $\mathbb{Z}^2$:

$\text{cl}_a(x) = \text{cl}_a(y) \Rightarrow a \mid x - y \Rightarrow (\forall i \in \{1,...,n\}, a_i \mid x - y) \Rightarrow (\forall i \in \{1,...,n\}, \text{cl}_{a_i}(x) = \text{cl}_{a_i}(y))$

- θ là một đồng cấu nhóm, bởi vì với mọi (x,y) thuộc $\mathbb{Z}^2$:

$$\theta(\text{cl}_a(x) + \text{cl}_a(y)) = \theta(\text{cl}_a(x + y)) = (\text{cl}_{a_1}(x + y),..., \text{cl}_{a_n}(x + y))$$
$$= (\text{cl}_{a_1}(x) + \text{cl}_{a_1}(y), ..., \text{cl}_{a_n}(x) + \text{cl}_{a_n}(y)) = \theta(\text{cl}_a(x)) + \theta(\text{cl}_a(y)).$$

- θ là đơn ánh vì, với mọi x thuộc $\mathbb{Z}$:

$$\theta(\text{cl}_a(x)) = 0 \Rightarrow \text{cl}_{a_1}(x) = ... = \text{cl}_{a_n}(x) = 0 \Rightarrow (\forall i \in \{1,..., n\}, a_i \mid x) \Rightarrow \text{cl}_a(x) = 0.$$

- Tính toàn ánh của θ

Phương pháp thứ 1

Giả sử $(\xi_1, ..., \xi_n) \in \mathbb{Z}/_{a_1\mathbb{Z}} \times ... \times \mathbb{Z}/_{a_n\mathbb{Z}}$.

Tồn tại $(b_1, ..., b_n) \in \mathbb{Z}^n$ sao cho : $\forall i \in \{1, ..., n\}, \xi_i = \text{cl}_{a_i}(b_i)$.

Theo a), tồn tại $\beta \in \mathbb{Z}$ sao cho : $\forall i \in \{1, ..., n\}, \beta_i \equiv b_i(a_i)$.

Thế thì ta có : $\theta(\text{cl}_a(\beta)) = (\text{cl}_{a_i}(\beta),..., \text{cl}_{a_n}(\beta)) = \text{cl}_{a_1}(b_1)),..., \text{cl}_{a_n}(b_n) = (\xi_1,...,\xi_n)$.

Phương pháp thứ hai

Vì θ là đơn ánh và vì $\mathbb{Z}/_{a\mathbb{Z}}$ và $\mathbb{Z}/_{a_1\mathbb{Z}} \times ... \times \mathbb{Z}/_{a_n\mathbb{Z}}$ đều hữu hạn và có cùng một bản số; nên θ là song ánh. Điều này cũng chứng tỏ rằng có thể suy ra định lý Trung Hoa chỉ từ tính đơn ánh của θ.

4.3.17 Thay x bởi $\frac{y-a}{2}$, suy ra: $(3y)^2 = 3(4b - a)^2$. Vì $3(4b - a^2) \in \mathbb{Z}$, theo bài tập 4.3.11, *b*), ta có: $3y \in \mathbb{Z}$. Ký hiệu $Y = 3y$: $Y^2 = 3(4b - a^2)$, vậy $3 \mid Y$, do đó $y \in \mathbb{Z}$.

Cuối cùng, vì $3y^2 = 4b - a^2$, nên y và a đều cùng tính chẵn lẻ, vậy $x = \frac{y-a}{2} \in \mathbb{Z}$.

4.3.18 Vì $(bc - ad)^2 = (bc + ad)^2 - 4(ac)(bd)$, ta suy ra $n^2 \mid (bc - ad)^2$, rồi $n \mid bc - ad$, xem bài tập 4.3.11, *a*).

Tồn tại $(\lambda, \mu) \in \mathbb{Z}^2$ sao cho $bc + ad = \lambda n$ và $bc - ad = \mu n$, từ đó, với ký hiệu $\alpha = \lambda + \mu$ và $\beta = \lambda - \mu$, ta có: $2bc = \alpha n$ và $2ad = \beta n$. Mặt khác, tồn tại $(\gamma, \delta) \in \mathbb{Z}^2$ sao cho: $ac = \gamma n$ và $bd = \delta n$.

Ta suy ra: $\alpha\beta n^2 = 4abcd = 4\gamma\delta n^2$, từ đó $4 \mid \alpha\beta$.

Hơn nữa, α và β đều cùng tính chẵn lẻ, vì $\alpha + \beta = 2\lambda$.

Suy ra rằng α và β đều chẵn, và cuối cùng: $n \mid bc$ và $n \mid ad$.

4.3.19 Giả sử (x, y, z) thích hợp, $(\alpha, \beta, \gamma) \in \mathbb{N}^3$ sao cho: $xy = 1 + \alpha z$, $xz = 1 + \beta y$, $yz = 1 + \gamma x$.

Ta có: $(xy - 1)x = \alpha z x = \alpha(1 + \beta y)$, từ đó, với ký hiệu $\lambda = x^2 - \alpha\beta$ ta có: $\lambda y = x + \alpha$ và $\lambda \in \mathbb{N}^*$.

Tương tự, tồn tại $\mu \in \mathbb{N}^*$ sao cho: $\mu x = y + \alpha$.

Ta có: $y + \alpha = \mu x = \mu(\lambda y - \alpha)$, từ đó: $(\lambda\mu - 1)y = (1 + \mu)\alpha$.

Nhưng, vì $xy = 1 + \alpha y$, $y \wedge \alpha = 1$, nên $y \mid 1 + \mu$. Tồn tại $k \in \mathbb{N}^*$ sao cho $1 + \mu = ky$.

Thế thì: $x + y + \alpha = x + \mu x = kxy$, rồi $xz + yz + \alpha z = kxyz$, vậy:

$$xy + xz + yz - 1 = kxyz.$$

- $3yz > xy + xz + yz - 1 = kxyz \geq xyz$, từ đó $x < 3$, $x = 2$. Ta suy ra: $2y + 2z - 1 = (2k - 1)yz$.
- $4z > 2y + 2z - 1 = (2k - 1)yz \geq yz$, từ đó $y < 4$. Vì $x \wedge y = 1$, ta suy ra $y = 3$.
- $5 + 2z = 3(2k - 1)z$, từ đó $z \mid 5$. Vì $z \geq y = 4$, ta kết luận $z = 5$.

Khẳng định đảo là hiển nhiên.

◇ **Trả lời**: $\{(2, 3, 5)\}$.

4.3.20 Giả sử $(x, y, z) \in \mathbb{Z}^3 - \{(0, 0, 0)\}$ là một nghiệm sao cho $|x| + |y| + |z|$ là cực tiểu.

Ta có: $3 \mid x^3$, vậy $3 \mid x$, $x = 3X$, $X \in \mathbb{Z}^*$, từ đó: $y^3 + 3z^3 + 9X^3 - 9Xyz = 0$.

Như thế, (y, z, X) là nghiệm; theo định nghĩa của (x, y, z) ta có: $|y| + |z| + |X| \geq |x| + |y| + |z|$ từ đó $X = 0$, $x = 0$, $y^3 + 3z^3 = 0$.

Nếu $(y, z) \neq (0, 0)$, với ký hiệu $\delta = y \wedge z$, thì tồn tại $(\alpha, \beta) \in (\mathbb{Z}^*)^2$ sao cho: $y = \delta\alpha$, $z = \delta\beta$, $\alpha \wedge \beta = 1$, và ta có: $\alpha^3 + 3\beta^3 = 0$.

Thế thì $3 \mid \alpha^3$, vậy $3 \mid \alpha$, $\alpha = 3\alpha'$, $\alpha' \in \mathbb{Z}^*$; rồi $9\alpha'^3 + \beta^3 = 0$, $3 \mid \beta^3$, $3 \mid \beta$, $3 \mid \alpha \wedge \beta$, mâu thuẫn.

Ta cũng có thể kết thúc bằng cách chứng minh rằng -3 không phải là một lập phương của một số hữu tỷ (xem Tập 1, bài tập 1.1.1).

Lời giải trên minh họa phương pháp "đi xuống vô hạn".

4.3.21 $(\exists k \in \mathbb{Z}, k\hat{x} = \hat{1}) \Leftrightarrow (\exists \hat{y} \in \mathbb{Z}/_{n\mathbb{Z}}, \hat{y}\hat{x} = \hat{1})$, và áp dụng 4.3.41, *1*), Mệnh đề.

◇ **Trả lời**: Các phần tử sinh của nhóm $(\mathbb{Z}/_{n\mathbb{Z}}, +)$ là các $\hat{x}$, $x \in \mathbb{Z}$ sao cho $x \wedge n = 1$.

4.3.22 Cho $\xi \in \mathbb{Z}/_{n\mathbb{Z}}$, $x \in \mathbb{Z}$ sao cho $\xi = \hat{x}$.

1) Nếu $x \wedge n = 1$ thì $\hat{x}$ khả nghịch trong $\mathbb{Z}/_{n\mathbb{Z}}$ (xem 4.3.4, *1*). Mệnh đề), vậy không phải là ước của không.

2) Nếu $n \nmid x$ và $x \wedge n \neq 1$, với ký hiệu $\delta = x \wedge n$, tồn tại $(a, b) \in (\mathbb{Z}^*)^2$ sao cho $x = \delta a$, $y = \delta b$, $a \wedge b = 1$, và ta có: $\hat{b}\hat{x} = \widehat{\delta ab} = \widehat{an} = \hat{0}$, $\hat{x} \neq \hat{0}, b \neq \hat{0}$ (vì $|b| < n$ và $b \neq 0$) vậy $\hat{x}$ là ước của không.

◇ **Trả lời**: Các ước của 0 trong $\mathbb{Z}/_{n\mathbb{Z}}$ là các $\hat{x}$, $x \in \mathbb{Z}$ và $x \wedge n \neq 1$.

4.4.1 a) $n^4 - n^2 + 16 = (n^2 + 4)^2 - 9n^2 = (n^2 - 3n + 4)(n^2 + 3n + 4)$, và $n^2 - 3n + 4$, $n^2 + 3n + 4$ đều chẵn vì $n^2 - n \equiv 0$ [2].

b) $4n^3 + 6n^2 + 4n + 1 = (2n + 1)(2n^2 + 2n + 1)$ và $1 < 2n + 1 < 2n^2 + 2n + 1$.

c) $2^{4n+2} + 1 = (2^{2n+1} + 1)^2 - 2.2^{2n+1} = (2^{2n+1} + 2^{n+1} + 1)(2^{2n+1} - 2^{n+1} + 1)$, và $2^{2n+1} + 2^{n+1} + 1 > 1$, $2^{2n+1} - 2^{n+1} + 1 > 1$ (vì $n \geq 1$).

Ví dụ: $2^{18} + 1 = (2^9 + 2^5 + 1)(2^9 - 2^5 + 1) = 545.481 = 5.109.13.37$.

4.4.2 Chú ý rằng $5^n - 3^n$ chẵn và $\neq 2$.

4.4.3 Ta ký hiệu $\delta = a \wedge c$; tồn tại $(a', c') \in (\mathbb{N}^*)^2$ sao cho: $a = \delta a'$, $c = \delta c'$, $a' \wedge c' = 1$

Vì $ab = cd$, ta có: $a'b = c'd$. Vì $a' \mid c'd$ và $a' \wedge c' = 1$, định lý Gauss chứng tỏ: $a' \mid d$; tồn tại $D \in \mathbb{N}^*$ sao cho $d = a'D$. Ta suy ra: $b = c'D$. Thế thì ta có: $a = \delta a'$, $b = Dc'$, $c = \delta c'$, $d = Da'$, từ đó: $a^n + b^n + c^n + d^n = (\delta^n + D^n)(a'^n + c'^n)$ và $\delta^n + D^n \geq 2$, $a'^n + c'^n \geq 2$, vậy $a^n + b^n + c^n + d^n$ là hợp số.

4.4.4 Ta ký hiệu $q = p^3 + p^2 + 11p + 2$ và chuyển qua modulo 3:

p mod. 3	-1	0	1
q mod. 3	0	2	0

Vậy, vì $q > 3$, nếu q nguyên tố, thì $p \equiv 0$ [3], rồi vì p nguyên tố, $p = 3$.

Ngược lại, $p = 3$ và $q = 71$ đều nguyên tố.

◇ **Trả lời**: {3}.

4.4.5 Tồn tại $N \in \mathbb{N}^*$ sao cho: $\left\{\frac{1}{x_1}, \ldots, \frac{1}{x_n}\right\} \subset \left\{\frac{1}{2^i 3^j}; (i, j) \in \{0, \ldots, N\}^2\right\}$, từ đó:

$$\sum_{k=1}^{n} \frac{1}{x_k} \leq \sum_{\substack{0 \leq i \leq N \\ 0 \leq j \leq N}} \frac{1}{2^i 3^j} = \left(\sum_{i=0}^{N} \frac{1}{2^i}\right)\left(\sum_{j=0}^{N} \frac{1}{3^j}\right) = \frac{1 - \frac{1}{2^{N+1}}}{1 - \frac{1}{2}} \cdot \frac{1 - \frac{1}{3^{N+1}}}{1 - \frac{1}{3}} < 3.$$

Hoặc giả, sử dụng khái niệm chuỗi số (Xem Tập 3, chương 3):

$$\sum_{k=1}^{n} \frac{1}{x_k} < \left(\sum_{i=0}^{+\infty} \frac{1}{2^i}\right)\left(\sum_{j=0}^{+\infty} \frac{1}{3^j}\right) = \frac{1}{1 - \frac{1}{2}} \cdot \frac{1}{1 - \frac{1}{3}} = 3.$$

4.4.6 Quy nạp theo n.

Tính chất là tầm thường với $n = 0$.

Giả thiết tính chất đúng với n; tồn tại $m \in \mathbb{N}$ sao cho: $(1+p)^{p^n} = 1 + p^{n+1} + mp^{n+2}$, từ đó

$$(1+p)^{p^{n+1}} = ((1+p)^{p^n})^p = (1+p^{n+1}+mp^{n+2})^p = 1 + p(p^{n+1}+mp^{n+2}) + \sum_{k=2}^{p} C_p^k p^{(n+1)k}(1+mp)^k.$$

Vì $\forall k \in \{2,..,p\}$, $(n+1)k \geq n+3$, ta kết luận: $(1+p)^{p^{n+1}} \equiv 1 + p^{n+2}\ [p^{n+3}]$.

4.4.7 1) Cho $m \in \mathbb{N}$, $h \in \{0,...,(m+1)^2 - m^2 - 1\}$, $n = m^2 + h$; ta có: $E(\sqrt{n}) = m$, từ đó $u_n = n + 5 + E(\sqrt{n}) = m^2 + m + h + 5$. Như thế, các u_n ($m^2 \leq n \leq (m+1)^2 - 1$) liền kề nhau.

Hơn nữa, $u_{(m+1)^2-1} = m^2 + 3m + 5$ lẻ và $u_{(m+1)^2} = m^2 + 3m + 7$.

2) Điều này chứng tỏ rằng $(u_n)_{n\geq 0}$ chứa tất cả các số nguyên lẻ $\geq u_0 = 5$, tức là tất cả các số nguyên tố ≥ 5.

4.4.8 Nếu a và b chẵn, thì $4 \left| \frac{1}{2}(a^3+b^3) \right.$, mâu thuẫn.

Nếu a chẵn và b lẻ (hoặc ngược lại), thì $\frac{1}{2}(a^3+b^3) \notin \mathbb{N}$.

Vậy a và b đều lẻ, và: $\frac{1}{2}(a^3+b^3) = \frac{a+b}{2}(a^2-ab+b^2)$, $\frac{a+b}{2} \in \mathbb{N}$, $a^2 - ab + b^2 \in \mathbb{N}$.

Vì $\frac{1}{2}(a^3+b^3)$ nguyên tố, ta suy ra: $\frac{1}{2}(a+b) = 1$ hoặc $a^2 - ab + b^2 = 1$.

- Nếu $a^2 - ab + b^2 = 1$, thì $(2a+b)^2 + 3b^2 = 4$, từ đó $b = |2a - b| = 1$, rồi $a = b = 1$.
- Nếu $\frac{a+b}{2} = 1$, thì $a = b = 1$.

4.4.9 Chuyển qua modulo 3: $n - 10 \equiv n + 2$, $n + 10 \equiv n + 1$, $n + 60 \equiv n$. Một trong ba số này là bội của 3, vậy bằng 3, vì chúng đều nguyên tố. Ta được $n - 10 = 3$, rồi $n + 90 = 103$, vốn nguyên tố.

4.4.10 Nếu $3 \not| n$, thì $n^2 \equiv 1$ [3], $n^2 + 8 \equiv 0$ [3], vậy $n^2 + 8$ là hợp số (bội của 3, và $\neq 3$). Như thế 3| n, $n = 3$, $n^3 + 4 = 31$ là số nguyên tố.

4.4.11 $n^4 + 4n^3 + 6n^2 + 4n + 5 = (n+1)^4 + 4 = ((n+1)^2 + 2)^2 - 4(n+1)^2 = ((n+1)^2 - 2(n+1) + 2)((n+1)^2 + 2(n+1) + 2) = (n^2+1)((n+2)^2+1)$.

Nếu số đã cho là nguyên tố, thì $n^2 + 1 = 1$ hoặc $(n+2)^2 + 1 = 1$, từ đó $n = 0$ hoặc -2.

Kiểm chứng lại khẳng định đảo.

◇ **Trả lời**: $\{-2, 0\}$.

4.4.12

- $p = 2$ không thích hợp, $p = 3$ thích hợp.
- Nếu p nguyên tố và ≥ 5, thì, chuyển qua modulo 3: $\begin{cases} 2^p \equiv (-1)^p = -1 \\ p^2 \equiv 1 \end{cases}$

suy ra $2^p + p^2 \equiv 0$ [3]. Vì $2^p + p^2$ nguyên tố, nên ta có: $2^p + p^2 = 3$, mâu thuẫn.

◇ **Trả lời**: $\{3\}$.

4.4.13 $$\sum_{k=0}^{p-1}(n+k)^2 = n^2\sum_{k=0}^{p-1}1+2n\sum_{k=0}^{p-1}k+\sum_{k=0}^{p-1}k^2$$

$$= n^2p+2n\frac{(p-1)p}{2}+\frac{(p-1)p(2p-1)}{6} = p\left(n^2+n(p-1)+\frac{(p-1)(2p-1)}{6}\right)$$

Chỉ cần chứng minh: $\frac{(p-1)(2p-1)}{6} \in \mathbb{N}$.

Vì p nguyên tố ≥ 5, ta có:

• p lẻ, vậy $(p-1)(2p-1) \equiv 0[2]$

• $3 \nmid p$, vậy $p-1 \underset{[3]}{\equiv} 0$ hoặc $2p-1 \underset{[3]}{\equiv} 0$, từ đó $(p-1)(2p-1) \equiv 0\ [3]$.

4.4.14 Giả thiết tồn tại p nguyên tố lẻ sao cho $p \mid m$ và $p \mid n$; tồn tại $(m', n') \in (\mathbb{N}^*)$ sao cho: $m = pm'$, $n = pn'$. Vì p lẻ ta có:

$$a^m + b^n = (a^{m'})^p + (b^{n'})^p = (a^{m'} + b^{n'})\sum_{k=0}^{p-1}(-1)^k (a^{m'})^k (b^{n'})^{p-1-k}.$$

Như thế $a^{m'} + b^{n'} \mid a^m + b^n$ và, vì $p \geq 2$, $2 \leq a^{m'} + b^{n'} < a^m + b^n$, mâu thuẫn với $a^m + b^n$ nguyên tố.

Điều này chứng tỏ rằng m và n chỉ có ước chung nguyên tố là 2.

4.4.15

• p và $p+2$ nguyên tố và không chia hết cho 3, vậy $p \equiv -1[3]$, $3 \mid p+1$.

• p lẻ, vậy $p \equiv -1\ [2]$, $2 \mid p+1$.

• $2 \wedge 3 = 1$, vậy $6 \mid p+1$.

4.4.16 Nếu $3 \notin \{p, q, r\}$, thì $p \equiv \pm 1\ [3]$, $q \pm 1\ [3]$, $r = \pm 1\ [3]$, vậy $p^2 + q^2 + r^2 \equiv 0\ [3]$, $p^2 + q^2 + r^2 = 3$, mâu thuẫn.

4.4.17 Nếu $n \geq 1$, thì $2^{2^n} + 5 \geq 9$ và $2^{2^n} + 5 \underset{[3]}{\equiv} 1 + 5 \underset{[3]}{\equiv} 0$ vậy $2^{2^n} + 5$ không nguyên tố.

Nếu $n = 0$, $2^{2^n} + 5 = 7$, là số nguyên tố.

◇ **Trả lời**: {7}.

4.4.18 Tồn tại $m \in \mathbb{N} - \{0, 1\}$ sao cho $n = pm$. Giả thiết m là hợp số; tồn tại $(m_1, m_2) \in \mathbb{N}^2$ sao cho: $m = m_1m_2$, $1 < m_1 < m$, $1 < m_2 < m$. Vì p là ước nguyên tố nhỏ nhất của n, nên ta có: $m_1 \geq p$ và $m_2 \geq p$, từ đó $n = pm_1m_2 \geq p^3$, mâu thuẫn.

4.4.19

• Nếu $p \geq 13$, thì $p = 9 + (p-9)$, trong đó 9 và $p-9$ (số này chẵn ≥ 4) đều là hợp số.

• Khảo sát các trường hợp $p = 2, 3, 5, 7, 11$.

◇ **Trả lời**: Các số nguyên tố ≥ 13.

4.4.20 Trước tiên chứng minh $p \equiv \pm 1$ [6].

Thế thì tồn tại $(q,\varepsilon) \in \mathbb{N} \times \{-1, 1\}$ sao cho: $p = 6q + \varepsilon$ và $q \geq 1$. Ta có:

$$4p^2 + 1 = 144q^2 + 48\varepsilon q + 5 = (8q + 2\varepsilon)^2 + (8q + \varepsilon)^2 + (4q)^2,$$

từ đó $(8q + 2\varepsilon, 8q + \varepsilon, 4q) \in (\mathbb{N}^*)^3$.

4.4.21 a) Vì : $p! = k!(p-k)!C_p^k$, nên p chia hết $k!(p-k)!C_p^k$.

Ta có: $\forall k \in \{1,..., p-1\}$, $p \wedge k = p \wedge (p-k) = 1$, vậy $p \wedge (k!(p-k)!) = 1$

Định lý Gauss cho phép kết luận: $p \mid C_p^k$.

b) $\dfrac{p!}{i_1!..i_n!}$ là một số nguyên, bởi vì đó chính là hệ tử của $X_1^{i_1} \cdots X_n^{i_n}$ trong khai triển của $(X_1 + ... + X_n)^p$ theo công thức *đa thức Newton*, là sự tổng quát hóa công thức nhị thức Newton. Kết thúc tương tự như a).

4.4.22 Khảo sát trường hợp $p = 2$.

Giả thiết p là số nguyên tố lẻ: tồn tại $k \in \mathbb{N}^*$ sao cho $p = 2k + 1$.

Ta có : $2^p + 3^p = (2 + 3)a$, trong đó $a = 2^{2k} - 2^{2k-1}.3 + ... + 3^{2k}$, chuyển qua modulo 5: $a \equiv (2k + 1)2^{2k} = p.2^{2k}$.

Nếu $p \neq 5$, thì $p \neq 0$ [5] và $2^{2k} \neq 0$ [5], từ đó, vì 5 nguyên tố, $p2^{2k} \equiv 0$ [5]. Điều này chứng tỏ rằng: $5 \mid 2^p + 3^p$ và $5^2 \not\mid 2^p + 3^p$. Vậy tồn tại $(a, n) \in (\mathbb{N}-\{0,1\})^2$ sao cho $2^p + 3^p = a^n$.

Khảo sát trường hợp $p = 5$.

4.4.23 Ta suy luận phản chứng: Giả thiết tồn tại $n \in \mathbb{Z}$ sao cho $49 \mid U_n$,

trong đó $U_n = n^3 - n^2 - 2n + 1$. Vì $U_n = (n + 2)^3 - 7n^2 - 14n - 7$, ta suy ra $7 \mid (n + 2)^3$, rồi $7 \mid n + 2$ vì 7 nguyên tố. Tồn tại $k \in \mathbb{Z}$ sao cho $n = 7k - 2$. Thế thì ta có $U_n = 7^2(7k^3 - 7k^2 + 2k) - 7$, vậy $7^2 \not\mid U_n$, mâu thuẫn.

4.4.24 1) Giả sử $n \in \mathbb{N}$; ta ký hiệu $\delta = (2n^7 + 1) \wedge (3n^2 + 2)$. Sử dụng phép chia Euclide:

$$9(2n^7 + 1) = (3n^3 + 2)(6n^3 - 4n) + 8n + 9,$$

từ đó $\delta \mid 8n + 9$.

Rồi cũng theo cách tương tự:

$$512(3n^3 + 2) = (8n + 9)(192n^2 - 216n + 243) - 1163,$$

từ đó $\delta \mid 1163$.

Vì 1163 nguyên tố, ta được $\delta = 1163$

Vậy tồn tại $a \in \mathbb{N}^*$ sao cho $8n + 9 = 1163a$. Chuyển qua modulo 8:

$$1163a \equiv 9\ [8] \Rightarrow 3a \equiv 1\ [8] \Rightarrow a \equiv 9a \equiv 3\ [8].$$

Vậy tồn tại $b \in \mathbb{N}$ sao cho $a = 8b + 3$, rồi $n = 1163b + 435$.

2) Ngược lại, giả sử $b \in \mathbb{N}$ và $n = 1163b + 435$. Sử dụng các phép chia Euclide đã thấy ở 1), ta có $1163 \mid 8n + 9$, $1163 \mid 3n^2 + 2$, $1163 \mid 2n^7 + 1$, từ đó $(2n^7 + 1) \wedge (3n^2 + 2) \neq 1$.

◇ **Trả lời**: $\{1163b + 435;\ b \in \mathbb{N}\}$.

4.4.25 a) Tồn tại $(n, a) \in \mathbb{N}^2$ sao cho $k = 2^n(2a + 1)$. Ta có:

$$2^k + 1 = (2^{2^n})^{2a+1} + 1 = (2^{2^n} + 1) \sum_{i=0}^{2a} (-1)^i (2^{2^n})^i$$

Vì $2^k + 1$ nguyên tố và $2^{2^n} + 1 \in \mathbb{N}^*$, ta suy ra $2^k + 1 = 2^{2^n}$, $k = 2^n$.

b) Giả sử $(m, n) \in \mathbb{N}^2$ sao cho chẳng hạn $m > n$. Ta chuyển qua modulo F_n:

$$F_m - 1 = 2^{2^m} = (2^{2^n})^{2^{m-n}} \underset{[F_n]}{\equiv} (-1)^{2^{m-n}} = 1,$$

từ đó $F_m \equiv 2[F_n]$

Kết quả là: $F_m \wedge F_n \mid 2$. Vì F_m và F_n đều lẻ, ta kết luận: $F_m \wedge F_n = 1$.

4.4.26 Tồn tại $m \in \mathbb{N}^*$ sao cho $n = mp$. Ta có : $4^n - 2^n + 1 = A_p(2^m)$ trong đó $A_p = X^{2p} - X^p + 1 \in \mathbb{Z}[X]$. Ký hiệu $A_1 = X^2 - X + 1 \in \mathbb{Z}[X]$, ta chứng minh rằng A_1 chia hết A_p trong $\mathbb{C}[X]$:

$$A_1 = (X + j)(X + j^2), \quad A_p(j) = A_p(j^2) = j^{2p} + j^p + 1 = \frac{j^{3p} - 1}{j^p - 1} = 0, \quad A_p(j^2) = 0.$$

Kết quả là A_1 chia hết A_p trong $\mathbb{Z}[X]$, rồi $A_1(2^m) \mid A_p(2^m)$ trong $\mathbb{Z}$.

Cuối cùng, chứng minh rằng $1 < A_1(2^m) < A_p(2^m)$.

4.4.27 Ta ký hiệu $\beta_k = 4^k + 2^k + 1$ và $B_k = X^{2k} + X^k + 1 \in \mathbb{Z}[X]$ với mọi k thuộc $\mathbb{N}^*$, do đó $\beta_k = B_k(2)$.

Khảo sát trường hợp $n = 1$.

Ta giả thiết $n \geq 2$ và β_n nguyên tố. Tồn tại $(k, m) \in \mathbb{N}^2$ sao cho: $\begin{cases} n = 3^k m \\ m \not\equiv 0[3] \end{cases}$ (k là 3- định giá của n).

Như thế: $B_n(X) = (X^{3^k})^{2m} + (X^{3^k})^m + 1 = B_m(X^{3^k})$.

Giả thiết $m \geq 2$.

Vì $m \not\equiv 0$ [3], ta có $B_m(j) = B_m(j^2) = j^{2m} + j^m + 1 = \frac{j^{3m} - 1}{j - 1} = 0$, vậy $B_1 \mid B_m$ trong $\mathbb{C}[X]$.

Vì $(B_1, B_m) \in (\mathbb{Z}[X])^2$, kết quả là $B_1 \mid B_m$ trong $\mathbb{Z}[X]$, rồi $B_1(2^{3^k}) \mid B_m(2^{3^k}) = B_m(2) = \beta_n$ trong $\mathbb{Z}$.

Vì $1 < B_1(2^{3^k}) < \beta_n$, nên β_n là hợp số, mâu thuẫn.

Ta kết luận: $m = 1$, $n = 3^k$.

4.4.28 1) Nếu n là hợp số, thì tồn tại $(a, b) \in \mathbb{N}^2$ sao cho: $1 < a < n$, $1 < b < n$, $n = ab$, $a \geq b$.

Vì 1, a, n đều là các ước ≥ 1 của n, từng đôi khác nhau, nên ta có $\sigma(n) \geq 1 + a + n$.

Nhưng $a^2 \geq ab = n$, vậy $a \geq \sqrt{n}$, từ đó $\sigma(n) \geq 1 + \sqrt{n} + n > n + \sqrt{n}$.

2) Nếu n là nguyên tố, $\sigma(n) = n + 1 < n + \sqrt{n}$.

4.4.29 1) Với mọi ước d (≥ 1) của a, bắt đầu từ a, bd là một ước (≥ 1) của ab, từ đó:

$$\sigma(ab) = \sum_{\delta \mid ab} \delta \geq \sum_{d \mid a} bd = b\sigma(a), \text{ vậy } \frac{\sigma(ab)}{ab} \geq \frac{\sigma(a)}{a}.$$

2) Giả sử D là một ước (≥ 1) của ab. Ta ký hiệu $d = D \wedge a$; tồn tại $(a', \delta) \in (\mathbb{N}^*)^2$ sao cho: $a = da'$, $D = d\delta$, $a' \wedge \delta = 1$. Vì $\delta \mid a'b$ và $\delta \wedge a' = 1$, định lý Gauss chứng tỏ rằng : $\delta \mid b$.

Như thế ta được: $D = \delta$, $d \mid a$, $\delta \mid b$.

• Ta suy ra: $\sigma(ab) = \sum_{D \mid ab} D \leq \sum_{\substack{d \mid a \\ \delta \mid b}} d\delta = \left(\sum_{d \mid a} d\right)\left(\sum_{\delta \mid b} \delta\right) = \sigma(a)\sigma(b)$.

4.4.30 Ta ký hiệu $\delta = a \wedge b$; tồn tại $(a', b') \in (\mathbb{N}^*)^2$ sao cho: $a = \delta a'$, $b = \delta b'$, $a' \wedge b' = 1$. Ta có: $(a^2 + ab + b^2) \wedge (ab) = \delta^2 \cdot ((a'^2 + a'b' + b'^2) \wedge (a'b'))$. Giả thiết tồn tại một ước nguyên tố chung p của $a'^2 + a'b' + b'^2$ và $a'b'$. Vì p nguyên tố và $p \mid a'b'$, ta có (nếu cần trao đổi a' và b') : $p \mid a'$. Như thế, $p \mid a'$ và $p \mid a'^2 + a'b' + b'^2$, vậy $p \mid b'^2$, $p \mid b'$ (vì p nguyên tố). Ta đi đến mâu thuẫn với $a' \wedge b' = 1$.

Như thế $a'^2 + a'b' + b'^2$ và $a'b'$ không có một ước nguyên tố chung nào, từ đó $(a'^2 + a'b' + b'^2) \wedge (a'b') = 1$, rồi $(a^2 + ab + b^2) \wedge (ab) = \delta^2 = (a \wedge b)^2$.

4.4.31 ◇ **Trả lời**: Không; ví dụ: $a = 4$, $b = 10$.

4.4.32 Ta viết các phân tích nguyên tố của a và b dưới dạng:

$$a = \left(\prod_{i \in I} p_i^{\alpha_i}\right)\left(\prod_{i \in J} p_i^{\alpha'_i}\right)\left(\prod_{i \in K} p_i^{\alpha''_i}\right), \quad b = \left(\prod_{i \in L} p_i^{\beta_i}\right)\left(\prod_{i \in J} p_i^{\beta'_i}\right)\left(\prod_{i \in K} p_i^{\beta''_i}\right).$$

trong đó
- I, J, K, L rời nhau từng đôi
- các p_i ($i \in I \cup J \cup K \cup L$) nguyên tố, khác nhau từng đôi
- $\forall_i \in J$, $\alpha'_i \geq \beta_i \geq 1$
- $\forall_i \in K$, $\beta''_i \geq \alpha''_i > 1$

Vậy chỉ cần lấy: $x = \left(\prod_{i \in I} p_i^{\alpha_i}\right)\left(\prod_{i \in J} p_i^{\alpha'_i}\right)$, $y = \left(\prod_{i \in L} p_i^{\beta_i}\right)\left(\prod_{i \in K} p_i^{\beta''_i}\right)$.

Ví dụ: $a = 2^4.3^2.5.7$, $b = 2.3^2.5^2.11$; phương pháp trên cho phép chọn $x = 2^4.3^2.7$, $y = 5^2.11$.

4.4.33 Xét các phân tích nguyên tố: $a = \prod_{i=1}^{N} p_i^{r_i}$, $b = \prod_{i=1}^{N} p_i^{s_i}$, trong đó $N \in \mathbb{N}^*$, $p_1, \ldots, p_N$ nguyên tố, từng đôi khác nhau, và $r_1, \ldots, r_N, s_1, \ldots, s_N \in \mathbb{N}$.

Vì $a \wedge b = 1$, ta có $\forall_i \in \{1, \ldots, N\}$ ($r_i = 0$ hoặc $s_i = 0$). Nhưng $c^k = \prod_{i=1}^{N} p_i^{r_i + s_i}$, từ đó, do tính duy nhất của dạng phân tích nguyên tố của c^k: $\forall_i \in [1, \ldots, N]$, $k \mid r_i + s_i$.

Ta suy ra : $\forall i \in \{1, \ldots, N\}$, ($k \mid r_i$ và $k \mid s_i$).

Tồn tại $\alpha_1, \ldots, \alpha_N, \beta_1, \ldots, \beta_N \in \mathbb{N}$ sao cho: $\forall_i \in \{1, \ldots, N\}$, ($r_i = k\alpha_i$ và $s_i = k\beta_i$).

Ký hiệu: $\alpha = \prod_{i=1}^{N} p_i^{\alpha_i}$ và $\beta = \prod_{i=1}^{N} p_i^{\beta_i}$, ta có: $(\alpha, \beta) \in \mathbb{N}^*)^2$, $a = \alpha^k$, $b = \beta^k$.

4.4.34 Chuyển qua dạng các phân tích nguyên tố của a và b.

Ví dụ: $a^3 \mid b^5 \Rightarrow a \mid b^2$.

4.4.35 Ta ký hiệu $A = (a \vee b)(a \vee c)(b \vee c)(a \wedge b \wedge c)$ và $B = (a \vee b \vee c) \mid abc \mid$. Giả sử p là một số nguyên tố và α, β, γ là p- định giá tương ứng của a, b, c. Do các vai trò đối xứng của a, b, c ta có thể giả thiết $\alpha \le \beta \le \gamma$. Ta có:

- $v_p(A) = v_p(a \vee b) + v_p(a \vee c) + v_p(b \vee c) + v_p(a \wedge b \wedge c)$

  $= \text{Max}(\alpha, \beta) + \text{Max}(\alpha, \gamma) + \text{Max}(\beta, \gamma) + \text{Min}(\alpha, \beta, \gamma) = \beta + \gamma + \gamma + \alpha$
- $v_p(B) = v_p(a \vee b \vee c) + v_p(a) + v_p(b) + v_p(c) = \text{Max}(\alpha, \beta, \gamma) + \alpha + \beta + \gamma = \gamma + \alpha + \beta + \gamma$.

Như thế: $\begin{cases} \forall p \in \mathcal{P}, v_p(A) = v_p(B) \\ (A, B) \in (\mathbf{N}^*)^2 \end{cases}$, từ đó $A = B$.

4.4.36 Suy luận như trong lời giải bài tập 4.4.35.

4.4.37 Chú ý rằng ánh xạ $(s_1, \ldots, s_N) \mapsto \prod_{i=1}^{N} p_i^{s_i}$ là một song ánh từ $\prod_{i=1}^{N} \{0, \ldots, r_i\}$ lên tập hợp các ước (≥ 1) của n. Từ đó:

1) $\text{d}(n) = \text{Card}\left(\prod_{i=1}^{N} \{0, \ldots, r_i\}\right) = \prod_{i=1}^{N} (r_i + 1)$

2) $\sigma(n) = \sum_{\substack{1 \le i \le N \\ 0 \le s_i \le r_i}} \left(\prod_{i=1}^{N} p_i^{s_i}\right) = \prod_{i=1}^{N} \left(\sum_{k=0}^{r_i} p_i^k\right) = \prod_{i=1}^{N} \frac{p_i^{r_i+1} - 1}{p_i - 1}$.

4.4.38 Xét dạng phân tích nguyên tố $n = \prod_{i=1}^{N} p_i^{r_i}$, và $\text{d}(n)$ là số các ước (≥ 1) của n. Ta ký hiệu $\text{p}(n)$ là tích các ước (≥ 1) của n.

1) Nếu n không phải là một bình phương của số nguyên, ta có thể nhóm lại các ước của n từng đôi có tích bằng n, từ đó: $(\text{p}(n))^2 = n^{\text{d}(n)}$

2) Nếu n là một bình phương của số nguyên, $n = k^2$ ($k \in \mathbb{N}^*$), ta có thể nhóm lại các ước của n, khác với k, từng đôi có tích bằng n, từ đó: $(\text{p}(n))^2 = k^2 n^{\text{d}(n)-1} = n^{\text{d}(n)}$.

◇ **Trả lời:** $n^{\frac{\text{d}(n)}{2}}$.

Hơn nữa: $\text{d}(n) = \prod_{i=1}^{N} (r_i + 1)$, xem bài tập 4.4.37.

4.4.39 Ký hiệu $q(n) = \prod_{\substack{1 \le d < n \\ d \mid n}} d$

1) Nếu n có ít nhất ba ước nguyên tố p_1, p_2, p_3, khác nhau từng đôi thì:

$q(n) \ge p_1 p_2 \frac{n}{p_1} > n$.

2) Nếu n có đúng hai ước nguyên tố p_1, p_2 khác nhau, và nếu, chẳng hạn $p_1^2 \mid n$, thì:

$q(n) \geq p_1 p_2^2 \dfrac{n}{p_1} > n$.

3) Nếu $n = p_1 p_2$, p_1, p_2 nguyên tố khác nhau, thì: $q(n) = p_1 p_2 = n$.

4) Nếu $n = p^\alpha$, p nguyên tố, $\alpha \in \mathbb{N}^*$, thì: $q(n) = \prod_{k=0}^{\alpha-1} p^k = p^{\frac{(\alpha-1)\alpha}{2}}$, từ đó:

$q(n) = n \Leftrightarrow \dfrac{(\alpha-1)\alpha}{2} = \alpha \Leftrightarrow \alpha = 3$.

4.4.40 a) Suy luận như trong lời giải bài tập 4.4.37, tính $\sigma(n) = \sigma_1(n)$).

b) Giả sử $(a, b) \in (\mathbb{N}^*)^2$ sao cho $a \wedge b = 1$; xét các phân tích nguyên tố $a = \prod_{i=1}^{N} p_i^{r_i}$,

$b = \prod_{i=1}^{N} p_i^{s_i}$; Vì $a \wedge b = 1$, ta có: $\forall_i \in \{1,...,N\}$, ($r_i = 0$ hoặc $s_i = 0$). Giả sử $i \in \{1,...,N\}$.

Ta giả thiết, chẳng hạn $s_i = 0$. Thế thì: $\dfrac{p_i^{k(r_i+s_i+1)}-1}{p_i^k-1} = \dfrac{p_i^{k(r_i+1)}-1}{p_i^k-1} \cdot \dfrac{p_i^{k(s_i+1)}-1}{p_i^k-1}$.

Ta kết luận: $\sigma_k(a, b) = \sigma_k(a)\ \sigma_k(b)$.

4.4.41 Theo bài tập 4.4.37:

$$\sigma(N) = \frac{2^{n+1}-1}{2-1} \cdot \frac{3^2-1}{3-1} \cdot \frac{p^2-1}{p-1} = (2^{n+1}-1)4(p+1)$$

Vậy: $\sigma(N) = 3N \Leftrightarrow (2^{n+1}-1)4(p+1) = 2^n.3^2 p$.

Vì $2^n \wedge (2^{n+1}-1) = 1$, ta suy ra $2^n \mid 4(p+1)$; vậy tồn tại $\lambda \in \mathbb{N}^*$ sao cho $4(p+1) = 2^n\lambda$.

Như thế: $(1) \Leftrightarrow (2^{n+1}-1)\lambda = 9p \Leftrightarrow 2.2^n\lambda = \lambda + 9p \Leftrightarrow \lambda = 8 - p$.

Vì $\lambda \in \mathbb{N}^*$ và $p \geq 5$, p nguyên tố, ta suy ra $p \in \{5, 7\}$.

- $p = 5$: $\lambda = 8 - p = 3.2^n = 8$, $n = 3$, $N = 2^3.3.5 = 120$, $\sigma(N) = (2^4 - 1).4.6 = 360 = 3N$.
- $p = 7$: $\lambda = 8 - p = 1$, $2^n = 32$, $n = 5$, $N = 2^5.3.7 = 672$, $\sigma(N) = (2^6 - 1)4.8 = 2016 = 3N$.

◇ **Trả lời:** $\{(3, 5), (5, 7)\}$.

4.4.42 a) $\mathbb{Z}/_{11\mathbb{Z}}$ là một thể (11 nguyên tố) và:

$$x^2 + \hat{4}x + \hat{1} = \hat{0} \Leftrightarrow (x+\hat{2})^2 - \hat{3} = \hat{0} \Leftrightarrow (x+\hat{2})^2 - \widehat{25} = \hat{0} \Leftrightarrow (x+\hat{3})(x-\hat{4}) = \hat{0}.$$

◇ **Trả lời:** $\{\hat{3}, \hat{4}\}$.

2) $\mathbb{Z}/_{12\mathbb{Z}}$ không phải là một thể (12 không nguyên tố). Vì $\hat{5}$ là khả nghịch trong $\mathbb{Z}/_{12\mathbb{Z}}$ ($\hat{5}.\hat{5} = \hat{1}$) nên ta có:

$$\hat{5}x + \hat{2}y = \hat{3} \Leftrightarrow \hat{5}(\hat{5}x + \hat{2}y) = \hat{5}.\hat{3} \Leftrightarrow x + \widehat{10}y = \widehat{15} \Leftrightarrow x = \hat{2}y + \hat{3}.$$

Rồi: $\begin{cases} \hat{5}x + \hat{2}y = \hat{3} \\ \hat{2}x + \hat{4}y = \hat{6} \end{cases} \Leftrightarrow \begin{cases} x = \hat{2}y + \hat{3} \\ \hat{2}(\hat{2}y + \hat{3}) + \hat{4}y = \hat{6} \end{cases} \Leftrightarrow \begin{cases} x = \hat{2}y + \hat{3} \\ \hat{8} = \hat{0} \end{cases}$

Ta có, mọi a thuộc $\mathbb{Z}$: $8\hat{a} = \hat{0} \Leftrightarrow 12 \mid 8a \Leftrightarrow 3 \mid 2a \Leftrightarrow 3 \mid a \Leftrightarrow \hat{a} \in \{\hat{0}, \hat{3}, \hat{6}, \hat{9}\}$.

◇ **Trả lời:** $(\hat{3},\hat{0}), (\widehat{-3},\hat{3}), (\hat{3},\hat{6}), (\hat{-3},\widehat{-3})$.

4.4.43 a) Xem bài tập 4.4.21 a).

b) Quy nạp theo f.

1) Trường hợp $f = 1$

Quy nạp theo N.

- Tính chất là hiển nhiên với $N = 1$.
- Với $N = 2$: $(x_1 + x_2)^p = x_1^p + \sum_{k=1}^{p-1} C_p^k x_1^{p-k} x_2^k + x_2^p \equiv_{[p]} x_1^p + x_2^k$ [p], theo a).
- Giả thiết tính chất đúng với một N thuộc $\mathbb{N}^*$. Giả sử $(x_1, \ldots x_{N+1}) \in \mathbb{Z}^{N+1}$ ta có:

$$\left(\sum_{i=1}^{N+1} x_i\right)^p = \left(\left(\sum_{i=1}^{N} x_i\right) + x_{N+1}\right)^p \equiv_{[p]} \left(\sum_{i=1}^{N} x_i\right)^p + x_{N+1}^p \equiv_{[p]} \sum_{i=1}^{N} x_i^p + x_{N+1}^p = \sum_{i=1}^{N+1} x_i^p$$

2) Ta giả thiết công thức đúng với một f thuộc $\mathbb{N}^*$. Thế thì ta có:

$$\left(\sum_{i=1}^{N} x_i\right)^{p^{f+1}} = \left(\left(\sum_{i=1}^{N} x_i\right)^{p^f}\right)^p \equiv_{[p]} \left(\sum_{i=1}^{N} x_i^{p^f}\right)^p \equiv_{[p]} \sum_{i=1}^{N} \left(x_i^{p^f}\right)^p = \sum_{i=1}^{N} x_i^{p^{f+1}}$$

4.4.44 Giả thiết tồn tại $x \in \mathbb{Z}$ sao cho $5 \mid ax^3 + bx^2 + cx + d$. Ta có $5 \nmid x$, vì nếu không $5 \mid d$ nguyên tố, nên kết quả là $5 \wedge x = 1$, vậy (định lý Bezout), tồn tại $(u, v) \in \mathbb{Z}^2$ sao cho $xy + 5v = 1$.

Vì $x^3(dy^3 + cy^2 + by + a) \equiv_{[5]} ax^3 + bx^2 + cx + d \equiv_{[5]} 0$ và $5 \nmid x^3$,

ta kết luận rằng: $dy^3 + cy^2 + by + a \equiv 0$ [5].

4.4.45 1) $(p-1)!C_{np-1}^{p-1} = \prod_{k=1}^{p-1}(np-k) \equiv_{[p]} \prod_{k=1}^{p-1}(-k) = (-1)^{p-1}(p-1)!$.

Vì p nguyên tố, nên $(p - 1)! \wedge p = 1$, vậy $(p - 1)!$ khả nghịch trong $\mathbb{Z}/p\mathbb{Z}$; vậy ta có thể giản ước cho $(p - 1)!$ và kết luận: $C_{np-1}^{p-1} = (-1)^{p-1}$ [p]

- Nếu p lẻ: $C_{np-1}^{p-1} \equiv 1$ [p]
- Nếu p chẵn: $p = 2$, $C_{np-1}^{p-1} \equiv -1 \equiv 1$ [2]

2) $C_{np}^{p} \equiv nC_{np-1}^{p-1} \equiv n$ [p].

4.4.46 Cho (x, y) là một nghiệm; ta có:

$$2(x^2 - xy + y^2) = 7(x + y) \qquad (1)$$

Vì $2 \mid 7(x + y)$ và $2 \wedge 7 = 1$, suy ra $2 \mid x + y$; tồn tại $u \in \mathbb{N}^*$ sao cho: $x + y = 2u$.

Do các vai trò đối xứng của x và y, ta có thể giả thiết $x \geq y$. Vì $x + y$ chẵn, nên $x - y$ cũng chẵn, vậy tồn tại $v \in \mathbb{N}$ sao cho $x - y = 2v$. Ta có:

$$(1) \Leftrightarrow u^2 + 3v^2 = 7u \Leftrightarrow u(7 - u) = 3v^2 \Rightarrow 1 \leq u < 7.$$

Thử với $u = 1, 2, 3, 4, 5, 6$.

◇ **Trả lời**: {(1, 5), (2, 6), (5, 1), (6, 2)}.

4.4.47 Ta giả thiết rằng tập hợp các nghiệm khác rỗng. Thế thì tồn tại một nghiệm (x, y, z) sao cho z là cực tiểu.

• **Trường hợp** $z \geq 2$

Thế thì $z \mid y$; $y = 3Y$, $Y \in \mathbb{N}$. Rồi: $5x^2 - 12Y^2 = 3^{z-1}$, vậy $3 \mid x$; $x = 3X$, $X \in \mathbb{N}$. Từ đó: $15X^2 - 4Y^2 = 3^{z-2}$, và $(X, Y, z-2)$ là một nghiệm, điều này mâu thuẫn với tính cực tiểu của z.

• **Trường hợp** $z = 1$

Thế thì $z \mid y$; $y = 3Y$, $Y \in \mathbb{N}$. Rồi $5x^2 - 12Y^2 = 1$, từ đó $x^2 \equiv -1$ [3], mâu thuẫn.

• **Trường hợp** $z = 0$

Thế thì $15x^2 - 4y^2 = 1$, từ đó $y^2 \equiv -1$ [3], mâu thuẫn.

4.4.48 Tồn tại $q \in \mathbb{N}^*$ sao cho $p = 2q + 1$. Ta có: $H_{p-1} = \sum_{k=1}^{q}\left(\frac{1}{k} + \frac{1}{p-k}\right) = pK_p$, trong đó: $K_p = \frac{1}{p}\sum_{k=1}^{q}\left(\frac{1}{k} + \frac{1}{p-k}\right) = \sum_{k=1}^{q}\frac{1}{k(p-k)}$.

Vậy : $(p-1)!K_p = \sum_{k=1}^{q}\alpha_{p,k}$, trong đó: $\alpha_{p,k} = \frac{(p-1)!}{k(p-k)} = \prod_{\substack{1<i<2q \\ i\neq k, i\neq p-k}} i$.

Ta có: $\forall k \in \{1,\ldots,q\}$, $k(p-k)\alpha_{p,k} = (p-1)!$, từ đó trong $\mathbb{Z}/p\mathbb{Z}$: $\widehat{(q-1)!}\hat{K}_p = -\sum_{k=1}^{q}\widehat{(q-1)!}(\hat{K}^2)^{-1}$.

Vì $\widehat{(p-1)!}$ khả nghịch, ta suy ra: $\hat{K}_p = -\sum_{k=1}^{q}(\hat{K}^2)^{-1}$.

Nhưng bằng phép đổi chỉ số: $l = p - k$: $\hat{K}_p = -\sum_{l=q+1}^{2q}(\widehat{p-l}^2)^{-1} = \sum_{l=q+1}^{2q}(\hat{l}^2)^{-1}$.

từ đó: $2\hat{K}_p = -\sum_{k=1}^{2q}(\hat{k}^2)^{-1} = -\sum_{k=1}^{2q}(\hat{k}^{-1})^2$.

Vì $\hat{k} \mapsto \hat{k}^{-1}$ là một hoán vị của $\mathbb{Z}/p\mathbb{Z} - \{0\}$, suy ra:

$$2\hat{K}_p = -\sum_{k=1}^{2q}\hat{k}^2 = -\left(\sum_{k=1}^{2q}k^2\right)^{\wedge} = -\left(\frac{2q(2q+1)(4q+1)}{6}\right)^{\wedge} = -\left(\frac{q(4q+1)}{3}p\right)^{\wedge}.$$

Nếu $q \equiv 1$ [3], thì $p \equiv 0$ [3], mâu thuẫn; *vậy* $q \equiv -1$ hoặc 0 [3], từ đó $q(4q+1) \equiv 0$ [3].

Như thế, $\frac{q(4q+1)}{3} \in \mathbb{N}$ vậy $2\hat{K}_p = \hat{0}$. Cuối cùng $2 \wedge p = 1$, từ đó $\hat{K}_p = \hat{0}, p \mid K_p, p^2 \mid H_{p-1}$.

4.4.49 a) và b) tương tự như lời giải của bài tập 4.4.48.

c) Ta có: $(p-1)!\ C_{2p-1}^{p-1} = \prod_{k=1}^{p-1}(k+p)$.

Bằng khai triển, ta thấy rằng tồn tại $c \in \mathbb{N}$ sao cho:

$$\prod_{k=1}^{p-1}(k+p) = (p-1)! + pa + p^2b + p^3c.$$

Vì $p^2 \mid a$ và $p \mid b$ (xem b)), ta suy ra : $(p-1)!\ C_{2p-1}^{p-1} - 1) \equiv 0\ [p^3]$, rồi: $C_{2p-1}^{p-1} - 1 \equiv 0[p^3]$, vì $(p-1)! \wedge p^3 = 1$

4.4.50 a) 1) Ta chứng minh bằng quy nạp theo n: $\forall n \in \mathbb{N}, n^p \equiv n\ [p]$.

Tính chất là hiển nhiên với $n = 0$.

Ta giả thiết tính chất đúng với một n thuộc $\mathbb{N}$. Sử dụng bài tập 4.4.21 a), ta có:

$$(n+1)^p = n^p + \sum_{k=1}^{p-1} C_p^k n^k + 1 \underset{[p]}{\equiv} n^p + 1 \underset{[p]}{\equiv} n+1.$$

2) Giả sử $n \in \mathbb{Z}$

Nếu p lẻ: $n^p = -(-n)^p \underset{[p]}{\equiv} -(-n) = n$.

Nếu $p = 2 : n^2 = (-n)^2 \underset{[2]}{\equiv} -n \underset{(2)}{\equiv} n$.

b) Giả sử $n \in \mathbb{Z}$ sao cho $p \nmid n$. Vì p nguyên tố, nên ta có $n \wedge p = 1$, vậy ta có thể giản ước bởi n trong đồng dư thức $n^p \equiv n\ [p]$, và được: $n^{p-1} \equiv 1\ [p]$.

4.4.51 Ta ký hiệu $A_n = 5n^7 + 7n^5 + 23n$.

Theo định lý nhỏ Fermat (bài tập 4.4.50): $n^5 \equiv n\ [5]$, từ đó $A_n \equiv 30n \equiv 0\ [5]$.

Tương tự $n^7 \equiv n\ [7]$, từ đó $A_n \equiv 28n \equiv 0\ [7]$. Cuối cùng $5 \wedge 7 = 1$, vậy $35 \mid A_n$.

4.4.52 a) Theo định lý nhỏ Fermat (bài tập 4.4.50):

Mod.2: $n^2 \equiv n$, từ đó $n^7 \equiv n$.

Mod.3: $n^3 \equiv n$, từ đó $n^7 \equiv n$.

Mod.7: $n^7 \equiv n$.

Như thế 2, 3, 7, vốn nguyên tố cùng nhau từng đôi, chia hết $n^7 - n$, từ đó: $42 = 2.3.7 \mid n^7 - n$.

b) $2730 = 2.3.5.7.13$ và suy luận như ở a).

c) $2^{15} - 2^3 = 2^3.3^2 . 5.7.13$.

Mod. 8: • Nếu n chẵn, thì $8 \mid n^3$, vậy $8 \mid n^5 - n^3$.

• Nếu n lẻ, thì $n^2 \equiv 1[8]$ (xem bài tập 4.1.1), từ đó $n^{15} \equiv n[8]$ và $n^3 \equiv n[8]$, vậy $8 \mid n^{15} - n^3$.

Mod. 9:

N	0	±1	±2	±3	±4
n^3	0	±1	±1	0	±1

Ta có: $\forall n \in Z, n^3 \equiv -1, 0$ hoặc $1[9]$. Vì $(-1)^5 = -1, 0^5 = 0, 1^5 = 1$, ta suy ra:

$\forall n \in \mathbb{Z}, n^{15} = (n^3)^5 \equiv n^3[9]$.

Mod. 5, 7, 13: áp dụng định lý nhỏ Fermat (bài tập 4.4.50).

4.4.53 a) $21840 = 2^4.3.5.7.13$.

Mod.16:

N	±1	±3	±5	±7
n^2	1	1	1	1

Thật vậy: $3^{12} = 9^6 \equiv (-7)^6 = (7^2)^3 \equiv 1^3 = 1 = 25^6 \equiv (-7)^6 \equiv 1$, $7^{12} = 49^6 = 1^6 = 1$

Mod.3, 5, 7, 13: Áp dụng định lý nhỏ Fermat (bài tập 4.4.50)

b) $16320 = 2^6.3.5.17$.

Mod. 64: Vì p lẻ, nên tồn tại $(q, \varepsilon) \in \mathbb{N}^* \times \{-1, 1\}$ sao cho $p = 4q + \varepsilon$, từ đó, bằng cách khai triển theo công thức nhị thức Newton:

$$p^{16} = (\varepsilon + 4q)^{16} = 1 + 16.4\varepsilon q + \frac{16.15}{2}(4q)^2 + \sum_{k=3}^{16} C_{16}^k (4q)^k \varepsilon^{16-k} \equiv 1\ [64].$$

Mod. 3, 5,17: Áp dụng định lý nhỏ Fermat (bài tập 4.4.50).

4.4.54 $30 = 2.3.5$.

Mod. 5: • Nếu $5 \mid a$, thì (định lý nhỏ Fermat, bài tập 4.4.50): $a^4 \equiv 1[5]$, từ đó $(a^4)^b \equiv (a^4)^c \equiv 1$, và do vậy $a^{4b+d} - a^{4c+d} \equiv 0\ [5]$.

• Nếu $5 \mid a$, thì $a^{4b+d} - a^{4c+d} \equiv 0\ [5]$.

Suy luận tương tự với modulo 2 và 3.

4.4.55 Ta chú ý: $1729 = 7.13.19$ và $6.12.18$ chia hết 1728: $1728 = 6.288 = 12.144 = 18.96$. Theo định lý Fermat nhỏ (bài tập 4.4.50):

Mod. 7: $n^6 \equiv 1\ [7]$, vậy $n^{1728} = (n^6)^{288} \equiv 1\ [7]$

Mod. 13: $n^{12} \equiv 1\ [13]$, vậy $n^{1728} = (n^{12})^{144} \equiv 1\ [13]$

Mod. 19: $n^{18} \equiv 1\ [19]$, vậy $n^{1728} = (n^{18})^{96} \equiv 1\ [19]$.

Vì 7, 13, 19 nguyên tố cùng nhau từng đôi, ta kết luận: $1^{1728} \equiv 1\ [1729]$.

4.4.56 a) Chú ý: $\frac{p-1}{2} \in \mathbb{N}^*$.

Theo định lý nhỏ Fermat (bài tập 4.4.50), p chia hết $n^{p-1} - 1$.

Vì $n^{p-1} - 1 = \left(n^{\frac{p-1}{2}} - 1\right)\left(n^{\frac{p-1}{2}} + 1\right)$ và p nguyên tố, ta kết luận:

$p \mid n^{\frac{p-1}{2}} - 1$ hoặc $p \mid n^{\frac{p-1}{2}} + 1$.

b) Theo định lý nhỏ Fermat, tồn tại $\lambda \in \mathbb{N}$ sao cho: $n^{p-1} = 1 + \lambda p$.

Thế thì ta có:

$$n^{p(p-1)} = (1+\lambda p)^p = 1 + C_p^1 \lambda p + \sum_{k=2}^{p} C_p^k \lambda^k p^k \equiv 1\ [p^2].$$

Ta chú ý: $\frac{p(p-1)}{2} \in \mathbb{N}^*$.

Ký hiệu $a = n^{\frac{p(p-1)}{2}} - 1$ và $b = n^{\frac{p(p-1)}{2}} + 1$, ta có: $a \in \mathbb{N}^*, b \in \mathbb{N}^*, p^2 \mid ab$.

Nếu $p^2 \nmid a$ và $p^2 \nmid b$, thì vì p là nguyên tố, nên ta có $p \mid a$ và $p \mid b$, từ đó $p \mid b - a = 2$, $p = 2$.

Thế thì n lẻ và: $4 \mid n - 1$ hoặc $4 \mid n + 1$, mâu thuẫn.

Vậy $p^2 \mid n^{\frac{p(p-1)}{2}} - 1$ hoặc $p^2 \mid n^{\frac{p(p-1)}{2}} + 1$.

4.4.57 **Mod.p**: Theo định lý nhỏ Fermat (bài tập 4.4.50): $\begin{cases}(n+1)^p \equiv n+1\ [p] \\ n^p \equiv n\ [p]\end{cases}$, từ đó

$(n + 1)^p - (n^p + 1) \equiv 0\ [p]$.

Mod. 2: Vì, với mọi x thuộc $\mathbb{Z}$ và mọi k thuộc $\mathbb{N}^*$, x^k và x cùng tính chất chẵn lẻ, nên ta có:

$\begin{cases}(n+1)^p \equiv n+1\ [2]\\ n^p \equiv n\ [2]\end{cases}$, từ đó: $(n+1)^p - (n^p+1) \equiv 0\ [2]$

Cuối cùng, vì $2 \wedge p = 1$, ta kết luận $(n+1)^p - (n^p+1) \equiv 0\ [2p]$.

4.4.58 Quy nạp theo k, với n cố định sao cho $n \wedge p = 1$.

Với $k = 0$, đây chính là định lý nhỏ Fermat (bài tập 4.4.50).

Ta giả thiết tính chất đúng với một k thuộc $\mathbb{N}$.

Tồn tại $\lambda \in \mathbb{Z}$ sao cho: $(n^{p^{k-1}})^{p^k} = 1 + \lambda p^{k+1}$, từ đó:

$$(n^{p^{k-1}})^{p^{k+1}} = ((n^{p^{k-1}})^{p^k})^p = (1+\lambda p^{k+1})^p = 1 + C_p^1 \lambda p^{k+1} \equiv + \sum_{i=2}^{p} C_p^i \lambda^i p^{(k+1)i}.$$

Vì $\forall i \in \{2,\ldots, p\}$, $(k+1)i \geq k+2$, ta suy ra: $(n^{p^{k-1}})^{p^{k+1}} \equiv 1\ [p^{k+2}]$

4.4.59 a) Vì các vai trò của (a, b) và (α, β) đối xứng, ta có thể giả thiết, chẳng hạn $\beta \geq b$. Tồn tại $\lambda \in \mathbb{N}$ sao cho: $\beta = b + \lambda(p-1)$. Theo định lý nhỏ Fermat (bài 4.4.50), $a^{p-1} \equiv 1[p]$, từ đó: $a^b = a^b(a^{p-1})^\lambda \equiv a^b\ [p]$.

Mặt khác, vì $\alpha \equiv a\ [p]$, ta có: $\alpha^\beta \equiv a^\beta\ [p]$.

Ta kết luận: $\alpha^\beta \equiv a^b\ [p]$

b) Cho $(x, y) \in (\mathbb{N}^*)^2$.

1) Nếu $5 \mid x$, thì $x^y \equiv 0\ [5]$; vậy ta có thể giả thiết $5 \nmid x$. Tồn tại $x \in \{-2,-1, 1, 2\}$ và $Y = \{0, 1, 2, 3\}$ sao cho:

$x \equiv X\ [5]$ và $y \equiv Y\ [4]$.

Ta tính X^Y modulo 5:

X \ Y	0	1	2	3
-2	1	-2	-1	②
-1	1	-1	1	-1
1	1	1	1	1
2	1	②	-1	-2

Như thế:

$$X^Y \equiv 2\ [5] \Leftrightarrow \begin{cases}(X = 2, Y = 1)\\ \text{hoặc}\\ (X = -2, Y = 3).\end{cases}$$

2) Tương tự, ta có thể giả thiết $7 \nmid y$, và tồn tại $u \in \{-3, -2, -1, 1, 2, 3\}$ và $v \in \{0, 1, 2, 3, 4, 5\}$ sao cho: $y \equiv u\ [7]$ và $x \equiv v\ [6]$.

u \ v	0	1	2	3	4	5
-3	1	-3	2	1	-3	2
-2	1	-2	-3	-1	2	③
-1	1	-1	1	-1	1	-1
1	1	-	1	1	1	1
2	1	2	-3	1	2	-3
3	1	③	2	-1	-3	-2

Như thế: $u^v \equiv 3\ [7] \Leftrightarrow \begin{cases} (u=3, v=1) \\ \text{hoặc} \\ (u=-2, v=5) \end{cases}$.

Vậy ta có: $\begin{cases} x^y \equiv 2\ [5] \\ y^x \equiv 3\ [7] \end{cases} \Leftrightarrow \begin{cases} x \equiv 2\ [5] \quad \text{và} \quad y \equiv 1\ [4] \\ \text{hoặc} \\ x \equiv -2\ [5] \text{và} \quad y \equiv 3\ [4] \\ x \equiv 2\ [6] \quad \text{và} \quad y \equiv 3\ [7] \\ \text{hoặc} \\ x \equiv 5\ [6] \quad \text{và} \quad y \equiv -2\ [7] \end{cases}$

Giải các hệ đồng dư thực trên, chú ý rằng: $5 \wedge 6 = 1$ và $4 \wedge 7 = 1$.

Chẳng hạn:

$$\begin{cases} x \equiv 2[5] \\ x \equiv 1[6] \end{cases} \Leftrightarrow \begin{cases} x \equiv 7[5] \\ x \equiv 7[6] \end{cases} \Leftrightarrow x \equiv 7[30].$$

Xem thêm định lý Trung Hoa, bài tập 4.3.16.

◇ **Trả lời:**

$((7+30\mathbb{N}) \times (17+28\mathbb{N})) \cup ((17+30\mathbb{N}) \times (5+28\mathbb{N})) \cup ((23+30\mathbb{N}) \times (3+28\mathbb{N})) \cup ((23+30\mathbb{N}) \times (19+28\mathbb{N}))$.

4.4.60 Theo định lý nhỏ Fermat (bài tập 4.4.50): $a^p \equiv a\ [p]$ và $b^p \equiv b\ [p]$.

Vì $a^p \equiv b^p [p]$, ta suy ra $a \equiv b\ [p]$; tồn tại $\lambda \in \mathbb{Z}$ sao cho $a = b + \lambda p$. Ta có:

$$a^p = (b+\lambda p)^p = b^p + C_p^1 b^{p-1} \lambda p + \sum_{k=2}^{p} C_p^k b^{p-k} (\lambda p)^k \equiv b^p [p^2].$$

4.4.61 Theo định lý nhỏ Fermat (bài tập 4.4.50): $p^{q-1} \equiv 1\ [q]$.

Mặt khác, vì $p - 1 \geq 1$: $q^{p-1} \equiv 0\ [q]$. Từ đó: $p^{q-1} + q^{p-1} \equiv 1\ [q]$.

Trao đổi p và q: $p^{q-1} + q^{p-1} \equiv 1\ [p]$

Vì $p \wedge q = 1$, ta kết luận: $p^{q-1} + q^{p-1} \equiv 1\ [pq]$.

4.4.62 Vì p nguyên tố và $p \nmid a$ và $p \nmid b$, ta suy ra $p \nmid ab$; như thế, $F_p(a), F_p(b), F_p(ab)$ tồn tại.

Sử dụng định lý nhỏ Fermat (bài tập 4.4.50):

$$\begin{cases} a^{p-1} \equiv 1\ [p] \\ b^{p-1} \equiv 1\ [p] \end{cases} \Rightarrow (a^{p-1}-1)(b^{p-1}-1) \equiv 0\ [p^2]$$

$$\Leftrightarrow (ab)^{p-1} - 1 \equiv (a^{p-1}-1) + (b^{p-1}-1)\ [p^2]$$

$$\Leftrightarrow \frac{(ab)^{p-1}-1}{p} \equiv \frac{a^{p-1}-1}{p} + \frac{b^{p-1}-1}{p}\ [p].$$

4.4.63 Theo định lý nhỏ Fermat (bài tập 4.4.50):

$$\forall z \in \mathbb{Z}, \quad z^4 \equiv 0 \text{ hoặc } 1\ [5]$$

Giả sử $(x, y) \in \mathbb{Z}^2$. Ta có: $\begin{cases} x^4 + 781 \equiv 1 \text{ hoặc } 2\ [5] \\ 3y^4 \equiv 0 \text{ hoặc } 4\ [5] \end{cases}$, vậy $x^4 + 781 \neq 3y^4$.

4.4.64 Giả sử (x, y) là một nghiệm; thế thì $x > y \geq 1$. Theo định lý nhỏ Fermat (bài tập 4.4.50), chẳng hạn: $x^3 \equiv x\ [3]$ và $y^3 \equiv y\ [3]$, từ đó $x - y \equiv x^3 - y^3 = 999 \equiv 0\ [3]$.

Ta suy ra: $x \geq y + 3$

Rồi: $999 = x^3 - y^3 \geq (y + 3)^3 - y^3 = 9y^2 + 27y + 27 > 9y^2$, từ đó $y^2 < 111$, $y \leq 10$.

Khảo sát trường hợp $y = 1$.

Giả thiết $y \geq 2$. Thế thì $x^3 = 999 + y^3 \geq 1007$, từ đó $x \geq 11$, rồi: $y^3 = x^3 - 999 \geq 11^3 - 999 \geq 332$, vậy $y \geq 7$.

Thử các trị 7, 8, 9, 10 của y.

◇ **Trả lời**: $\{(10, 1), (12, 9)\}$.

4.4.65 a) Theo định lý nhỏ Fermat (bài tập 4.4.50): $\forall \xi \in \mathbb{Z}/p\mathbb{Z} - \{0\}$, $\xi^{p-1} = \hat{1}$ (trong đó $\hat{}$ chỉ lớp modulo p).

Đa thức $X^{p-1} - \hat{1}$ của $(\mathbb{Z}/p\mathbb{Z})[X]$ có bậc $p - 1$, và nhận $\hat{1}, \ldots, \widehat{p-1}$ là các không điểm khác nhau từng đôi. Ta suy ra:

$$X^{p-1} - \hat{1} = \prod_{k=1}^{p-1} (X - \hat{k}).$$

Thay X bởi 0: $-1 \underset{[p]}{\equiv} \prod_{k=1}^{p-1} (-k) = (-1)^{p-1}.(p-1)!$

Nếu p lẻ, thì: $(p - 1)! \equiv -1\ [p]$.

Nếu p chẵn, thì $p = 2$ và: $(p - 1)! = 1 \equiv -1\ [2]$.

b) Ta giả thiết n là hợp số; tồn tại $a \in \mathbb{N}^*$ sao cho: $2 \leq a \leq n - 1$ và $a \mid n$. Thế thì $a \mid (n - 1)!$ và $a \mid n$, vậy $(n - 1)! \not\equiv -1\ [n]$.

4.4.66 Theo định lý Wilson (bài tập 4.4.65 *a*)): $(n + 1)! \equiv -1\ [n + 2]$.

Vì $(n + 1)! + 1 = (n + 2)n! - n! + 1$, ta suy ra $n + 2 \mid n! - 1$.

Sử dụng $n \geq 4$, chứng minh rằng: $n + 2 < n! - 1$.

4.4.67 Theo định lý Wilson (bài tập 4.4.65 *a*)): $(p - 1)! \equiv -1\ [p]$, tức là ở đây:

$$p \mid (2n)! + 1.$$

Hơn nữa:

$$(2n)! + 1 = (1.2...n)((n+1)(n+2)...(2n)) + 1 \underset{[p]}{\equiv} (1.2...n)((-n(-n(-n+1)...(-1)) + 1$$

$$= (-1)^n (n!)^2 + 1 = (n!)^2 + 1.$$

4.4.68 Ta ký hiệu $a = 2((p - 3)!)$. Theo định lý Wilson (bài tập 4.4.65 *a*)).

$$a(p - 2)(p - 1) = 2((p - 1)!) \equiv -2\ [p].$$

Mặt khác: $a(p - 2)(p - 1) \equiv 2a\ [p]$.

Từ đó $2a \equiv -2\ [p]$, rồi, vì $2 \wedge p = 1$: $a \equiv -1\ [p]$.

4.4.69 Tồn tại $q \in \mathbb{N}$ sao cho $p = 4q + 3$. Ta có:

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 = ((2q+1)!)^2 \underset{[p]}{\equiv} (1.2...(2q+1))((-(4q+2))(-(4q+1)))...(-(2q+2)))$$

$$= (-1)^{2q+1}(4q+2)! = -(p-1)! \equiv 1\ [p],$$

theo định lý Wilsson, bài tập 4.4.65, *a*).

4.4.70 Phép giải giống như đối với bài tập 4.4.69.

4.4.71 1) Giả thiết n và $n + 2$ đều nguyên tố. Theo định lý Wilson (bài tập 4.4.65, *a*))

- $(n + 1)! \equiv -1\ [n]$, từ đó $4((n - 1)! + 1) + n \equiv 0\ [n]$
- $(n + 1)! \equiv -1\ [n + 2]$, từ đó:

$$4((n-1)!+1)+n = 2(2(n-1)!)+4+n \underset{[n+2]}{\equiv} 2((n+1)n(n-1)!)+2 = 2((n+1)!+1) \underset{[n+2]}{\equiv} 0.$$

Cuối cùng, vì $n \wedge (n + 2) = 1$, ta kết luận: $4((n - 1)! + 1) + n \equiv 0\ [n(n + 2)]$.

2) Chứng minh phần đảo bằng cách "đi ngược lại" các phép tính ở *1*) và sử dụng bài tập 4.4.65, *b*).

4.4.72 Theo định lý Wilson (bài tập 4.4.65a)):

$$-1 \underset{[p]}{\equiv} (p-1)! = (p-n-1)!((p-n)(p-n+1)...(p-1)) \underset{[p]}{\equiv} (p-n-1)!((-1)^n n!) \underset{[p]}{\equiv} (p-n-1)!$$

Áp dụng: Lấy $p = 71$ (nguyên tố) và $n = 9$.

Ta có: $(-1)^n n! = -9! = -2.5.7(3.4.6)(8.9) \underset{[71]}{\equiv} -70 \underset{[71]}{\equiv} 1$, từ đó $61! = (71 - 9 - 1)! \equiv -1\ [71]$,

rồi $63! = 63.62.61! \underset{[71]}{\equiv} (-9)(-8)(-1) \underset{[71]}{\equiv} -1$.

4.4.73 Tương tự như các bài tập từ 4.4.68 đến 4.4.70.

4.4.74 Sử dụng các định lý Fermat và Wilson (bài tập 4.4.50 và bài tập 4.4.65a):

$$\begin{cases} n^p \equiv n\ [p] \\ (p-1)! \equiv -1\ [p] \end{cases}, \text{ từ đó } n^p + (p - 1)!n \equiv 0\ [p].$$

4.4.75 a) Theo bài tập 4.3.16, *b*), ánh xạ $\theta : \mathbb{Z}_{ab\mathbb{Z}} \to \mathbb{Z}_{a\mathbb{Z}} \times \mathbb{Z}_{b\mathbb{Z}}$

$$\mathrm{cl}_{ab}(x) \mapsto (\mathrm{cl}_{ab}(x), \mathrm{cl}_b(x))$$

được định nghĩa đúng đắn và là một đẳng cấu nhóm cộng. Hơn nữa:

- $\forall (x, y) \in \mathbb{Z}^2$, $\theta(\mathrm{cl}_{ab}(x)\ \mathrm{cl}_{ab}(y)) = \theta(\mathrm{cl}_{ab}(xy)) = (\mathrm{cl}_a(xy), \mathrm{cl}_b(xy))$

$= (\mathrm{cl}_a(x)\ (\mathrm{cl}_a(y), (\mathrm{cl}_b(x)\ (\mathrm{cl}_b(y) = ((\mathrm{cl}_a(x), (\mathrm{cl}_b(x)\ (\mathrm{cl}_a(y), (\mathrm{cl}_b(y) = \theta((\mathrm{cl}_{ab}(x))\theta(\mathrm{cl}_{ab}(y))$

- $\theta(\mathrm{cl}_{ab}(1)) = (\mathrm{cl}_a(1), (\mathrm{cl}_b(1))$.

Cuối cùng, θ là một đẳng cấu vành.

b) Với mọi n thuộc $\mathbb{N}^*$ ta ký hiệu U_n là tập hợp các phần tử khả nghịch của vành $\mathbb{Z}/_{n\mathbb{Z}}$. Theo 4.3.4, *1*) $\varphi(n) = \text{Card}(U_n)$. Vì θ là một đẳng cấu vành, nên θ vận chuyển các phần tử khả nghịch, tức là: với mọi x thuộc $\mathbb{Z}$, $(\text{cl}_{ab}(x)$ là khả nghịch trong $\mathbb{Z}/_{ab\mathbb{Z}}$ khi và chỉ khi $((\text{cl}_a(x), \text{cl}_b(x))$ là khả nghịch trong $\mathbb{Z}/_{a\mathbb{Z}} \times \mathbb{Z}/_{b\mathbb{Z}}$. Ta dễ dàng thấy rằng điều kiện cuối cùng này quy về điều kiện $\text{cl}_a(x)$ khả nghịch trong $\mathbb{Z}/_{a\mathbb{X}}$ và $\text{cl}_b(x)$ khả nghịch trong $\mathbb{Z}/_{b\mathbb{Z}}$. Ta suy ra: $\varphi(a,b) = \text{Card}(U_{ab}) = \text{Card}(U_a \times U_b) = \text{Card}\,(U_a) \cdot \text{Card}(U_b) = \varphi(a)\varphi(b)$.

c) Vì p nguyên tố, ta có, với mọi n thuộc $\{1, ..., p^r\}$;

$$n \wedge p^r \neq 1 \Leftrightarrow n \wedge p \neq 1 \Leftrightarrow p \mid n \Leftrightarrow n \in \{kp;\ 1 \leq k \leq p^{r-1}\}$$

Từ đó: $\varphi(p^r) = p^r - \text{Card}\{kp;\ 1 \leq k \leq p^{r-1}\} = p^r - p^{r-1}$.

d) Sử dụng b) ta suy ra (bằng quy nạp) rằng, nếu $a_1, ..., a_N$ là những số nguyên tố cùng nhau từng đôi, thì : $\varphi\left(\prod_{i=1}^{N} a_i\right) = \prod_{i=1}^{N} \varphi(a_i)$

Từ đó: $\varphi(n) = \prod_{i=1}^{N} \varphi(p_i^{\eta_i}) = \prod_{i=1}^{N} (p_i^{\eta_i} - p_i^{\eta_i - 1})$.

4.4.76 Tập hợp U_n các phần tử khả nghịch của vành $\mathbb{Z}/_{n\mathbb{Z}}$ là một nhóm nhân có bản số $\varphi(n)$. Theo định lý Lagrange (C2.1): $\forall \xi \in \mathbb{Z}/_{n\mathbb{Z}},\ \xi^{\varphi(n)} = \hat{1}$, tức là:

$$\forall a \in \mathbb{Z}^*,\ (a \wedge n = 1 \Rightarrow a^{\varphi(n)} \equiv 1\ [n]).$$

Định lý Euler là một sự tổng quát hoá của định lý nhỏ Fermat vì, nếu n nguyên tố thì $\varphi(n) = n - 1$.

4.4.77 Ta ký hiệu $n = \prod_{i=1}^{N} p_i^{\eta_i}$ là dạng phân tích nguyên tố của n. Theo bài tập 4.4.75, *d*):

$$\varphi(n^k) = \varphi\left(\prod_{i=1}^{N} p_i^{\eta_i k}\right) = \prod_{i=1}^{N} (p_i^{\eta_i k} - p_i^{\eta_i k - 1}) = \left(\prod_{i=1}^{N} p_i^{\eta_i (k-1)}\right)\left(\prod_{i=1}^{N} (p_i^{\eta_i} - p_i^{\eta_i - 1})\right) = n^{k-1}\varphi(n).$$

4.4.78 $13200 = 2^4 \cdot 3 \cdot 5^2 \cdot 11$.

Mod. 16: Theo bài tập 4.1.1, tồn tại $\lambda \in \mathbb{Z}$ sao cho $n^2 = 1 + 8\lambda$, từ đó $n^4 = 1 + 16\lambda + 64\lambda^2 \equiv 1\ [16]$, $n^{20} = (n^4)^5 \equiv 1^5 = 1\ [16]$, và cuối cùng $n^{21} \equiv n\ [16]$.

Mod. 3: Theo định lý nhỏ Fermat (bài tập 4.4.50) : $n^3 \equiv n\ [3]$, từ đó $n^{21} = (n^3)^7 \equiv n^7 = (n^3)^2 n \equiv n^2 n = n^3 \equiv n\ [3]$.

Mod. 25: Theo định lý Euler (bài tập 4.4.76), vì $\varphi(25) = 5^5 - 5 = 20$ và $5 \wedge n = 1$ ta có $n^{20} \equiv 1\ [25]$, từ đó $n^{21} \equiv n\ [25]$

Mod. 11. Theo định lý nhỏ Fermat: $n^{11} \equiv n\ [11]$, từ đó $n^{21} = n^{11} n^{10} \equiv n^{11} \equiv n\ [11]$. Vì 16, 3, 25, 11 nguyên tố cùng nhau từng đôi, ta kết luận: $13200 \mid n^{21} - n$.

4.4.79 a) Ta ký hiệu $U(n)$ là tập hợp các ước ≥ 1 của n. Quan hệ $\mathcal{R}$ xác định trong $\{1, ..., n\}$ bởi:

$$i \mathcal{R} j \Leftrightarrow i \wedge n = j \wedge n$$

rõ ràng là một quan hệ tương đương.

Mỗi lớp modulo $\mathcal{R}$ chứa một và chỉ một ước của n (lớp của i chứa $i \wedge n$). Từ đó:

$$n = \text{Card}(\{1,\ldots,n\}) = \sum_{d\in U(n)} \text{Card}(\text{cl}_{\mathcal{R}}(d)).$$

Mặt khác, với mọi d thuộc $U(n)$, ánh xạ $k \to kd$ là một song ánh từ

$\{k \in \{1,\ldots,\frac{n}{d}\}, k \wedge \left(\frac{n}{d}\right) = 1\}$ lên $\text{cl}_{\mathcal{R}}(d)$), do đó Card $(\text{cl}_{\mathcal{R}}(d)) = \varphi\left(\frac{n}{d}\right)$.

Như thế: $n = \sum_{d\in U(n)} \varphi\left(\frac{n}{d}\right) = \sum_{d\in U(n)} \varphi(d)$, vì ánh xạ $U(n) \to U(n)$, $d \mapsto \frac{n}{d}$ là một hoán vị.

b) Theo a): $\forall m \in \{1,\ldots,n\}, \sum_{d|m} \varphi(d) = m$. Với mỗi k thuộc $\{1,\ldots,n\}$, $\varphi(k)$ xuất hiện đúng $E\left(\frac{n}{k}\right)$ lần trong các tổng $\sum_{d|m} \varphi(d)$ trên $(1 \le m \le n)$. Từ đó:

$$\sum_{k=1}^{n} E\left(\frac{n}{k}\right)\varphi(k) = \sum_{m=1}^{n}\left(\sum_{d|m}\varphi(d)\right) = \sum_{m=1}^{n} m = \frac{n(n+1)}{2}.$$

4.4.80 Ta ký hiệu: $E_n = \{k \in \{1,\ldots,n-1\}; k \wedge n = 1\}$

Ánh xạ $k \to n - k$ là một phép đối hợp của E_n, vì : $\forall k \in E_n$, $\begin{cases}(n-k)\wedge n = 1\\ 1 \le n-k \le n-1\\ n-(n-k) = k\end{cases}$

Từ đó: $2\sum_{k\in E_n} k = \sum_{k\in E_n} k + \sum_{k\in E_n}(n-k) = n\text{Card}(E_n) = n\varphi(n)$.

4.4.81 Vì n chẵn và ≥ 2, nên tồn tại $(q, N) \in \mathbb{N}^*$ sao cho: $n = 2^q N$ và N lẻ.

1) $\sum_{\substack{d_1|n\\ d_1 \text{ lẻ}}} \varphi\left(\frac{n}{d_1}\right) = \sum_{d_1|N} \varphi\left(2^q \frac{N}{d_1}\right) = \sum_{d_1|N} \varphi(2^q)\varphi\left(\frac{N}{d_1}\right) = \varphi(2^q)\sum_{d_1|N} \varphi\left(\frac{N}{d_1}\right)$

$= (2^q - 2^{q-1})N = 2^{q-1}N = \frac{n}{2}$, nếu chú ý $2^q \wedge \frac{N}{d_1} = 1$ và sử dụng bài tập 4.4.79a).

2) $\sum_{\substack{d_2|n\\ d_2 \text{chẵn}}} \varphi\left(\frac{n}{d_2}\right) = \sum_{\substack{\delta|2^{q-1}N\\ (d_2=2\delta)}} \varphi\left(\frac{2^{q-1}N}{\delta}\right) = 2^{q-1}N = \frac{n}{2}$.

4.4.82 **Trường hợp thứ 1**: $n = p^r$, p nguyên tố, $r \ge 2$. Thế thì $\varphi(n) = p^r - p^{r-1}$, và ta có:

$$\varphi(n) \le n - \sqrt{n} \Leftrightarrow p^{r-1} \ge \sqrt{p^r} \Leftrightarrow 2(r-1)r \ge r \ge 2.$$

Trường hợp thứ 2: n có ít nhất hai ước nguyên tố khác nhau.

Thế thì tồn tại $(a, b) \in (\mathbb{N}^*)^2$ sao cho: $n = ab$, $a \ge 2$, $b \ge 2$, $a \wedge b = 1$. Ta có:

$$\varphi(n) = \varphi(ab) = \varphi(a)\varphi(b) \le (a-1)(b-1) = n - (a+b) + 1.$$

Vì $ab = n$, nên ta có, chẳng hạn $a \ge \sqrt{n}$, từ đó: $n - (a+b) + 1 \le n - (\sqrt{n} + 2) + 1 < n - \sqrt{n}$.

4.4.83 Cho $(a,b) \in (\mathbb{N}^*)^2$ sao cho $a \wedge b = 1$.

Theo định lý Euler (bài tập 4.4.7): $a^{\varphi(b)} \equiv 1\ [b]$

Vì mặt khác $\varphi(a) \geq 1$, ta có: $b^{\varphi(a)} \equiv 0\ [b]$. Từ đó: $b \mid a^{\varphi(b)} + b^{\varphi(a)} - 1$.

Trao đổi a và b: $a \mid a^{\varphi(b)} + b^{\varphi(a)} - 1$.

Cuối cùng $a \wedge b = 1$, vậy $ab \mid a^{\varphi(b)} + b^{\varphi(a)} - 1$.

4.4.84 $\left(\sum_{k=0}^{\varphi(n)-1} a^k\right)(a-1) = a^{\varphi(n)} - 1 \equiv 0\ [n]$, theo định lý Euler, bài tập 4.4.7.

Vì $(a-1) \wedge n = 1$, ta suy ra: $\sum_{k=0}^{\varphi(n)-1} a^k \equiv 0\ [n]$.

4.4.85 Cho $(a, b) \in (\mathbb{N}^*)^2$ sao cho $a \mid b$.

Xét các dạng phân tích nguyên tố: $a = \prod_{i=1}^{N} p_i^{\alpha_i}$, $b = \prod_{i=1}^{N} p_i^{\beta_i}$ (trong đó $1 \leq \alpha_i \leq \beta_i$)

Ta có : $a\varphi(b) = \left(\prod_{i=1}^{N} p_i^{\alpha_i}\right)\left(\prod_{i=1}^{N} (p_i^{\beta_i} - p_i^{\beta_i - 1})\right) = \prod_{i=1}^{N} (p_i^{\alpha_i + \beta_i} (p_i - 1)) = b\varphi(a)$

4.4.86 Vì $a \wedge b \mid ab$, $a \mid ab$, $b \mid ab$, nên ta có, theo bài tập 4.4.85:

$$ab\varphi(a \wedge b) = (a \wedge b)\varphi(ab), \quad a\varphi(ab) = ab\varphi(a), \quad b\varphi(ab) = ab\varphi(b),$$

từ đó, bằng phép nhân: $\varphi(a \wedge b)\varphi(ab) = (a \wedge b)\varphi(a)\varphi(b)$.

4.4.87 Cùng một suy luận như trong lời giải bài tập 4.4.86, thay $a \wedge b$ bởi c, vì $c \mid ab$.

4.4.88 Theo phép chia Euclide $\varphi(a^k - 1)$ cho k, tồn tại $(q, r) \in \mathbb{N}^*$ sao cho:

$$\varphi(a^k - 1) = kq + r \text{ và } 0 \leq r < k$$

Vì $a \wedge (a^k - 1) = 1$, định lý Euler (bài tập 4.4.76) chứng tỏ: $a^{\varphi(a^k-1)} \equiv 1\ [a^k - 1]$.

Nhưng: $a^{\varphi(a^k-1)} = (a^k)^q a^r \underset{[a^k-1]}{\equiv} a^r$.

Ta suy ra: $a^k - 1 \mid a^r - 1$

Mặt khác, $0 \leq r < k$, vậy $0 \leq a^r - 1 \leq a^k - 1$, từ đó $a^r - 1 = 0$, $r = 0$, $k \mid \varphi(a^k - 1)$.

4.4.89 Rõ ràng là : $\forall m \in \mathbb{N}^*, \begin{cases} \varphi(m) \leq m-1 & \text{nếu } m \geq 2 \\ \varphi(m) = 1 & \text{nếu } m = 1 \end{cases}$

Đặc biệt: $\forall m \in \mathbb{N}^*$, $\varphi(m) \leq m$, vậy $(u_k)_{k \in \mathbb{N}}$ là dãy giảm.

Vì $(\forall k \in \mathbb{N}, u_k \in \mathbb{N})$, ta suy ra rằng $(u_k)_{k \in \mathbb{N}}$ là dãy dừng. Vậy tồn tại $r \in \mathbb{N}$ sao cho $u_{r+1} = u_r$.
Vì $(\forall m \geq 2, \varphi(m) < m)$, nên ta nhất thiết phải có: $u_r = 1$.

C.4.1 *I* 1) a) Khai triển hai vế.

b) Kết quả đơn giản từ a)

2) a) Ta ký hiệu $F = f(\mathbb{Z}/_{p\mathbb{Z}})$, $G = g(\mathbb{Z}/_{p\mathbb{Z}})$.

Vì $\mathbb{Z}/_{p\mathbb{Z}}$ là một thể, ta có: $\forall X_1, X_2 \in \mathbb{Z}/_{p\mathbb{Z}}$, $\left(f(X_1) = f(X_2) \Leftrightarrow \begin{vmatrix} X_2 = -X_1 \\ \text{hoặc} \\ X_2 = X_1 \end{vmatrix} \right)$

Như thế, F có đúng $\frac{p+1}{2}$ phần tử, chúng là $f(\hat{0}), f(\hat{1}),...f\left(\left(\widehat{\frac{p-1}{2}}\right)\right)$. Tương tự, G có đúng $\frac{p+1}{2}$ chúng là $g(\hat{0}), g(\hat{1}),...g\left(\left(\widehat{\frac{p-1}{2}}\right)\right)$.

Vì $\text{Card}(F) + \text{Card}(G) = p + 1 > p = \text{Card}(\mathbb{Z}/_{p\mathbb{Z}})$, ta suy ra: $F \cap G \neq \varnothing$.

Vậy tồn tại $(x, y) \in \left\{0,...\frac{p-1}{2}\right\}^2$ sao cho : $x^2 + y^2 + 1 \equiv 0\ [p]$.

b) Với $p = 2$, chỉ cần chọn: $x = y = 1$, $z = t = 0$, $k = 1$.

Nếu p lẻ, theo a) tồn tại $(x, y) \in \left\{0,... \frac{p-1}{2}\right\}^2$ và $k \in \mathbb{Z}$ sao cho $x^2 + y^2 + 1 = kp$ và,

vì $0 < x^2 + y^2 + 1 \leq 2\left(\frac{p-1}{2}\right)^2 + 1 < p^2$, ta có: $1 \leq k \leq p - 1$.

Vậy chỉ cần chọn $z = 1$, $t = 0$.

3) Theo 2) *b*), tập hợp $\{k \in \{1,..., p - 1\}: \exists (x, y, z, t) \in \mathbb{N}^4; x^2 + y^2 + z^2 + t^2 = kp\}$ là một bộ phận khác rỗng của $\mathbb{N}$ nên có một phần tử bé nhất, ký hiệu m.

a) Nếu m là chẵn thì, nếu cần thì hoán vị x, y, z, t, ta có: $\begin{vmatrix} x, y, z, t \text{ chẵn} \\ \text{hoặc} \\ x, y \text{ chẵn và } z, t \text{ lẻ,} \end{vmatrix}$

Thế thì $\frac{x-y}{2}, \frac{x+y}{2}, \frac{z-t}{2}, \frac{z+t}{2}$ đều thuộc $\mathbb{Z}$ và:

$$\left(\frac{x-y}{2}\right)^2 + \left(\frac{x+y}{2}\right)^2 + \left(\frac{z-t}{2}\right)^2 + \left(\frac{z+t}{2}\right)^2 = \frac{1}{2}\left(x^2 + y^2 + z^2 + t^2\right) = \frac{m}{2}p,$$

điều này mâu thuẫn với định nghĩa của m.

b) Vì $a^2 + b^2 + c^2 + d^2 \underset{[m]}{\equiv} x^2 + y^2 + z^2 + t^2 \equiv 0\ [m]$, nên tồn tại $q \in \mathbb{N}$ sao cho:

$a^2 + b^2 + c^2 + d^2 = qm$. Vì $|a| \leq \frac{m-1}{2},..., |d| \leq \frac{m-1}{2}$, ta có $qm \leq 4\left(\frac{m-1}{2}\right)^2$, vậy $q < m$.

• Giả thiết $q = 0$.

Thế thì $a = b = c = d = 0$, $x \equiv y \equiv z \equiv t \equiv 0\ [m]$, $m^2 \mid x^2 + y^2 + z^2 + t^2 = mp$, $m \mid p$, mâu thuẫn với: $1 < m \leq p - 1$ và p nguyên tố.

• Giả thiết $q \geq 1$.

Ta có $(x^2 + y^2 + z^2 + t^2)(a^2 + b^2 + c^2 + d^2) = m^2qp$.

Ký hiệu $A = ax + by + cz + dt$, $B = ay - bx + ct - dz$, $C = az - bt - cx + dy$, $D = at + bz - cy - dx$, ta được, theo *I*) *a*): $A^2 + B^2 + C^2 + D^2 = m^2qp$.

Mặt khác, modulo m:

$$A \equiv x^2 + y^2 + z^2 + t^2 \equiv 0, \quad B \equiv xy - yx + zt - tz \equiv 0,$$
$$C \equiv xz - yt - zx + ty \equiv 0, \quad D \equiv xt + yz - zy - tx \equiv 0.$$

Vậy tồn tại $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ sao cho: $A = m\alpha,..., D = m\delta$. Ta suy ra $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = qp$ điều này mâu thuẫn với định nghĩa của m.

4) Mọi số nguyên (≥ 2) đều phân tích được (ít nhất thu một cách) thành tích những số nguyên tố. Theo *3) b)*, mỗi nhân tử nguyên tố phân tích được thành tổng của bốn bình phương. Thế thì, theo *I) b)*, n phân tích được thành tổng của bốn bình phương.

II 1) a) Ta có: $\forall (i, j)$, $(x_i + x_j)^4 + (x_i - x_j)^4 = 2x_i^4 + 12x_i^2x_j^2 + 2x_j^4$, từ đó:

$$\sum_{1\leq i<j\leq 4}(x_i+x_j)^4+(x_i-x_j)^4 = 2\sum_{1\leq i<j\leq 4}(x_i^4+x_j^4)+12\sum_{1\leq i<j\leq 4}x_i^2x_j^2$$

$$= 6\sum_{k=1}^{4}x_k^4 + 12\sum_{1\leq i<j\leq 4}x_i^2x_j^2 = 6\left(\sum_{k=1}^{4}x_k^2\right)^2.$$

b) Cho $n \in \mathbb{N}$. Theo I 4), tồn tại $(x_1, ..., x_4) \in \mathbb{N}^4$ sao cho $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$; rồi, theo *a)* $6n^2$ là tổng của 12 trùng phương.

2) Theo I 4), tồn tại $(n_1, ..., n_4) \in \mathbb{N}^4$ sao cho $m = n_1^2 + n_2^2 + n_3^2 + n_4^2$; rồi theo 1) b) mỗi $6n_k^2$ ($k = 1, ..., 4$) phân tích được thành 12 trùng phương. Vậy $6m$ phân tích được thành tổng của 48 ($= 4 \times 12$) trùng phương.

3) a) $0 = 0^4 + 0^4$, $1 = 1^4 + 0^4$, $2 = 1^4 + 1^4$, $81 = 3^4 + 0^4$, $16 = 2^4 + 0^4$, $17 = 2^4 + 1^4$.

b) Cho $N \in \mathbb{N}$ sao cho $N \geq 81$. Vì 0, 1, 2, 81, 16, 17 tương ứng đồng dư modulo 6 với 0, 1, 2, 3, 4, 5, nên tồn tại $r \in \{0, 1, 2, 81, 16, 17\}$ và $n \in \mathbb{N}$ sao cho $N = 6m + r$.

Theo 2), $6m$ phân tích được thành tổng của 48 trùng phương.

Theo 3) a) r phân tích được thành tổng của 2 trùng phương.

Vậy N phân tích được thành tổng của 50 trùng phương.

4) Cho $N \in \{1, ..., 80\}$.

• Nếu $N \leq 50$ thì N phân tích được thành tổng của 50 trùng phương (N hạng tử bằng 1^4, $50 - N$ hạng tử bằng 0^4).

• Nếu $N \in \{51, ..., 80\}$, thì $3 \leq N - (2^4 + 2^4 + 2^4) \leq 32$, vậy N phân tích được thành tổng của 35 trùng phương (3 hạng tử bằng 2^4, $N - 3.2^4$ hạng tử bằng 1^4).

Như thế ta được kết quả mong muốn.

C4.2 1) a) Thấy ngay

b) Cho $(x, y, z) \in E$.

Trước tiên, vì $xyz = x^2 + y^2 + 2 > 0$, ta có: $x \neq 0$, $y \neq 0$, $z \neq 0$.

Nếu ($x \geq 0$ và $y \geq 0$), thì $z \geq 0$

Nếu ($x \leq 0$ và $y \geq 0$), thì $z \leq 0$ và $(-x, y, -z) \in E$.

Nếu ($x \geq 0$ và $y \leq 0$), thì $z \leq 0$ và $(x, -y, -z) \in E$.

Vậy ta có thể quy về $(x, y, z) \in (\mathbb{N}^*)^3$.

Hơn nữa, nếu $y \geq x$, thì $(y, x, z) \in E$ và $y \leq x$; vậy ta có thể quy về $(x, y, z) \in (\mathbb{N}^*)^3$ và $x \leq y$.

2) a) Giả sử $(x, y, z) \in G$.

• $(zx - y)^2 + x^2 + 2 - (zx - y)xz = -xyz + y^2 + x^2 + 2 = 0$, vậy $(zx - y, x, z) \in E$.

• $y(zx - y) = xyz - y^2 = x^2 + 2 > 0$ và $y > 0$, vậy $zx - y > 0$.

• Ta giả thiết $zx - y > x$.

Thế thì $y < zx - x$, vậy $y^2 < y(zx - x) = x^2 + y^2 + 2 - xy$, từ đó $xy < x^2 + 2$.

Nhưng $x < y$, vậy $xy < x^2 + 2 < xy + 2$, từ đó $x^2 + 2 = xy + 1$, $x(y - x) = 1$, $x = 1$ và $y = 2$, rồi thì, vì $x^2 + y^2 + 2 = xyz$, $7 = 2z$, mâu thuẫn.

Điều này chứng tỏ: $(zx - y, x, z) \in F$.

b) Cho $(x, y, z) \in (\mathbb{N}^*)^3$ sao cho $x = y$. Ta có:

$$x^2 + y^2 + 2 = xyz \Leftrightarrow 2x^2 + 2 = x^2 z \Leftrightarrow x^2(z-2) = 2 \Leftrightarrow \left| \begin{array}{l} (x^2 = 2 \text{ và } z-2 = 1) \\ \text{hoặc} \\ (x^2 = 1 \text{ và } z-2 = 2) \end{array} \right.$$

$$\Leftrightarrow (x = 1 \text{ và } z = 4).$$

3) Cho $(x, y, z) \in F$.

Giả thiết: $\forall n \in \mathbb{N}, f^n(x, y, z) \neq (1, 1, 4)$.

Ta chứng minh bằng quy nạp rằng: $\forall n \in \mathbb{N}, f^n(x, y, z) \in G$.

Vì $(x, y, z) \in F$ và $(x, y, z) \neq (1, 1, 4)$, theo 2) b), ta có: $(x, y, z) \in G$.

Giả thiết rằng, với một n thuộc $\mathbb{N}$, $f^n(x, y, z) \in G$. Thế thì $f^{n+1}(x, y, z) \in F$ (xem 2) a)) và $f^{n+1}(x, y, z) \neq (1, 1, 4)$ theo giả thiết, vậy $f^{n+1}(x, y, z) \in G$.

Ký hiệu $(x_n, y_n, z_n) = f^n(x, y, z)$ với $n \in \mathbb{N}$, ta có:

$$\left\{ \begin{array}{l} \forall n \in \mathbb{N}, x_n < y_n, \quad \text{vì } (x_n, y_n, z_n) \in G \\ \forall n \in \mathbb{N}, y_{n+1} = x_n, \text{ vì } (x_{n+1}, y_{n+1}, z_{n+1}) = f(x_n, y_n, z_n) \end{array} \right.$$

Như thế, $(y_n)_{n \in \mathbb{N}}$ giảm nghiêm ngặt và có các trị thuộc $\mathbb{N}^*$, mâu thuẫn: đó là "nguyên lý đi xuống vô hạn".

Điều này chứng minh: $\exists n \in \mathbb{N}, f^n(x, y, z) = (1, 1, 4)$.

Và rõ ràng rằng $f : \mathbb{Z}^3 \to \mathbb{Z}^3$ là song ánh và f^{-1}: $\begin{array}{l} \mathbb{Z}^3 \to \mathbb{Z}^3 \\ (X, Y, Z) \mapsto (Y, YZ - X, Z) \end{array}$

N	0	1	2	3	4	...
$g^n(1, 1, 4)$	(1, 1, 4)	(1, 3, 4)	(3, 11, 4)	(11, 41, 4)	(41, 153, 4)	...

Tham khảo: *The College Mathematics Journal*, Vol 22, N°4, trang 347.

C.4.3 ***I*** 1) a) Giả thiết tồn tại $\xi_0 \in \mathbb{Z}/p\mathbb{Z}$ sao cho $\xi_0^2 = \hat{a}$. Ta có, với mọi ξ thuộc $\mathbb{Z}/p\mathbb{Z}$,

$$\xi^2 = \hat{a} \Leftrightarrow (\xi - \xi_0)(\xi + \xi_0) = 0 \Leftrightarrow \left| \begin{array}{l} \xi = \xi_0 \\ \text{hoặc} \\ \xi = -\xi_0 \end{array} \right. ,$$

vì $\mathbb{Z}/p\mathbb{Z}$ là một thể (vậy là một vành nguyên).

Hơn nữa, $\xi_0 \neq -\xi_0$, vì nếu không, $\hat{2}\xi_0 = 0$, do đó $\xi_0 = 0$ (vì $2 \wedge p = 1$), rồi thì $\hat{a} = \xi_0 = 0$, $p \mid a$, mâu thuẫn.

Điều này chứng tỏ phương trình $\xi^2 = \hat{a}$, với ẩn $\xi \in \mathbb{Z}/p\mathbb{Z}$, không có nghiệm hoặc có đúng hai nghiệm; hơn nữa, nếu có hai nghiệm, thì chúng thuộc $\mathbb{Z}/p\mathbb{Z} - \{0\}$.

b) Ta ký hiệu $G_p = \mathbb{Z}/p\mathbb{Z} - \{0\}$ và θ_p: $\begin{array}{l} G_p \to G_p \\ \xi \mapsto \xi^2 \end{array}$. Theo a), mỗi phần tử của $\theta_p(G_p)$ có đúng hai tạo ảnh, vậy $\text{Card}(\theta_p(G_p)) = \frac{1}{2}\text{Card}(G_p) = \frac{p-1}{2}$. Như thế có đúng $\frac{p-1}{2}$ RQ mod p. vì vậy cũng có $\frac{p-1}{2} = ((p-1) - \frac{p-1}{2})$ NRQ mod p.

α) Cho $a \in \mathbb{Z}$ sao cho $p \nmid a$. Với mỗi k thuộc $\{1, \ldots, p-1\}$, ta ký hiệu r_k là dư của phép chia Euclide ka cho p.

Giả sử tồn tại $(i, j) \in \{1,..., p-1\}^2$ sao cho $r_i = r_j$. Thế thì ta có $(i-j)a = a = ia - ja \underset{[p]}{\equiv} r_i - r_j = 0$.

Vì p nguyên tố và $p \mid a$, ta suy ra $p \mid i-j$, vậy $i = j$.

Điều này chứng minh rằng $r_1,..., r_{p-1}$ khác nhau từng đôi. Tương tự $r_1,..., r_{p-1}$ cũng đều khác không.

Suy ra $k \to r_k$ là một hoán vị của $\{1,..., p-1\}$.

Theo *b*), $\frac{p-1}{2}$ các số $r_1,..., r_{p-1}$ là những RQ mod p, và $\frac{p-1}{2}$ cũng là những NRQ mod p. Ta kết luận: $\sum_{k=1}^{p-1}\left(\frac{ka}{p}\right) = \frac{p-1}{2}.1 + \frac{p-1}{2}(-1) = 0$.

β) 1) Với $k \in \{1,..., p-2\}$, tồn tại đúng k' duy nhất thuộc $\{1,..., p-1\}$ sao cho $kk' \equiv 1$ [p], vì $\hat{k}$ (lớp modulo p của k) có nghịch đảo trong $\mathbb{Z}/p\mathbb{Z}$. Hơn nữa, $k' \neq p-1$ vì:

$k' = p-1 \Rightarrow \hat{k}' = \widehat{-1} \Rightarrow \hat{k} = \widehat{-1} \Rightarrow k = -1$.

- Giả thiết tồn tại $x \in \mathbb{Z}$ sao cho $x^2 \equiv k(k+1)$ [p]. Thế thì: $(k'x)^2 = k'^2x^2 \equiv 1 + k'$ [p]
- Ngược lại, tồn tại $y \in \mathbb{Z}$ sao cho $y^2 \equiv 1 + k'$ [p], thế thì: $(ky)^2 = k^2y^2 \equiv k^2 + k$ [p].

Điều này chứng minh rằng $k(k+10)$ là một RQ mod p khi và chỉ khi $k'+1$ là RQ mod p, vậy $\left(\frac{k(k+1)}{p}\right) = \left(\frac{k'+1}{p}\right)$.

2) Khi k chạy khắp $\{1,..., p-2\}$, k' (nghịch đảo của k modulo p) cũng chạy khắp $\{1,..., p-2\}$, từ đó sử dụng 1) và α):

$$\sum_{k=1}^{p-2}\left(\frac{k(k+1)}{p}\right) = \sum_{k'=1}^{p-2}\left(\frac{k'+1}{p}\right) = \sum_{k=2}^{p-1}\left(\frac{k}{p}\right) = -1$$

2) a) Ta phân biệt hai trường hợp:

Trường hợp thứ 1: $\left(\frac{a}{p}\right) = 1$.

Vậy tồn tại $x_0 \in \mathbb{Z}$ sao cho $x_0^2 \equiv a$ [p]. Theo định lý nhỏ Fermat (bài tập 4.4.50): $a^{\frac{p-1}{2}} = x_0^{p-1} \equiv 1$ [p]

(vì $x_0 \wedge p = 1$). vậy $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}$ [p]

Trường hợp thứ 2: $\left(\frac{a}{p}\right) = -1$.

Ta ký hiệu: $G_p = \mathbb{Z}/p\mathbb{Z} - \{0\}$ và $f : G_p \to G_p$, sao cho : $\forall \xi \in G_p$, $\xi f(\xi) = \hat{a}$.

$$\xi \mapsto \xi^{-1}\hat{a}$$

Rõ ràng f là một song ánh (thậm chí là một phép đối hợp).

Nếu tồn tại $\xi \in G_p$ sao cho $f(\xi) = \xi$, thì $\xi^2 = \hat{a}$, vậy a là một RQ mod p, mâu thuẫn. Vậy : $\forall \xi \in G_p, f(\xi) \neq \xi$.

Vậy các phần tử của G_p có thể được nhóm lại từng đôi có tích bằng $\hat{a}$, từ đó, tạo tích:

$$(\widehat{p-1})! = \prod_{\hat{k} \in G_p} \hat{k} = (\hat{a})^{\frac{1}{2}\mathrm{Card}(G_p)} = (\hat{a})^{\frac{p-1}{2}}.$$

Nhưng, theo định lý Wilson (bài tập 4.4.65 a)): $(p-1)! \equiv -1$ [p].

Ta suy ra: $a^{\frac{p-1}{2}} \equiv -1$ [p], vậy $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}$ [p].

Ví dụ: $\left(\frac{10}{31}\right) \underset{[31]}{\equiv} 10^{\frac{31-1}{2}} = (10^3)^5 \equiv 8^5 \equiv 1$.

b) Nếu $p = 4k + 1$ ($k \in \mathbb{N}^*$), thì $(-1)^{\frac{p-1}{2}} = (-1)^{2k} = 1$.

Nếu $p = 4k + 3$ ($k \in \mathbb{N}$), thì $(-1)^{\frac{p-1}{2}} = (-1)^{2k+1} = -1$.

c) α) Ta suy luận phản chứng: Giả thiết rằng không có một nhân tử nguyên tố nào đồng dư modul 4 với 3, và ký hiệu $n = \prod_{i=1}^{N} p_i^{\alpha_i}$ là dạng phân tích nguyên tố của n.

Trước tiên, $2 \nmid n$ (vì $n \equiv 3$ [4]. Và theo giả thiết: $\forall_i \in \{1,..., N\}$, $p_i \equiv 1$ [4].

Thế thì ta có: $\forall_i \in \{1,..., N\}$, $p_i^{\alpha_i} \equiv 1$[4], từ đó $n \equiv 1$ [4], mâu thuẫn.

β) Ta suy luận phản chứng: Giả thiết tồn tại (x, y, z) thuộc $\mathbb{Z}^3$ sao cho:

$$x^2 + y^3 - 8(2z + 1)^3 + 1 = 0.$$

• Trước tiên ta chứng minh y lẻ:

Thật vậy, nếu y chẵn, thì $y^3 \equiv 0$ [8], từ đó $x^2 + 1 = 8(2z + 1)^3 - y^3 \equiv 0$ [8], vậy $x^2 \equiv -1$ [8],mâu thuẫn vì bình phương của một số nguyên chỉ có thể đồng dư modulo 8 với 0, 1, 4 (xem bài tập 4.4.1).

• Ta có: $x^2 + 1 = 8(2z + 1)^3 - y^3 = (2(2z + 1) - y)A$, trong đó $A = 4(2z + 1)^2 + 2(2z + 1)y + y^2$.

Ký hiệu $y = 2Y + 1$ ($Y \in \mathbb{Z}$ Module 4): $A \equiv 2y + y^2 = 4Y^2 + 8Y + 3 \equiv 3$ [4].

Theo α, A có ít nhất một ước nguyên tố q sao cho $q \equiv 3$ [4]. Vì $A \mid x^2 + 1$, ta suy ra $q \mid x^2 + 1$, tức là -1 là RQ mod q.

Nhưng (xem b)): $\left(\frac{-1}{q}\right) = -1$ (vì $q \equiv 3$ [4]), vậy -1 là NRQ mod p, mâu thuẫn.

Ta được phương trình Lebesgues bằng cách chọn $z = 0$.

3) a) 1), 2),3) đều là hiển nhiên.

4) Sử dụng định lý Euler (2, a)): $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \underset{[p]}{\equiv} a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}} \underset{[p]}{\equiv} \left(\frac{ab}{p}\right)$.

Vì $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ và $\left(\frac{ab}{p}\right)$ đều thuộc {-1, 1} và $p \geq 3$, ta kết luận: $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

b) Cho $i \in \{1,..., N\}$.

• Nếu $i \in I$ thì $\left(\frac{p_i^{r_i}}{p}\right) = \left(\frac{\left(p_i^{\frac{r_i-1}{2}}\right)^2 p_i}{p}\right) = \left(\frac{\left(p_i^{\frac{r_i-1}{2}}\right)^2}{p}\right)\left(\frac{p_i^{r_i}}{p}\right) = \left(\frac{p_i^{r_i}}{p}\right)$.

• Nếu $i \notin I$, thì r_i chẵn và: $\left(\frac{p_i^{r_i}}{p}\right) = \left(\frac{\left(p_i^{\frac{r_i}{2}}\right)^2}{p}\right) = 1$.

Từ đó: $\left(\frac{a}{p}\right) = \prod_{i \in I}\left(\frac{p_i^{r_i}}{p}\right) = \prod_{i \in I}\left(\frac{p_i}{p}\right) = \left(\frac{a'}{p}\right)$.

4) a) Như trong 1)) c) α).

b) 1) Theo định nghĩa, $u_1,..., u_s$ đều khác nhau từng đôi, $v_1,...,v_t$ đều khác nhau từng đôi và:

$$\forall (i, k) \in \{1,..., s\} \times \{1,..., t\}, \; u_i \leq \frac{p-1}{2} < \frac{p+1}{2} \leq v_k.$$

Kết quả là $u_1,..., u_s, v_1,..., v_t$ đều khác nhau từng đôi.

Hơn nữa, vì mỗi phần tử của $\{r_1,..., r_{\frac{p-1}{2}}\}$ hoặc $\leq \frac{p-1}{2}$, hoặc $\geq \frac{p+1}{2}$, ta được:

2) Theo định nghĩa, $v_1,..., v_t$ đều khác nhau từng đôi, vậy $p - v_1, ..., p - v_t$ đều khác nhau từng đôi. Giả sử $(i, k \in \{1,...,s\}\times\{1,...,t\}$. Ta giả thiết $u_i = p - v_k$. Tồn tại: $(m,n) \in \left\{1,..., \frac{p-2}{2}\right\}^2$ sao cho $u_i \equiv ma\ [p]$ và $v_k \equiv na\ [p]$. Thế thì ta có: $(m + n)a = u_i + v_k \equiv 0\ [p]$, vậy $p \mid (m + n)$ (vì p nguyên tố và $p \mid a$). Nhưng $2 \le m + n \le p - 1$, từ đó gặp mâu thuẫn.

Điều này chứng minh $\{u_1,..., u_s\} \cap \{p - v_1,..., p - v_t\} = \varnothing$.

Cuối cùng, $u_1,..., u_s, p - v_1,..., p - v_t$ khác nhau từng đôi.

Hơn nữa: $\begin{cases} \forall i \in \{1,..., s\},\ 1 \le u_i \le \dfrac{p-1}{2} \\ \forall i \in \{1,..., t\},\ 1 \le p - v_k \le \dfrac{p-1}{2} \quad (\text{Vì } \dfrac{p-1}{2} \le v_k \le p-1) \end{cases}$

Và theo 1), $s + t = \dfrac{p-1}{2}$.

Như thế, $u_1 ... u_s, p - v_1,..., p - v_t$ là $\dfrac{p-1}{2}$ số nguyên khác nhau từng đôi và thuộc $\left\{1,... \dfrac{p-1}{2}\right\}$, vậy: $\{u_1,..., u_s, p - v_1, ... p - v_t\} = \left\{1,... \dfrac{p-1}{2}\right\}$.

c) Từ *b) 1)*, ta suy ra:

$$u_1 ... u_s (p - v_1)...(p - v_t) = r_1,..., r_{\frac{p-1}{2}} \underset{[p]}{\equiv} (a)(2a)...\left(\frac{p-1}{2}a\right) = a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!.$$

Từ đó b) 2), ta suy ra:

$$u_1,..., u_s (p - v_1)...(p - v_t) \underset{[p]}{\equiv} (-1)^t u_1,..., u_s v_1,..., v_t = (-1)^t 1.2... \frac{p-1}{2} = (-1)^t\left(\frac{p-1}{2}\right)!.$$

Từ đó: $a^{\frac{p-1}{2}}\left(\dfrac{p-1}{2}\right)! \equiv (-1)^t\left(\dfrac{p-1}{2}\right)!\ [p]$.

Vì $1 \wedge p = 1, 2 \wedge p = 1,..., \dfrac{p-1}{2} \wedge p = 1$, ta có $\left(\dfrac{p-1}{2}\right)! \wedge p = 1$ vậy ta có thể giản ước bởi $\left(\dfrac{p-1}{2}\right)!$ và ta được: $a^{\frac{p-1}{2}} \equiv (-1)^t\ [p]$.

Theo định lý Euler: $a^{\frac{p-1}{2}} \equiv \left(\dfrac{a}{p}\right)\ [p]$, vậy $\left(\dfrac{a}{p}\right) \equiv (-1)^t\ [p]$. Vì $\left(\dfrac{a}{p}\right)$ và $(-1)^t$ đều thuộc $\{-1, 1\}$ và $p \ge 3$, ta kết luận: $\left(\dfrac{a}{p}\right) = (-1)^t$.

Ví dụ: $p = 29$, $a = 8$.

j	1	2	3	4	5	6	7	8	9	10	11	12	13	14
ja	8	16	24	32	40	48	56	64	72	80	88	96	104	112
$ja \bmod p$	8	(16)	(24)	3	11	(19)	(27)	6	14	(22)	1	9	(17)	(25)

Ở đây: $t = 27$, vậy $\left(\dfrac{8}{29}\right) = (-1)^{27} - 1$.

◇ **Trả lời:** $\left(\dfrac{8}{29}\right) = -1$.

d) Với các ký hiệu của b): $a = 2, r_i = 2,..., r_{\frac{p-1}{2}} = p - 1$. Vậy ta có: $\left(\dfrac{2}{p}\right) = (-1)^t$, trong đó t là số các số nguyên $> \dfrac{p}{2}$ thuộc $\{2,4,..., p-1\}$

Vậy có đúng $E\left(\frac{p}{4}\right)$ số nguyên $\le \frac{p}{2}$ trong $\{2, 4,..., p-1\}$. Vậy có đúng $\frac{p-1}{2} - E\left(\frac{p}{4}\right)$ số nguyên $\ge \frac{p}{2}$.

Như thế: $\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2} - E\left(\frac{p}{4}\right)}$.

Ta tách các trường hợp theo dư của phép chia p cho 8.

p	$8k+1$	$8k+3$	$8k+5$	$8k+7$
$\frac{p-1}{2} - E\left(\frac{p}{4}\right)$	$2k$	$2k+1$	$2k+1$	$2k+2$
$\frac{p^2-1}{8}$	$k(8k+2)$	$(2k+1)(4k+1)$	$(2k+1)(4k+3)$	$(8k+6)(k+1)$

Rõ ràng rằng, trong mỗi một trong bốn trường hợp ($p = 8k+1, p = 8k+3, p = 8k+5, p+8k+7$), thì $\frac{p-1}{2} - E\left(\frac{p}{4}\right)$ và $\frac{p^2-1}{8}$ có cùng tính chẵn lẻ. Như thế: $(-1)^{\frac{p-1}{2} - E\left(\frac{p}{4}\right)} = (-1)^{\frac{p^2-1}{8}}$.

Ví dụ: $\left(\frac{8}{31}\right) = \left(\frac{2^3}{31}\right) = \left(\frac{2}{31}\right) = (-1)^{\frac{31^2-1}{8}} = (-1)^{120} = 1$.

◇ **Trả lời:** $\left(\frac{8}{31}\right) = 1$.

e) Ta ký hiệu $p = 8n+7$, được giả thiết là nguyên tố.

Theo d): $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{(8n+6)(n+1)} = 1$.

Và, theo định lý Euler: $\left(\frac{2}{p}\right) = (-2)^{\frac{p-1}{2}} [p]$.

Từ đó: $2^{\frac{p-1}{2}} \equiv 1 [p]$, tức là: $8n+7 \mid 2^{4n+3} - 1$.

Chứng minh (chẳng hạn, bằng quy nạp theo n): $\forall n \in \mathbb{N}^*, 8n+7 < 2^{4n+3} - 1$

II 1) a) $\text{Card}\left\{\alpha \in \mathbf{N}^*; 0 < \alpha < \frac{p}{2}\right\} = \text{Card}\left(\left\{1,..., \frac{p-1}{2}\right\}\right) = \frac{p-1}{2}$ và

$\text{Card}\left\{\beta \in \mathbf{N}^*; 0 < \beta < \frac{q}{2}\right\} = \frac{q-1}{2}$, từ đó: $\text{Card}\left\{(\alpha, \beta) \in (\mathbf{N}^*)^2; \begin{cases} 0 < \alpha < \frac{p}{2} \\ 0 < \beta < \frac{p}{2} \end{cases}\right\} = \frac{p-1}{2} \cdot \frac{q-1}{2}$.

b) Ta giả thiết tồn tại $(m,n) \in \left\{1,..., \frac{p-1}{2}\right\} \times \left\{1,..., \frac{q-1}{2}\right\}$ sao cho $(m, n) \in OC$. Khi đó ta có: $\frac{n}{m} = \frac{q}{p}$, từ đó $pn = qm$. Vì p và q đều nguyên tố và khác nhau, ta suy ra $p \mid n$ và $p \mid m$, mâu thuẫn.

Như thế, đường chéo OC của hình chữ nhật $OACB$ không chứa điểm nào thuộc $(\mathbb{N}^*)^2$.

c) 1) Giả sử $(j, k) \in \left\{1,... \frac{p-1}{2}\right\} \times \left\{1,..., \frac{q-1}{2}\right\}$. Muốn cho (j, k) ở trong tam giác OAC, cần và đủ là: $k < \frac{q}{p} j$. Với j cố định, có đúng $E\left(\frac{jq}{p}\right)$ số nguyên k trong $\left\{1,..., \frac{q-1}{2}\right\}$ thỏa mãn $k < \frac{jq}{p}$ (vì $\frac{jq}{p} \notin \mathbb{N}$).

Vậy số điểm thuộc $(\mathbb{N}^*)^2$ nằm trong tam giác OAC (tức là trong hình chữ nhật $OACB$ và ở dưới OC) là: $\sum_{j=1}^{\frac{p-1}{2}} E\left(\frac{jq}{p}\right)$.

2) Tương tự, với $k \in \left\{1,\ldots,\frac{q-1}{2}\right\}$ cố định, có đúng $E\left(\frac{kp}{q}\right)$ số nguyên j thuộc $\left\{1,\ldots,\frac{p-1}{2}\right\}$ thỏa mãn $j < \frac{kp}{q}$. Số các điểm của $(\mathbb{N}^*)^2$ nằm trong tam giác OBC là: $\sum_{k=1}^{\frac{q-1}{2}} E\left(\frac{kp}{q}\right)$.

d) Nhờ a), b), c), ta được: $\sum_{j=1}^{\frac{p-1}{2}} E\left(\frac{jq}{p}\right) + \sum_{k=1}^{\frac{q-1}{2}} E\left(\frac{kp}{q}\right) = \frac{p-1}{2}.\frac{q-1}{2}$.

Mặt khác, ta ký hiệu, với $j \in \left\{1,\ldots,\frac{p-1}{2}\right\}$ α_j và r_j là thương và dư của phép chia Euclide jq cho p : $jq = p\alpha_j + r_j$ và $0 \le r_j < p - 1$.

Ta chú ý: $\alpha_j = E\left(\frac{jq}{p}\right)$. Ta ký hiệu (với các ký hiệu của I.4): $u = \sum_{i=1}^{s} u_i, v = \sum_{k=1}^{t} v_k$.

Vậy ta có: $n + v = \sum_{i=1}^{s} u_i + \sum_{k=1}^{t} v_k = \sum_{j=1}^{\frac{p-q}{2}} r_j$ và $u + pt - v = \sum_{i=1}^{s} u_i + \sum_{k=1}^{t} (p - v_k) = \sum_{j=1}^{\frac{p-1}{2}} j = \frac{p^2-1}{8}$,

từ đó: $t \underset{[2]}{\equiv} pt \underset{[2]}{\equiv} (u+v) + (u+pt-v) = \frac{p^2-1}{8} + \sum_{j=1}^{\frac{p-1}{2}} r_j$.

Mặt khác: $\sum_{j=1}^{\frac{p-1}{2}} E\left(\frac{jq}{p}\right) \underset{[2]}{\equiv} p\sum_{j=1}^{\frac{p-1}{2}} \alpha_j = \sum_{j=1}^{\frac{p-1}{2}} (jq - r_j) = q\frac{p^2-1}{8} - \sum_{j=1}^{\frac{p-1}{2}} r_j \underset{[2]}{\equiv} \frac{p^2-1}{8} + \sum_{j=1}^{\frac{p-1}{2}} r_j$.

Kết quả là: $t \underset{[2]}{\equiv} \sum_{j=1}^{\frac{p-1}{2}} E\left(\frac{jq}{p}\right)$, vậy $\left(\frac{q}{p}\right) = (-1)^t = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} E\left(\frac{jq}{p}\right)}$.

Tương tự, trao đổi p và q: $\left(\frac{p}{q}\right) = (-1)^{\sum_{k=1}^{\frac{q-1}{2}} E\left(\frac{kp}{q}\right)}$.

Cuối cùng: $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} E\left(\frac{jq}{p}\right) + \sum_{k=1}^{\frac{q-1}{2}} E\left(\frac{kp}{q}\right)} = (-1)^{\frac{p-1}{2}.\frac{q-1}{2}}$.

2) a) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1 \Leftrightarrow \frac{p-1}{2}.\frac{q-1}{2}$ lẻ $\Leftrightarrow \left(\frac{p-1}{2}$ và $\frac{q-1}{2}$ lẻ$\right) \Leftrightarrow \begin{cases} p \equiv 3\ [4] \\ q \equiv 3\ [4] \end{cases}$.

b) Ta có: $6417 = 3^2.23.31$, từ đó $\left(\frac{6617}{6607}\right) = \left(\frac{23}{6607}\right)\left(\frac{31}{6607}\right)$.

- Vì $\begin{cases} 23 \equiv 3\ [4] \\ 6607 \equiv 3\ [4] \end{cases}$ nhờ luật tương hỗ bậc hai: $\left(\frac{23}{6607}\right) = -\left(\frac{6617}{3}\right) = -\left(\frac{6}{23}\right) = -\left(\frac{2}{23}\right)\left(\frac{3}{23}\right)$.

Theo *I 4) c)* $\left(\frac{2}{23}\right) = (-1)^{\frac{23^2-1}{8}} = (-1)^{66} = 1$.

Vì $\begin{cases} 3 \equiv 3\ [4] \\ 23 \equiv 3\ [4] \end{cases}$, ta có: $\left(\frac{3}{23}\right) = -\left(\frac{23}{3}\right) = -\left(\frac{2}{3}\right) = -(-1)^{\frac{3^2-1}{8}} = 1$

$\left(\frac{23}{\ldots}\right)$

- $\begin{cases} 31 \equiv 3\ [4] \\ 6607 \equiv 3\ [4] \end{cases}$, vậy $\left(\frac{31}{6607}\right) = -\left(\frac{6607}{31}\right) = -\left(\frac{4}{31}\right) = -\left(\frac{2^2}{31}\right) = -1$.

◇ **Trả lời:** $\left(\frac{6417}{6607}\right) = 1$.

3) 1) Ta giả thiết F_n nguyên tố. Vì $3 \equiv 3\ [4]$ và $F_n = 2^{2^n} + 1 \equiv 1\ [4]$ (vì $n \geq 1$), ta có: $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$.

Modulo 3 : $F_n = 2^{2^n} + 1 \underset{[3]}{\equiv} (-1)^{2^n} + 1 = 2$.

Từ đó: $\left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1$. Nhưng theo định lý Euler: $\left(\frac{3}{F_n}\right) \underset{[F_n]}{\equiv} 3^{\frac{F_n-1}{2}}$.

Cuối cùng: $3^{\frac{F_n-1}{2}} \equiv -1\ [F_n]$.

2) Ngược lại, giả thiết $3^{\frac{F_n-1}{2}} \equiv -1\ [F_n]$. Thế thì: $3^{F_n-1} = \left(3^{\frac{F_n-1}{2}}\right)^2 \equiv 1\ [F_n]$

Giả sử p là một ước nguyên tố bất kỳ của F_n (tất nhiên $p \geq 5$, vì $2 \nmid F_n$ và $3 \nmid F_n$). Thế thì ta có: $3^{F_n-1} \equiv 1\ [p]$.

Tập hợp $\{m \in \mathbb{N}^*;\ 3^m \equiv 1\ [p]\}$ là một bộ phận khác rỗng của $\mathbb{N}^*$ (vì nó chứa $F_n - 1$) nên có một phần tử bé nhất, ký hiệu α.

Thực hiện phép chia Euclide $F_n - 1$ cho α: tồn tại $q \in \mathbb{N}$ và $r \in \{0,...,\alpha - 1\}$ sao cho $F_n - 1 = q\alpha + r$. Ta có, modulo p : $3^{F_n-1} = (3^\alpha)^q 3^r = 3^r\ [p]$.

Vì $3^{F_n-1} \equiv 1\ [p]$, kết quả là $3^r \equiv 1\ [p]$, rồi theo định nghĩa α, $r = 0$.

Điều này chứng minh: $\alpha \mid F_n - 1 = 2^{2^n}$.

Mặt khác: $3^{\frac{F_n-1}{2}} \equiv -1\ [F_n]$, vậy $3^{\frac{F_n-1}{2}} \not\equiv 1\ [F_n]$ (vì $F_n \neq 2$), từ đó $\alpha \nmid \frac{F_n-1}{2} = 2^{2^n-1}$ (nếu α chia hết $\frac{F_n-1}{2}$, ta sẽ có $3^{\frac{F_n-1}{2}} \equiv 1\ [F_{n-1}]$).

Vì $\alpha \mid 2^{2^n}$ và $\alpha \nmid 2^{2^n-1}$, nên rõ ràng rằng: $\alpha = 2^{2^n}$.

Mặt khác, theo định lý nhỏ Fermat: $3^{p-1} \equiv 1\ [p]$ (vì $p \nmid 3$), vậy $\alpha \leq p - 1$.

Thế thì: $\alpha = F_n - 1 \leq p - 1$, vậy $F_n \leq p$. Nhưng $p \mid F_n$, từ đó $F_n = p$, F_n nguyên tố

Ví dụ: $F_5 = 2^{2^5} + 1 = 4\,294\,967\,297$.

$3^{\frac{F_5-1}{2}} = 3^{2^{31}} \equiv 10\,324\,303 \neq -1\ [4\,294\,967\,297]$, vậy F_5 là hợp số.

Ta cũng có thể "chú ý" : $F_5 = 641.6700417$.

4) a) Ta phải biện luận theo đồng dư modulo 4 của p (để sử dụng luật tương hỗ bậc hai), và đồng dư modulo 3 của p (để giản ước $\left(\frac{p}{3}\right)$), từ đó biện luận modulo 12.

Ta xét, chẳng hạn trường hợp $p \equiv -1\ [12]$; tồn tại $k \in \mathbb{N}^*$ sao cho $p = 12k - 1$.

Vì: $\begin{cases} 3 \equiv 3\ [4] \\ p \equiv 3\ [4] \end{cases}$, ta có: $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$. Rồi: $\left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1$.

Ta suy ra: $\left(\frac{3}{p}\right) = 1$.

Các trường hợp khác được xét một cách tương tự.

b) $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$ và sử dụng *I* 2) *b*) và *II* 4) *a*).

Chỉ dẫn và trả lời
các bài tập chương 5

5.1.1 ◇ **Trả lời**: $(\lambda, \mu) \in \{(-6,5),(6,13)\}$.

5.1.2 Hệ tử của hạng tử X^{2n} trong $(1 + X)^{2n}(1 - X)^{2n}$ là $\sum_{k=0}^{2n}(-1)^k C_{2n}^k C_{2n}^{2n-k}$ và $C_{2n}^{2n-k} = C_{2n}^k$.

5.1.3 $(P(1))^2 - 2b_{n+1} = (a_0 + \ldots + a_n)^2 - 2(a_1a_n + a_2a_{n-1} + \ldots + a_na_1)$

$= a_0^2 + 2a_0(a_1 + \ldots + a_n) - 2(a_1a_n + \ldots + a_na_1) + (a_1 + \ldots + a_n)^2$

$= a_0^2 + \sum_{K=1}^{n} a_k(a_0 - a_{n+1-k}) + (a_1 + \ldots + a_n)^2 \geq 0$.

5.1.4 Các P_k đều có bậc kế tiếp (xem 5.1.4, Nhận xét).

5.1.5 a) Giả sử $P \in \mathbb{R}_n[X]$; $P(X)P(-X)$ là một đa thức chẵn, có bậc $\leq 2n$. Vậy tồn tại $a_0, \ldots, a_n \in \mathbb{R}$ sao cho $P(X)P(-X) = \sum_{K=1}^{n} a_k X^{2k}$, từ đó suy ra sự tồn tại và duy nhất của $\hat{P}$, và $\hat{P} = \sum_{k=0}^{n} a_k X^k$.

b) $\widehat{PQ}(X^2) = (PQ)(X)(PQ)(-X) = P(X)Q(X)P(-X)Q(-X) = P(X)P(-X)Q(X)Q(-X)$
$= \hat{P}(X^2)\hat{Q}(X^2) = (\hat{P}\hat{Q})(X^2)$ vậy (do tính duy nhất của các hệ tử): $\widehat{PQ} = \widehat{P}\widehat{Q}$

c) Rõ ràng rằng $-\hat{1}(X^2) = (-1)^2 = 1$ (vậy $\varphi(-1) = 1$.

◇ **Trả lời**: Không.

5.1.6 Ta xét Δ: $\mathbb{C}[X] \to \mathbb{C}[X]$, $A \mapsto A(X + 1) - A(X)$, được gọi *toán tử sai phân*.

Rõ ràng rằng Δ tuyến tính và bằng quy nạp ta chứng minh rằng:

$$\forall A \in \mathbb{C}[X], \quad \forall k \in \mathbb{N}, \quad \Delta^k(A) = (-1)^k \sum_{i=0}^{k} (-1)^i C_k^i A(X + i).$$

Nói riêng: $(\Delta^n P)(0) = (-1)^n \sum_{k=0}^{n} (-1)^k C_n^k P(k)$

Nhưng $\deg(P) < n$, từ đó $\deg(\Delta P) < n - 1, \ldots, \deg(\Delta^n P) < 0$, vậy $\Delta^n P = 0$.

5.1.7 Do trường hợp $A = 0$ có thể thấy ngay, ta giả thiết $A \neq 0$ và ký hiệu $n = \deg(A)$. Ánh xạ f: $\mathbb{C}_n[X] \to \mathbb{C}_n[X]$, $P \mapsto P(X - \alpha) + P(X - \beta)$ tuyến tính và là song ánh, vì nếu ký hiệu $e_i = X^i$ $(0 \leq i \leq n)$ thì $f(e_i)$ có bậc i.

5.1.8 1) Cho f là một tự đẳng cấu của K - đại số $K[X]$. Tồn tại $A \in K[X] - \{0\}$, sao cho $f(A) = X$; ta ký hiệu $A = \sum_{i=0}^{n} a_i X^i$.

Ta có: $X = f(A) = f\left(\sum_{i=0}^{n} a_i X^i\right) = \sum_{i=0}^{n} a_i (f(X))^i = A \circ (f(X))$

So sánh các bậc (xem 5.1.5, Mệnh đề 1), ta suy ra: $\deg(A) = \deg(f(X)) = 1$.

Vậy tồn tại $(\alpha, \beta) \in K^* \times K$ sao cho $f(X) = \alpha X + \beta$.

Với mọi đa thức $P = \sum_{k=0}^{p} b_k X^k$ thuộc $K[X]$, ta có:

$$f(P) = \sum_{k=0}^{p} b_k (\alpha X + \beta)^k = P(\alpha X + \beta) \text{ (hợp thành).}$$

2) Ngược lại, giả sử $(\alpha, \beta) \in K^* \times K$ và $f : K[X] \to K[X]$, $P \mapsto P(\alpha X + \beta)$

Thế thì $f(1) = 1$ (trong đó $1 \in K[X]$) và với mọi λ thuộc K và mọi P, Q thuộc $K[X]$:

- $f(P + Q) = (P + Q)(\alpha X + \beta) = P(\alpha X + \beta) + Q(\alpha X + \beta) = f(P) + f(Q)$
- $f(\lambda P) = (\lambda P)(\alpha X + \beta) = \lambda P(\alpha X + \beta) = \lambda f(P)$
- $f(PQ) = (PQ)(\alpha X + \beta) = P(\alpha X + \beta)Q(\alpha X + \beta) = f(P)f(Q)$.

Cuối cùng với ký hiệu $g : K[X] \to K[X]$, $Q \mapsto Q\left(\frac{X - \beta}{\alpha}\right)$, rõ ràng rằng $g \circ f = f \circ g = \mathrm{Id}_{K[X]}$, vậy f là song ánh.

◇ **Trả lời:** $\left\{ \begin{array}{l} K[X] \to K[X] \\ P \mapsto P(\alpha X + \beta) \end{array} ; (\alpha, \beta) \in K^* \times K \right\}$.

5.1.9 a) Giả sử P là chuẩn tắc thích hợp sao cho $P \neq 0$ và $n = \deg(P)$. Hệ tử của hạng tử X^n của $X(X + 1)P'' + (X + 2)P' - P$ là $n^2 - 1$, từ đó $n = 1$. Ký hiệu $P = X + \beta$ và xác định $\beta \in \mathbb{R}$.

◇ **Trả lời:** $\{\alpha(X + 2); \alpha \in \mathbb{R}\}$.

b) Suy luận như ở a) để xác định bậc của P, nếu P thích hợp

◇ **Trả lời:** $\left\{\frac{4}{9}X^3\right\}$.

5.1.10 Trước tiên chú ý rằng, nếu P_n thích hợp thì $\deg(P_n) = n$.

Ký hiệu $P_n = \sum_{k=0}^{n} a_k X^k$, ta có:

$P_n - P'_n = X^n \Leftrightarrow (a_n = 1, a_{n-1} = na_n, \ldots, a_0 = a_1)$

$\Leftrightarrow (a_n = 1, a_{n-1} = n, a_{n-2} = n(n - 1), \ldots, a_1 = n(n - 1)\ldots 2, a_0 = n!)$.

◇ **Trả lời:** $P_n = n! \sum_{k=0}^{n} \frac{X^k}{k!}$.

5.1.11 a) $P'_n = \frac{1}{n!}(X+n)^{n-1} + \frac{n-1}{n!}X(X+n)^{n-2} = \frac{(X+n)^{n-2}}{n!}(X+n+(n-1)X)$

$= \frac{1}{(n-1)!}(X+n)^{n-2}(X+1) = P_{n-1}(X+1)$.

b) *Quy nạp theo n*

Công thức là hiển nhiên với $n = 0$.

Ta giả thiết công thức đúng với một n thuộc $\mathbb{N}$. Ta có:

$$\frac{d}{dx}\left(\sum_{i+j=n+1} P_i(x)P_j(y)\right) = \sum_{i+j=n+1} P'_i(x)P_j(y)$$

$$= \sum_{\substack{i+j=n+1 \\ i\neq 1}} P_{i-1}(x+1)P_j(y) = \sum_{k+j=n} P_k(x+1)P_j(y)$$

$$= P_n((x+1)+y) = P'_{n+1}(x+y) = \frac{d}{dx}\left(P_{n+1}(x+y)\right).$$

Vậy, với $y \in \mathbb{R}$ cố định, tồn tại $C_n(y) \in \mathbb{R}$ sao cho:

$$\forall x \in \mathbb{R},\ \sum_{i+j=n+1} P_i(x)P_j(y) = P_{n+1}(x+y) + C_n(y).$$

Với hơn nữa: $\sum_{i+j=n+1} P_i(0)P_j(y) = P_{n+1}(y) = P_{n+1}(0+y) + C_n(y)$, ta suy ra $C_n(y) = 0$, từ đó được công thức mong muốn, ở cấp $n+1$.

c) Thay x vào y bởi 1.

5.1.12 a) Đa thức đã cho, xem như tam thức của X^2, có $(Y+Z)^2$ và $(Y-Z)^2$ là các "không điểm".

◇ **Trả lời:** $(X+Y+Z)(X+Y-Z)(Y+Z-X)(Z+X-Y)$.

b) ◇ **Trả lời:** $5(X+Y)(X+Z)(Y+Z)(X^2+Y^2+Z^2+XY+XZ+YZ)$.

5.1.13 1) Việc kiểm chứng rằng I và J là những iđêan là dễ dàng.

2) Rõ ràng rằng X_1X_3, X_1X_4, X_2X_3 đều thuộc E. Ta ký hiệu $P = X_1X_3 + X_1X_4 + X_2X_3$, và giả thiết $P \in E$.

Tồn tại $P_1, P_2, P_3, P_4 \in A$ sao cho: $P = (P_1X_1 + P_2X_2)(P_3X_3 + P_4X_4)$.

Với mỗi i thuộc $\{1, \ldots, 4\}$, tồn tại $p_i \in K$ và $Q_i \in A$ sao cho : $\begin{cases} P_i = p_i + Q_i \\ \mathrm{val}(Q_i) \geq 1 \end{cases}$

(trong đó $\mathrm{val}(Q_i)$ là "định giá toàn phần" của Q_i).

Thế thì: $P = (p_1X_1 + p_2X_2 + Q_1X_1 + Q_2X_2)(p_3X_3 + p_4X_4 + Q_3X_3 + Q_4X_4)$.

$= p_1p_3X_1X_3 + p_1p_4X_1X_4 + p_2p_3X_2X_3 + p_2p_4X_2X_4 + R$,

trong đó $R \in A$ là định giá toàn phần ≥ 3.

Ta suy ra: $p_1p_3 = 1$, $p_1p_4 = 1$, $p_2p_3 = 1$, $p_2p_4 = 0$, mâu thuẫn.

Như thế, $P \notin E$ và E không phải là một iđêan của A.

5.2.1 Với $n \geq 2$: $(X+1)^n - nX - 1 = \sum_{k=2}^{n} C_n^k X^k$.

5.2.2 Ta ký hiệu $A = \sum_{i=0}^{n-1} X^i$, $B = \left(\sum_{i=0}^{n} X^i\right)^p - X^n$

Ta có: $B = (A + X^n)^p - X^n = \sum_{k=1}^{p} C_p^k A^k (X^n)^{p-k} + (X^{np} - X^n)$,

và : $X^{np} - X^n = (X^n - 1)\sum_{k=1}^{p-1} (X^n)^k = A(X-1)\sum_{k=0}^{p-1} (X^n)^k$.

5.2.3 Chú ý rằng $B_n = XB_{n-1} + A\sin(n-1)\theta$, từ đó, bằng quy nạp:

$$B_n = A(\sin(n-1)\theta + X\sin(n-2)\theta + \ldots + X^{n-2}\sin\theta)$$

◇ **Trả lời:** $C_n = \sum_{k=0}^{n-2} X^k \sin(n-k-1)\theta$.

5.2.4 Thực hiện phép chia Euclide $X^4 - X + a$ cho $X^2 - aX + 1$, ta được dư:

$R = (a^3 - 2a - 1)X + (-a^2 + a + 1)$. Rõ $R = 0 \Leftrightarrow \begin{cases} a^3 - 2a - 1 = 0 \\ a^2 - a - 1 = 0 \end{cases} \Leftrightarrow a^2 - a - 1 = 0$.

◇ **Trả lời:** $\left\{\frac{1-\sqrt{5}}{2}, \frac{1+\sqrt{5}}{2}\right\}$.

5.2.5 Theo phép chia Euclide $(X\sin\theta + \cos\theta)^n$ cho $X^2 + 1$, tồn tại $Q \in \mathbb{R}[X]$ và $(a, b) \in \mathbb{R}^2$ sao cho $(X\sin\theta + \cos\theta)^n = (X^2 + 1)Q + aX + b$.

Thay X bởi i và -i : $\begin{cases} ai + b = e^{in\theta} \\ -ai + b = e^{-in\theta} \end{cases}$.

◇ **Trả lời:** $X\sin n\theta - \cos n\theta$.

5.2.6 $X^k = (X^{qn} - 1)X^r + X^r = (X^n - 1)\left(\sum_{i=0}^{q-1} X^{in+r}\right) + X^r$, và $\deg(X^r) = r < n = \deg(X^n - 1)$.

5.2.7 Ký hiệu Q là thương của phép chia Euclide P cho $X - a$, ta có: $P = (X - a)Q + \tilde{P}(a)$. Sử dụng công thức Taylor đối với đa thức:

$$(X - a)Q = P - \tilde{P}(a) = \sum_{k=1}^{n} \frac{\tilde{P}^{(k)}(a)}{k!}(X-a)^k \quad , \quad \text{trong đó } n = \deg(P).$$

◇ **Trả lời:** $\sum_{k=0}^{n-1} \frac{\widetilde{P^{(k+1)}}(a)}{(k+1)!}(X-a)^k$ trong đó $n = \deg(P)$.

5.2.8 a) Vì $\deg(P) \geq 1$ và $B \neq 0$, nên rõ ràng ràng: $B(P) \neq 0$.

Vì $\begin{cases} A = BQ + R \\ \deg(R) < \deg(B) \end{cases}$, nên ta có : $\begin{cases} A \circ P = (B \circ P)(Q \circ P) + R \circ P \\ \deg(R \circ P) = \deg(R)\deg(P) < \deg(B)\deg(P) = \deg(B \circ P). \end{cases}$

b) Trường hợp $B = 0$ có thể khảo sát dễ dàng. Nếu $B \neq 0$, với các ký hiệu của a):

$$B \mid A \Leftrightarrow R = 0 \Leftrightarrow R \circ P = 0 \Leftrightarrow B \circ P \mid A \circ P.$$

5.2.9 Chú ý rằng UCLN được tính bằng thuật toán Euclide, trong đó các đa thức trung gian đều như nhau đối với các thể K và L.

5.2.10 a) Quy nạp theo n.

• Trường hợp $n = 0$: $P_0 = 1$, $P_1 = X$, $P_2 = X^2 - 1$, vậy $P^2_1 - P_0P_2 = 1$.

• Ta giả thiết công thức đúng với một n thuộc $\mathbb{N}$. Thế thì:

$P^2_{n+2} - P_{n+1}P_{n+3} = P^2_{n+2} - P_{n+1}(XP_{n+2} - P_{n+1}) = P_{n+2}(P_{n+2} - XP_{n+1}) + P^2_{n+1} = -P_{n+2}P_n + P^2_{n+1} = 1$.

b) Suy ra từ a), theo định lý Bezout.

5.2.11 Ta suy luận phản chứng: Giả thiết $AB + BC + CA$ và ABC là không nguyên tố cùng nhau. Thế thì tồn tại một đa thức bất khả quy D thuộc $K[X]$ sao cho: $D \mid (AB + BC + CA)$ và $D \mid (ABC)$. Vì $D \mid ABC$ và D là bất khả quy, nên D chia hết A hoặc B hoặc C, chẳng hạn: $D \mid A$. Vì $D \mid A$ và $D \mid (AB + BC + CA)$, nên $D \mid BC$, rồi thì (D là bất khả quy), $D \mid B$ hoặc $D \mid C$. Như thế, chẳng hạn, $D \mid A$ và $D \mid B$, điều này mâu thuẫn với $A \wedge B = 1$.

5.2.12 (i) $\Rightarrow$ (ii):

Ta giả thiết $A \wedge B \neq 1$ và ký hiệu $D = A \wedge B$, $\deg(D) \geq 1$.

Tồn tại $(A_1, B_1) \in (K[X] - \{0\})^2$ sao cho: $A = DA_1$ và $B = DB_1$.

Ký hiệu $U = B_1$, $V = -A_1$, ta có: $AU + BV = 0$, $\deg(U) < \deg(B)$, $\deg(V) < \deg(A)$.

(ii) $\Rightarrow$ (i):

Ta giả thiết tồn tại $(U, V) \in (K[X] - \{0\})^2$ sao cho: $AU + BV = 0$, $\deg(U) < \deg(B)$, $\deg(V) < \deg(A)$. Ta ký hiệu $D = A \wedge B$. Tồn tại $(A_1, B_1) \in (K[X] - \{0\})^2$ sao cho: $A = DA_1$, $B = DB_1$, $A_1 \wedge B_1 = 1$. Vì $UA_1 + VB_1 = 0$, ta suy ra $A_1 \mid VB_1$, rồi thì $A_1 \mid V$ (vì $A_1 \wedge B_1 = 1$, định lý Gauss). Vậy tồn tại $P \in K[X] - \{0\}$ sao cho $V = PA_1$. Thế thì: $\deg(A_1) \leq \deg(V) < \deg(A)$, vậy $\deg(D) \geq 1$, $D \neq 1$.

Cuối cùng: $A \wedge B \neq 1$.

5.2.13
$$(b-a)^{2n-1} = ((X-a)-(X-b))^{2n-1} = \sum_{k=0}^{2n-1} C^k_{2n-1}(-1)^k(X-a)^{2n-1-k}(X-b)^k$$

$$= \left(\sum_{k=0}^{n-1} C^k_{2n-1}(-1)^k (X-a)^{n-1-k}(X-b)^k\right)(X-a)^n$$

$$+ \left(\sum_{k=n}^{2n-1} C^k_{2n-1}(-1)^k (X-a)^{2n-1-k}(X-b)^{k-n}\right)(X-b)^n.$$

◇ **Trả lời:**
$$U = \frac{1}{(b-a)^{2n-1}} \sum_{k=0}^{n-1} C^k_{2n-1}(-1)^k (X-a)^{n-1-k}(X-b)^k$$

$$V = \frac{1}{(b-a)^{2n-1}} \sum_{l=0}^{n-1} C^{n+l}_{2n-1}(-1)^{n+l}(X-a)^{n-1-l}(X-b)^l.$$

5.2.14 Một bước khởi đầu của phép chia dẫn đến sự dự đoán:

$$1 - abX^2 = (1 - (a+b)X + abX^2)\left(1 + \sum_{k=1}^{n}(a^k + b^k)X^k\right) + (a^{n+1} + b^{n+1} - ab(a^n + b^n)X)X^{n+1}.$$

Chứng minh hệ thức này bằng quy nạp theo n.

◇ **Trả lời:** $Q = 1+\sum_{k=1}^{n}(a^k + b^k)X^k$, $R = a^{n+1} + b^{n+1} - ab(a^n + b^n)X$.

5.2.15 Ta ký hiệu Q và R là thương và dư cần tìm: $A = BQ + X^{n+1}R$ và $\deg(Q) \leq n$.

Vì: $(1 - X)A = 1 - X^{n+1}$ và $(1 + X)B = 1 + (-1)^n X^{n+1}$,

nên ta có: $(1 + X)(1 - X^{n+1}) = (1 + X)(1 + (-1)^n X^{n+1})\, Q + (1 - X^2)X^{n+1}R$,

từ đó : $1 + X = (1 - X)Q + X^{n+1}S$, trong đó : $S = 1 + X + (-1)^n(1 - X)Q + (1 - X^2)R$.

Vì : $(1 + X) - (1 - X)Q = X^{n+1}\, S$ và $\deg(1 + X - (1 - X)Q) \leq n + 1$, ta suy ra $\deg(S) = 0$. Hơn nữa, $\widetilde{S}(1) = 2$. Như thế $S = 2$, vậy $1 + X = (1 - X)Q + 2X^{n+1}$.

Vì $\deg(Q) \leq n$, hệ thức $1 + X = (1 - X)Q + 2X^{n+1}$ chứng tỏ rằng Q là thương của phép chia $1 + X$ cho $1 - X$ theo lũy thừa tăng đến cấp n, từ đó: $Q = 1 + 2\sum_{k=1}^{n} X^k$.

Rồi thì: $(1 + X)R = 1 - (-1)^n Q$, từ đó suy ra biểu thức của R, bằng cách tách ra làm hai trường hợp tùy theo n chẵn hoặc lẻ.

◊ **Trả lời:** $Q = 1 + 2\sum_{k=1}^{n} X^k$, $R = \begin{cases} 2\sum_{k=1}^{n} X^{2k} & \text{nếu } n = 2p+1, p \in \mathbb{N} \\ -2X\sum_{k=0}^{p-1} X^{2k} & \text{nếu } n = 2p, p \in \mathbb{N}^* \end{cases}$

5.3.1 Theo phép chia Euclide A cho P, tồn tại $(Q, R) \in (K[X])^2$ sao cho:

$$A = PQ + R \text{ và } \deg(R) < n.$$

• Ta chứng minh rằng $(L_i)_{0 \leq i \leq n}$ là một cơ sở của $K_n[X]$. Cho $(\lambda_i)_{0 \leq i \leq n} \in K^{n+1}$ sao cho $\sum_{i=0}^{n} \lambda_i L_i = 0$.

Thế thì: $\forall j \in \{0, \ldots, n\}$, $\lambda_j = \left(\sum_{i=0}^{n} \alpha_i \widetilde{L}_i\right)(x_j) = 0$. Điều này chứng tỏ rằng $(L_i)_{0 \leq i \leq n}$ độc lập.

Vì hơn nữa $\dim(K_n[X]) = n + 1$ nên ta kết luận $(L_i)_{0 \leq i \leq n}$ là một cơ sở của $K_n[X]$.

• Vậy tồn tại $(\alpha_i)_{0 \leq i \leq n} \in K^{n+1}$ sao cho $R = \sum_{i=0}^{n} \alpha_i L_i$. Ta có, với mọi j thuộc $\{0, \ldots, n\}$:

$$\widetilde{A}(x_j) = \widetilde{P}(x_j)\widetilde{Q}(x_j) + \widetilde{R}(x_j) = \widetilde{R}(x_j) = \left(\sum_{i=0}^{n} \alpha_i \widetilde{L}_i\right)(x_j) = \alpha_j$$

Cuối cùng: $R = \sum_{i=0}^{n} \widetilde{A}(x_i) L_i$.

5.3.2 Tồn tại $Q \in \mathbb{R}[X]$ và $(\alpha, \beta) \in \mathbb{R}^2$ sao cho: $P_n = (X^2 + 1)Q + \alpha X + \beta$.

Thay X bởi i, ta suy ra:

$$\alpha i + \beta = P_n(i) = \prod_{k=1}^{n} (\cos a_k + i \sin a_k) = e^{i\sum_{k=1}^{n} a_k}$$

◇ **Trả lời:** $R = X\sin a + \cos a$, trong đó $a = \sum_{k=1}^{n} a_k$.

5.3.3 a) Giả sử $X - 1 \mid P(X^n)$. Thế thì $P(1) = P(1^n) = 0$, vậy tồn tại $Q \in K[X]$ sao cho $P = (X - 1)Q$. Thay X bởi X^{2n}, ta được:

$$P(X^{2n}) = (X^{2n} - 1)Q(X^{2n}) = \left(\sum_{k=0}^{2n-1} X^k\right)((X - 1)Q(X^{2n})).$$

b) Suy luận tương tự như của a).

5.3.4 Trước tiên ta chú ý rằng dư cần tìm cũng là dư của phép chia Euclide trong $\mathbb{K}[X]$ (Xem 5.2.2, Nhận xét).

Tồn tại $Q \in \mathbb{K}[X]$, $(\alpha, \beta) \in \mathbb{K}^2$ sao cho: $X^{2n+1} + (X + 1)^{n+2} = (X^2 + X + 1)Q + \alpha X + \beta$.

Thay X bởi j, ta suy ra:

$$\alpha j + \beta = j^{2n+1} + (j + 1)^{n+2} = j^{2n+1} + (-j^2)^{n+2}.$$

Tách trường hợp theo đồng dư modulo 6 của n.

◇ **Trả lời**:

$n \equiv ... [6]$	0	1	2	3	4	5
R	2X	0	-2X-2	0	2	0

5.3.5 Ký hiệu $\xi_k = \exp\left(\frac{(2k+1)i\pi}{5}\right)$ $(0 \le k \le 4)$ là các căn bậc 5 của -1 trong $\mathbb{C}$, ta có:

$$X^5 + 1 = \prod_{k=0}^{4} (X - \xi_k).$$

Thế thì: $A \mid P_n \Leftrightarrow (\forall k \in \{0, ..., 4\}, P_n(\xi_k) = 0)$.

• Rõ ràng rằng: $P_n(\xi_2) = P_n(-1) = 0$.

• Giả sử $k \in \{0, 1, 2, 3, 4\}$. Thế thì ta có: $\xi_k^4 - \xi_k^3 + \xi_k^2 - \xi_k + 1 = \frac{\xi_k^5 + 1}{\xi_k + 1} = 0$, từ đó:

$$P_n(\xi_k) = (\xi_k^4 - 1)(\xi_k^4)^n + (\xi_k + 1)\xi_k^{4n-1} = \xi_k^{4n-1}((\xi_k^3 - \xi_k) + (\xi_k + 1)) = 0.$$

5.3.6 Vì $ab = \frac{abc}{c} = -\frac{1}{c}$ và $a + b = (a + b + c) - c = -3 - c$, ta suy ra: $a^2b + ab^2 + 3ab = ab(a + b + 3) = 1$.

◇ **Trả lời**: 1.

5.3.7 a) $E = \frac{1}{x_1^2} + \frac{1}{x_2^2} + \frac{1}{x_3^2} = \frac{x_1^2x_2^2 + x_2^2x_3^2 + x_1^2x_3^2}{x_1^2x_2^2x_3^2} = \frac{\sigma_2^2 - 2\sigma_1\sigma_3}{\sigma_3^2}$, và $\sigma_1 = 0$, $\sigma_2 = p$, $\sigma_3 = -q$.

◇ **Trả lời**: $\frac{p^2}{q^2}$.

b) $E = (x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2)(x_1 + x_2 + x_3) - (x_1x_2^2x_3^2 + x_1^2x_2x_3^2 + x_1^2x_2^2x_3) = (\sigma_2^2 - 2\sigma_1\sigma_3)\sigma_1 - \sigma_2\sigma_3$, và: $\sigma_1 = 3$, $\sigma_2 = 1$, $\sigma_3 = 1$.

◇ **Trả lời**: -16.

c) • $E = 2\sum x_1^3 + 3\sum x_1^2 x_2$.

• $\sum x_1^2 x_2 = \left(\sum x_1 x_2\right)\left(\sum x_3\right) - 3x_1x_2x_3 = \sigma_2\sigma_1 - 3\sigma_3$.

• Lấy tổng ba đẳng thức $x_k^3 + px_k^2 + qx_k + r = 0$ ($k = 1, 2, 3$), ta được: $S_3 + pS_2 + qS_1 + 3r = 0$, từ đó ta suy ra trị của S_3.

◇ **Trả lời:** $-2p^3 + 3pq + 3r$.

d) **Phương pháp thứ nhất**

$E = \left(\sum x_1^2 x_2^2\right)\left(\sum x_1^3\right) - \sum x_1^2 x_2^2 x_3^2 = (\sigma_2^2 - 2\sigma_1\sigma_3)S_3 - \sigma_1\sigma_3^2$, trong đó: $S_3 = x_1^3 + x_2^3 + x_3^3$.

Ta có $\sigma_1 = 0$, $\sigma_2 = p$, $\sigma_3 = -q$ và $S_3 + pS_1 + 3q = 0$, từ đó $S_3 = -3q$.

Ta suy ra trị của E.

Phương pháp thứ hai:

$E = S_5S_2 - S_7$, trong đó $S_k = x_1^k + x_2^k + x_3^k$, với $k \in \mathbb{N}$. Ta có: $S_0 = 3$, $S_1 = \sigma_1 = 0$, $S_2 = \sigma_1^2 - 2\sigma_2 = -2p$.

Rồi cộng ba đẳng thức $x_i^3 + px_i + q = 0$ ($1 \le i \le 3$), ta được $S_3 + pS_1 + 3q = 0$, từ đó $S_3 = -3q$.

Tương tự:

$S_4 + pS_2 + qS_1 = 0$, từ đó $S_4 = 2p^2$

$S_5 + pS_3 + qS_2 = 0$, từ đó $S_5 = 5pq$

$S_7 + pS_5 + qS_4 = 0$, từ đó $S_7 = -7p^2q$.

Ta suy ra trị của E.

◇ **Trả lời:** $-3p^2q$.

e) • $E = \left(\sum x_1x_2\right)\left(\sum x_1^3\right) - \sum x_1^3x_2x_3$, $\sum x_1^3x_2x_3 = \left(\sum x_1x_2x_3\right)\left(\sum x_1^2\right) - \sum x_1^2x_2x_3x_4$.

$\sum x_1^2x_2x_3x_4 = \left(\sum x_1x_2x_3x_4\right)\left(\sum x_1\right) - 5\sigma_5$ từ đó $E = \sigma_2S_3 - \sigma_3S_2 + \sigma_4S_1 - 5\sigma_5$ nếu ký hiệu $S_k = \sum x_1^k$, $k \in \mathbb{N}^*$.

• $S_2 = \sigma_1^2 - 2\sigma_2$

• $S_3 = \left(\sum x_1^2\right)\left(\sum x_1\right) - \sum x_1^2x_2$, $\sum x_1^2x_2 = \left(\sum x_1x_2\right)\left(\sum x_1\right) - 3\sum x_1x_2x_3$

• $\sigma_1 = -4$, $\sigma_2 = 3$, $\sigma_3 = 0$, $\sigma_4 = 1$, $\sigma_5 = -1$.

◇ **Trả lời** : -83.

5.3.8 • $\sigma_1 = \sum z_1z_2 = \tau_2$

• $\sigma_2 = \sum z_1^2z_2z_3 = \left(\sum z_1z_2z_3\right)\left(\sum z_1\right) - 4\tau_4 = \tau_1\tau_3 - 4\tau_4$

• $\sigma_3 = \sum z_1^2z_2z_3z_4 + \sum z_1^2z_2^2z_3^2 = \tau_4\left(\sum z_1^2\right) + \left(\left(\sum z_1z_2z_3\right)^2 - 2\left(\sum z_1^2z_2^2z_3z_4\right)\right)$

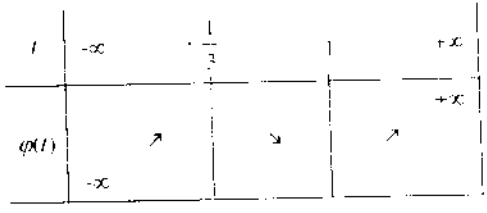
$= \tau_4(\tau_1^2 - 2\tau_2) + (\tau_3^2 - 2\tau_2\tau_4)$.

◇ **Trả lời** : $\sigma_1 = \tau_2$, $\sigma_2 = \tau_1\tau_3 - 4\tau_4$, $\sigma_3 = \tau_1^2\tau_4 + \tau_3^2 - 4\tau_2\tau_4$.

5.3.9 Bộ ba (x, y, z) thuộc $\mathbb{C}^3$ là nghiệm của hệ đã cho khi và chỉ khi x, y, z đều là nghiệm của phương trình đại số $t^3 - 2t^2 + t - p = 0$, ẩn $t \in \mathbb{C}$.

Ta khảo sát sự biến thiên của

$\varphi : \mathbb{R} \to \mathbb{R}$,
$t \mapsto t^3 - 2t^2 + t - p$



◇ **Trả lời** : $0 \le p \le \frac{4}{27}$.

5.3.10 Ký hiệu $\sigma_1, \sigma_2, \sigma_3$ là các hàm đối xứng cơ bản của x, y, z, các số phức x, y, z đều là nghiệm của phương trình $t^3 - \sigma_1 t^2 + \sigma_2 t^2 - \sigma_3 = 0$, ẩn $t \in \mathbb{C}$. Vậy ta sẽ thử thay hệ đã cho bởi một hệ tương đương đối với $\sigma_1, \sigma_2, \sigma_3$, và x, y, z sẽ được xác định như là nghiệm của một phương trình bậc ba.

Từ đó suy ra : $\begin{cases} \sigma_1 = 3 \\ \sigma_2 = 2 \\ S_3 = 9 \end{cases} \Leftrightarrow \begin{cases} \sigma_1 = 3 \\ \sigma_2 = 2 \\ \sigma_3 = 0 \end{cases}$

◇ **Trả lời** : $\{(0, 1, 2)$ và các hoán vị của chúng$\}$.

b) Ta ký hiệu $(p, q, r) \in \mathbb{C}^3$ sao cho x, y, z là nghiệm của $t^3 - pt^2 + qt - r = 0$ (ẩn $t \in \mathbb{C}$) và, với $k \in \mathbb{N}$: $S_k = x^k + y^k + z^k$.

Ta có :

- $p = \sigma_1$
- $S_3 = pS_2 - qS_1 + 3r$, vậy : $\begin{cases} \sigma_1 = 0 \\ S_3 = 6 \end{cases} \Leftrightarrow \begin{cases} p = 0 \\ r = 2 \end{cases}$
- $S_2 = \sigma_1^2 - 2\sigma_2 = p^2 - q$ và $S_5 = -qS_3 + rS_2$, vậy :

$$\begin{cases} \sigma_1 = 0 \\ S_3 = 6 \\ S_5 = 30 \end{cases} \Leftrightarrow \begin{cases} p = 0 \\ r = 2 \\ -10q = 30 \end{cases} \Leftrightarrow \begin{cases} p = 0 \\ q = -3 \\ r = 2 \end{cases}$$

◇ **Trả lời** : $\{(-1, -1, 2), (-1, 2, -1), (2, -1, -1)\}$.

c) ◇ **Trả lời**: $\{(1, i, -i)$ và các hoán vị nó$\}$.

d) ◇ **Trả lời**: $\{(1, j, j^2)$ và các giao hoán vị của nó$\}$.

5.3.11 a) Ký hiệu $\pi = z_1 z_2$, ta có:

$$\text{ĐKCĐ} \Leftrightarrow \left(\exists (z_3, \pi) \in \mathbb{C}^2 \begin{cases} -1 + z_3 = -5 \\ -z_3 + \pi = -8 \\ \pi z_3 = -1 \end{cases} \right) \Leftrightarrow \left(\exists (z_3, \pi) \in \mathbb{C}^2, \begin{cases} z_3 = -4 \\ \pi = -12 \\ \lambda = -48 \end{cases} \right) \Leftrightarrow \lambda = -48.$$

◇ **Trả lời**: • ĐCKĐ: $\lambda = -48$

• Trong trường hợp này, các nghiệm là -4 (kép), 3 (đơn).

b) Ta ký hiệu z_1, z_2, z_3 là các nghiệm và $\sigma = z_1 + z_2$, $\pi = z_1z_2$. Vì z_1, z_2 giữ những vai trò đối xứng, nên ta có thể thay điều kiện $z_1 - z_2 = 1$ bởi $(z_1 - z_2)^2 = 1$, tức là $\sigma^2 - 4\pi = 1$.

Rồi thì :

$$\left(\exists(\sigma,\pi,z_3)\in\mathbb{C}^3,\begin{cases}\sigma+z_3=0\\ \sigma z_3+\pi=p\\ \pi z_3=-q\\ \sigma^2-4\pi=1\end{cases}\right)\Leftrightarrow\left(\exists(\sigma,\pi,z_3)\in\mathbb{C}^3,\begin{cases}z_3=-\sigma\\ \pi=\dfrac{\sigma^2-1}{4}\\ -4\sigma^2+(\sigma^2-1)=4p\\ (\sigma^2-1)\sigma=4q\end{cases}\right)$$

$$\Leftrightarrow\left(\exists\sigma\in\mathbb{C},\begin{cases}\sigma^2=-\dfrac{4p+1}{3}\\ (p+1)\sigma=-3q\end{cases}\right).$$

◇ **Trả lời** : $(p + 1)^2 (4p + 1) + 27q^2 = 0$.

c) Theo bài tập 2.3.3 của Tập 1, các điểm có tọa vị z_1, z_2, z_3 tạo thành một tam giác đều thuận khi và chỉ khi $z_1 + jz_2 + j^2z_3 = 0$, tạo thành một tam giác đều nghịch khi và chỉ khi $z_1 + j^2z_2 + jz_3 = 0$; vậy chúng tạo thành một tam giác đều khi và chỉ khi $(z_1 + jz_2 + j^2z_3)(z_1 + j^2z_2 + jz_3) = 0$, tức là $z_1^2 + z_2^2 + z_3^2 - (z_1z_2 + z_2z_3 + z_1z_3) = 0$

◇ **Trả lời** : $p^2 - 3q = 0$.

d) $$\left(\exists(z_1,z_2,z_3)\in\mathbb{C}^3,\begin{cases}z_2=2z_1\\ z_1+z_2+z_3=0\\ z_1z_2+z_2z_3+z_3z_1=-7\\ z_1z_2z_3=-\lambda\end{cases}\right)\Leftrightarrow\left(\exists(z_1z_2)\in\mathbb{C}^2,\begin{cases}3z_1+z_3=0\\ 2z_1^2+3z_1z_3=-7\\ 2z_1^2z_3=-\lambda\end{cases}\right)$$

$$\Leftrightarrow\left(\exists z_1\in\mathbb{C},\begin{cases}z_1^2=1\\ 6z_1^3=\lambda\end{cases}\right).$$

◇ **Trả lời**: $\lambda = 6$ hoặc $\lambda = -6$.

e) *Phương pháp thứ nhất:*

Đầu tiên ĐKCĐ được biểu diễn bởi: $\exists(\alpha,\beta)\in\mathbb{C}^2$, $\begin{cases}2(\alpha+\beta)=-a\\ \alpha^2+4\alpha\beta+\beta^2=b\\ 2(\alpha^2\beta+\alpha\beta^2)=-c\\ \alpha^2\beta^2=d\end{cases}$, rồi nếu ký hiệu

$s = \alpha + \beta$, $p = \alpha\beta$, bởi: $\exists(s,p)\in\mathbb{C}^2$, $\begin{cases}2s=-a\\ s^2+2p=b\\ 2sp=-c\\ p^2=d\end{cases}$.

Phương pháp thứ 2:

$$(\exists(\lambda,\mu)\in\mathbb{C}^2, X^4+aX^3+bX^2+cX+d=(X^2+\lambda X+\mu)^2)$$

$$\Leftrightarrow(\exists(\lambda,\mu)\in\mathbb{C}^2, 2\lambda=a, \lambda^2+2\mu=b, 2\lambda\mu=c, \mu^2=d).$$

$$\Leftrightarrow\begin{cases}a\neq0,\left(\dfrac{a}{2}\right)^2+2\dfrac{a}{c}=b,\left(\dfrac{c}{a}\right)^2=d\\ \text{hoặc}\\ a=0,\ c=0,\left(\dfrac{b}{2}\right)^2=d.\end{cases}$$

◇ **Trả lời**: $\begin{cases}a(4b-a^2)=8c\\ (4b-a^2)^2=64d.\end{cases}$

f) Ký hiệu: $s = z_1 + z_2$, $p = z_1z_2$, $s' = z_3 + z_4$, $p' = z_3z_4$, ta có:

$$\begin{cases} p = 1 \\ \sigma_1 = 0 \\ \sigma_2 = 0 \\ \sigma_3 = -a \\ \sigma_4 = b \end{cases} \Leftrightarrow \begin{cases} p = 1 \\ s + s' = 0 \\ ss' + p + p' = 0 \\ sp' + s'p = -a \\ pp' = b \end{cases} \Leftrightarrow \begin{cases} p = 1 \\ p' = b \\ s' = -s. \\ -s^2 + (1 + b) = 0. \\ (b - 1)s = -a. \end{cases}$$

Việc khử s cho ta: $(b - 1)^2 (b + 1) - a^2 = 0$.

Áp dụng: Điều kiện được thỏa mãn. Ta có ở đây: $p = 1$, $s = 3$, $s' = -3$, $p' = 8$. Như thế, các không điểm phải tìm là các không điểm của $z^2 - 3z + 1 = 0$ và $z^2 + 3z + 8 = 0$.

◇ **Trả lời:** • $(b - 1)^2 (b + 1) - a^2 = 0$.

• *Áp dụng*: $\left\{\frac{3-\sqrt{5}}{2}, \frac{3+\sqrt{5}}{2}, \frac{-3-i\sqrt{23}}{2}, \frac{-3+i\sqrt{23}}{2}\right\}$.

g) ◇ **Trả lời:** $2\lambda + \mu - 9 = 0$.

h) ◇ **Trả lời:** • $\lambda = -7$.

• Các không điểm là: $1-\sqrt{6}$, $1+\sqrt{6}$, $\frac{3-i\sqrt{7}}{2}$, $\frac{3+i\sqrt{7}}{2}$.

i) Với ký hiệu: $\begin{cases} s, p \text{ các hàm đối xứng cơ bản của } z_1, z_2 \\ \sigma_1, \sigma_2, \sigma_3 \text{ các h.đ.x.cb. của } z_3, z_4, z_5 \end{cases}$ thì các hàm đối xứng cơ bản $\tau_1, \ldots, \tau_5$ của $z_1, \ldots, z_5$ là:

$$\tau_1 = \sigma_1 + s,\ \tau_2 = \sigma_2 + \sigma_1 s + p,\ \tau_3 = \sigma_3 + \sigma_2 s + \sigma_1 p,\ \tau_4 = \sigma_3 s + \sigma_2 p,\ \tau_5 = \sigma_3 p.$$

ĐKCĐ được biểu diễn bởi: $\exists (\sigma_1, \sigma_2, \sigma_3, s, p) \in \mathbb{C}^5$ $\begin{cases} p = 1,\ \sigma_1 = -s,\ \sigma_2 = s^2 - 1. \\ \sigma_3 = -s^3 + 2s. \\ s^4 - 3s^2 - 208 = 0. \\ \lambda = s^3 - 2s. \end{cases}$

◇ **Trả lời:** $\lambda = -56$ hoặc $\lambda = 56$.

5.3.12 a) Chú ý trước tiên rằng -1 là nghiệm, và nhân tử hóa bởi $x + 1$. Rồi với $x \in \mathbb{C}^*$:

$$x^4 + 2x^3 - x^2 + 2x + 1 = 0 \Leftrightarrow \left(x^2 + \frac{1}{x^2}\right) + 2\left(x + \frac{1}{x}\right) - 1 = 0$$

$$\Leftrightarrow y^2 + 2y - 3 = 0 \Leftrightarrow (y = 1 \text{ hoặc } y = -3).$$

Giải: $x + \frac{1}{x} = 1, x + \frac{1}{x} = -3$

◇ **Trả lời:** $\left\{-1, \frac{-3-\sqrt{5}}{2}, \frac{-3+\sqrt{5}}{2}, \frac{1-i\sqrt{3}}{2}, \frac{1+i\sqrt{3}}{2}\right\}$

b) ◇ **Trả lời:**

$$\left\{-j, -j^2, \frac{1}{4}\left(3+\sqrt{5}+\varepsilon_1 i\sqrt{6\sqrt{5}-2}\right), \frac{1}{4}\left(3-\sqrt{5}+\varepsilon_2 i\sqrt{6\sqrt{5}+2}\right); (\varepsilon_1, \varepsilon_2) \in \{-1,1\}^2\right\}.$$

5.3.13 Tồn tại $z_0 \in \mathbb{C}^*$ sao cho z_0 và $-z_0$ là nghiệm, từ đó do tổ hợp:

$$\begin{cases} z_0^6 - 4z_0^3 - 41z_0^2 - 36 = 0 \\ -z_0^4 + 5z_0^2 + 36 = 0 \end{cases}$$

Bây giờ ta chú ý rằng: $X^4 - 5X^2 - 36 \mid X^6 - 4X^3 - 41X^2 - 36$, điều này cho phép ta nhân tử hoá trong phương trình:

$$(z^2 - z + 1)(z^4 - 5z^2 - 36) = 0.$$

◇ **Trả lời**: $\{-3, 3, 2i, -2i, -j, -j^2\}$.

5.3.14 a) Thay x bởi $z - \frac{a}{3}$, ta được:

$$x^3 + ax^2 + bx + c = z^3 + \left(b - \frac{a^2}{3}\right)z + \left(c - \frac{ab}{3} + \frac{2a^3}{27}\right)$$

b) Giả sử $(\alpha, \beta) \in \mathbb{C}^2$ sao cho cả α lẫn β đều không phải là nghiệm của $z^3 + pz + q = 0$ (ẩn $z \in \mathbb{C}$).

Phép đổi biến: $y = \dfrac{\alpha - z}{\beta - z}$ sau vài dòng tính toán, quy phương trình $z^3 + pz + q = 0$ (ẩn $z \in \mathbb{C}$) về phương trình:

$(\beta^3 + p\beta + q)y^3 - (3\alpha\beta^2 + p(\alpha + 2\beta) + 3q)\,y^2 + (3\alpha^2\beta + p(2\alpha + \beta) + 3q)y - (\alpha^3 + p\alpha + q) = 0$,

(ẩn $y \in \mathbb{C}$).

Muốn cho phương trình theo y có dạng $y^3 + A = 0$, cần và đủ là: $\begin{cases} 3\alpha\beta^2 + p(\alpha + 2\beta) + 3q = 0 \\ 3\alpha^2\beta + p(2\alpha + \beta) + 3q = 0 \end{cases}$

tức là (do tổ hợp): $\begin{cases} \alpha\beta(\alpha + \beta) + p(\alpha + \beta) + 2q = 0 \\ 3\alpha\beta + p = 0. \end{cases}$

Ký hiệu $\sigma = \alpha + \beta$, $\pi = \alpha\beta$, hệ trên quy về: $\pi = -\frac{p}{3}$, $\sigma = -3\frac{q}{p}$.

Vậy chỉ cần giải một phương trình bậc 2: $t^2 + \frac{3q}{p}t - \frac{p}{3} = 0$ (ẩn $t \in \mathbb{C}$), để được α, β, rồi giải $(\beta^3 + p\beta + q)y^3 - (\alpha^3 + p\alpha + q) = 0$ (ẩn $y \in \mathbb{C}$) để được y và cuối cùng z.

Hơn nữa, với ký hiệu t cho α hoặc β, ta có:

$$t^3 + pt + q = t\left(-\frac{3q}{p}t + \frac{p}{3}\right) + pt + q = -\frac{3q}{p}\left(-\frac{3q}{p}t + \frac{p}{3}\right) + \frac{4p}{3}t + q = \frac{4p^3 + 27q^2}{3p^2}t.$$

Như thế, nếu $4p^3 + 27q^2 \neq 0$ và $\beta \neq 0$, thì ta có: $(\beta^3 + p\beta + q)y^3 - (\alpha^3 + p\alpha + q) = 0 \Leftrightarrow y^3 = \dfrac{\alpha}{\beta}$.

5.3.15 a) và b) Nếu $(P, Q) \neq (0, 0)$, thì $(X - a)^{\omega_P(a)} \mid P$ và $(X - a)^{\omega_Q(a)} \mid Q$, vậy $(X - a)^{\operatorname{Min}(\omega_P(a), \omega_Q(a))} \mid P + Q$ và $(X - a)^{\omega_P(a) + \omega_Q(a)} \mid PQ$.

Trường hợp ($P = 0$ hoặc $Q = 0$) có thể khảo sát dễ dàng.

c) Các đa thức $(X - a)^{\omega_P(a)}$ ($a \in \mathbb{Z}(P)$) nguyên tố cùng nhau từng đôi và chia hết P, vậy:

$$\prod_{a \in \mathbb{Z}(P)} (X - a)^{\omega_P(a)} \mid P, \quad \text{từ đó:} \quad \sum_{a \in \mathbb{Z}(P)} \omega_P(a) = \deg\left(\prod_{a \in \mathbb{Z}(P)} (X - a)^{\omega_P(a)}\right) \leq \deg(P)$$

d) Hơn nữa: $\displaystyle\sum_{a \in \mathbb{Z}(P)} \omega_P(a) = \deg(P) \Leftrightarrow \left(\exists \lambda \in K - \{0\},\ P = \lambda \prod_{a \in \mathbb{Z}(P)} (X - a)^{\omega_P(a)}\right)$.

5.3.16 Ta ký hiệu $P = \lambda X^n + \mu X^{n-1} + \ldots$ và, với mọi k thuộc $\{0, \ldots, n - 1\}$, s_k là tổng các không điểm của $P^{(k)}$.

Cho $k \in \{0, \ldots, n-1\}$. Vì : $P^{(k)} = \lambda \dfrac{n!}{(n-k+1)!} X^{n-k} + \mu \dfrac{(n-1)!}{(n-k)!} X^{n-k-1} + \ldots$, ta có:

$$s_k = -\frac{\mu(n-1)!}{(n-k)!} \cdot \frac{(n-k+1)!}{\lambda n!} = -\frac{(n+1)\mu}{n\lambda} + k\frac{\mu}{\lambda n}.$$

5.3.17 Ký hiệu $P = X^2 + pX + q$ và $Q = (X - \alpha)(X - \beta)$, ta có:

$$\begin{cases} P(\alpha) = \beta \\ P(\beta) = \alpha \end{cases} \Leftrightarrow \begin{cases} \alpha^2 + p\alpha + q = \beta \\ \beta^2 + p\beta + q = \alpha \end{cases} \Leftrightarrow \begin{cases} \alpha^2 + \beta^2 + p(\alpha + \beta) + 2q = \alpha + \beta \\ (\alpha - \beta)(\alpha + \beta + p + 1) = 0. \end{cases}$$

Ký hiệu $\sigma = \alpha + \beta$, $\pi = \alpha\beta$, hệ trên quy về: $\begin{cases} \sigma^2 - 2\pi + (p-1)\sigma + 2q = 0 \\ \sigma + p + 1 = 0 \end{cases}$, hoặc $\begin{cases} p = 1 - \sigma \\ q = \sigma + \pi \end{cases}$.

Thế thì: $PQ = (X^2 - \sigma X + \pi)(X^2 + pX + q)$

$$= X^4 - (1 + 2\sigma)X^3 + (\sigma^2 + 2\sigma + 2\pi)X^2 - (\sigma^2 + 2\sigma\pi + \pi)X + \pi(\sigma + \pi).$$

Vậy:

$$A = PQ \Leftrightarrow \begin{cases} 1 + 2\sigma = -(2a+1) \\ \sigma^2 + 2\sigma + 2\pi = (a-1)^2 \\ \sigma^2 + 2\sigma\pi + \pi = -b \\ \pi(\sigma + \pi) = 4 \end{cases} \Leftrightarrow \begin{cases} \sigma = -a - 1 \\ \pi = 1 - a \\ b = -3a^2 - a \\ a^3 - a - 2 = 0 \end{cases} \Leftrightarrow \left(\begin{cases} a = -1 \\ \sigma = 0 \\ \pi = 2 \\ b = -2 \end{cases} \text{ hoặc } \begin{cases} a = 2 \\ \sigma = -3 \\ \pi = -1 \\ b = -14 \end{cases} \right).$$

Cuối cùng: $(\alpha, \beta) \in \mathbb{R}^2 \Leftrightarrow \sigma^2 - 4\pi \geq 0$.

◇ **Trả lời:** $\{(2, -14)\}$.

5.3.18 • $a^2 - bc = a^2 - (ab + ac + bc) + a(b + c) = a^2 - \sigma_2 + a(\sigma_1 - a) = -\sigma_2 + a\sigma_1 = -(pa + q)$

• Phép đổi biến $y = -(px + q)$ thay phương trình $x^3 + px^2 + qx + r = 0$ (ẩn $x \in \mathbb{C}$) bởi phương trình:

$$y^3 + (3q - p^2)y^2 + (3q^2 - p^2q)y + (q^3 - rp^3) = 0.$$

◇ **Trả lời:** $y^3 + (3q - p^2)y^2 + (3q^2 - p^2q)y + (q^3 - rp^3) = 0$.

5.3.19 Điều kiện đã cho quy về: $\deg(\mathrm{UCLN}(X^4 + 2X^2 + p, X^3 + X + q)) \geq 2$.

◇ **Trả lời:** $p = 1$ và $q = 0$.

5.3.20 1) $\Rightarrow$: Hiển nhiên.

2) $\Leftarrow$:

Tất cả các hệ tử của $P = \prod_{i=1}^{n} (X + x_i) = X^n + \sum_{k=1}^{n} \sigma_k X^{n-k}$ đều ≥ 0. Vậy P không có một không điểm nào thuộc $\mathbb{R}_+^*$.

Nhưng các không điểm của P là các $-x_i$, $1 \leq i \leq n$; trong đó : $\forall i \in \{1, \ldots, n\}, x_i \geq 0$.

5.3.21 Giả sử A là một ước bất khả quy của P. Vì Q là tách được và $A \mid Q$, nên A có bậc 1. Điều này chứng tỏ rằng P là tách được.

5.3.22 Ký hiệu $x_1, \ldots, x_n$ là các không điểm của B, ta có:

$$B \mid P^2 - A \Leftrightarrow (\forall k \in \{1, \ldots, n\},\ (\tilde{P}(x_k))^2 = \tilde{A}(x_k)).$$

Ta ký hiệu, với $i \in \{1, \ldots, n\}$, $C_i = \prod_{\substack{j=1 \\ j \neq i}}^{n} (X - x_j)$ xem 5.3.1, Ví dụ).

Ta tìm P dưới dạng $P = \sum_{i=1}^{n} \lambda_i C_i$, $(\lambda_1, \ldots, \lambda_n) \in K^n$ phải tìm.

Ta có: $B \mid P^2 - A \Leftrightarrow \left(\forall k \in \{1, \ldots, n\}, \lambda_k^2 = \dfrac{\widetilde{A}(x_k)}{(\widetilde{C}_k(x_k))^2} \right)$, điều này chứng tỏ sự tồn tại của các λ_k.

5.2.23 Với $P \in \mathbb{R}[X]$, theo phép chia Euclide P cho $X^2(X-1)^2$, tồn tại $A \in \mathbb{R}[X]$ và $(a, b, c, d) \in \mathbb{R}^4$ sao cho: $P = X^2(X-1)^2 A + aX^3 + bX^2 + cX + d$.

Rồi : $\begin{cases} P(0) = 1 \\ P(1) = 0 \\ P'(0) = 0 \\ P'(1) = 1 \end{cases} \Leftrightarrow \begin{cases} d = 1 \\ a+b+c+d = 0 \\ c = 0 \\ 3a+2b+c = 1 \end{cases} \Leftrightarrow \begin{cases} a = 3 \\ b = -4 \\ c = 0 \\ d = 1 \end{cases}$.

◇ **Trả lời:** $\{ X^2(X-1)^2 A + 3X^3 - 4X^2 + 1, A \in \mathbb{R}[X] \}$.

5.3.24 a) Ký hiệu $P_n = \left(\sum_{k=0}^{n-1} X^k \right)^2 - n^2 X^{n-1}$, ta có: $P_n(1) = 0$

và $P'_n = 2\left(\sum_{k=0}^{n-1} X^k \right)\left(\sum_{k=1}^{n-1} kX^{k-1} \right) - n^2(n-1)X^{n-2}$, từ đó: $P'_n(1) = 2n\dfrac{n(n-1)}{2} - n^2(n-1) = 0$.

Kết quả là 1 là không điểm bội ít nhất là 2 của P_n, tức là: $(X-1)^2 \mid P_n$.

b) Ta ký hiệu $P_n = nX^{n+2} - (n+2)X^{n+1} + (n+2)X - n$, trong đó $P'_n = n(n+2)X^{n+1} - (n+2)(n+1)X^n + n + 2$ và $P''_n = n(n+1)(n+2)(X^n - X^{n-1})$. Ta được dễ dàng: $P_n(1) = P'_n(1) = P''_n(1) = 0$, vậy 1 là không điểm ít nhất bội ba của P_n, tức là: $(X-1)^3 \mid P$.

5.2.25 Ta ký hiệu Q, R là thương và dư của phép chia Euclide A cho B:

$$A = BQ + R \text{ và } \deg(R) \leq 3.$$

Vì $\begin{cases} R(a) = A(a) = (a-b)^{2n} \\ R(b) = A(b) = (b-a)^{2n} \end{cases}$, nên tồn tại $S \in \mathbb{C}[X]$ sao cho:

$$R - (b-a)^{2n} = (X-a)(X-b)S \text{ và } \deg(S) \leq 1.$$

Hơn nữa, lấy đạo hàm: $A' = B'Q + BQ' + R'$, từ đó: $\begin{cases} 2n(a-b)^{2n-1} = A'(a) = R'(a) = (a-b)S(a) \\ 2n(b-a)^{2n-1} = A'(b) = R'(b) = (b-a)S(b) \end{cases}$

(từ đó $S(a) = S(b) = 2n(b-a)^{2n-2}$. Vì $\deg(S) \leq 1$, ta được $S = 2n(b-a)^{2n-2}$.

◇ **Trả lời:** $R = 2n(b-a)^{2n-2}(X-a)(X-b) + (b-a)^{2n}$.

5.3.26 Khử x trong: $\begin{cases} x^4 + ax^3 + bx + 1 = 0 \\ 4x^3 + 3ax^2 + b = 0 \\ 12x^2 + 6ax = 0 \end{cases}$. Ta được: $b = -\dfrac{a^3}{4}$ và $a^4 = -16$.

◇ **Trả lời:** $(a, b) = (\sqrt{2}(\varepsilon_1 + \varepsilon_2 i), \sqrt{2}(\varepsilon_1 - \varepsilon_2 i)), (\varepsilon_1, \varepsilon_2) \in \{-1, 1\}^2$.

5.2.27 * Tính $P_n(1), P'_n, P'_n(1), P''_n, P''_n(1), \ldots$ ta được:

- $P_n(1) = 0$.
- $P'_n = 2nX^{2n-1} - n^2(n+1)X^n + 2n(n^2-1)X^{n-1} - n^2(n-1)X^{n-2}$, $P'_n(1) = 0$.
- $P''_n = 2n(2n-1)X^{2n-2} - n^3(n+1)X^{2n-1} + 2n(n^2-1)(n-1)X^{n-2} - n^2(n-1)(n-2)X^{n-3}$, $P''_n(1) = 0$.

• $P^{(3)}_n = n(n-1)(4(2n-1)X^{2n-3} - n^2(n+1)X^{n-2} + 2(n^2-1)(n-2)X^{n-3} - n(n-2)(n-3)X^{n-4})$, $P^{(3)}_n(1) = 0$.

• $P^{(4)}_n = n(n-1)(4(2n-1)(2n-3)X^{2n-4} - n^2(n+1)(n-2)X^{n-3} + 2(n^2-1)(n-2)(n-3)X^{n-4}$
$- n(n-2)(n-3)(n-4)X^{n-5})$, $P^{(4)}_n = 2n^2(n-1)(n+1) \neq 0$.

◇ **Trả lời**: Cấp bội của 1 xem như không điểm của P_n là: 4.

5.3.28 Vì $A = (X^p - 1)(X^q - 1)$, nên tất cả các không điểm của A đều có cấp ≤ 2, vậy $A \wedge A'$ là tích các $X - z$, trong đó z chạy trên tập hợp các không điểm kép của A, tức là tập hợp các căn đồng thời bậc p và bậc q của 1.

◇ **Trả lời**: $A \wedge A' = X^{(p,q,\mathrm{Ucln}(p,q))} - 1$.

5.3.29 Ta có: $\begin{cases}(P(a))^2 + \lambda(Q(a))^2 = 0\\ P(a)P'(a) + \lambda q(a)Q'(a) = 0\end{cases}$

• Nếu $Q(a) = 0$, thì $P(a) = 0$, vậy $(PQ' - P'Q)(a) = 0$.

• Nếu $Q(a) \neq 0$, thì vì $\lambda P(a)Q(a)Q'(a) = -(P(a))^2 P'(a) = \lambda(Q(a))^2 P'(a)$, ta suy ra : $P(a)Q'(a) - P'(a)Q(a) = 0$.

5.3.30 Giả sử $P \in \mathbb{C}[X]$ bất khả quy, thỏa mãn $P \mid A'B - AB'$ và $P \mid B^2$.
Vì $P \mid B^2$ và P là bất khả quy, nên $P \mid B$. Rồi ($P \mid B$ và $P \mid A'B - AB'$), vậy $P \mid AB'$. Vì $A \wedge B = 1$, ta suy ra $P \mid B'$.
Vì $P \mid B$ và B là tách được, nên P là tách ra được (xem bài tập 5.3.21), vậy $\deg(P) = 1$ (vì P bất khả quy). Thế thì B và B' có ít nhất một không điểm chung, mâu thuẫn
Điều này chứng tỏ: $(A'B - AB') \wedge B^2 = 1$.

5.3.31 *Tìm một không điểm hữu tỷ (nếu có):*

Giả sử $(p, q) \in \mathbb{Z}^* \times \mathbb{N}^*$ sao cho $p \wedge q = 1$ và $\frac{p}{q}$ là không điểm của $2X^3 - X^2 - X - 3$.

Thế thì ta có: $2p^3 - p^2q - pq^2 - 3q^3 = 0$.

Ta suy ra: $\begin{cases}p \mid 3q^3, \text{ vậy } p \mid 3\\ q \mid 2p^3, \text{ vậy } q \mid 2\end{cases}$.

Từ đó: $\frac{p}{q} \in \left\{-3, -1, 1, 3, -\frac{3}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{3}{2}\right\}$

Ta nhận thấy rằng $\frac{3}{2}$ là nghiệm.

◇ **Trả lời**: $(2X - 3)(X - j)(X - j^2)$.

5.3.32 • Ký hiệu $\omega_k = \exp\left(\frac{2ik\pi}{n}\right)$, $0 \leq k \leq n-1$, ta có:

$$\left(\frac{1+iz}{1-iz}\right)^n = a^n \Leftrightarrow \left(\exists k \in \{0, \ldots, n-1\}, \frac{1+iz}{1-iz} = a\omega_k\right) \Leftrightarrow \left(\exists k \in \{0, \ldots, n-1\}, z = i\frac{1-a\omega_k}{1+a\omega_k}\right).$$

• Với mọi ω có môđun bằng 1:

$$i\frac{1-a\omega}{1+a\omega} \in \mathbb{R} \Leftrightarrow i\frac{1-a\omega}{1+a\omega} = -i\frac{1+\frac{\overline{a}}{\omega}}{a+\frac{\overline{a}}{\omega}} \Leftrightarrow (1-|a|^2)\omega = 0 \Leftrightarrow |a| = 1.$$

◇ **Trả lời:** • Nếu $|a| = 1$ và $a^n \neq (-1)^n$, các nghiệm là: $\tan\left(\frac{\theta}{2} + \frac{k\pi}{n}\right)$, $0 \leq k \leq n-1$, trong đó $\theta = \text{Arg}(a)\ [2\pi]$

• Nếu $|a| = 1$ và $a^n = (-1)^n$, tồn tại $k_0 \in \{0, \ldots, n-1\}$ sao cho $\text{Arg}(a) = \pi - \frac{2k_0\pi}{n}\ [2\pi]$, và các nghiệm là: $\tan\left(\frac{\theta}{2} + \frac{k\pi}{n}\right)$, $k \in \{0, \ldots, n-1\} - \{k_0\}$.

5.3.33 a) Tương tự như bài tập 5.3.32. Ký hiệu $\omega_k = \exp\left(\frac{2ik\pi}{2n+1}\right)$ $k \in \{1, \ldots, 2n\}$, ta có:

$$(z+i)^{2n+1} - (z-1)^{2n+1} = 0 \Leftrightarrow \left(\exists k \in \{1, \ldots, 2n\}, \frac{z+1}{z-1} = \omega_k\right)$$

$$\Leftrightarrow \left(\exists k \in \{1, \ldots, 2n\}, z = i\frac{\omega_k + 1}{\omega_k - 1} = \text{cotan}\,\frac{k\pi}{2n+1}\right)$$

Mặt khác, áp dụng công thức nhị thức Newton, ta thấy rằng đa thức P_n có bậc $2n$, với hệ tử cao nhất là $2i(2n+1)$.

◇ **Trả lời:** $P_n = 2i(2n+1)\prod_{k=1}^{2n}\left(X - \text{cotan}\,\frac{k\pi}{2n+1}\right)$.

b) Vì $\text{cotan}\,\frac{(2n+1-k)\pi}{2n+1} = -\text{cotan}\,\frac{k\pi}{2n+1}$, nhóm các nhân tử từng đôi:

$$P_n = 2i(2n+1)\prod_{k=1}^{n}\left(X^2 - \text{cotan}^2\,\frac{k\pi}{2n+1}\right).$$

Thay X bởi ai, ta được: $P_n(ai) = 2(-1)^n i(2n+1)\prod_{k=1}^{n}\left(a^2 + \text{cotan}^2\,\frac{k\pi}{2n+1}\right)$.

Mặt khác: $P_n(ai) = (ai+i)^{2n+1} - (ai-i)^{2n+1}$

◇ **Trả lời:** $\prod_{k=1}^{n}\left(a^2 + \text{cotan}^2\,\frac{k\pi}{2n+1}\right) = \frac{(a+1)^{2n+1} - (a-1)^{2n+1}}{2(2n+1)}$

Chẳng hạn: $\prod_{k=1}^{n}\left(4 + \text{cotan}^2\,\frac{k\pi}{2n+1}\right) = \frac{3^{2n+1} - 1}{2(2n+1)}$.

5.3.34 a) ◇ **Trả lời:** $P_n = \prod_{k=1}^{n}(X - \omega_k)$ trong đó: $\omega_k = \exp\left(\frac{2ikp}{n+1}\right)$

b) Thay X bởi 1.

◇ **Trả lời:** $\prod_{k=1}^{n}\sin\frac{k\pi}{n+1} = \frac{n+1}{2^n}$.

5.3.35 a) Ký hiệu $P_n = (X^n + 1)^n - X^n$, ta có: $P_n(j) = (j^n + 1)^n - j^n$. Tách trường hợp theo đồng dư modulo 3 của n:

n	$3p$	$3p+1$	$3p+2$
$P_n(j)$	$2^n - 1$	$(-1)^{p+1}j^2 - j$	$(-1)^p j^2 - j^2$

◇ **Trả lời:** $n \equiv 2\ [6]$.

b) Ký hiệu $A = X^3 - X^2 + X - 1 = (X - 1)(X - 0)(X + 1)$, vốn là tách được và có các không điểm đơn, và $P_n = (X^2 - X + 1)^n - X^{2n} + X^n - 1$, ta có: $A \mid P_n \Leftrightarrow P_n(1) = P_n(0) = 0$, với $P_n \in \mathbb{Z}[X]$.

Trước tiên: $P_n(1) = 0$.

- Nếu $n = 2p$ $(p \in \mathbb{N})$, thì: $P_n(0) = 2(0-1)^p - 1$.
- Nếu $n = 2p + 1$ $(p \in \mathbb{N})$, thì: $P_n(0) = 0$.

◇ **Trả lời:** $n \notin 2\mathbb{N}$.

c) Ký hiệu $Z = \mathbb{U}_{12} = \mathbb{U}_4$, ta có $X^8 + X^4 + 1 = \prod_{\omega \in Z} (X - \omega)$, vốn là tách được và có các không điểm đơn. Vậy:

$$X^8 + X^4 + 1 \mid X^{8n} + pX^{4n} + q \Leftrightarrow (\forall \omega \in Z,\ \omega^{8n} + p\omega^{4n} + q = 0) \Leftrightarrow \begin{cases} 1^{2n} + p1^n + q = 0 \\ j^{4n} + pj^{2n} + q = 0 \end{cases}$$

$$\Leftrightarrow 1^{2n} + p1^n + q = 0 \ (\forall p, q) \in \mathbb{Z}^2.$$

Tách ra làm ba trường hợp theo lớp đồng dư modulo 3 của n.

◇ **Trả lời:** $\begin{cases} n \equiv 0\ [3] \\ 1 + p + q = 0 \end{cases}$ hoặc $\begin{cases} n \not\equiv 0\ [3] \\ p = q = 1 \end{cases}$.

5.3.36 Ký hiệu $P = (X - 1)(X^n - 1)A(X) = (X^n - 1)(X^{p+1} - 1)$ và $Q = (X - 1)(X^n - 1)A(X^n) = (X - 1)(X^{n(p+1)} - 1)$, ta có: $A \mid A(X^n) \Leftrightarrow P \mid Q$.

- Nếu $n \wedge (p + 1) = 1$, thì:
  - các không điểm của P là 1 (kép) và các phần tử của $\mathbb{U}_n \cup \mathbb{U}_{p+1} - \{1\}$ (đơn)
  - các không điểm của Q là 1 (kép) và các phần tử của $\mathbb{U}_{n(p+1)} - \{1\}$ (đơn),

vậy, vì $\mathbb{U}_n \cup \mathbb{U}_{p+1} \subset \mathbb{U}_{n(p+1)}$, nên $P \mid Q$.

- Nếu $n \wedge (p + 1) \neq 1$ thì P có ít nhất một không điểm kép khác 1, khi đó Q chỉ có 1 là không điểm kép, vậy $P \not\mid Q$.

◇ **Trả lời:** $n \wedge (p + 1) = 1$.

5.3.37 Các tập hợp $\mathbb{U}_p - \{1\}$, $\mathbb{U}_q - \{1\}$, $\mathbb{U}_r - \{1\}$ đôi một rời nhau (vì $p \wedge q = p \wedge r = q \wedge r = 1$), bao hàm trong $\mathbb{U}_{pqr} - \{1\}$, vậy:

$$(X^p - 1)(X^q - 1)(X^r - 1) = (X - 1)^3 \prod_{z \in \mathbb{U}_{pqr} - \mathbb{U}_p \cup \mathbb{U}_q \cup \mathbb{U}_r - \{1\}} (X - z) \prod_{z \in \mathbb{U}_p \cup \mathbb{U}_q \cup \mathbb{U}_r - \{1\}} (X - z) = (X^{pqr} - 1).$$

5.3.38 $(X^n - 1)(X^p - 1)$ là tách được và có các không điểm là :

- các phần tử của $\mathbb{U}_n \cap \mathbb{U}_p$ (kép)
- các phần tử của $(\mathbb{U}_n \cup \mathbb{U}_p) - (\mathbb{U}_n \cap \mathbb{U}_p)$ (đơn).

Hơn nữa : $\mathbb{U}_n \cap \mathbb{U}_p = \mathbb{U}_{n \wedge p}$ và $\mathbb{U}_n \cup \mathbb{U}_p \subset \mathbb{U}_{n \vee p}$.

5.3.39 Ta giả thiết P có ít nhất một không điểm z thỏa mãn $|z| < \dfrac{1}{M+1}$. Thế thì

$$1 = \left| -\sum_{k=1}^{n} a_k z^k \right| \leq \sum_{k=1}^{n} |a_k| |z|^k \leq M \sum_{k=1}^{n} |z|^k < M \sum_{k=1}^{n} \left(\frac{1}{M+1} \right)^k = \frac{M}{M+1} \cdot \frac{1 - \dfrac{1}{(M+1)^n}}{1 - \dfrac{1}{M+1}} < 1,$$

mâu thuẫn.

5.3.40 a) Ta có: $P^{(n-2)} = \frac{n!}{2}X^2 + (n-1)!X + (n-2)! = \frac{(n-2)!}{2}(n(n-1)X^2 + 2(n-1)X + 2)$,

là một tam thức thực với biệt thức: $\Delta' = (n-1)^2 - 2n(n-1) = 1 - n^2 < 0$.

Ta suy luận phản chứng: Giả thiết tất cả các không điểm của P đều thực. Áp dụng định lý Rolle có tính đến các cấp bội, ta suy ra rằng tất cả các không điểm của P' cũng đều thực, rồi tất cả các không điểm của $P^{(n-2)}$ đều thực, mẫu thuẫn.

b) Đưa về a) bằng cách ký hiệu $Y = \frac{1}{X}$.

5.3.41 a) Với mọi a thuộc $]1; +\infty[$, ta có:

$$P(x) = (a_n x^n + \ldots + a_{p+1}x^{p+1}) + (a_p x^p + \ldots + a_0) \geq a_n x^n - \sum_{i=0}^{p}|a_i|x^i \geq a_n x^n - M\sum_{i=0}^{p} x^i$$

$$= a_n x^n - M\frac{x^{p+1}-1}{x-1}.$$

b) Ta suy luận phản chứng: Giả thiết P có ít nhất một không điểm thực thỏa mãn: $x > 1 + \left(\frac{M}{a_n}\right)^{\frac{1}{n-p}}$, vậy $x \in]1; +\infty[$.

Thế thì ta có: $a_n x^n (x-1) = a_n x^{n-p-1}(x-1)x^{p+1} \geq a_n(x-1)^{n-p}x^{p+1} > Mx^{p+1}$,

từ đó, sử dụng a):

$$0 \geq a_n x^n(x-1) - M(x^{p+1}-1) > M, \text{ mâu thuẫn.}$$

c) *Ví dụ:* $n = 10$, $a_n = 6$, $p = 2$, $M = 7$, từ đó với mọi không điểm thực x: $x \leq 1 + \left(\frac{7}{6}\right)^{\frac{1}{8}} < 2{,}02$.

5.3.42 Ta suy luận phản chứng: Giả thiết P có ít nhất một không điểm z thỏa mãn

$$|z| < \frac{\sqrt{5}-1}{2}(<1).$$

Trường hợp thứ 1: $n_1 \geq 2$

Ta có: $0 = |P(z)| = |1 + z^{n_1} + z^{n_2} + \ldots + z^{n_N}| \geq 1 - (|z|^2 + |z|^3 + \ldots + |z|^{N+1})$

$$= 1 - |z|^2\frac{1-|z|^N}{1-|z|} \geq 1 - \frac{|z|^2}{1-|z|} = \frac{1-|z|-|z|^2}{1-|z|}$$

Nhưng rõ ràng: $|z| < \frac{\sqrt{5}-1}{2} \Rightarrow 1 - |z| - |z|^2 > 0$, từ đó gặp mâu thuẫn.

Trường hợp thứ 2: $n_1 = 1$

Ta xét $(1 - X)P(X)$ và chú ý rằng có tồn tại $\varepsilon_2, \ldots, \varepsilon_{n_N+1}$ thuộc $\{-1, 0, 1\}$ sao cho:

$$(1 - X)(1 + X + X^{n_2} + \cdots + X^{n_N}) = 1 + \sum_{k=2}^{n_N+1}\varepsilon_k X^{n_N}$$

và kết quả của trường hợp thứ 1 cũng áp dụng được cho đa thức này.

5.3.43 Ánh xạ φ : $]0;\infty[\to \mathbb{R}$ khả vi trên $]0;+\infty[$ và:

$$x \mapsto \frac{P(x)}{x^n} = 1 - \sum_{k=0}^{n-1} \frac{a_k}{x^{n-k}}$$

$$\forall x \in]0;+\infty[,\ \varphi'(x) = \sum_{k=0}^{n-1} \frac{(n-k)a_k}{x^{n+1-k}} > 0.$$

Như thế, φ tăng nghiêm ngặt trên $]0;+\infty[$. Hơn nữa, φ liên tục và $\lim_{0^+}\varphi = -\infty$, $\lim_{+\infty}\varphi = 1$..

Như thế: $\exists! x_0 \in]0;+\infty[,\ \varphi(x_0) = 0$.

5.3.44 Ta có, với mọi x thuộc $\mathbb{R}^*$: $\frac{P_n(x)}{x^{2n}} = \sum_{k=0}^{2n}(k+1)\left(-\frac{1}{x}\right)^k$.

Xét $f : \mathbb{R} \to \mathbb{R}$ và $g: \mathbb{R} \to \mathbb{R}$.

$$t \mapsto \sum_{k=0}^{2n}(k+1)t^k \qquad t \mapsto \sum_{k=0}^{2n+1} t^k$$

Rõ ràng rằng g khả vi trên $\mathbb{R}$ và $\forall t \in \mathbb{R}$, $g'(t) = f(t)$. Vì: $\forall t \in \mathbb{R} - \{1\}$, $g(t) = \frac{t^{2n+2}-1}{t-1}$, ta suy ra: $\forall t \in \mathbb{R} - \{1\}$, $f(t) = \frac{(2n+1)t^{2n+2} - (2n+2)t^{2n+2} + 1}{(t-1)^2}$. Từ đó, với mọi x thuộc $\mathbb{R} - \{-1, 0\}$:

$$P_n(x) = x^{2n} f\left(-\frac{1}{x}\right) = \frac{2n+1+(2n+2)x+x^{2n+2}}{(x+1)^2}.$$

Khảo sát sự biến thiên của h: $\mathbb{R} \to \mathbb{R}$ xác định bởi: $h(x) = 2n + 1 + (2x + 2)x + x^{2n+2}$.

Bảng biến thiên chứng tỏ: $\forall x \in \mathbb{R} - \{-1\}$, $h(x) > 0$, từ đó: $\forall x \in \mathbb{R} - \{-1, 0\}$, $P_n(x) > 0$.

Cuối cùng, $P_n(-1) > 0$ và $P_n(0) = 1 > 0$.

x	$-\infty$		-1		$+\infty$
$h'(x)$		$-$	0	$+$	
$h(x)$	$\searrow$		0	$\nearrow$	

5.3.45 1) Giả sử P thích hợp. Ta ký hiệu tập hợp các không điểm của P trong $\mathbb{C}$ là Z và giả thiết $\deg(P) \geq 1$.

• Giả sử $z \in Z$. Thế thì ta có $P(z) = 0$ và $P((z-1)+1) = 0$, từ đó, theo giả thiết: $P(z^2 + z + 1) = 0$ và $P((z-1)^2 + (z-1) + 1) = 0$, vậy: $z^2 + z + 1 \in Z$ và $z^2 - z + 1 \in Z$.

• Theo định lý d' Alembert, Z là một bộ phận hữu hạn khác rỗng của $\mathbb{C}$. Vậy tồn tại $u \in Z$ sao cho: $\forall z \in Z, |z| \leq |u|$. Đặc biệt: $|u^2 + u + 1| \leq |u|$ và $|u^2 - u + 1| \leq |u|$.

Nhưng: $2|u| = |(u^2 + u + 1) - (u^2 - u + 1)| \leq |u^2 + u + 1| + |u^2 - u + 1| \leq 2|u|$, từ đó $|u^2 + u + 1| = |u^2 - u + 1| = |u|$ và, theo sự khảo sát trường hợp đẳng thức trong bất đẳng thức tam giác trong $\mathbb{C}$, tồn tại $\lambda \in \mathbb{R}_+$ sao cho $u^2 - u + 1 = \lambda(u^2 + u + 1)$ (trường hợp $(u^2 + u + 1) = 0$ có thể khảo sát dễ dàng).

Vậy ta suy ra $\lambda = 1$ (vì $|\lambda| = 1$ và $\lambda \in \mathbb{R}_+$) rồi $u^2 + 1 = 0$.

Vì $P \in \mathbb{R}[X]$, nên tồn tại $n \in \mathbb{N}^*$ và $Q \in \mathbb{R}[X]$ sao cho:

$$P = (X^2 + 1)^n Q, \quad Q(i) \neq 0, \quad Q(-i) \neq 0.$$

Chứng minh: $Q(X)Q(X+1) = Q(X^2 + X + 1)$.

Phép suy luận trên, áp dụng vào Q thay cho P, chứng tỏ Q là một hằng.

2) Với $(\alpha, n) \in \mathbb{R}^* \times \mathbb{N}^*$, ký hiệu $P = \alpha(X^2 + 1)^n$, ta có:

$$P(X^2 + X + 1) = \alpha((X^2 + X + 1)^2 + 1)^n = \alpha(X^2 + 1)^n((X+1)^2 + 1)^n,$$

từ đó: $P(X)P(X+1) = P(X^2 + X + 1) \Leftrightarrow \alpha^2 = \alpha$.

5.3.46 Giả sử $P \in \mathbb{C}[X]$ thích hợp, sao cho $\deg(P) \geq 1$.

Ta ký hiệu tập hợp các không điểm của P trong $\mathbb{C}$ là Z. Theo định lý d'Alembert: $Z \neq \emptyset$.

Giả sử $z \in Z$. Ta có: $P(z+1)P(z+2) = P(z)\,P(z+3) = 0$, vậy : $z+1 \in Z$ hoặc $z+2 \in Z$.

Một phép quy nạp đơn giản chứng tỏ rằng, với mọi n thuộc $\mathbb{N}$:

$$z + n \in Z \quad \text{hoặc} \quad z+n+1 \in Z, \quad \text{hoặc} \ldots \text{hoặc } z+2n \in Z.$$

Đặc biệt, với mọi k thuộc $\mathbb{N}$: $z + 2^k - 1 \in Z$ hoặc $z + 2^k \in Z$ hoặc .... hoặc $z + 2^{k+1} - 2 \in Z$.

Nhưng các tập hợp $\{z+p;\ p \in \{2^k - 1, 2^k, \ldots, 2^{k+1} - 2\}\}$, $k \in \mathbb{N}$, đều rời nhau từng đôi.

Vậy Z sẽ vô hạn, mâu thuẫn.

5.3.47 a) Ký hiệu $B = aX^2 + bX + c$, $(a, b, c) \in \mathbb{C}^3$, ta có:

$$\begin{cases} B(1) = 1 \\ B(\alpha) = \beta \\ B(\beta) = \alpha \end{cases} \Leftrightarrow \begin{cases} a+b+c = 1 \\ a\alpha^2 + b\alpha + c = \beta \\ a\beta^2 + b\beta + c = \alpha \end{cases} \Leftrightarrow \begin{cases} a+b+c = 1 \\ a(\alpha+\beta) + b = -1 \\ a((\alpha+\beta)^2 - 2\alpha\beta) + (b-1)(\alpha+\beta) + 2c = 0 \end{cases}$$

Mặt khác, $X^3 + X - 2 = (X-1)(X^2 + X + 2)$, vậy $\alpha + \beta = -1$ và $\alpha\beta = 2$.

Như thế ta quy về việc giải hệ: $\begin{cases} a+b+c = 1 \\ -a+b = -1 \\ -3a+1-b+2c = 0 \end{cases}$

◇ **Trả lời**: $B = \frac{3}{4}X^2 - \frac{1}{4}X + \frac{1}{2}$.

b) **Phương pháp thứ nhất**

Vì $A = (X-1)(X-\alpha)(X-\beta)$ tách được và có tất cả các không điểm đơn, với ký hiệu $C = B \circ B - X$, ta có:

$$A \mid C \Leftrightarrow C(1) = C(\alpha) = C(\beta) = 0.$$

Và : $\begin{cases} C(1) = B(B(1)) - 1 = B(1) - 1 = 0 \\ C(\alpha) = B(B(\alpha)) - \alpha = B(\beta) - \alpha = 0 \\ C(\beta) = B(B(\beta)) - \beta = B(\alpha) - \beta = 0. \end{cases}$

Phương pháp thứ hai

Vì $B = \frac{3}{4}X^2 - \frac{1}{4}X + \frac{1}{2}$, một phép tính trực tiếp cho ta:

$$B \circ B - X = \frac{9}{64}(3X^4 - 2X^3 + 3X^2 - 8X + 4) = \frac{9}{64}(3X-2)(X^3 + X - 2).$$

5.3.48 a) Ta ký hiệu $P = \sum_{k=0}^{N} \alpha_k X^k$, trong đó $N \in \mathbb{N}$, $\alpha_0, \ldots, \alpha_N \in \mathbb{Q}$.

Sử dụng công thức nhị thức Newton:

$$P(a-\sqrt{b}) = P(a+\sqrt{b}) + P(a-\sqrt{b}) = \sum_{k=0}^{N} \alpha_k (a+\sqrt{b})^k + (a-\sqrt{b})^k \in \mathbb{Q},$$

$$-P(a-\sqrt{b}) = P(a+\sqrt{b}) - P(a-\sqrt{b}) = \sum_{k=0}^{N} \alpha_k (a+\sqrt{b})^k - (a-\sqrt{b})^k \in \sqrt{b}\,\mathbb{Q}.$$

Vì $\sqrt{b} \notin \mathbb{Q}$, ta có: $\mathbb{Q} \cap (\sqrt{b}\,\mathbb{Q}) = \{0\}$, từ đó $P(a - \sqrt{b}) = 0$.

b) Theo a), $a + \sqrt{b}$ và $a - \sqrt{b}$ là những không điểm của P trong $\mathbb{R}$, khác nhau (vì $b \neq 0$). Vậy khi ký hiệu $P_2 = (X - (a + \sqrt{b}))(X - (a - \sqrt{b})) = (X - a)^2 - b^2$, thì ta có: P_2 chia hết P trong $\mathbb{R}[X]$. Vì P_2 và P đều thuộc $\mathbb{Q}[X]$, nên kết quả là P_2 chia hết P trong $\mathbb{Q}[X]$ (Xem 5.2.2, Nhận xét). Vậy tồn tại $Q \in \mathbb{Q}[X]$ sao cho: $P = P_2Q$.

Áp dụng a) vào Q thay cho P, ta có: $P_2 \mid Q$ trong $\mathbb{Q}[X]$. Vậy tồn tại $P_1 \in \mathbb{Q}[X]$ sao cho $Q = P_2P_1$, từ đó $P = P_1P^2_2$.

5.3.49 Thay X bởi 1, j, j^2, ta được: $P(1) + Q(1) = 3R(1)$, $P(1) + jQ(1) = 0$, $P(1) + j^2Q(1) = 0$, từ đó $P(1) = Q(1) = 0$, $R(1) = 0$.

5.3.50 a) Ta ký hiệu $P = X^{2p} - X^p + 1$.

Vì $X^2 - X + 1 = (X + j)(X + j^2)$, vốn tách được và có các không điểm đều đơn, ta có, trong $\mathbb{C}[X]$:

$$X^2 - X + 1 \mid P \Leftrightarrow P(-j) = P(-j^2) = 0 \Leftrightarrow P(-j) = 0, \text{ vì } P \in \mathbb{R}[X],$$

và vì p lẻ và không phải là bội của 3: $P(-j) = (-j)^{2p} - (-j)^p + 1 = j^{2p} + j^p + 1 = 0$.

Điều này chứng tỏ: $X^2 - X + 1 \mid P$ trong $\mathbb{C}[X]$.

Vì $X^2 - X + 1$ và P đều thuộc $\mathbb{Q}[X]$, suy ra (xem 5.2.2, Nhận xét): $X^2 - X + 1 \mid P$ trong $\mathbb{Q}[X]$.

Cuối cùng, vì hệ tử bậc cao nhất của $X^2 - X + 1$ là 1, phép chia Euclide P cho $X^2 - X + 1$ chứng tỏ rằng các hệ tử của thương A đều thuộc $\mathbb{Z}$.

b) Giả sử p là số nguyên tố ≥ 5, $k \in \mathbb{N}^*$, $n = kp$. Thay X bởi 2^k trong a, và vì $A(2^k) \in \mathbb{Z}$, ta suy ra:

$$(2^k)^2 - 2^k + 1 \mid (2^k)^{2p} - (2^k)^p + 1 = 2^{2N} - 2^N + 1 \text{ trong } \mathbb{Z}.$$

Cuối cùng: • $2^{2k} - 2^k + 1 \geq 2$ vì $k \geq 1$.

• $2^{2k} - 2^k + 1 \neq 2^{2kp} - 2^{kp} + 1$ vì $p \geq 2$.

Ví dụ: Với $N = 2^{168} - 2^{84} + 1$, ta có: $n = 84$, $p = 7$, $k = 12$ và N là bội của $m = 2^{24} - 2^{12} + 1 = 16\,773\,121$.

5.3.51 Vì $a, b, c, \in \mathbb{Q}$, $P \in \mathbb{Q}[X]$ và $P(a) = P(b) = P(c) = 2$, trong $\mathbb{Q}[X]$ đa thức $P - 2$ chia hết cho $(X - a)(X - b)(X - c)$. Hơn nữa, vì $P \in \mathbb{Z}[X]$ và $(X - a)(X - b)(X - c)$ là chuẩn tắc, phép chia Euclide P cho $(X - a)(X - b)(X - c)$ chứng tỏ rằng thương có các hệ tử thuộc $\mathbb{Z}$.

Như thế, tồn tại $Q \in \mathbb{Z}[X]$ (tức là: $Q \in \mathbb{Q}[X]$ và các hệ tử trong Z.

Như thế, tồn tại $Q \in \mathbb{Z}[X]$ (tức là: $Q \in \mathbb{Q}[X]$ và các hệ tử của Q đều thuộc $\mathbb{Z}$) sao cho:

$$P = (X - a)(X - b)(X - c)Q + 2.$$

Ta giả thiết tồn tại $x \in \mathbb{Z}$ sao cho $P(x) = 3$. Thế thì ta có: $(x - a)(x - b)(x - c)\,Q(x) = 1$. Vì $x - a$, $x - b$, $x - c$, $Q(x)$ đều thuộc $\mathbb{Z}$, kết quả là $x - a$, $x - b$, $x - c$ đều thuộc $\{-1, 1\}$, vậy không khác nhau từng đôi, mâu thuẫn.

5.3.52 Ta suy luận phản chứng: giả thiết tồn tại $a, b, c \in \mathbb{Z}$, khác nhau từng đôi và $P \in \mathbb{Z}[X]$ sao cho: $P(a) = b$, $P(b) = c$, $P(c) = a$. Vì $P(a) - b = 0$, tồn tại $Q \in \mathbb{Q}[X]$ sao cho : $P - b = (X - a)Q$. Phép chia Euclide $P - b$ cho $X - a$ chứng tỏ rằng các hệ tử của Q đều thuộc $\mathbb{Z}$. Thay X bởi b: $c - b = (b - a)Q(b)$ và $Q(b) \in \mathbb{Z}$, vậy: $b - a \mid c - b$.

Hoán vị vòng tròn a, b, c ta được: $b - a \mid c - b$, $c - b \mid a - c$, $a - c \mid b - a$, từ đó: $|b - a| = |a - c| = |c - b|$.

• Nếu $b - a = c - a$, thì $b = c$, mâu thuẫn.

• Vậy $b - a = a - c$, và tương tự $a - c = c - b$. Suy ra $a = b = c$, mâu thuẫn.

5.3.53 Ta suy luận phản chứng: giả thiết $P = X^3 + X + 3a$ không bất khả quy trong $\mathbb{Q}[X]$. Thế thì tồn tại $A,B \in \mathbb{Q}[X]$ sao cho: $P = AB$, $1 \le \deg(A) \le 2$. Ta có : $\deg(A) = 1$ và $\deg(B) = 2$, sai khác về thứ tự.

Vậy P có ít nhất một không điểm trong $\mathbb{Q}$.

Giả sử $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ sao cho: $p \wedge q = 1$ và $P\left(\frac{p}{q}\right) = 0$. Thế thì ta có: $p^3 + pq^2 + 3q^3 = 0$, từ đó:

$$\begin{cases} p \mid 3q^3, \text{ vậy } (p \wedge q = 1) : p \mid 3 \\ q \mid p^3, \text{ vậy } (p \wedge q = 1) : q = 1 \end{cases}$$

Như thế: $\left(\frac{p}{q}\right) \in \{-3,-1,1,3\}$.

Ta kiểm chứng dễ dàng rằng bốn số hữu tỷ đó không phải là không điểm của P.

Cuối cùng: P là bất khả quy trong $\mathbb{Q}[X]$.

5.3.54 Với $i \in \{0,\dots,n\}$, ta ký hiệu $L_i = \prod_{\substack{0 \le k \le n \\ k \ne i}} \frac{X-k}{i-k}$ (đa thức nội suy Lagrange tại các điểm 0, 1,..., n, xem 5.3.1, Ví dụ).

Theo 5.3.1, Ví dụ, ta có : $P = \sum_{i=0}^{n} P(i)L_i$, trong đó : $\forall a = \mathbb{Z}$, $P(a) = \sum_{i=0}^{n} P(i)L_i(a)$

Với $(i,a) \in \{0,\dots,n\} \times \mathbb{Z}$, ký hiệu: $u_{i,a} = \prod_{0 \le k \le i-1} \frac{a-k}{i-k}$ và $v_{i,a} = \prod_{i+1 \le k \le n} \frac{a-k}{i-k}$

(với quy ước: một tích được chỉ số hóa bởi $\varnothing$ thì bằng 1); như thế: $L_i(a) = u_{i,a}\, v_{i,a}$.

• Nếu $0 \le a \le n$, thì $L_i(a) = \begin{cases} 0 & \text{nếu } i \ne a \\ 1 & \text{nếu } i = a \end{cases}$, vậy $L_i(a) \in \mathbb{Z}$.

• Nếu $a > n$: $u_{i,a} = \frac{a(a-1)\dots(a-i+1)}{i(i-1)\dots 1} = C_a^i \in \mathbf{Z}$, và $v_{i,a} = \frac{(a-i-1)(a-i-2)\dots(a-n)}{(-1)(-2)\dots(i-n)}$

$$= \frac{(a-n)(a-n-1)\dots(a-i-1)}{(-1)^{n-i}(n-i)!} = (-1)^{n-i} C_{a-n}^{a-i} \in \mathbf{Z}.$$

• Nếu $a < 0$: $u_{i,a} = \frac{a(a-1)\dots(a-i+1)}{i(i-1)\dots 1} = \frac{(-1)i\,|a|\,(|a|+1)\dots(|a|+i-1)}{i!} = (-1)^i C_{|a|+i-1}^{i} \in \mathbf{Z}$

và $v_{i,a} = \frac{(a-i-1)(a-i-2)\dots(a-n)}{(-1)^{n-i}(n-i)!} = \frac{(-1)^i(|a|+i+1)(|a|+i+2)\dots(|a|+n)}{(-1)^{n-i}(n-i)!}$

$$= (-1)^n C_{|a|-n}^{a-i} \in \mathbf{Z}$$

Như thế: $\forall i \in \{0,\dots,n\}$, $L_i(a) \in \mathbb{Z}$.

Vì $P(a) = \sum_{i=0}^{n} P(i)L_i(a)$, suy ra $P(a) \in \sum_{i=0}^{n} P(i)\,\mathbb{Z} = \text{ƯCLN}((P(i)_{0 \le i \le n})\mathbb{Z}$, vậy $\text{ƯCLN}(P(i)_{0 \le i \le n}) \mid P(a)$.

5.3.55 Ta suy luận bằng phản chứng: Giả thiết tồn tại $A,B \in \mathbb{Z}[X]$ sao cho:

$$P = AB,\ 1 \le \deg(A) < n,\ 1 \le \deg(B) < n.$$

Thế thì ta có, với mọi k thuộc $\{1,\dots,n\}$: $A(a_k)B(a_k) = P(a_k) = -1$, từ đó vì $A(a_k)$ và $B(a_k)$ đều là những số nguyên: $\begin{cases} A(a_k) = 1 \\ B(a_k) = -1 \end{cases}$ hoặc $\begin{cases} A(a_k) = -1 \\ B(a_k) = 1 \end{cases}$ vậy $A(a_k) + B(a_k) = 0$.

Điều này chứng tỏ $A + B$ triệt tiêu tại $a_1, \dots, a_n$, những số này đều khác nhau từng đôi.

Vì mặt khác: $\deg(A+B) \le \text{Max}(\deg(A), \deg(B)) < n$, suy ra: $A + B = 0$

Nhưng thế thì $P = AB = -A^2 \le 0$, mâu thuẫn với: $p(x) \xrightarrow[x \to +\infty]{} +\infty$.

5.3.56 a) Chú ý rằng 3 là một không điểm:

◇ **Trả lời**: $(X - 3)^2(X + 1)$

b) Trong $\mathbb{C}[X]$: $(X^2 - X + 2)^2 + (X - 2)^2 = (X^2 - X + 2 + i(X - 2))(X^2 - X + 2)^2 - i(X - 2))$

$= (X^2 + (-1 + i)X + (2 - 2i))(X^2 - (1 + i)X + (2 + 2i))$

Các không điểm của $X^2 + (-1 + i)X + (2 - 2i)$ là $-2i$ và $1 + i$ (đơn). Từ đó:

$$(X^2 - X + 2)^2 + (X - 2)^2 = (X - 1 - i)(X + 2i)(X - 1 + i)(X - 2i) = ((X - 1)^2 + 1)(X^2 + 4).$$

◇ **Trả lời** : $(X^2 - 2X + 2)(X^2 + 4)$.

c) **Phương pháp thứ 1**

Vì các căn bậc 6 của 1 trong $\mathbb{C}$ là : $1, j, j^2, -1, -j, -j^2$, nên ta có trong $\mathbb{C}[X]$:

$(X + 1)^6 - X^6 = (X + 1 - X)(X + 1 + j^2X)(X + 1 - jX)(X + 1 + X)(X + 1 - j^2X)(X + 1 + jX)$

$= (2X + 1)((-jX + 1)(-j^2X + 1))((1 - j)X + 1)((1 - j^2)X + 1)$.

Phương pháp thứ 2

$(X + 1)^6 - X^6 = ((X + 1)^3 - X^3)((X + 1)^3 + X^3)$

$= ((X + 1) - X)((X + 1)^2 + (X + 1)X + X^2)((X + 1) + X)((X + 1)^2 - (X + 1)X + X^2)$.

◇ **Trả lời**: $(2X + 1)(X^2 + X + 1)(3X^2 + 3X + 1)$

d) Các không điểm bội có thể có là nghiệm của: $\begin{cases} z^5 - 7z^3 - 2z^2 + 12z + 8 = 0 \\ 5z^4 - 21z^2 - 4z + 12 = 0 \end{cases}$

Chú ý rằng -1 và 2 đều là nghiệm.

◇ **Trả lời**: $(X - 2)^2(X + 1)^2(X + 2)$.

e) Trước tiên : $X^5 + 1 = (X + 1)(X^4 - X^3 + X^2 - X + 1)$.

Phương trình $z^4 - z^3 + z^2 - z + 1 = 0$ (ẩn $z \in \mathbb{C}$) là một phương trình thuận nghịch (xem bài tập 5.3.12).

◇ **Trả lời**: $(X + 1)\left(X^2 - \frac{1+\sqrt{5}}{2}X + 1\right)\left(X^2 - \frac{1-\sqrt{5}}{2}X + 1\right)$.

f) Chú ý rằng đa thức đã cho chia hết cho $X^2 + 3$.

◇ **Trả lời** : $(X^2 + 3)\left(X^2 - \sqrt{2\sqrt{3} - 1}\,X + \sqrt{3}\right)\left(X^2 + \sqrt{2\sqrt{3} - 1}\,X + \sqrt{3}\right)$.

g) Xem bài tập 5.3.12, phương trình thuận nghịch.

◇ **Trả lời**: $(X + 1)^2\left(X^2 + \frac{\sqrt{5}+1}{2}X + 1\right)\left(X^2 - \frac{\sqrt{5}-1}{2}X + 1\right)$.

h) $X^3 + X^4 + 1 = (X^4 + 1)^2 - X^4 = (X^4 + X^2 + 1)(X^4 - X^2 + 1) = ((X^2 + 1)^2 - X^2)((X^2 + 1)^2 - 3X^2)$.

◇ **Trả lời**: $(X^2 + X + 1)(X^2 - X + 1)(X^2 + \sqrt{3}X + 1)(X^2 - \sqrt{3}X + 1)$.

i) $X^{12} + 1 = (X^4 + 1)(X^8 - X^4 + 1)$, rồi thì như h).

◇ **Trả lời:** $(X^2 - X\sqrt{2} + 1)(X^2 + X\sqrt{2} + 1)(X^2 - \sqrt{2+\sqrt{3}}\,X + 1)(X^2 + \sqrt{2+\sqrt{3}}\,X + 1)$

$(X^2 - \sqrt{2-\sqrt{3}}\,X + 1)(X^2 + \sqrt{2-\sqrt{3}}\,X + 1)$.

j) $X^{2n} - 2\cos aX^n + 1 = (X^n - e^{ia})(X^n - e^{-ia}) = \prod_{k=0}^{n-1}\left(X - \omega_k e^{\frac{ia}{n}}\right)\prod_{k=0}^{n-1}\left(X - \omega_k e^{-\frac{ia}{n}}\right)$,

trong đó $\omega_k = \exp\left(\frac{2ik\pi}{n}\right) \in \mathbb{Z}$.

Nhóm các nhân tử:

$$X^{2n} - 2\cos aX^n + 1 = \prod_{k=0}^{n-1}\left(\left(X - \omega_k e^{\frac{ia}{n}}\right)\left(X - \omega_{n-k} e^{-\frac{ia}{n}}\right)\right) = \prod_{k=0}^{n-1}\left(X^2 - 2\cos\frac{a+2k\pi}{n}X + 1\right).$$

và với mọi k thuộc $\{0,\ldots,n-1\}$, biệt thức của tam thức $X^2 - 2\cos\frac{a+2k\pi}{n}X + 1$ là $-\sin^2\frac{a+2k\pi}{n} < 0$ vì $a \notin \pi\mathbb{Z}$.

◇ **Trả lời:** $\prod_{k=0}^{n-1}\left(X^2 - 2\cos\frac{a+2k\pi}{n}X + 1\right)$.

5.3.57 Các ước chuẩn tắc bất khả quy của P (trong $\mathbb{R}[X]$) là:

• Các $X - z_k$ với những k thỏa mãn $z_k \in \mathbb{R}$.

• Các $X^2 - 2\mathrm{Re}(z_k)X + |z_k|^2$ với những k thỏa mãn $z_k \in \mathbb{C} - \mathbb{R}$.

Vì $(\forall k, \mathrm{Re}(z_k) \le 0)$, các đa thức $X + z_k$ và $X^2 - 2\mathrm{Re}(z_k)X + |z_k|^2$ đều có các hệ tử ≥ 0, vậy tất cả các hệ tử của P đều cùng một dấu.

5.3.58 • Khảo sát trước tiên trường hợp $\deg(P) \le 0$.

• Giả sử P thích hợp sao cho $\deg(P) \ge 1$. Vì ánh xạ đa thức P liên tục trên khoảng $\mathbb{R}$, và khác hằng, nên tập hợp $P(\mathbb{R})$ là một khoảng của $\mathbb{R}$ (định lý về giá trị trung gian, Tập 1, 4.3.3, Định lý) khác rỗng, không suy biến thành một điểm. Đặc biệt, $P(\mathbb{R})$ là vô hạn.

Nhưng, theo giả thiết: $\forall x \in \mathbb{R}, P(P(x)) = (P(x))^k$, vậy: $\forall y \in P(\mathbb{R}), P(y) = y^k$.

Như thế, $P - X^k$ triệt tiêu tại vô hạn các số thực, vậy $P - X^k = 0$.

Ngược lại, X^k hiển nhiên thích hợp.

◇ **Trả lời:** $\{(1, \lambda); \lambda \in \mathbb{R}\} \cup \{(k, 1); k \in \mathbb{N}\} \cup \{(k, 0); k \in \mathbb{N} - \{0, 1\}\} \cup \{(k, X^k); k \in \mathbb{N}\}$.

5.3.59 Xét $Q = 1 + \frac{X}{1} + \frac{X(X-1)}{2} + \ldots + \frac{X(X-1)\ldots(X-n+1)}{n!}$.

Vì Q có bậc n và: $\forall k \in \{0,\ldots,n\}, Q(k) = \sum_{i=0}^{n} C_k^i = 2^k$, ta có: $Q = P$.

Thế thì: $P(n+1) = Q(n+1) = \sum_{i=0}^{k} C_{n+1}^i = 2^{n+1} - 1$.

◇ **Trả lời:** $2^{n+1} - 1$.

5.3.60 Xét $Q = XP - 1$.

Ta có: $\forall k \in \{1, \ldots, n+1\}, Q(k) = kP(k) - 1 = 0$.

Vì $\deg(Q) \leq n+1$, tồn tại $\lambda \in \mathbb{R}$ sao cho: $Q = \lambda \prod_{k=1}^{n+1} (X - k)$.

Vì $Q(0) = -1$, ta suy ra $\lambda = \frac{(-1)^n}{(n+1)!}$. Như thế : $Q = \frac{(-1)^n}{(n+1)!} \prod_{k=1}^{n+1} (X - k)$

Đặc biệt: $Q(n+2) = \frac{(-1)^n}{(n+1)!}(n+1)! = (-1)^n$.

◇ **Trả lời:** $\frac{1+(-1)^n}{n+2}$.

5.3.61 **Trường hợp thứ 1:** n chẵn

Xét $Q = P - P(n+1-X)$.

Rõ ràng rằng $\deg(Q) \leq n-1$ và : $\forall k \in \{1, \ldots, n\}, Q(k) = \frac{1}{C_{n-1}^{k}} - \frac{1}{C_{n+1}^{n+1-k}} = 0$.

Suy ra $Q = 0$, từ đó: $P(0) - P(n+1) = Q(0) = 0$, $P(n+1) = P(0) = 1$.

Trường hợp thứ hai: n lẻ

Xét $Q = (X+1)P - (n+1-X)P(n-X)$.

Rõ ràng $\deg(Q) \leq n$ và $\forall k \in \{0, \ldots, n\}, Q(k) = \frac{k+1}{C_{n+1}^{k}} - \frac{n+1-k}{C_{n+1}^{n-k}} = 0$.

Suy ra $Q = 0$; đặc biệt $Q(-1) = 0$, từ đó $P(n+1) = 0$.

◇ **Trả lời :** $\begin{cases} 1 & \text{nếu } n \text{ chẵn} \\ 0 & \text{nếu } n \text{ lẻ} \end{cases}$

5.3.62 Ánh xạ $\varphi : \mathbb{R} \to \mathbb{R}$, $x \mapsto P(x) - Q(x)$ liên tục trên khoảng $\mathbb{R}$ và không triệt tiêu tại một số thực nào. Theo định lý về giá trị trung gian (Tập 1, 4.3.3, Định lý) ta suy ra chẳng hạn : $\forall x \in \mathbb{R}, P(x) > Q(x)$. Thế thì: $\forall x \in \mathbb{R}, P(P(x)) > Q(P(x)) = P(Q(x)) > Q(Q(x))$.

Chú ý: Kết quả vẫn còn hiệu lực khi thay P, Q bằng những ánh xạ liên tục.

5.3.63 Ta có: $(C+A)(C-A) = B^2$.

Giả sử z_0 là không điểm của $C - A$, thế thì $C(z_0) + A(z_0) = C(z_0) - A(z_0) = 0$, vậy $C(z_0) = A(z_0) = 0$, rồi $(B(z_0))^2 = 0$ và $X - z_0$ chia hết A, B, C mâu thuẫn.

Như thế, cấp bội của z_0 trong $C + A$ cũng như trong B^2, vậy chẵn.

Tương tự đối với $C - A$, $C + B$, $C - B$.

5.3.64 Tồn tại $\lambda \in \mathbb{R}^*$ sao cho $P = \lambda \prod_{k=1}^{n} (X - x_k)$. Ta có: $|P'(x_1)| = |\lambda| \prod_{k=2}^{n} |x_1 - x_k|$, và với mọi k thuộc $\{1, \ldots, n\}$: $|x_1 - x_k| \leq |x_1 - x| + |x - x_k| \leq 2|x - x_k|$, từ đó:

$$|P'(x_1)|\,|x - x_1| \leq |\lambda| 2^{n-1} \prod_{k=1}^{n} |x - x_k| = 2^{n-1} |P(x)|.$$

5.3.65 Theo định lý d'Alembert, P tách được trên $\mathbb{C}$; ký hiệu $n = \deg(P) \geq 2$, tồn tại $\lambda \in \mathbb{C}^*, z_1, \ldots, z_n \in \mathbb{C}$ sao cho: $P = \lambda \prod_{k=1}^{n} (X - z_k)$.

1) Nếu $z_1, \ldots, z_n$ không đều bằng nhau, thì tồn tại $(k, l) \in \{1, \ldots, n\}^2$ sao cho $z_k \neq z_l$, và $P(z_k) = P(z_l) = 0$, Vậy $\tilde{P}$ không phải là đơn ánh.

2) Nếu $z_1 = \ldots = z_n$, ta xét $Q = P + 1$, có bậc n. Tất cả các không điểm của Q đều đơn vì với mọi z thuộc $\mathbb{C}$:

$$Q'(z) = 0 \Leftrightarrow \lambda n (z - z_1)^{n-1} = 0 \Leftrightarrow z = z_1 \Rightarrow Q(z) = 1 \neq 0.$$

Vậy ta có thể áp dụng 1) cho Q thay vì P: Q không phải là đơn ánh. Vậy vì $P = Q - 1$, nên P không phải là đơn ánh.

5.3.66 1) **Trường hợp $n = 1$**

Ta ký hiệu $Q = a_0 P - a_1 P'$, $\gamma = \dfrac{a_0}{a_1}$, $P = \lambda \prod_{k=1}^{N} (X - x_k)^{\alpha_k}$, trong đó $\lambda \in \mathbb{R}^*$, $N \in \mathbb{N}^*$, $x_1, \ldots, x_N \in \mathbb{R}$, $x_1 < \ldots < x_N$, $\alpha_1, \ldots, \alpha_n \in \mathbb{N}^*$.

Ánh xạ $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto e^{\gamma x} P(x)$. khả vi trên $\mathbb{R}$ và: $\forall x \in \mathbb{R}, f'(x) = \dfrac{e^{\gamma x}}{a_1} Q(x)$.

Với giả thiết chẳng hạn $\gamma > 0$, thì vì $\lim_{\infty} f = f(x_1) = \ldots = f(x_N) = 0$, nên định lý Rolle (suy rộng) chứng tỏ rằng f' triệt tiêu tại ít nhất N số thực $y_1, \ldots, y_N$ sao cho:

$$y_1 < x_1 < y_2 < x_2 < \ldots < y_N < x_N.$$

Mặt khác, với mọi k thuộc $\{1, \ldots, n\}$ sao cho $\alpha_k \geq 2$, P' nhận x_k làm không điểm cấp $\alpha_k - 1$, nên Q cũng thế.

Vì: $N + \sum_{\substack{1 \leq k \leq N \\ \alpha_k \geq 2}} (\alpha_k - 1) = N + \sum_{1 \leq k \leq N} (\alpha_k - 1) = N + (n - N) = n = \deg(Q)$, ta suy ra Q tách được trên $\mathbb{R}$.

Trường hợp $\lambda = 0$ khi đó ($\deg(Q) = n - 1$) được khảo sát tương tự.

2) **Trường hợp tổng quát**

Ta ký hiệu các không điểm của A là $u_1, \ldots, u_n$ và với mọi $k \in \{1, \ldots, n\}$, $T_k : \mathbb{R}[X] \to \mathbb{R}[X]$, $M \mapsto M' - u_k M$.

Ta có, chẳng hạn, với mọi M thuộc $\mathbb{R}[X]$:

$$T_2 \circ T_1 (M) = (M' - u_1 M)' - u_2 (M' - u_1 M) = M'' - (u_1 + u_2) M' + u_1 u_2 M.$$

Nếu ký hiệu $\sigma_1, \ldots, \sigma_n$ là các hàm đối xứng cơ bản của $u_1, \ldots, u_n$, thì rõ ràng (bằng quy nạp):

$$T_n \circ \ldots \circ T_1 (M) = M^{(n)} - \sigma_1 M^{(n-1)} + \ldots + (-1)^n \sigma_n M = \frac{1}{a_n} \sum_{k=0}^{n} a_k M^{(k)}.$$

Vì P tách được trên $\mathbb{R}$, theo trường hợp $n = 1$, $T_1(P)$ tách được trên $\mathbb{R}$, rồi lặp lại nhiều lần, ta có: $T_n \circ \ldots \circ T_1(P)$ tách ra được trên $\mathbb{R}$.

5.4.1 Ta có: $\sum_{k=0}^{n} X^k = \dfrac{1 - X^{n+1}}{1 - X}$, từ đó, bằng cách đạo hàm:

$$\sum_{k=0}^{n-1} (k+1) X^k = \frac{nX^{n+1} - (n+1)X^n + 1}{(X-1)^2} = \frac{nX^n \left(X - \left(1 + \dfrac{1}{n}\right)\right) + 1}{(X-1)^2}. \text{ Vậy: } P_n\left(1 + \frac{1}{n}\right) = n^2.$$

5.4.2 Phân thức 0 không có nghiệm:

Nếu $F \neq 0$ và $F^2 = X$, thì $\deg(F) \in \mathbb{Z}$ và $2\deg(F) = 1$, mâu thuẫn.

5.4.3 Theo định lý d'Alembert, P tách được trên $\mathbb{C}$: tồn tại $\lambda \in \mathbb{C}^*, z_1, \ldots, z_n \in \mathbb{C}$, sao cho:

$$P = \lambda \prod_{k=1}^{n} (X - z_k).$$

Thế thì ta có: $\dfrac{P'}{P} = \sum_{k=1}^{n} \dfrac{1}{X - z_k}$, từ đó: $\dfrac{P'(-1)}{P(-1)} = \sum_{k=1}^{n} \dfrac{1}{1 + z_k}$.

Như thế: $\dfrac{n}{2} + \dfrac{P'(-1)}{P(-1)} = \sum_{k=1}^{n} \left(\dfrac{1}{2} - \dfrac{1}{1 + z_k} \right) = \dfrac{1}{2} \sum_{k=1}^{n} \dfrac{z_k - 1}{z_k + 1}$.

Ta có, với mọi k thuộc $\{1, \ldots, n\}$: $\dfrac{z_k - 1}{z_k + 1} = \dfrac{(z_k - 1)(\bar{z}_k + 1)}{|z_k + 1|^2}$, từ đó: $\operatorname{Re}\left(\dfrac{z_k - 1}{z_k + 1} \right) = \dfrac{|z_k|^2 - 1}{|z_k + 1|^2}$.

Vì $\dfrac{n}{2} + \dfrac{P'(-1)}{P(-1)}$ là thực, ta suy ra: $\dfrac{1}{2} \sum_{k=1}^{n} \dfrac{|z_k|^2 - 1}{|z_k + 1|^2} = \dfrac{n}{2} + \dfrac{P'(-1)}{P(-1)} \geq 0$.

Nếu $(\forall k \in \{1, \ldots, n\}, |z_k| < 1)$, thì $\dfrac{1}{2} \sum_{k=1}^{n} \dfrac{|z_k|^2 - 1}{|z_k + 1|^2} < 0$, mâu thuẫn.

Điều này chứng tỏ rằng P có ít nhất một không điểm với môđun ≥ 1.

5.4.4 ◇ **Trả lời:**

a) $\dfrac{1}{X^3} - \dfrac{1}{X} + \dfrac{1}{(X-1)^4} - \dfrac{1}{(X-1)^2} + \dfrac{1}{X-1}$

b) $\dfrac{2}{(X-1)^3} + \dfrac{1}{(X-1)^2} + \dfrac{3}{X-1} - \dfrac{2}{(X+1)^3} + \dfrac{1}{(X+1)^2} - \dfrac{3}{X+1}$

c) $\dfrac{-3}{(X+1)^4} + \dfrac{2}{(X-1)^3}$.

5.4.5 ◇ **Trả lời:**

a) $X^2 - 6X + 18 + \dfrac{15}{(X^2+2X+2)^3} + \dfrac{32X}{(X^2+2X+2)^2} + \dfrac{-32X-40}{X^2+2X+2}$

b) $\dfrac{\frac{1}{2}}{X^2 - \sqrt{2}X + 1} + \dfrac{\frac{1}{2}}{X^2 + \sqrt{2}X + 1}$

c) $\dfrac{\frac{1}{2}X - \frac{\sqrt{2}}{4}}{X^2 - \sqrt{2}X + 1} + \dfrac{\frac{1}{2}X + \frac{\sqrt{2}}{4}}{X^2 + \sqrt{2}X + 1}$

d) $\dfrac{\frac{1}{2}X + \frac{1}{2}}{X^2 + X + 1} + \dfrac{-\frac{1}{2}X + \frac{1}{2}}{X^2 - X + 1}$

e) $\dfrac{1}{X-1} + \dfrac{-\frac{2\sqrt{3}+3}{6}X + \frac{3+\sqrt{3}}{6}}{X^2 - \sqrt{3}X + 1} + \dfrac{\frac{2\sqrt{3}-3}{6}X + \frac{3-\sqrt{3}}{6}}{X^2 + \sqrt{3}X + 1}$

f) $\dfrac{\frac{1}{3}X}{X^2+2X+3}+\dfrac{-\frac{2}{3}X+\frac{1}{3}}{2X^2+3X+4}$

g) $\dfrac{1}{X^3}-\dfrac{1}{X}+\dfrac{X+1}{(X^2+1)^2}+\dfrac{2X-1}{X^2+1}$

h) $X+3+\dfrac{1}{(X+1)^2}+\dfrac{2}{X+1}+\dfrac{2X+1}{X^2+X+1}$

i) $\dfrac{X-1}{(X^2+1)^2}+\dfrac{1}{X^2+1}+\dfrac{X+1}{(X^2+X+1)^2}+\dfrac{-1}{X^2+X+1}$

j) Chú ý : $\left(\dfrac{X^2}{X^2+1}\right)^n=\left(1-\dfrac{1}{X^2+1}\right)^n$.

◇ **Trả lời:** $\displaystyle\sum_{k=0}^{n}(-1)^k C_n^k\frac{1}{(X^2+1)^k}$.

5.4.6 Phép phân tích thành phần tử đơn giản (PTĐG) cho ta:

$$\frac{3X^2-1}{(X-1)^2X^2(X+1)^2}=\frac{\frac{1}{2}}{(X-1)^2}-\frac{1}{X^2}+\frac{\frac{1}{2}}{(X+1)^2}.$$

Từ đó, với mọi N thuộc $\mathbb{N}$ thỏa mãn $N\geq 2$:

$$\begin{aligned}\sum_{n=2}^{N}\frac{3n^2-1}{(n-1)^2n^2(n+1)^2}&=\frac{1}{2}\sum_{n=2}^{N}\frac{1}{(n-1)^2}-\sum_{n=2}^{N}\frac{1}{n^2}+\frac{1}{2}\sum_{n=2}^{N}\frac{1}{(n+1)^2}\\&=\frac{1}{2}\sum_{n=2}^{N-1}\frac{1}{n^2}-\sum_{n=2}^{N}\frac{1}{n^2}+\frac{1}{2}\sum_{n=3}^{N+1}\frac{1}{n^2}\\&=\frac{1}{2}\left(1+\frac{1}{4}\right)-\left(\frac{1}{4}+\frac{1}{N^2}\right)+\frac{1}{2}\left(\frac{1}{N^2}+\frac{1}{(N+1)^2}\right)\end{aligned}$$

◇ **Trả lời:** $\dfrac{3}{8}-\dfrac{2N+1}{2N^2(N+1)^2}$.

5.4.7 Một PTĐG cho: $\dfrac{X^3+2}{(X^2-1)^2}=\dfrac{\frac{3}{4}}{(X-1)^2}+\dfrac{\frac{1}{4}}{(X+1)^2}+\dfrac{1}{X+1}$.

Từ đó, $\displaystyle\sum_{k=1}^{4}\frac{z_k^3+2}{(z_k^2-1)^2}=\frac{3}{4}u+\frac{1}{4}v+w$, trong đó : $u=\displaystyle\sum_{k=1}^{4}\frac{1}{(z_k-1)^2}$, $v=\displaystyle\sum_{k=1}^{4}\frac{1}{(z_k+1)^2}$, $w=\displaystyle\sum_{k=1}^{4}\frac{1}{z_k+1}$.

Ta ký hiệu $P=X^4-X^3+1$.

- Ta có: $\dfrac{P'}{P}=\displaystyle\sum_{k=1}^{4}\frac{1}{X-z_k}$, từ đó $w=-\dfrac{P'(-1)}{P(-1)}=\dfrac{7}{3}$.
- Rồi bằng cách đạo hàm: $\dfrac{P''P-P'^2}{P^2}=-\displaystyle\sum_{k=1}^{4}\frac{1}{(X-z_k)^2}$.

từ đó: $u = \dfrac{(P'(1))^2 - P(1)P''(1)}{(P(1))^2} = -5$ và $v = \dfrac{(P'(-1))^2 - P(-1)P''(-1)}{(P(-1))^2} = -\dfrac{5}{9}$.

◇ **Trả lời**: $-\dfrac{14}{9}$.

5.4.8 a) ◇ **Trả lời**:

$$\frac{1}{16}\left(-\frac{2}{(X-1)^3} - \frac{3}{(X-1)^2} + \frac{3}{X-1} - \frac{2}{(X+1)^3} - \frac{3}{(X+1)^2} - \frac{3}{X+1}\right)$$

b) Theo a): $\dfrac{16}{(X-1)^3(X+1)^3} = \dfrac{2-3(X-1)+3(X-1)^2}{(X-1)^3} + \dfrac{-2-3(X+1)-3(X+1)^2}{(X+1)^3}$.

◇ **Trả lời**: $U = \dfrac{1}{16}(8 - 9X + 3X^2)$, $V = -\dfrac{1}{16}(8 + 9X + 3X^2)$.

5.4.9 Một PTĐG cho, với $k \in \{0,\dots,n-1\}$:

$$\frac{a^k(X+a^{k+1})}{(X-a^k)(X-a^{k+1})(X-a^{k+2})} = \frac{1}{(1-a)^2}\left(\frac{1}{X-a^k} - \frac{2}{X-a^{k+1}} + \frac{1}{X-a^{k+2}}\right)$$

Ta suy ra:

$$\begin{aligned}(1-a)^2 F_n &= \sum_{k=0}^{n-1}\frac{1}{X-a^k} - 2\sum_{k=1}^{n}\frac{1}{X-a^k} + \sum_{k=2}^{n+1}\frac{1}{X-a^k}\\ &= \left(\frac{1}{X-1}+\frac{1}{X-a}\right) - 2\left(\frac{1}{X-a}+\frac{1}{X-a^n}\right) + \left(\frac{1}{X-a^n}+\frac{1}{X-a^{n+1}}\right).\end{aligned}$$

◇ **Trả lời**: $\dfrac{1}{(1-a)^2}\left(\dfrac{1}{X-1} - \dfrac{1}{X-a} - \dfrac{1}{X-a^n} + \dfrac{1}{X-a^{n+1}}\right)$.

5.4.10 Ta ký hiệu: $Q = \prod_{k=0}^{n-1}(X-\omega_k) = X^n - 1$, $F_p = \sum_{k=0}^{n-1}\dfrac{\omega_p^k}{X-\omega_k}$, $P = QF_p$: vậy ta có:

$$P \in \mathbb{C}[X] \quad \text{và} \quad \deg(P) < n.$$

Theo 5.4.2, *a*), Mệnh đề 2, với mọi k thuộc $\{0,\dots,n-1\}$: $\omega_k^p = \dfrac{P(\omega_k)}{Q'(\omega_k)} = \dfrac{P(\omega_k)}{n\omega_k^{n-1}} = \dfrac{\omega_k P(\omega_k)}{n}$,

từ đó: $\forall k \in \{0,\dots,n-1\}, P(\omega_k) = n\omega_k^{p-1}$

• Nếu $p \in \{1,\dots,n-1\}$ thì đa thức $P - nX^{p-1}$, có bậc $\le n-1$, triệt tiêu tại n số phức khác nhau từng đôi (các ω_k), vậy đa thức bằng 0, từ đó $P = nX^{p-1}$.

• Nếu $p = 0$, phép suy luận tương tự cũng áp dụng cho $P - nX^{n-1}$.

◇ **Trả lời**: $\begin{cases}\dfrac{nX^{n-1}}{X^n-1} & \text{nếu } p = 0\\ \dfrac{nX^{n-1}}{X^n-1} & \text{nếu } p \in \{1,\dots,n-1\}\end{cases}$

5.4.11 a) Đó chính là PTĐG của $\dfrac{P}{(X-a)(X-b)(X-c)}$.

b) Chọn $P = X^2$ trong kết quả của a) rồi thay X bởi $\dfrac{a+b+c}{2}$.

◇ **Trả lời**: $\dfrac{(a+b+c)^2}{(b+c-a)(c+a-b)(a+b-c)}$.

5.4.12 Việc xác định các cực điểm và phần nguyên đòi hỏi phải tách ra làm hai trường hợp tùy theo tính chẵn lẻ của n.

Trường hợp thứ 1: n **chẵn**

Các cực điểm của F_n là các $x_k = \tan\left(\dfrac{\pi}{2n} + \dfrac{k\pi}{n}\right)$, $k \in \{0,\dots, n-1\}$, tất cả đều đơn và phần nguyên bằng không (xem Tập 1, 2.5.1). Vậy tồn tại $\lambda_0,\dots,\lambda_{n-1} \in \mathbb{R}$ sao cho: $F_n = \sum_{k=0}^{n-1} \dfrac{\lambda_k}{X - x_k}$.

Cho $k \in \{0,\dots, n-1\}$. Ta có: $\lambda_k = \lim_{x \to x_k} ((x - x_k)F_n(x))$. Các ánh xạ $C_n, S_n : \mathbb{R} \to \mathbb{R}$ xác định bởi $\forall x \in \mathbb{R}$, $(C_n(x) = \cos(n \operatorname{Arctan} x)$, $S_n(x) = \sin(n \operatorname{Arctan} x))$ khả vi trên $\mathbb{R}$ và với mọi x thuộc $\mathbb{R} - \{x_k;\ 0 \le k \le n-1\}$: $(x - x_k)F_n(x) = S_n(x)\left(\dfrac{C_n(x) - C_n(x_k)}{x - x_k}\right)^{-1}$,

từ đó, vì $C'_n(x_k) = -\dfrac{n}{1+x_k^2} S_n(x_k) \neq 0$: $(x - x_k)F_n(x) \xrightarrow[x \to x_k]{} \dfrac{S_n(x_k)}{C'_n(x_k)} = -\dfrac{1+x_k^2}{n}$.

Trường hợp thứ 2: n **lẻ**

Ta ký hiệu $p = \dfrac{n-1}{2}$, $p \in \mathbb{N}^*$.

Các cực điểm của F_n là các $x_k = \tan\left(\dfrac{\pi}{2n} + \dfrac{k\pi}{n}\right)$, $k \in \{0,\dots,n-1\} - \{p\}$, tất cả đều đơn và phần nguyên của F_n là $\dfrac{1}{n}X$. Vậy tồn tại $\lambda_0,\dots,\lambda_{p-1}, \lambda_{p+1},\dots,\lambda_{2p} \in \mathbb{C}$ sao cho:

$$F_n = \frac{1}{n}X + \sum_{\substack{0 \le k \le 2p \\ k \neq p}} \frac{\lambda_k}{X - x_k}.$$

Ta tính các λ_k như trong trường hợp thứ 1.

◇ **Trả lời**:

$$F_n = \begin{cases} -\dfrac{1}{n}\displaystyle\sum_{k=0}^{n-1} \frac{1+x_k^2}{X - x_k} & \text{nếu } n \text{ chẵn} \\ \dfrac{1}{n}X - \dfrac{1}{n}\displaystyle\sum_{\substack{0 \le k \le n-1 \\ k \neq \frac{n-1}{2}}} \frac{1+x_k^2}{X - x_k} & \text{nếu } n \text{ lẻ} \end{cases}, \text{ trong đó: } x_k = \tan\left(\frac{\pi}{2n} + \frac{k\pi}{n}\right).$$

5.4.13 a) Tồn tại $\lambda_1,...,\lambda_n \in \mathbb{C}$ sao cho $\frac{X^p}{Q} = \sum_{k=1}^{n} \frac{\lambda_k}{X - z_k}$, và (xem 5.4.2, 2), *a*), Mệnh đề 2)

$\lambda_k = \frac{z_k^p}{Q'(z_k)}$.

◇ **Trả lời:** $\frac{X^p}{Q} = \sum_{k=1}^{n} \frac{z_k^p}{Q'(z_k)(X - z_k)}$.

b) Với $k \in \{1,..., n\}$, $Q_k = \frac{Q}{X - z_k} = \prod_{\substack{1 \le i \le n \\ i \ne k}} (X - z_i)$, ta có, theo a) : $X^p = \sum_{k=1}^{n} \frac{z_k^p}{Q'(z_k)} Q_k$.

Chú ý rằng hệ tử của X^{n-1} trong vế thứ hai là $\sum_{k=1}^{n} \frac{z_k^p}{Q'(z_k)}$.

◇ **Trả lời:** 0 nếu $p < n - 1$, 1 nếu $p = n - 1$.

5.4.14 Ta có PTĐG: $\frac{P}{Q} = \sum_{k=1}^{n} \frac{P(z_k)}{Q'(z_k)} \frac{1}{X - z_k}$, từ đó: $\frac{X}{Q} = \sum_{k=1}^{n} \frac{P(z_k)}{Q'(z_k)} \frac{X}{X - z_k}$.

Cho X tiến ra vô tận, ta kết luận: $\sum_{k=1}^{n} \frac{P(z_k)}{Q'(z_k)} = 0$.

5.4.15 Ta ký hiệu $Q = \prod_{k=1}^{n} (X - z_k)$ và, với mọi k thuộc $\{1,...,n\}$, $Q_k = \prod_{\substack{1 \le i \le n \\ i \ne k}} (X - z_i)$.

• Cho $k \in \{1,...,n\}$. Ta có: $Q = (X - z_k)Q_k$, từ đó, bằng cách đạo hàm : $Q' = (X - z_k)Q'_k + Q_k$, vậy: $Q'(z_k) = Q_k(z_k) = \prod_{\substack{1 \le i \le n \\ i \ne k}} (z_k - z_i)$.

Như thế: $\forall k \in \{1,..., n\}$, $u_k = z_k - \frac{P(z_k)}{Q'(z_k)}$.

• Ta có PTĐG: $\frac{P}{Q} = 1 + \sum_{k=1}^{n} \frac{P(z_k)}{Q(z_k)} \frac{1}{X - z_k}$, trong đó phần nguyên bằng 1 vì $\deg(P) = \deg(Q)$ và P cùng Q đều chuẩn tắc.

Ta ký hiệu $\alpha_0,..., \alpha_{n-1} \in \mathbb{C}$ sao cho $Q = X^N + \alpha_{n-1} X^{n-1} + ... + \alpha_0$.

Vì $\sum_{k=1}^{n} \frac{P(z_k)}{Q(z_k)} \frac{X}{X - z_k} = \frac{X(P - Q)}{Q}$, ta suy ra, khi cho X tiến ra vô tận:

$$\sum_{k=1}^{n} \frac{P(z_k)}{Q(z_k)} = a_{n-1} - \alpha_{n-1}.$$

Từ đó: $\sum_{k=1}^{n} u_k = \sum_{k=1}^{n} \left(z_k - \frac{P(z_k)}{Q'(z_k)} \right) = \sum_{k=1}^{n} z_k - (a_{n-1} - \alpha_{n-1})$

Mặt khác, vì $z_1,..., z_n$ là các không điểm của Q, ta có: $\sum_{k=1}^{n} z_k = -\alpha_{n-1}$.

Cuối cùng: $\sum_{k=1}^{n} u_k = -a_{n-1}$.

Chỉ dẫn và trả lời
các bài tập chương 6

6.2.1 a) 1)

$$\left.\begin{array}{l}\left.\begin{array}{l}F\cap G\subset F\\ F\cap H\subset F\end{array}\right|\Rightarrow (F\cap G)+(F\cap H)\subset F\\ \left.\begin{array}{l}F\cap G\subset G\\ F\cap H\subset H\end{array}\right|\Rightarrow (F\cap G)+(F\cap H)\subset G+H\end{array}\right|\Rightarrow (F+G)+(F\cap H)\subset F\cap (G+H)$$

2) Vì G và H có những vai trò đối xứng, nên có thể giả thiết, chẳng hạn, $G\subset F$.

Giả sử $x\in F\cap (G+H)$. Thế thì $x\in F$ và tồn tại $(g, h)\in G\times H$ sao cho $x = g + h$. Ta suy ra $h = x - g\in F$, vì $x\in F$ và $g\in G\subset F$. Sau đó $x = g + h$, trong đó $g\in G = F\cap G$ và $h\in F\cap H$. Điều này chứng tỏ: $F\cap (G+H)\subset (F\cap G)+(F\cap H)$, do đó, từ 1) ta suy ra đẳng thức.

3) ◇ **Trả lời:** $K = \mathbb{R}_2$, $E = \mathbb{R}^2$, $F = \mathbb{R}(1, 0)$, $G = \mathbb{R}(0, 1)$, $H = \mathbb{R}(1, 1)$.

Trong ví dụ này: $(F\cap G)+(F\cap H) = \{0\}+\{0\} = \{0\}$ và $F\cap (G+H) = F\cap E = F\neq \{0\}$.

b) 1) $$\left.\begin{array}{l}\left.\begin{array}{l}F\subset F+G\\ F\subset F+H\end{array}\right|\Rightarrow F\subset (F+G)\cap (F+H)\\ \left.\begin{array}{l}G\subset F+G\\ H\subset F+H\end{array}\right|\Rightarrow G\cap H\subset (F+G)\cap (F+H)\end{array}\right|\Rightarrow F+(G\cap H)\subset (F+G)\cap (F+H)$$

2) Cũng như trong a) 2), ta có thể giả thiết, chẳng hạn, $F\subset G$.

Cho $x\in (F+G)\cap (F+H)$.

Tồn tại $(f, g)\in F\times G$ và $(f', h)\in F\times H$ sao cho $x = f + g = f' + h$. Suy ra $h = f + g - f'\in G$.

Như vậy: $x = f' + h$, $f'\in F$, $h\in G\cap H$, từ đó suy ra $x\in F+(G\cap H)$.

Điều đó chứng tỏ: $(F+G)\cap (F+H)\subset F+(G\cap H)$, do đó, từ 1) ta suy ra đẳng thức.

3) ◇ **Trả lời :** Cũng ví dụ như ở *a) 3)*.

6.2.2 Lập luận bằng phản chứng: giả sử $F\neq E$ và $G\neq E$. Tồn tại $x\in E$ sao cho $x\notin F$, và $y\in E$ sao cho $y\notin G$. Vì $E = F\cup G$, ta suy ra $x\in G$ và $y\in F$.

Xét $x + y$; $x + y\in E = F\cup G$.

Nếu $x + y\in F$, thì $x = (x + y) - y\in F$, mâu thuẫn.

Nếu $x + y\in G$, thì $y = (x + y) - x\in G$, mâu thuẫn.

Điều đó chứng tỏ $F = E$ hoặc $G = E$.

6.2.3 Đặt $F = \bigcup_{i\in I} F_i$.

1) Vì $I\neq\varnothing$, tồn tại $i_0\in I$, và do $F\supset F_{i_0}\supset\{0\}$, nên $F\neq\varnothing$.

2) Giả sử $x, y\in F$. Tồn tại $(i, j)\in I^2$ sao cho: $x\in F_i$ và $y\in F_j$. Theo giả thiết tồn tại $k\in I$ sao cho $F_i\cup F_j\subset F_k$. Khi đó ta có $x\in F_k$, $y\in F_k$ nên $x + y\in F_k\subset F$.

3) Giả sử $\lambda\in K$, $x\in F$. Tồn tại $i\in I$ sao cho $x\in F_i$. Ta có: $\lambda x\in F_i\subset F$.

Như vậy, F là một kgvc của E.

6.2.4 ◇ **Trả lời:** $K = \mathbb{Z}_{2\mathbb{Z}}$, $E = K^2$, $F_1 = \{(0,0), (1,0)\}$, $F_2 = \{(0,0), (0,1)\}$, $F_3 = \{(0,0), (1,1)\}$.

6.2.5 Chứng minh rằng E là một kgvc của $\mathbb{R}^{\mathbb{R}}$ đối với các luật thông thường.

1) $E \neq \emptyset$, vì $0 \in E$.

2) Giả sử $f_1, f_2 \in E$. Tồn tại $A_1, A_2 \in \mathbb{R}_+^*$, $g_1, h_1, g_2, h_2 : \mathbb{R}_+ \to \mathbb{R}_+$ tăng sao cho:

$$\forall x \in \mathbb{R}_+, \quad (|x| \geq A_1 \Rightarrow f_1(x) = g_1(x) - h_1(x))$$
$$\forall x \in \mathbb{R}_+, \quad (|x| \geq A_2 \Rightarrow f_2(x) = g_2(x) - h_2(x)).$$

Ký hiệu $A = \text{Max}(A_1, A_2)$, $g = g_1 + g_2$, $h = h_1 + h_2$, ta có:

$$\begin{cases} A \in \mathbb{R}_+^* \\ g, h \text{ tăng} \\ \forall x \in \mathbb{R}_+, (|x| \geq A \Rightarrow (f_1 + f_2)(x) = g(x) - h(x) \end{cases}$$

từ đó suy ra $f_1 + f_2 \in E$.

3) Giả sử $\lambda \in \mathbb{R}$, $f \in E$. Tồn tại $A \in \mathbb{R}_+^*$, $f, g : \mathbb{R}_+ \to \mathbb{R}_+$ tăng sao cho:

$$\forall x \in \mathbb{R}_+, (|x| \geq A \Rightarrow f(x) = g(x) - h(x)).$$

Nếu $\lambda \geq 0$, thì λg, λh tăng và: $\forall x \in \mathbb{R}_+, (|x| \geq A \Rightarrow (\lambda f)(x) = (\lambda g)(x) - (\lambda h)(x))$.

Nếu $\lambda \leq 0$, thì $-\lambda h$, $-\lambda g$ tăng và: $\forall x \in \mathbb{R}_+, (|x| \geq A \Rightarrow (\lambda f)(x) = (-\lambda h)(x) - (-\lambda g)(x))$.

Như vậy: $\lambda f \in E$.

6.2.6 1) • $E \neq \emptyset$ vì $0 \in E$.

• Nếu $(f_1, f_2) \in E^2$ thì: $\forall i \in \{0, ..., N\}$, $(f_1 + f_2)(a_i) = f_1(a_i) + f_2(a_i) = 0$,

do vậy $f_1 + f_2 \in E$.

• Tương tự: $\forall \lambda \in \mathbb{R}$, $\forall f \in E$, $\lambda f \in E$.

2) Rõ ràng G là một kgvc của E (xem 5.1.4).

3) Giả sử $f \in E \cap G$; thế thì f là một đa thức bậc $\leq N$, triệt tiêu tại $N + 1$ số thực khác nhau từng đôi một, vì vậy $f = 0$.

Như vậy: $E \cap G = \{0\}$.

4) Giả sử $\varphi \in E$. Tồn tại $g \in G$ sao cho: $\forall i \in \{0, ..., N\}$, $g(a_i) = \varphi(a_i)$, xem đa thức nội suy Lagrange, 5.3.1, Ví dụ.

Đặt $f = \varphi - g$, ta có $f \in E$, $g \in G$, $\varphi = f + g$.

Điều đó chứng tỏ: $E + G = E$.

6.2.7 a) • $X' \subset A$, và $X' \neq \emptyset$ vì $0 \in X'$.

• Giả sử $(y, z) \in X'^2$. Ta có:

$\forall x \in X$, $x(y + z) = xy + xz = yx + zx = (y + z)x$, nên $y + z \in X'$.

• Giả sử $(\lambda, y) \in K \times X'$. Ta có: $\forall x \in X$, $x(\lambda y) = \lambda(xy) = \lambda(yx) = (\lambda y)x$, nên $\lambda y \in X'$.

• Giả sử $(y, z) \in X'^2$. Ta có : $\forall x \in X$, $x(yz) = (xy)z = (yx)z = y(xz) = y(zx) = (yz)x$,

nên $yz \in X'$.

Điều đó chứng tỏ X' là một đại số con của A.

b) 1) Cho $X \subset Y$, và giả sử $z \in Y'$.

Ta có: $\forall y \in Y$, $yz = zy$.

vì vậy: $\forall y \in X$, $yz = zy$.

do đó $z \in X'$. Như vậy: $Y' \subset X'$.

2) Giả sử $x \in X$. Từ định nghĩa của X' suy ra: $\forall y \in X'$, $xy = yx$, do vậy $x \in (X')' = X''$.

6.3.1 Với mọi $(\alpha, \beta, \gamma) \in \mathbb{Q}^3$:

$$\alpha u + \beta v + \gamma w = 0 \Leftrightarrow (\alpha + \gamma)x + (\alpha + \beta)y + (\beta + \gamma)z = 0 \Leftrightarrow \begin{cases} \alpha + \gamma = 0 \\ \alpha + \beta = 0 \\ \beta + \gamma = 0 \end{cases} \Leftrightarrow \alpha = \beta = \gamma = 0.$$

6.3.2 Lập luận bằng quy nạp: giả sử $\sqrt[n]{N} \in \mathbb{Q}$. Tồn tại $(a, b) \in (\mathbb{N}^*)^2$ sao cho :

$\sqrt[n]{N} = \frac{a}{b}$ và $a \wedge b = 1$.

Vì $a^n = b^n N$ nên b chia hết a^n.

Mặt khác , $b \wedge a^n = 1$, vì $a \wedge b = 1$ (xem 4.3.3 , Mệnh đề 2).

Ta suy ra $b = 1$, $N = a^n$, mâu thuẫn .

b) Giả sử $(\alpha, \beta) \in \mathbb{Q}^2$ sao cho $\alpha + \beta\sqrt[n]{N} = 0$. Nếu $\beta \neq 0$ thì $\sqrt[n]{N} = -\frac{\alpha}{\beta} \in \mathbb{Q}$, mâu thuẫn . Vì vậy $\beta = 0$ và sau đó $\alpha = 0$.

6.3.3 *Quy nạp theo n*

Trường hợp $n = 0$ là tầm thường.

Giả sử tính chất đúng với một n (thuộc $\mathbb{N}$), và giả sử $z_0, \ldots, z_{n+1} \in \mathbb{C}$ khác nhau từng đôi một ,

$\lambda_0, \ldots, \lambda_{n+1} \in \mathbb{C}$ sao cho $\sum_{k=0}^{n+1} \lambda_k (X - z_k)^{n+1} = 0$

Lấy đạo hàm: $\sum_{k=0}^{n+1} \lambda_k (X - z_k)^n = 0$, sau đó nhân với $(X - z_{n+1})$: $\sum_{k=0}^{n+1} \lambda_k (X - z_{n+1})(X - z_k)^n = 0$,

suy ra : $\sum_{k=0}^{n+1} \lambda_k ((X - z_k) + (z_k + z_{n+1}))(X - z_k)^n = 0$.

Do $\sum_{k=0}^{n+1} \lambda_k (X - z_k)^{n+1} = 0$, nên ta suy ra $\sum_{k=0}^{n} \lambda_k (z_k - z_{n+1})(X - z_k)^n = 0$,

rồi theo giả thiết quy nạp: $\forall k \in \{0, \ldots, n\}$, $\lambda_k (z_k - z_{n+1}) = 0$, vì vậy: $\forall k \in \{0, \ldots, n\}$, $\lambda_k = 0$.

Điều này dẫn tới: $\lambda_{n+1} (X - z_{n+1})^{n+1} = 0$, do đó $\lambda_{n+1} = 0$.

6.3.4 a) Giả sử $n \in \mathbb{N}^*$, $a_1, \ldots, a_n \in]0; 1[$, khác nhau từng đôi một sao cho $\sum_{i=1}^{n} \lambda_i f_i = 0$,

nghĩa là: $\forall x \in]0, 1[$, $\sum_{i=1}^{n} \frac{\lambda_i}{1 - a_i x} = 0$.

Cho $i \in \{1, \ldots, n\}$. Ta có : $\forall x \in]0, 1[$, $\lambda_i = -(1 - a_i x) \sum_{\substack{1 \leq j \leq n \\ j \neq i}} \frac{\lambda_j}{1 - a_j x}$.

Lấy giới hạn khi x dần tới $\frac{1}{a_i}$, ta suy ra $\lambda_i = 0$.

Nhận xét : Cũng có thể dùng tính duy nhất của dạng phân tích thành tích các phân tử đơn giản của phân thức hữu tỷ $\sum_{i=1}^{n} \frac{\lambda_i}{1-a_i X}$.

b) Dùng tính duy nhất của dạng phân tích thành tích các phân tử đơn giản (trong $\mathbb{R}[X]$) của phân thức hữu tỷ 0 trong hệ thức $\sum_{i=1}^{n} \frac{\lambda_i}{X+a_i^2+1} = 0$, với $n \in \mathbb{N}^*$, $a_1, \ldots, a_n \in]0,+\infty[$ khác nhau từng đôi một, $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$.

c) Giả sử $n \in \mathbb{N}^*$, $a_1, \ldots, a_n \in \mathbb{R}$, sao cho $a_1 < \ldots < a_n$, $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ sao cho $\sum_{i=1}^{n} \lambda_i f_{a_i} = 0$.

Đặc biệt: $\sum_{i=1}^{n} \lambda_i f_{a_i}(a_1) = 0$, nhưng $f_{a_i}(a_1) = \begin{cases} 1 & \text{nếu } i = 1 \\ 0 & \text{nếu } i \geq 1 \end{cases}$, từ đó suy ra $\lambda_1 = 0$.

Lặp lại lập luận trên, ta sẽ suy ra : $\lambda_1 = 0, \ldots, \lambda_n = 0$.

d) Giả sử $n \in \mathbb{N}^*$, $a_1, \ldots, a_n \in \mathbb{R}$ sao cho $a_1 < \ldots < a_n$; $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$, sao cho $\sum_{i=1}^{n} \lambda_i f_{a_i} = 0$,

nghĩa là: $\forall x \in \mathbb{R}, \sum_{i=1}^{n} \lambda_i e^{a_i x} = 0$.

Thế thì: $\forall x \in \mathbb{R}, \lambda_n = -\sum_{i=1}^{n-1} \lambda_i e^{(a_i - a_n)x}$, do đó khi cho n dần tới $+\infty$, ta sẽ nhận được $\lambda_n = 0$.

Lặp lại lập luận trên ta suy ra $\lambda_n = 0, \lambda_{n-1} = 0, \ldots, \lambda_1 = 0$.

e) Trước hết nhận xét rằng với mọi họ hữu hạn I của $\mathbb{R}^2$, tồn tại hai họ hữu hạn J, K của $\mathbb{R}$ sao cho $I \subset J \times K$. Tính độc lập tuyến tính của $(f_{a,b})_{(a,b) \in J \times K}$ suy ra từ tính độc lập tuyến tính của $(f_{a,b})_{(a,b) \in J \times K}$.

Do vậy, giả sử $(n, p) \in (\mathbb{N}^*)^2$, $a_1, \ldots, a_n \in \mathbb{R}$ khác nhau từng đôi một ; $b_1, \ldots, b_p \in \mathbb{R}$, khác nhau từng đôi một , $(\lambda_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}} \in \mathbb{R}^{np}$ sao cho $\sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}} \lambda_{ij} f_{a_i, b_j} = 0$.

Thế thì ta có: $\forall (x, y) \in \mathbb{R}^2, \sum_{j=1}^{p} \left(\sum_{i=1}^{n} \lambda_{ij} e^{a_i x} \right) e^{b_j y} = 0$

Giả sử $x \in \mathbb{R}$, theo d), họ $\begin{pmatrix} \mathbb{R} \to \mathbb{R} \\ y \mapsto e^{b_j y} \end{pmatrix}_{1 \leq j \leq p}$ độc lập tuyến tính, từ đó suy ra: $\forall j \in \{1, \ldots, p\}$, $\sum_{i=1}^{n} \lambda_{ij} e^{a_i x} = 0$.

Như vậy: $\forall j \in \{1, \ldots, p\}$, $\forall x \in \mathbb{R}$, $\sum_{i=1}^{n} \lambda_{ij} e^{a_i x} = 0$, từ đó, vẫn theo d), ta suy ra:

$$\forall j \in \{1, \ldots, p\}, \forall i \in \{1, \ldots, n\}, \lambda_{ij} = 0.$$

f) Quy về d) bằng phép đổi biến $x' = e^{\alpha \ln x}$.

g) Quy về e) như trên đây.

h) Giả sử $N \in \mathbb{N}^*$, $\lambda_1, \ldots, \lambda_N \in \mathbb{R}$ sao cho $\sum_{n=1}^{N} \lambda_n f_n = 0$, nghĩa là: $\forall x \in \mathbb{R}$, $\sum_{n=1}^{N} \lambda_n \sin(x^n) = 0$.

Lấy đạo hàm: $\forall x \in \mathbb{R}, \sum_{n=1}^{N} n\lambda_n x^{n-1}\cos(x^n) = 0$

Giả sử $(\lambda_1, \ldots, \lambda_N) \neq (0, \ldots, 0)$ và gọi n_0 là số nguyên nhỏ nhất ≥ 1 sao cho $\lambda_{n_0} \neq 0$. Thế thì:

$$0 = \sum_{n=1}^{N} n\lambda_n x^{n-1}\cos(x^n) \underset{x \to 0}{\sim} n_0\lambda_{n_0} x^{n_0-1}, \text{ mâu thuẫn.}$$

i) Cho $(\lambda, \mu, \nu) \in \mathbb{R}^3$ sao cho : $\lambda f + \mu f \circ f + \nu f \circ f \circ f = 0$.

Viết các khai triển hữu hạn tới cấp 5 tại lân cận của 0 :

$$f(x) = x - \frac{x^3}{6} + \frac{x^5}{120} + o(x^5), (f \circ f)(x) = x - \frac{x^3}{3} - \frac{x^5}{10} + o(x^5), \ (f \circ f \circ f)(x) = x - \frac{x^3}{2} + \frac{11x^5}{40} + o(x^5).$$

Do đó, từ tính duy nhất của khai triển hữu hạn tới cấp 5 tại lân cận 0 của hàm không, ta suy ra

$$\begin{cases} \lambda + \mu + \nu = 0 \\ -\frac{\lambda}{6} - \frac{\mu}{3} - \frac{\nu}{2} = 0 \\ \frac{\lambda}{120} + \frac{\mu}{10} + \frac{11\nu}{40} = 0 \end{cases}$$, sau khi thực hiện các phép tính ta sẽ có $\lambda = \mu = \nu = 0$.

6.3.5 ◇ **Trả lời :** không vì $f_{0,1} + f_{1,1} = 2f_{0,2}$.

6.3.6 i) Giả sử $(f, f', g) \in F \times F' \times (G \cap G')$ sao cho $f + f' + g = 0$.

Vì $F' \subset G$ nên $f' + g \in G$, do đó, vì F và G bù nhau trong E : $f = f' + g = 0$.

Sau đó, vì $f' \in F'$, $g \in G'$, F' và G' bù nhau trong E, nên : $f' = g = 0$.

Điều đó chứng tỏ F, F', $G \cap G'$ có tổng trực tiếp.

ii) • $\left|\begin{matrix} F' \subset G \\ G \cap G' \subset G \end{matrix}\right| \Rightarrow F' + (G \cap G') \subset G$.

• Giả sử $x \in G$. Tồn tại $f' \in F'$, $g' \in G'$ sao cho $x = f' + g'$. Vì $F' \subset G$ nên $f' \in G$, từ đó suy ra $g' = x - f' \in G$, và vì vậy $g' \in G \cap G'$. Như vậy, $x = f' + g'$ trong đó $f' \in F'$ và $g' \in G \cap G'$, điều này chứng tỏ: $G \subset F' + (G \cap G')$.

Ta đã nhận được : $F' + (G \cap G') = G$.

iii) $F + F' + (G \cap G') = F + (F' + (G \cap G')) = F + G = E$.

6.3.7 i) Giả sử $(x_1, \ldots, x_n)$ độc lập tuyến tính.

• Hiển nhiên rằng: $\forall i \in \{1, \ldots, n\}, x_i \neq 0$.

• Giả sử $(y_1, \ldots, y_n) \in \prod_{i=1}^{n} Kx_i$ sao cho $\sum_{i=1}^{n} y_i = 0$.

Với mỗi $i \in \{1, \ldots, n\}$, tồn tại $\lambda_i \in K$ sao cho $y_i = \lambda_i x_i$. Vì $\sum_{i=1}^{n} \lambda_i x_i = 0$ và $(x_i)_{1 \leq i \leq n}$ độc lập tuyến tính, ta suy ra $(\forall i \in \{1, \ldots, n\}, \lambda_i = 0)$, và sau đó: $(\forall i \in \{1, \ldots, n\}, y_i = 0)$.

Điều đó chứng tỏ $\sum_{i=1}^{n} Kx_i$ là tổng trực tiếp.

2) Ngược lại, giả sử : $\begin{cases} \forall i \in \{1,\dots,n\}, x_i \neq 0 \\ \sum_{i=1}^{n} Kx_i \text{ là tổng trực tiếp} \end{cases}$

Giả sử $(\lambda_1, \dots, \lambda_n) \in K^n$ sao cho $\sum_{i=1}^{n} \lambda_i x_i = 0$. Vì $(\forall i \in \{1, \dots, n\}, \lambda_i x_i \in Kx_i)$ và $\sum_{i=1}^{n} Kx_i$ là tổng trực tiếp, ta suy ra : $(\forall i \in \{1, \dots, n\}, \lambda_i x_i = 0)$, và $(\forall i \in \{1,\dots,n\}, \lambda_i = 0)$.

Điều đó chứng tỏ $(x_1, \dots, x_n)$ độc lập tuyến tính.

6.3.8 Cho $(x_1,\dots,x_n) \in \prod_{i=1}^{n} G_i$ sao cho $\sum_{i=1}^{n} x_i = 0$. Vì $(\forall i \in \{1, \dots, n\}, G_i \subset F_i)$ và $F_1, \dots, F_n$ có tổng trực tiếp, ta suy ra. $\forall i \in \{1, \dots, n\}, x_i = 0$.

6.3.9 a) Một họ con hữu hạn của $\bigcap_{i=1}^{n} \mathcal{L}_i$ có thể viết dưới dạng $(x_{ij})_{(i,j)\in\Phi}$,

trong đó $\Phi = \{(i, j) : 1 \leq i \leq n, 1 \leq j \leq N_i\}$, $n, N_1, \dots, N_n \in \mathbb{N}^*$.

Giả sử họ $(\lambda_{ij})_{(i,j)\in\Phi}$ thỏa mãn $\sum_{(i,j)\in\Phi} \lambda_{ij} x_{ij} = 0$.

Vì $\sum_{i=1}^{n} \left(\sum_{j=1}^{N_i} \lambda_{ij} x_{ij} \right) = 0$, và do $\left(\forall i \in \{1,\dots,n\}, \sum_{j=1}^{N_i} \lambda_{ij} x_{ij} \in F_i \right)$, và $F_1, \dots, F_n$ có tổng trực tiếp nên ta suy ra: $\forall i \in \{1, \dots, n\}, \sum_{j=1}^{N_i} \lambda_{ij} x_{ij} = 0$, do đó, từ tính độc lập tuyến tính của các $\mathcal{L}_i$ nên :

$$\forall i \in \{1, \dots, n\}, \forall j \in \{1, \dots, N_i\}, \lambda_{ij} = 0.$$

b) $\text{Vect}\left(\bigcup_{i=1}^{n} G_i \right) = \sum_{i=1}^{n} \text{Vect}(G_i) = \sum_{i=1}^{n} F_i = E$.

c) Suy ra từ *a*) và *b*).

6.4.1 Với mọi $(x, y, z) \in \mathbb{C}^3$:

$$\begin{cases} x + y + z = 0 \\ x + iy - z = 0 \end{cases} \Leftrightarrow \begin{cases} x = -y - z \\ (i-1)y = 2z \end{cases} \Leftrightarrow \begin{cases} x = iz \\ y = -(1+i)z \end{cases}$$

Như vậy $F = \{z(i, -(1+i), 1) ; z \in \mathbb{C}\}$, vì vậy F là kgvc của $\mathbb{C}^3$ sinh bởi vecto $(i, -(1+i), 1)$.

◇ **Trả lời:** • Một cơ sở của F là $(i, -(1+i), 1)$

• $\dim(F) = 1$

6.4.2 Với $i \in \{1, \dots, 4\}$, ta ký hiệu g_i : $\begin{array}{ccc}]-1;1[& \to & \mathbb{R} \\ x & \mapsto & \sqrt{1-x^2} f_i(x) \end{array}$

Như vậy, với mọi x thuộc $]-1 ; 1[$, ta có: $g_1(x) = 1 - x$, $g_2(x) = 1 + x$, $g_3(x) = 1$, $g_4(x) = x$.

Rõ ràng là (g_3, g_4) độc lập tuyến tính và : $g_1 = g_3 - g_4$, $g_2 = g_3 + g_4$: từ đó suy ra rằng (f_3, f_4) độc lập tuyến tính và $f_1 = f_3 - f_4$, $f_2 = f_3 + f_4$.

◇ **Trả lời :** • Một cơ sở của f là (f_3, f_4)

• $\dim(F) = 2$.

6.4.3 1) Với mọi $(\alpha, \beta, \gamma) \in \mathbb{R}^3$:

$$\alpha u + \beta v + \gamma w = 0 \Leftrightarrow \begin{cases} \alpha + \gamma = 0 \\ \beta + \gamma = 0 \\ \alpha - \beta + \gamma = 0 \\ \gamma = 0 \end{cases} \Leftrightarrow \alpha = \beta = \gamma = 0.$$

vì vậy (u, v, w) độc lập tuyến tính và $\dim(F) = 3$.

2) Hiển nhiên (x,y) là độc lập tuyến tính , nên $\dim(G) = 2$.

3) Họ (u, v, w, x) độc lập tuyến tính vì với mọi $(\alpha, \beta, \gamma, \delta)$ thuộc $\mathbb{R}^4$:

$$\alpha u + \beta v + \gamma w + \delta x = 0 \Leftrightarrow \begin{cases} \alpha + \gamma = 0 \\ \beta + \gamma = 0 \\ \alpha - \beta + \gamma + \delta = 0 \\ \lambda = 0 \end{cases} \Leftrightarrow \alpha = \beta = \gamma = \delta = 0.$$

Mặt khác từ đây ta cũng suy ra (u, v, w) độc lập tuyến tính .

Như vậy, $\dim(F + G) \geq 4$, nên, vì $F + G \subset \mathbb{R}^4$: $F + G = \mathbb{R}^4$.

4) $\dim(F \cap G) = \dim(F) + \dim(G) - \dim(F + G) = 3 + 2 - 4$.

◇ **Trả lời**: $\dim(F) = 3$, $\dim(G) = 2$, $\dim(F + G) = 4$, $\dim(F \cap G) = 1$.

6.4.4 Theo 6.4, Mệnh đề 6, F có ít nhất một phần bù G trong E.

kgvc F (tương ứng: G) có ít nhất một cơ sở $\mathcal{B} = (f_1, \ldots, f_p)$, $p \geq 1$ (tương ứng: $\mathcal{C} = (g_1, \ldots, g_q)$, $q \geq 1$). Đặt $\mathcal{C}' = (f_1 + g_1, g_2, \ldots, g_q)$ và $G' = \text{Vect}(\mathcal{C}')$

1) Ta chứng minh: $F \cap G' = \{0\}$.

Giả sử $x \in F \cap G'$. Tồn tại $\lambda_1, \ldots, \lambda_p, \mu_1, \ldots, \mu_q \in K$ sao cho $x = \sum_{i=1}^{p} \lambda_i f_i = \mu_1 (f_1 + g_1) + \sum_{j=2}^{q} \mu_j g_j$.

Khi đó: $\sum_{i=1}^{p} \lambda_i f_i - \mu_1 f_1 = \sum_{j=2}^{q} \mu_j g_j \in F \cap G = \{0\}$, nên $\sum_{j=1}^{q} \mu_j g_j = 0$, sau đó vì $\mathcal{C}$ là độc lập tuyến tính, nên $(\forall j \in \{1, \ldots, q\}, \mu_j = 0)$, do đó $x = 0$

2) Ta chứng minh: $F + G' = E$.

Cho $x \in E$. Tồn tại $\lambda_1, \ldots, \lambda_p, \mu_1, \ldots, \mu_q \in K$ sao cho $x = \sum_{i=1}^{p} \lambda_i f_i + \sum_{j=1}^{q} \mu_j g_j$.

Khi đó: $x = \left((\lambda_1 - \mu_1) f_1 + \sum_{i=2}^{p} \lambda_i f_i \right) + \left(\mu_1 (f_1 + g_1) + \sum_{j=2}^{q} \mu_j g_j \right) \in F + G'$.

3) Ta có $f_1 + g_1 \in G'$, và $f_1 + g_1 \notin G$, vì nếu trái lại thì: $f_1 = (f_1 + g_1) - g_1 \in G$, mâu thuẫn .

Do đó: $G \neq G'$.

6.4.5 Sử dụng: $\dim(F) + \dim(G) = \dim(F + G) - \dim(F \cap G)$.

6.4.6 Vì $E \times F$ hữu hạn chiều, nên $E \times F$ có ít nhất một họ sinh hữu hạn $(x_i, y_i)_{1 \le i \le n}$.

Cho $x \in E$. Vì $(x, 0) \in E \times F$, nên tồn tại $(\lambda_i)_{1 \le i \le n} \in K^n$ sao cho $(x,0) = \sum_{i=1}^{n} \lambda_i (x_i y_i)$, từ đó suy ra $x = \sum_{i=1}^{n} \lambda_i x_i$.

Điều đó chứng tỏ $(x_i)_{1 \le i \le n}$ sinh ra E, và do vậy E hữu hạn chiều.

6.4.7 1) Ký hiệu: $c : \mathbf{R} \xrightarrow[x \mapsto \cos x]{} \mathbf{R}$, $s : \mathbf{R} \xrightarrow[x \mapsto \sin x]{} \mathbf{R}$, ta có: $\forall i \in \{1, 2, 3\}$, $f_{a_i} = (\cos a_i)c - (\sin a_i)s$;

từ đó suy ra $\mathrm{Vect}(f_{a_1}, f_{a_2}, f_{a_3}) \subset \mathrm{Vect}(c, s)$ và do vậy $\mathrm{rank}(f_{a_1}, f_{a_2}, f_{a_3}) \le 2$.

2) Vì $f_{a_1} \neq 0$, ta có $\mathrm{rank}(f_{a_1}, f_{a_2}, f_{a_3}) \ge 1$.

3) Hạng của $(f_{a_1}, f_{a_2}, f_{a_3})$ là 1 khi và chỉ khi f_{a_2} và f_{a_3} đồng phương với f_{a_1}. Vì (c, s) độc lập tuyến tính:

$$(f_{a_1}, f_{a_2}) \text{ phụ thuộc tuyến tính} \Leftrightarrow \left(\exists \lambda \in \mathbf{R}, \begin{cases} \cos a_2 = \lambda \cos a_1 \\ \sin a_2 = \lambda \sin a_1 \end{cases} \right)$$

$$\Leftrightarrow \cos a_2 \sin a_1 = \sin a_2 \cos a_1 \Leftrightarrow \sin(a_2 - a_1) = 0 \Leftrightarrow a_2 - a_1 \in \pi \mathbf{Z}.$$

◇ **Trả lời**: $\begin{cases} 1 & \text{nếu } (a_2 - a_1, a_3 - a_1) \in (\pi \mathbf{Z})^2 \\ 2 & \text{nếu } (a_2 - a_1, a_3 - a_1) \notin (\pi \mathbf{Z})^2 \end{cases}$.

6.4.8 1) $\Rightarrow$ 2)

• Ta đã biết rằng $\mathcal{F}$ là một họ sinh của E.

• Giả sử $\mathcal{G}$ là một họ sinh của E sao cho $\mathcal{G} \subset \mathcal{F}$. Vì $\mathcal{F}$ hữu hạn nên $\mathcal{G}$ hữu hạn. Vì $\mathcal{G}$ là hữu hạn và là một họ sinh của E nên theo 6.4, Mệnh đề 3.3, $\mathrm{Card}(\mathcal{G}) \ge \dim(E) = \mathrm{Card}(\mathcal{F})$.

Vì $\begin{cases} \mathcal{G} \subset \mathcal{F} \\ \mathrm{card}(\mathcal{G}) \ge \mathrm{card}(\mathcal{F}) \end{cases}$, nên $\mathcal{G} = \mathcal{F}$.

2) $\Rightarrow$ 1)

Lập luận bằng phản chứng: giả sử $\mathcal{F}$ phụ thuộc tuyến tính, tồn tại $x \in \mathcal{F}$ sao cho x phân tích tuyến tính được trên $\mathcal{F}' = \mathcal{F} - \{x\}$.

Như vậy $\mathcal{F}$ là một họ sinh của E, $\mathcal{F}' \subset \mathcal{F}$, $\mathcal{F}' \neq \mathcal{F}$, điều này mâu thuẫn với 2).

1) $\Rightarrow$ 3)

• Ta đã biết rằng $\mathcal{F}$ độc lập tuyến tính.

• Giả sử $\mathcal{L}$ là một họ độc lập tuyến tính của E sao cho $\mathcal{F} \subset \mathcal{L}$. Theo 6.4, Mệnh đề 3, 1), $\mathcal{L}$ hữu hạn và $\mathrm{Card}(\mathcal{L}) \le \dim(E) = \mathrm{Card}(\mathcal{F})$.

Vì $\begin{cases} \mathcal{F} \subset \mathcal{L} \\ \mathrm{Card}(\mathcal{L}) \le \mathrm{Card}(\mathcal{F}) \end{cases}$, nên $\mathcal{L} = \mathcal{F}$.

3) $\Rightarrow$ 1)

Lập luận bằng phản chứng: Giả sử $\mathcal{F}$ không phải là một họ sinh của E, khi đó tồn tại $x \in E$ sao cho $x \notin \mathrm{Vect}(\mathcal{F})$. Như vậy họ $\mathcal{F}'$ xác định bởi $\mathcal{F}' = \mathcal{F} \cup \{x\}$ độc lập tuyến tính, $\mathcal{F} \subset \mathcal{F}'$, $\mathcal{F}' \neq \mathcal{F}$, điều này mâu thuẫn với 3).

6.4.9 a) Được suy ra từ phép chứng minh của 6.4, Định lý - Định nghĩa 1.

b) Đó là định lý về cơ sở không đầy đủ, dạng yếu, 6.4, Định lý 2.

c) Theo a), tồn tại một cơ sở $\mathcal{B}_1$ của E sao cho $\mathcal{B}_1 \subset \mathcal{G}$. Theo định lý về cơ sở không đầy đủ (dạng mạnh), có thể bổ sung cho $\mathcal{L}$ những vectơ thuộc $\mathcal{B}_1$ (vì vậy của $\mathcal{G}$) để nhận được một cơ sở $\mathcal{B}_2$ của E. Hiển nhiên ta có $\mathcal{L} \subset \mathcal{B}_2 \subset \mathcal{G}$.

d) Được suy từ c) áp dụng cho $\mathcal{L} \cup \mathcal{G}$ thay vì $\mathcal{G}$

6.4.10 a) • Từ định nghĩa của A suy ra A là kgvc của $\mathbb{Q}$ - kgv $\mathbb{R}$ sinh bởi họ $\mathcal{G} = (1, \sqrt{2}, \sqrt{3}, \sqrt{6})$

• Hiển nhiên rằng : $\forall (\alpha, \beta) \in \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}^2$, $\alpha\beta \in A$

Do đó, từ tính chất $\mathbb{Q}$- tuyến tính suy ra: $\forall (x, y) \in A^2$, $xy \in A$.

Theo 6. 2, Định nghĩa 4, A là một đại số con của $\mathbb{Q}$- đại số $\mathbb{R}$.

b) Giả sử $(a, b, c, d) \in \mathbb{Q}^4$ sao cho $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0$.

Ta suy ra $\begin{cases} (a + b\sqrt{2})^2 = 3(c + d\sqrt{2})^2 \\ (a + c\sqrt{3})^2 = 2(b + d\sqrt{3})^2 \end{cases}$, sau đó, theo Bài tập 6. 3. 2 :

$$\left.\begin{cases} a^2 + 2b^2 - 3c^2 - 6d^2 = 0 \\ ab = 3cd \\ a^2 + 3c^2 - 2b^2 - 6d^2 = 0 \\ ac = 2bd \end{cases}\right| \text{ , suy ra } \begin{cases} a^2 = 6d^2 \\ 2b^2 = 3c^2 \end{cases}.$$

Vì $\sqrt{6} \notin \mathbb{Q}$ và $\sqrt{\frac{2}{3}} \notin \mathbb{Q}$, vẫn theo bài tập trên, ta được : $a = d = 0$ và $b = c = 0$.

Điều đó chứng tỏ $\mathcal{G}$ độc lập tuyến tính.

Vì, theo định nghĩa của A, $\mathcal{G}$ sinh ra A, nên $\mathcal{G}$ là một cơ sở của A, và $\dim(A) = 4$

c) Giả sử $x \in A - \{0\}$. Vì $x \in \mathbb{R}^*$, x có một nghịch đảo trong $\mathbb{R}$, ký hiệu là x^{-1}. Ta chỉ cần phải chứng tỏ rằng $x^{-1} \in A$. Tồn tại $(a, b, c, d) \in \mathbb{Q}^4$ sao cho $x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$. Ta sẽ tính x^{-1} bằng cách dùng các "lượng liên hợp".

Hiển nhiên $(a, b, c, d) \neq (0, 0, 0, 0)$. Vì vậy, theo b), $(a + b\sqrt{2}) - (c\sqrt{3} + d\sqrt{6}) \neq 0$, nên $x^{-1} = \dfrac{y}{\alpha + \beta\sqrt{2}}$, trong đó $y = (a + b\sqrt{2}) - (c\sqrt{3} + d\sqrt{6})$, $\alpha = a^2 + 2b^2 - 3c^2 - 6d^2$, $\beta = 2ab - 6cd$.

Vì $\alpha + \beta\sqrt{2} \neq 0$, nên nhất thiết $(\alpha, \beta) \neq (0,0)$, và do vậy vì $(1, \sqrt{2})$ độc lập tuyến tính , nên $\alpha - \beta\sqrt{2} \neq 0$ Ta được : $x^{-1} = \dfrac{y(\alpha - \beta\sqrt{2})}{\alpha^2 - 2\beta^2} \in A$.

◇ **Trả lời** : $\dfrac{1}{4} - \dfrac{1}{4}\sqrt{3} + \dfrac{1}{4}\sqrt{6}$.

Chỉ dẫn và trả lời
các bài tập chương 7

7.1.1 1) Giả sử $f(A) \subset f(B)$, và giả sử $x \in A + \text{Ker}(f)$. Tồn tại $a \in A$ và $u \in \text{Ker}(f)$ sao cho $x = a + u$. Vì $f(a) \in f(A) \subset f(B)$, nên tồn tại $b \in B$ sao cho $f(a) = f(b)$, và do đó $a - b \in \text{Ker}(f)$. Khi đó: $x = b + (a - b + u)$, $b \in B$, $a - b + u \in \text{Ker}(f)$, từ đó suy ra $x \in B + \text{Ker}(f)$.

Ta kết luận : $A + \text{Ker}(f) \subset B + \text{Ker}(f)$.

2) Ngược lại, giả sử $A + \text{Ker}(f) \subset B + \text{Ker}(f)$, và giả sử $y \in f(A)$. Tồn tại $a \in A$ sao cho $y = f(a)$. Vì $a \in A \subset A + \text{Ker}(f) \subset B + \text{Ker}(f)$, nên tồn tại $b \in B$ và $v \in \text{Ker}(f)$ sao cho $a = b + v$. Vậy $y = f(b + v) = f(b) + f(v) = f(b) \in f(B)$. Ta kết luận: $f(A) \subset f(B)$.

7.1.2 Giả sử $\lambda \in K$, $a, a' \in E$. Ta có: $(a + \lambda a', f(a) + \lambda f(a')) = (a, f(a)) + \lambda(a', f(a')) \in G$. Do đó, từ tính duy nhất của phần tử c của E sao cho $(a' + \lambda a', c) \in G$, ta suy ra: $f(a) + \lambda f(a') = f(a + \lambda a')$.

7.1.3 Dễ dàng chứng minh tính chất tuyến tính của f.

Với mọi $P = \sum_{k=0}^{n} a_k X^k$ thuộc $\mathbb{R}[X]$ ta có:

$$f(P) = \sum_{k=0}^{n} a_k X^k - X\sum_{k=1}^{n} k a_k X^{k-1} = \sum_{k=0}^{n} (1-k) a_k X^k$$

• $P \in \text{Ker}(f) \Leftrightarrow (\forall k \in \{0, \ldots, n\}, (1 - k)a_k = 0) \Leftrightarrow (\forall k \in \{0, \ldots, n\} - \{1\}, a_k = 0)$, do đó $\text{Ker}\, f = \mathbb{R}X$.

• $\text{Im} f = \text{Vect}((X^k)_{k \in \mathbb{N}-\{1\}})$, vì : $\forall k \in \mathbb{N}, f(X^k) = (1 - k)X^k$.

◇ **Trả lời** : $\text{Ker}(f) = \mathbb{R}X$, $\text{Im} f = \text{Vect}((X^k)_{k \in \mathbb{N}-\{1\}})$.

7.1.4 Trước hết: $\forall P \in E$, $P - P' \in E$.

Dễ dàng chứng minh tính tuyến tính của f.

1) Giả sử $P \in E - \{0\}$; vì $\deg(P) \neq \deg(P')$, ta có $P - P' \neq 0$. Điều đó chứng tỏ $\text{Ker}(f) = \{0\}$, và do vậy f là đơn ánh.

2) Giả sử $Q \in E$.

• Giả sử tồn tại $P \in E - \{0\}$ sao cho $f(P) = Q$. Đặt $n = \deg(P) = \deg(Q)$ và lấy đạo hàm: $Q = -P' + P$, $Q' = -P'' + P'$, ... , $Q^{(n)} = -P^{(n+1)} + P^{(n)} = P^{(n)}$, do đó bằng cách cộng từng vế ta suy ra: $Q + Q' + \ldots + Q^{(n)} = P$.

• Vậy ta xét ánh xạ $g: E \to E$ xác định bởi : $\forall Q \in E, g(Q) = \sum_{k=0}^{\deg(Q)} Q^{(k)}$ (và $g(0) = 0$) ; ta có thể ký hiệu $g(Q) = \sum_{k=0}^{+\infty} Q^{(k)}$. Hiển nhiên g tuyến tính, và :

$$\forall P \in E,\ (g \circ f)(P) = g(P - P') = (P - P') + (P' - P'') + \cdots + (P^{(n)} - 0) = P$$

$$\forall Q \in E,\ (f \circ g)(Q) = f(Q + Q' + \cdots + Q^{(n)}),$$

$$= (Q + Q' + \cdots + Q^{(n)}) - (Q' + Q'' + \cdots + Q^{(n+1)}) = Q.$$

trong đó $n = \deg(P) = \deg(Q)$

Điều đó chứng tỏ f là một tự đẳng cấu của E, và $g = f^{-1}$.

◇ **Trả lời :** $\forall Q \in E,\ f^{-1}(Q) = \sum_{k=0}^{+\infty} Q^{(k)}$.

7.1.5 a) Hiển nhiên

b) Tính tuyến tính của ϕ là hiển nhiên .

1) $\forall f \in E,\ (f \in \mathrm{Ker}(\phi) \Leftrightarrow f' = 0 \Leftrightarrow f \in \mathbb{R}.1$), trong đó $\mathbf{1} : \mathbb{R} \xrightarrow[x \mapsto 1]{} \mathbb{R}$

2) • Giả sử $g \in \mathrm{Im}(\phi)$, $f \in E$ sao cho $g = \phi(f) = f'$.

Bằng cách lấy nguyên hàm, ta suy ra rằng tồn tại $\lambda \in \mathbb{R}$ sao cho: $\forall x \in \mathbb{R},\ f(x) = \lambda + \int_0^x g(t)dt$.

Vì f là T- tuần hoàn nên: $f(T) = f(0)$, từ đó suy ra $\int_0^T g(t)dt = 0$.

• Ngược lại, giả sử $g \in E$ sao cho $\int_0^T g = 0$. Xét f : $\mathbb{R} \xrightarrow[x \mapsto \int_0^x g(t)dt]{} \mathbb{R}$

Ta biết rằng f thuộc lớp C^1 trên $\mathbb{R}$, và $f' = g$ (xem Tập 1, 6.4.1, Hệ quả 1)). Hơn nữa:

$$\forall x \in \mathbb{R},\quad f(x+T) - f(x) = \int_x^{x+T} g(t)dt = \int_x^0 g(t)dt + \int_0^T g(t)dt + \int_T^{x+T} g(t)dt .$$

$$\underset{[u=t-T]}{=} -\int_0^x g(t)dt + \int_0^x g(u+T)du = 0,$$

điều này chứng tỏ : $f \in E$.

◇ **Trả lời :** $\mathrm{Ker}(\phi) = \mathbb{R}.1$, $\mathrm{Im}(\phi) = \left\{ g \in E ; \int_0^T g(t)dt = 0 \right\}$.

7.1.6 Theo giả thiết: $\forall x \in E - \{0\}, \exists!\ \lambda_x \in K,\ f(x) = \lambda_x x$ Như vậy chỉ cần chứng tỏ rằng λ_x không phụ thuộc x . Giả sử $(x, y) \in (E - \{0\})^2$

1) Giả sử (x, y) độc lập tuyến tính .

Ta có $\begin{cases} f(x+y) = f(x) + f(y) = \lambda_x x + \lambda_y y \\ f(x+y) = \lambda_{x+y}(x+y) \end{cases}$, từ đó suy ra $(\lambda_{x+y} - \lambda_x)x + (\lambda_{x+y} - \lambda_y)y = 0$,

và do vậy $\lambda_{x+y} - \lambda_x = \lambda_{x+y} - \lambda_y = 0$, $\lambda_x = \lambda_y$.

2) Giả sử (x, y) phụ thuộc tuyến tính.

Tồn tại $\alpha \in K - \{0\}$ sao cho $y = \alpha x$, và ta có: $f(y) = \alpha f(x) = \alpha\lambda_x x$ và $f(y) = \lambda_y y = \lambda_y \alpha x$, nên $\lambda_x = \lambda_y$.

Điều đó chứng tỏ : $\exists \lambda \in K, \forall x \in E - \{0\}, f(x) = \lambda x$. Cuối cùng: $f(0) = 0 = \lambda 0$.

7.1.7 Quy nạp theo n

Trường hợp $n = 1$ là tầm thường

Giả sử tính chất đúng với một n thuộc $\mathbb{N}^*$, và giả sử $\lambda_1, \ldots, \lambda_{n+1} \in K$ khác nhau từng đôi một, $N_i = \operatorname{Ker}(f - \lambda_i e)$, $1 \leq i \leq n+1$.

Giả sử $(x_1, \ldots, x_{n+1}) \in N_1 \times \ldots \times N_{n+1}$ sao cho $\sum_{i=1}^{n+1} x_i = 0$.

Tác động bằng f : $0 = f(0) = f\left(\sum_{i=1}^{n+1} x_i\right) = \sum_{i=1}^{n+1} f(x_i) = \sum_{i=1}^{n+1} \lambda_i x_i$.

Kết hợp hai đẳng thức : $0 = \sum_{i=1}^{n+1} \lambda_i x_i - \lambda_{n+1} \sum_{i=1}^{n+1} x_i = \sum_{i=1}^{n} (\lambda_i - \lambda_{n+1}) x_i$.

Vì $\sum_{i=1}^{n} N_i$ là tổng trực tiếp, nên : $\forall i \in \{1, \ldots, n\}$, $(\lambda_i - \lambda_{n+1}) x_i = 0$,

rồi, vì $(\forall i \in \{1, \ldots, n\}, \lambda_i \neq \lambda_{n+1})$, nên : $\forall i \in \{1, \ldots, n\}, x_i = 0$, và cuối cùng : $x_{n+1} = -\sum_{i=1}^{n} x_i = 0$.

Điều đó chứng tỏ $N_1, \ldots, N_{n+1}$ độc lập tuyến tính.

7.2.1 a) Dễ dàng.

b) ◇ **Trả lời** : $\psi \circ \varphi$: $\begin{matrix} E \to E \\ x \mapsto f(0) \end{matrix}$, $\varphi \circ \psi = \mathrm{Id}_E$

c) Hiển nhiên $\psi \circ \varphi$ không phải là đơn ánh (vì $(\varphi \circ \psi)(1) = 0$), không phải là toàn ánh (vì $1 \notin \operatorname{Im}(\psi \circ \varphi)$).

◇ **Trả lời** . $\begin{cases} \varphi \text{ là toàn ánh , không là đơn ánh} \\ \psi \text{ là đơn ánh , không là toàn ánh} \end{cases}$

7.2.2 Vì $(\alpha e + g)^n = e$, nên bằng cách khai triển theo công thức nhị thức Newton (e và g giao hoán được với nhau), ta được :

$$(\alpha^n - 1)e + \sum_{k=1}^{n} C_n^k \alpha^{n-k} g^k = 0$$

Vậy nếu ký hiệu $u = \dfrac{1}{1-\alpha^n} \sum_{k=1}^{n} C_n^k \alpha^{n-k} g^{k-1}$, thì ta sẽ có: $g \circ u = u \circ g = e$, điều đó chứng tỏ g là song ánh và $g^{-1} = u$.

◇ **Trả lời** : $g^{-1} = \dfrac{1}{1-\alpha^n} \sum_{k=1}^{n} C_n^k \alpha^{n-k} g^{k-1}$.

7.2.3 Với mọi (x, y), (X, Y) thuộc $E \times F$:

$$\varphi(x, y) = (X, Y) \Leftrightarrow \begin{cases} x + g(y) = X \\ y = Y \end{cases} \Leftrightarrow \begin{cases} x = X - g(Y) \\ y = Y \end{cases}$$

Vì ψ : $\begin{matrix} E \times F \to E \times F \\ (X, Y) \mapsto (X - g(Y), Y) \end{matrix}$ tuyến tính và $\psi \circ \varphi = \varphi \circ \psi = \mathrm{Id}_{E \times F}$, nên ta kết luận rằng φ là một tự đẳng cấu của $E \times F$, và $\varphi^{-1} = \psi$.

7.2.4 Ta có: $f \circ (g \circ f) = (f \circ g) \circ f = e \circ f = f$, nên : $f \circ (g \circ f - e) = 0$, và sau đó: $f \circ (g \circ f - e + g) = f \circ (g \circ f - e) + f \circ g = f \circ g = e$.

Do đó, theo giả thiết ta suy ra : $g \circ f - e + g = g$, do đó $g \circ f = e$.

7.2.5 Giả sử $(\lambda_0, \ldots, \lambda_{p-1}) \in K^p$ sao cho $\sum_{i=0}^{p-1} \lambda_i f^i = 0$.

Lấy hàm hợp với f^{p-2}, ta suy ra $\lambda_0 = 0$.

Sau đó lấy hàm hợp với f^{p-2} trong $\sum_{i=1}^{p-1} \lambda_i f^i = 0$, ta suy ra $\lambda_1 = 0$, ...

7.2.6 Ánh xạ f, vốn là tuyến tính, là đơn ánh khi và chỉ khi:

$$\forall (x_1, \ldots, x_n) \in E_1 \times \ldots \times E_n, \left(\sum_{i=1}^{n} x_i = 0 \Rightarrow \forall i \in \{1, \ldots, n\}, x_i = 0 \right),$$

nghĩa là khi và chỉ khi $E_1, \ldots, E_n$ độc lập tuyến tính (xem 6.3.3, Định nghĩa 2).

7.2.7 Rõ ràng f tuyến tính.

a) Giả sử $x \in E$ và $(x_1, \ldots, x_n) \in E_1 \times \ldots \times E_n$ sao cho $x = \sum_{i=1}^{n} x_i$. Ta có:

$$x \in \mathrm{Ker}(f) \Leftrightarrow \sum_{i=1}^{n} f_i(x_i) = 0 \Leftrightarrow (\forall i \in \{1, \ldots, n\}, f_i(x_i)) = 0)$$

$$\Leftrightarrow \left(\forall i \in \{1, \cdots, n\}, x_i \in \mathrm{Ker}(f_i)\right) \Leftrightarrow x \in \sum_{i=1}^{n} \mathrm{Ker}(f_i).$$

từ đó suy ra : $\mathrm{Ker}(f) = \sum_{i=1}^{n} \mathrm{Ker}(f_i)$.

Hơn nữa, vì $(\forall i \in \{1, \ldots, n\}, \mathrm{Ker}(f_i) \subset E_i)$ và $\sum_{i=1}^{n} E_i$ là tổng trực tiếp , nên $\sum_{i=1}^{n} \mathrm{Ker}(f_i)$ là tổng trực tiếp.

b) Cho $y \in \mathrm{Im}(f)$. Tồn tại $x \in E$ sao cho $y = f(x)$, và $(x_1, \ldots, x_n) \in E_1 \times \ldots \times E_n$ sao cho $x = \sum_{i=1}^{n} x_i$, nên ta có : $y = \sum_{i=1}^{n} f_i(x_i) \in \sum_{i=1}^{n} \mathrm{Im}(f_i)$.

Ta chứng minh phần đảo theo cách tương tự , do đó : $\mathrm{Im}(f) = \sum_{i=1}^{n} \mathrm{Im}(f_i)$.

Hơn nữa, vì ($\forall i \in \{1, \ldots, n\}, \mathrm{Im}(f_i) \subset E_i$) và do $\sum_{i=1}^{n} E_i$ là tổng trực tiếp , nên $\sum_{i=1}^{n} \mathrm{Im}(f_i)$ là tổng trực tiếp .

7.2.8 1) Cho $x \in \mathrm{Ker}(f)$. Ta có : $f(g(x)) = (f \circ g)(x) = (g \circ f)(x) = g(f(x)) = g(0) = 0$, vậy $g(x) \in \mathrm{Ker}(f)$.

Điều đó chứng tỏ $\mathrm{Ker}(f)$ ổn định đối với g.

2) Cho $y \in \mathrm{Im}(f)$. Tồn tại $x \in E$ sao cho $y = f(x)$, và ta có:

$$g(y) = g(f(x)) = (g \circ f)(x) = (f \circ g)(x) = f(g(x)) \in \mathrm{Im}(f) .$$

Điều đó chứng tỏ rang $\mathrm{Im}(f)$ ổn định với g.

7.2.9 a) • $\forall x \in E,\ \big(x \in \mathrm{Ker}(g \circ f)\big) \Leftrightarrow \big(g \circ f\big)(x) = 0 \Leftrightarrow g\big(f(x)\big) = 0$

$\Leftrightarrow f(x) \in \mathrm{Ker}(g) \Leftrightarrow x \in f^{-1}(\mathrm{Ker}(g)))$.

• Vì $\mathrm{Ker}(g) \supset \{0\}$, ta có $\mathrm{Ker}(g \circ f) = f^{-1}\big(\mathrm{Ker}(g)\big) \supset f^{-1}(\{0\}) = \mathrm{Ker}(f)$.

b) • $\mathrm{Im}(g \circ f) = \big(g \circ f\big)(E) = g\big(f(E)\big) = g\big(\mathrm{Im}(f)\big)$.

• $\mathrm{Im}(g \circ f) = g\big(\mathrm{Im}(f)\big) \subset g(F) = \mathrm{Im}(g)$.

7.2.10 1) Giả sử $\mathrm{Ker}(g \circ f) = \mathrm{Ker}(h \circ f)$.

Cho $y \in \mathrm{Im}(f) \cap \mathrm{Ker}(g)$; tồn tại $x \in E$ sao cho $y = f(x)$ và $g(y) = 0$, từ đó suy ra $g(f(x)) = 0$.

Như vậy $x \in \mathrm{Ker}(g \circ f) = \mathrm{Ker}(h \circ f)$, do đó $h(y) = h(f(x)) = 0$, $y \in \mathrm{Ker}(h)$.

Điều đó chứng tỏ: $\mathrm{Im}(f) \cap \mathrm{Ker}(g) \subset \mathrm{Im}(f) \cap \mathrm{Ker}(h)$. Vai trò đối xứng của g và h trong giả thiết cho phép ta kết luận là có đẳng thức.

2) Ngược lại, giả sử $\mathrm{Im}(f) \cap \mathrm{Ker}(g) = \mathrm{Im}(f) \cap \mathrm{Ker}(h)$.

Cho $x \in \mathrm{Ker}(g \circ f)$. Khi đó $f(x) \in \mathrm{Im}(f) \cap \mathrm{Ker}(g) = \mathrm{Im}(f) \cap \mathrm{Ker}(h)$, vì vậy $h(f(x)) = 0$, $x \in \mathrm{Ker}(h \circ f)$.

Điều đó chứng tỏ $\mathrm{Ker}(g \circ f) \subset \mathrm{Ker}(h \circ f)$, sau đó, vai trò đối xứng của g và h cho phép ta có đẳng thức.

7.2.11 a) Với mọi $x \in V$, ta có :

• $\big(f + g\big)(x) = f(x) + g(x) \in V$

• $\big(\lambda f\big)(x) = \lambda f(x) \in V$

• $\big(g \circ f\big)(x) = g\big(f(x)\big) \in V$

b) Dễ dàng chứng minh bằng quy nạp theo n, bằng cách dùng a) $(g \circ f)$.

c) ◇ **Trả lời** : $E = \mathbb{R}^{\mathbb{R}}$ (các luật thông thường), $f : E \underset{u \mapsto f(u)}{\to} E$ trong đó $f(u) : \mathbb{R} \underset{x \mapsto u(x)-u(1)}{\to} \mathbb{R}$.

$V = \{u \in E;\ \forall x \in \mathbb{R},\ u(x) = 0\}$.

7.2.12 Lập luận bằng phản chứng: giả sử tồn tại $\alpha \in K - \{0\}$ sao cho $q = \alpha p$. Khi đó: $\alpha p = q = q^2 = (\alpha p)^2 = \alpha^2 p^2 = \alpha^2 p$, từ đó suy ra $\alpha = \alpha^2$, $\alpha = 1$, $q = p$, mâu thuẫn.

7.2.13 Cho $x \in E$. Vì $x - p(x) \in \mathrm{Ker}(p) = \mathrm{Ker}(q)$, nên ta có $q(x - p(x)) = 0$, suy ra $q(x) = (q \circ p)(x)$. Vì p, q có những vai trò đối xứng trong giả thiết, nên ta cũng có $p(x) = (p \circ q)(x)$, do đó $p(x) = q(x)$.

7.2.14 1) Nếu $p \circ q = q \circ p = 0$ thì : $(p+q)^2 = p^2 + p \circ q + q \circ p + q^2 = p^2 + q^2 = p + q$, nên $p + q$ là một phép chiếu.

2) Ngược lại, giả sử $p + q$ là một phép chiếu. Ta có :

$$p + q = (p+q)^2 = p^2 + p \circ q + q \circ p + q^2 = p + p \circ q + q \circ p + q$$

nên $p \circ q = -q \circ p$, sau đó $p \circ q = -p \circ (q \circ p) = -(p \circ q) \circ p = (q \circ p) \circ p = q \circ p$, và do đó $2p \circ q = 2q \circ p = 0$, $p \circ q = q \circ p = 0$.

7.2.15 (i) $\Rightarrow$ (ii) :

Ta có: $f \circ f = f \circ (g \circ f) = (f \circ g) \circ f = g \circ f = f$, và tương tự $g \circ g = g$.

Giả sử $x \in \mathrm{Im}(f)$. Vì f là một phép chiếu: $f(x) = x$.

Sau đó: $x = f(x) = (g \circ f)(x) = g(f(x)) \in \mathrm{Im}(g)$.

Như vậy: $\mathrm{Im}(f) \subset \mathrm{Im}(g)$.

Vai trò đối xứng của f và g trong giả thiết cho phép ta kết luận rằng có đẳng thức .

(ii) $\Rightarrow$ (i)

Giả sử $x \in E$. Ta có : $f(x) \in \mathrm{Im}(f) = \mathrm{Im}(g)$, do đó vì g là một phép chiếu: $g(f(x)) = f(x)$

Như vậy $g \circ f = f$, và tương tự , $f \circ g = g$.

7.2.16 1) • $0 \in L$

• Nếu $\lambda \in K$ và $(f_1, f_2) \in L^2$, tồn tại $(u_1, u_2) \in (\mathcal{L}(E))^2$ sao cho $f_1 = u_1 \circ p$ và $f_2 = u_2 \circ p$, từ đó suy ra $\lambda f_1 + f_2 = (\lambda u_1 + u_2) \circ p \in L$.

Điều đó chứng tỏ L là một kgvc của $\mathcal{L}(E)$.

Áp dụng kết quả này cho phép chiếu $q = e - p$, ta sẽ suy ra rằng M cũng là một kgvc của $\mathcal{L}(E)$.

7.2.17 a) 1) Nếu $f \circ g = \mathrm{Id}_F$ thì f là toàn ánh vì: $\forall y \in F,\ y = (f \circ g)(y) = f(g(y))$.

2) Ngược lại, giả sử f là toàn ánh.

Kgvc $\mathrm{Ker}(f)$ của E có ít nhất một phần bù H trong E : $E = \mathrm{Ker}(f) \oplus H$.

Ánh xạ $\varphi : H \to \mathrm{Im}(f)$, $x \mapsto f(x)$ là tuyến tính, hiển nhiên là toàn ánh, là đơn ánh vì nếu $x \in H$ thỏa mãn $\varphi(x) = 0$, thì $x \in H \cap \mathrm{Ker}(f) = \{0\}$, vì vậy $x = 0$.

Xét ánh xạ tuyến tính $g: F = \mathrm{Im}(f) \to E$ được xác định bởi: $\forall y \in F,\ g(y) = \varphi^{-1}(y)$.

Ta có: $\forall y \in F,\ (f \circ g)(y) = f(\varphi^{-1}(y)) = \varphi(\varphi^{-1}(y)) = y$, do vậy $f \circ g = \mathrm{Id}_F$.

b) 1) Nếu $h \circ f = \mathrm{Id}_E$, khi đó f là đơn ánh vì: $\forall x \in \mathrm{Ker}(f),\ x = (h \circ f)(x) = h(f(x)) = h(0) = 0$

2) Ngược lại, giả sử f là đơn ánh. Kgvc $\mathrm{Im}(f)$ của F có ít nhất một phần bù L trong F: $F = \mathrm{Im}(f) \oplus L$. Vì f là đơn ánh, nên ánh xạ tuyến tính $\varphi : E \to \mathrm{Im}(f)$, $x \mapsto f(x)$ hiển nhiên là song ánh .

Xét ánh xạ tuyến tính h: $F \to E$ được xác định bởi phép dán : $\begin{cases} \forall y \in \mathrm{Im}(f), & h(y) = \psi^{-1}(y) \\ \forall y \in L & h(y) = 0 \end{cases}$.

Ta có: $\forall x \in E$, $(h \circ f)(x) = h(f(x)) = \psi^{-1}(f(x)) = x$, vì vậy $h \circ f = \mathrm{Id}_E$.

7.2.18 a) 1) Nếu tồn tại $h \in \mathcal{L}(F, G)$ sao cho $g = h \circ f$, thì :

$\forall x \in \mathrm{Ker}(f),\ g(x) = h(f(x)) = h(0) = 0$, vậy $\mathrm{Ker}(f) \subset \mathrm{Ker}(g)$.

2) Ngược lại, giả sử $\mathrm{Ker}(f) \subset \mathrm{Ker}(g)$.

Kgvc $\mathrm{Im}f$ của F có ít nhất một phần bù L trong F : $F = \mathrm{Im}(f) \oplus L$.

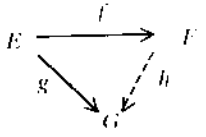
Giả sử $y \in F$. Tồn tại $(z, u) \in \mathrm{Im}(f) \times L$ duy nhất sao cho $y = z + u$, sau đó tồn tại $x \in E$ sao cho $z = f(x)$.

Nếu $x_1, x_2 \in E$ thỏa mãn $z = f(x_1) = f(x_2)$, thì $x_1 - x_2 \in \mathrm{Ker}(f) \subset \mathrm{Ker}(g)$, vì vậy $g(x_1) = g(x_2)$. Như vậy phần tử $g(x)$ không phụ thuộc vào cách chọn x trong E sao cho $z = f(x)$ (z cố định).

Xét ánh xạ $h : \begin{array}{c} F \to G \\ y \mapsto g(x) \end{array}$ được xác định như vậy.

Nếu $\lambda \in K$, $y, y' \in F$, $x, x' \in E$, $u, u' \in L$ thỏa mãn $y = f(x) + u$ và $y' = f(x') + u'$, thì $\lambda y + y' = f(\lambda x + x') + (\lambda u + u')$, vì vậy $h(\lambda y + y') = g(\lambda x + x') = \lambda g(x) + g(x') = \lambda h(y) + h(y')$. Điều đó chứng tỏ h tuyến tính.

Cuối cùng : $\forall x \in E$, $(h \circ f)(x) = h\big(f(x)\big) = g(x)$, vậy $h \circ f = g$



b) 1) Nếu tồn tại $k \in \mathcal{L}(E, F)$ sao cho $g = f \circ k$, thì, với mọi x thuộc E: $g(x) = f(k(x)) \in \mathrm{Im}(f)$, nên $\mathrm{Im}(g) \subset \mathrm{Im}(f)$.

2) Ngược lại, giả sử $\mathrm{Im}(g) \subset \mathrm{Im}(f)$. Không gian vectơ con $\mathrm{Ker}(f)$ của E có ít nhất một phần bù H trong E : $E = \mathrm{Ker}(f) \oplus H$. Giả sử $x \in E$. Ta có: $g(x) \in \mathrm{Im}(g) \subset \mathrm{Im}(f)$. Vì vậy: tồn tại $y \in F$ sao cho $g(x) = f(y)$, rồi tồn tại $u \in \mathrm{Ker}(f)$, $z \in H$ sao cho $y = u + z$.

Ta chứng tỏ rằng z không phụ thuộc cách chọn y trong F. Nếu $y_1, y_2 \in F$ thỏa mãn $g(x) = f(y_1) = f(y_2)$ và $u_1, u_2 \in \mathrm{Ker}(f)$, $z_1, z_2 \in H$ thỏa mãn $y_1 = u_1 + z_1$ và $y_2 = u_2 + z_2$, thì $y_1 - y_2 \in \mathrm{Ker}(f)$, vì vậy : $z_1 - z_2 = (y_1 - y_2) - (u_1 - u_2) \in \mathrm{Ker}(f) \cap H$, do đó $z_1 = z_2$.

Xét ánh xạ $k : \begin{array}{c} E \to F \\ x \mapsto z \end{array}$ được xác định như vậy.

Nếu $\lambda \in K$, $x, x' \in E$, $y, y' \in F$ sao cho $g(x) = f(y)$, $g(x') = f(y')$, sau đó $u, u' \in \mathrm{Ker}(f)$, $z, z' \in H$ sao cho $y = u + z$, $y' = u' + z'$, thì :

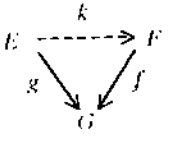
$$g(\lambda x + x') = \lambda g(x) + g(x') = \lambda f(y) + f(y') = f(\lambda y + y') \quad \text{và} \quad \lambda y + y' = (\lambda u + u') + (\lambda z + z'),$$

từ đó suy ra $k(\lambda x + x') = \lambda z + z' = \lambda k(x) + k(x')$.

Điều đó chứng tỏ k tuyến tính.

Cuối cùng, với các ký hiệu trên :

$\forall x \in E$, $(f \circ k)(x) = f\big(k(x)\big) = f(z) = f(y - u) = f(y) - f(u) = f(y) = g(x)$, vậy $f \circ k = g$.



Nhận xét : Bài tập 7.2.17 là một trường hợp đặc biệt của bài tập 7.2.18 khi ta lấy $G = E$ và $g = \mathrm{Id}_E$.

7.2.19 Rõ ràng rằng:

- $\forall f \in \mathcal{L}(E, F)$, $\forall g \in \mathcal{L}(F, G)$, $g \circ f \in \mathcal{L}(E, G)$
- Với mọi f thuộc $\mathcal{L}(E, F)$, $\phi(f)$ tuyến tính, vì vậy $\phi(f) \in \mathcal{L}\big(\mathcal{L}(F, G), \mathcal{L}(E, G)\big)$
- Tương tự: $\forall g \in \mathcal{L}(F, G)$, $\psi(g) \in \mathcal{L}\big(\mathcal{L}(E, F), \mathcal{L}(E, G)\big)$.

a) 1) Nếu f là toàn ánh, thì $\mathrm{Ker}(\phi(f)) = \{g \in \mathcal{L}(E, F) ; F = \mathrm{Im}(f) \subset \mathrm{Ker}(g)\} = \{0\}$, vì vậy $\phi(f)$ là đơn ánh.

2) Ngược lại, giả sử $\phi(f)$ là đơn ánh. Kgvc $\mathrm{Im}(f)$ của F có ít nhất một phần bù L trong F : $F = \mathrm{Im}(f) \oplus L$. Giả sử $L \neq \{0\}$; tồn tại $y_0 \in L - \{0\}$, rồi, kgvc Ky_0 của L có ít nhất một phần bù L' trong L sao cho $F = \mathrm{Im}(f) \oplus L' \oplus (Ky_0)$.

Mặt khác, vì $G \neq \{0\}$, nên tồn tại $z_0 \in G$ sao cho $z_0 \neq 0$.

Xét ánh xạ tuyến tính $g : F \to G$ xác định bởi phép dán : $\begin{cases} \forall y \in \mathrm{Im}(f) \oplus L', & g(y) = 0 \\ g(y_0) = z_0 \end{cases}$

Khi đó ta có $\big(\phi(f)\big)(g) = g \circ f = 0$ và $g \neq 0$, mâu thuẫn.

Điều đó chứng tỏ $\mathrm{Im}(f) = F$, vì vậy f là toàn ánh.

b) 1) Giả sử f là đơn ánh.

Với mọi h thuộc $\mathcal{L}(E, G)$, ta có $\mathrm{Ker}(f) = \{0\} \subset \mathrm{Ker}(h)$, vì vậy (xem bài tập 7.2.18 a)), tồn tại $g \in \mathcal{L}(F, G)$ sao cho $h = g \circ f = \big(\phi(f)\big)(g)$.

Điều đó chứng tỏ $\phi(f)$ là toàn ánh.

2) Ngược lại, giả sử $\phi(f)$ là toàn ánh.

Giả sử $\mathrm{Ker}(f) \neq \{0\}$.

Tồn tại $x_0 \in \mathrm{Ker}(f) - \{0\}$, rồi kgvc Kx_0 của E có ít nhất một phần bù H trong E : $E = (Kx_0) \oplus H$. Vì $G \neq \{0\}$, tồn tại $z_0 \in G$ sao cho $z_0 \neq 0$.

Xét ánh xạ tuyến tính $h: E \to G$ xác định bởi phép dán : $\begin{cases} h(x_0) = z_0 \\ \forall x \in H, \quad h(x) = 0 \end{cases}$

Vì $\phi(f)$ là toàn ánh, tồn tại $g \in \mathcal{L}(F, G)$ sao cho $h = \big(\phi(f)\big)(g) = g \circ f$, do đó : $z_0 = h(x_0) = \big(g \circ f\big)(x_0) = g\big(f(x_0)\big) = g(0) = 0$, mâu thuẫn.

Điều đó chứng tỏ $\mathrm{Ker}(f) = \{0\}$, nên f là đơn ánh.

c) 1) Giả sử g là đơn ánh.

Giả sử $f \in \mathrm{Ker}(\psi(g))$, nghĩa là : $f \in \mathcal{L}(E, F)$ và $\big(\psi(g)\big)(f) = g \circ f = 0$.

Khi đó: $\forall x \in E$, $g(f(x)) = 0$, do đó, vì g là đơn ánh : $\forall x \in E$, $f(x) = 0$, và do vậy $f = 0$.

Điều đó chứng tỏ $\mathrm{Ker}(\psi(g)) = \{0\}$, $\psi(g)$ là đơn ánh.

2) Ngược lại, giả sử $\psi(g)$ là đơn ánh.

Nếu g không là đơn ánh, tồn tại $y_0 \in \mathrm{Ker}(g)$ sao cho $y_0 \neq 0$.

Vì $E \neq \{0\}$, tồn tại $x_0 \in E$ sao cho $x_0 \neq 0$. Kgvc Kx_0 của E có ít nhất một phần bù H trong E : $E = (Kx_0) \oplus H$.

Xét ánh xạ tuyến tính $f: E \to F$ xác định bởi phép dán : $\begin{cases} \forall x \in H, \quad f(x) = 0 \\ f(x_0) = y_0 \end{cases}$

Ta có: $\begin{cases} \forall x \in H, \big(g \circ f\big)(x) = g\big(f(x)\big) = g(0) = 0 \\ \big(g \circ f\big)(x_0) = g(y_0) = 0 \end{cases}$, vì vậy $g \circ f = 0$.

Vì $\big(\psi(g)\big)(f) = g \circ f = 0$ và vì vậy $\psi(g)$ là đơn ánh, ta suy ra $f = 0$, mâu thuẫn với $f(x_0) = y_0 \neq 0$.

Điều đó chứng tỏ g là đơn ánh.

d) 1) Giả sử g là toàn ánh.

Với mọi h thuộc $\mathcal{L}(E, G)$, ta có $\mathrm{Im}(h) \subset G = \mathrm{Im}(g)$, vì vậy, (xem bài tập 7.2.18, b)), tồn tại $f \in \mathcal{L}(E, F)$ sao cho $h = g \circ f = \big(\psi(g)\big)(f)$.

Điều đó chứng tỏ $\psi(g)$ là toàn ánh.

2) Ngược lại, giả sử $\psi(g)$ là toàn ánh.

Cho $z \in G$.

Vì $E \neq \{0\}$, tồn tại $x_0 \in E$ sao cho $x_0 \neq 0$, rồi kgvc Kx_0 của E có ít nhất một phần bù H trong E: $E = (Kx_0) \oplus H$. Xét ánh xạ tuyến tính $h : E \to G$ xác định bởi phép dán : $\begin{cases} \forall x \in H, & h(x) = 0 \\ h(x_0) = z_0 \end{cases}$. Vì $\psi(g)$ là toàn ánh, nên tồn tại $f \in \mathcal{L}(E, F)$ sao cho $h = (\psi(g))(f) = g \circ f$.

Vì vậy ta có : $z_0 = h(x_0) = (g \circ f)(x_0) = g(f(x_0)) \in \mathrm{Im}(g)$.

Điều đó chứng tỏ : $\forall z_0 \in G, z_0 \in \mathrm{Im}(g)$, và do đó g là toàn ánh.

7.2.20 (i) $\Rightarrow$ (ii) :

Giả sử tồn tại $f \in \mathcal{L}(E)$ sao cho $\mathrm{Im}(f) = F$ và $\mathrm{Ker}(f) = G$.

Kgvc G của E có ít nhất một phần bù H trong E : $E = G \oplus H$.

Xét ánh xạ tuyến tính $\tilde{f} : H \to F$, $x \mapsto f(x)$ là hạn chế của f trên tập nguồn H.

- $\tilde{f}$ là đơn ánh, vì nếu $x \in H$ và $\tilde{f}(x) = 0$, thì $x \in H \cap G = \{0\}$, vì vậy $x = 0$
- $\tilde{f}$ là toàn ánh, vì với mọi y thuộc $F(= \mathrm{Im}(f))$, tồn tại $t \in E$ sao cho $y = f(t)$, sau đó tồn tại $(u, x) \in G \times H$ sao cho $t = u + x$, và ta có $y = f(t) = f(u) + f(x) = f(x) = \tilde{f}(x)$.

Như vậy $\tilde{f}$ là một đẳng cấu từ H lên F.

(ii) $\Rightarrow$ (i) :

Giả sử tồn tại một phần bù H của G trong E sao cho $H \simeq F$. Vậy tồn tại một đẳng cấu $\varphi : H \to F$.

Giả sử $f : E \to E$ là ánh xạ tuyến tính xác định bởi phép dán : $\begin{cases} \forall x \in G, & f(x) = 0 \\ \forall x \in H, & f(x) = \varphi(x). \end{cases}$

Rõ ràng, $\mathrm{Im}(f) = \mathrm{Im}(\varphi) = F$ và $\mathrm{Ker}(f) = G$.

Nhận xét : Nếu E hữu hạn chiều, thì điều kiện (ii) tương đương với: $\dim(F) + \dim(G) = \dim(E)$ (xem 6.4, Mệnh đề 6).

7.2.21 a) Ký hiệu $i : E' \to E$ và $j : F \to F'$ là các đơn ánh chính tắc, ta có: $\forall f \in \mathcal{L}(E, F)$, $\phi(f) = j \circ f \circ i$, từ đó dễ dàng suy ra rằng ϕ tuyến tính.

$$\begin{array}{ccc} E' & \xrightarrow{\ i\ } & E \\ {\scriptstyle \phi(f)}\downarrow & & \downarrow{\scriptstyle f} \\ F' & \xleftarrow[\ j\ ]{} & F \end{array}$$

b) • Với mọi $f \in \mathcal{L}(E, F)$:

$$f \in \mathrm{Ker}(\phi) \Leftrightarrow j \circ f \circ i = 0 \Leftrightarrow f \circ i = 0 \Leftrightarrow \mathrm{Im}(i) \subset \mathrm{Ker}(f) \Leftrightarrow E' \subset \mathrm{Ker}(f)$$

• 1) Giả sử $f' \in \mathrm{Im}(\phi)$. Tồn tại $f \in \mathcal{L}(E, F)$ sao cho: $f' = \phi(f) = j \circ f \circ i$

nên : $\forall x' \in E', f'(x') = f(x')$, và do đó: $\mathrm{Im}(f') \subset F$.

2) Ngược lại, giả sử $f' \in \mathcal{L}(E', F')$ sao cho $\mathrm{Im}(f') \subset F$.

Kgvc E' của E có ít nhất một phần bù G trong E : $E = E' \oplus G$.

Xét ánh xạ tuyến tính $f : E \to F$ xác định bởi phép dán : $\begin{cases} \forall x \in E', & f(x) = f'(x) \\ \forall x \in G, & f(x) = 0. \end{cases}$

Khi đó: $\forall x \in E', (j \circ f \circ i)(x) = f(x) = f'(x)$, vậy $f' = j \circ f \circ i = \phi(f)$.

◇ **Trả lời** : $\begin{cases} \mathrm{Ker}(\phi) = \{f \in L(E, F); \mathrm{Ker}(f) \supset E'\} \\ \mathrm{Im}(\phi) = \{f' \in L(E', F'); \mathrm{Im}(f') \subset F\}. \end{cases}$

7.2.22 Kgvc $\mathrm{Ker}(f)$ của E có ít nhất một phần bù G trong E: $E = \mathrm{Ker}(f) \oplus G$.

Giả sử $\varphi : G \to \mathrm{Im}(f)$, $x \mapsto f(x)$. Ta chứng tỏ rằng φ là một đẳng cấu không gian vectơ (xem lời giải của bài tập 7.2.17, *a*)).

Kgvc $\mathrm{Im}(f)$ của E có ít nhất một phần bù L trong E : $E = \mathrm{Im}(f) \oplus L$. Xét ánh xạ tuyến tính $g : E \to E$ xác định bởi phép đán : $\begin{cases} \forall y \in \mathrm{Im}(f), g(y) = \varphi^{-1}(y) \\ \forall y \in L, g(y) = 0. \end{cases}$

Ta có :

• $\forall x \in E,\ (f \circ g \circ f)(x) = f\big(g(x)\big) = f(\varphi^{-1}(f(x))) = \varphi(\varphi^{-1}(f(x))) = f(x)$,

vậy $f \circ g \circ f = f$.

• $\begin{cases} \forall y \in \mathrm{Im}(f), (g \circ f \circ g)(y) = (g \circ f)(\varphi^{-1}(y)) = g(\varphi(\varphi^{-1}(y))) = g(y) \\ \forall y \in L, (g \circ f \circ g)(y) = (g \circ f)(g(y)) = (g \circ f)(0) = 0 = g(y) \end{cases}$, như vậy $g \circ f \circ g = g$

7.2.23 a) Có thể nhận xét rằng G khác rỗng vì nó chứa phep chiếu lên E_2 song song với E_1.

Giả sử $f \in G$. Vì $f(E_2) \subset f(E) = E_2$ nên E_2 ổn định đối với f. Ký hiệu $f' : E_2 \to E_2$ là tự đồng cấu của E_2 cảm sinh bởi f.

1) **f' là đơn ánh.**

Giả sử $x \in E_2$ sao cho $f'(x) = 0$. Khi đó ta có $x \in E_2$ và $x \in \mathrm{Ker}(f) = E_1$, nên $x = 0$.

Điều đó chứng tỏ f' là đơn ánh.

2) **f' là toàn ánh**

Giả sử $y \in E_2 = \mathrm{Im}(f)$. Tồn tại $x \in E$ sao cho $y = f(x)$, sau đó tồn tại $(x_1, x_2) \in E_1 \times E_2$ sao cho $x = x_1 + x_2$.

Ta có : $y = f(x_1) + f(x_2) = f(x_2) = f'(x_2)$.

Như vậy, f' là toàn ánh.

b) Xét ánh xạ $\theta : \underset{f \mapsto f'}{G \to GL(E_2)}$, trong đó f' là tự đồng cấu của E_2 cảm sinh bởi f.

1) Ta chứng tỏ $\circ$ là một luật hợp thành trong trong G.

Cho $f, g \in G$.

• Ta có: $(g \circ f)(E_2) = g(f(E_2)) = g(E_2) = E_2$.

• $E_1 = \mathrm{Ker}(f) \subset \mathrm{Ker}(g \circ f)$.

• Giả sử $x \in \mathrm{Ker}(g \circ f)$. Tồn tại $(x_1, x_2) \in E_1 \times E_2$ sao cho $x = x_1 + x_2$, ta có

$$0 = (g \circ f)(x) = g\big(f(x_1)\big) + g\big(f(x_2)\big) = g'\big(f'(x_2)\big) = (g' \circ f')(x_2)$$

Vì f', g' là song ánh, ta suy ra $x_2 = 0$, rồi $x = x_1 \in E_1 = \mathrm{Ker}(f)$.

Như vậy: $\begin{cases} \mathrm{Ker}(g \circ f) = \mathrm{Ker}(f) = E_1 \\ \mathrm{Im}(g \circ f) = E_2 \end{cases}$, và do vậy $g \circ f \in G$.

2) Ánh xạ $\theta : G \to GL(E_2)$ là một đồng cấu đối với luật $\circ$ vì :

$$\forall f, g \in G,\ \forall x \in E_2,\ \big(\theta(g \circ f)\big)(x) = (g \circ f)'(x) = (g \circ f)(x) = (g' \circ f')(x).$$

vì vậy : $\forall f, g \in G,\ \theta(g \circ f) = \theta(g) \circ \theta(f)$.

3) **Tính đơn ánh của θ**

Giả sử $f \in G$ sao cho $f' = \theta(f) = 0$

Cho $x \in E$. Tồn tại $(x_1, x_2) \in E_1 \times E_2$ sao cho $x = x_1 + x_2$.

Ta có: $f(x) = f(x_1) + f(x_2) = f(x_2) = f'(x_2) = 0$.

Điều đó chứng tỏ $f = 0$, và vì vậy θ là đơn ánh.

4) **Tính toàn ánh của θ**

Cho $\varphi \in GL(E)$. Xét ánh xạ tuyến tính $f : E \to E$ xác định bởi phep đán :

$$\begin{cases}\forall x \in E_1,\ f(x) = 0\\ \forall x \in E_2,\ f(x) = \varphi(x)\end{cases}.$$

Rõ ràng: $\mathrm{Ker}(f) = E_1$, $\mathrm{Im}(f) = E_2$, vì vậy $f \in G$ và : $\theta(f) = f^* = \varphi$.

7.3.1 Rõ ràng rằng với mọi P thuộc E_n : $\sum_{i=0}^{n} P^{(i)}\left(\frac{X}{2^i}\right)$ thuộc E_n và ánh xạ

$f : E_n \to E_n$ tuyến tính.

$$P \mapsto \sum_{i=0}^{n} P^{(i)}\left(\frac{X}{2^i}\right).$$

Họ $(f(X^k))_{0 \le k \le n}$ là một họ đa thức với bậc kế tiếp, nên là một cơ sở của E_n (xem 5.1.4, Nhận xét).

Điều đó chứng tỏ f là một song ánh, từ đó suy ra kết quả cần chứng minh.

7.3.2 Giả sử u_1, u_2, u_3 (tương ứng: v_1, v_2, v_3) là các vectơ chỉ phương của D_1, D_2, D_3 (tương ứng : Δ_1, Δ_2, Δ_3).

Giả sử $(\alpha_1, \alpha_2) \in (K - \{0\})^2$, mà ta sẽ chọn sau này, và f là tự đồng cấu của E xác định bởi :

$$f(u_1) = \alpha v_1, \text{ và } f(u_2) = \alpha v_2$$

Hiển nhiên f là một tự đẳng cấu của E, và $f(D_1) = \Delta_1$, và $f(D_2) = \Delta_2$.

Ta còn phải chọn (α_1, α_2) sao cho $f(D_3) = \Delta_3$.

Vì f là không gian 2 chiều, nên tồn tại $(a, b, c, d) \in K^4$ sao cho: $u_3 = au_1 + bu_2$, $v_3 = cv_1 + dv_2$.

Vì D_1, D_2, D_3 (tương ứng: $\Delta_1, \Delta_2, \Delta_3$) khác nhau từng đôi một, nên ta có : $(a, b, c, d) \in (K - \{0\})^4$.

Ta có :

$$f(D_3) = \Delta_3 \Leftrightarrow (\exists \lambda \in K - \{0\},\ f(u_3) = \lambda v_3) \Leftrightarrow (\exists \lambda \in K - \{0\},\ a\alpha_1 v_1 + b\alpha_2 v_2 = \lambda c v_1 + \lambda d v_2)$$

$$\Leftrightarrow \left(\exists \lambda \in K - \{0\},\ \begin{cases} a\alpha_1 = \lambda c \\ b\alpha_2 = \lambda d \end{cases}\right).$$

Chỉ cần chọn: $\alpha_1 = bc$, $\alpha_2 = ad$, $\lambda = ab$.

7.3.3 Tồn tại một cơ sở $(e_1, ..., e_n)$ của E, trong đó $n = \dim(E)$. Với mỗi i thuộc $\{1, ..., n\}$, tồn tại $p_i \in \mathbb{N}^*$ sao cho $f^{p_i}(e_i) = e_i$. Đặt $p = \prod_{i=1}^{n} p_i$.

Ta có: $\forall i \in \{1, ..., n\}$, $f^p(e_i) = (f^{p_i})^{\prod_{j \neq i} p_j}(e_i) = e_i$, vì e_i là bất biến đối với f^{p_i}, nên cũng bất biến đối với mọi lũy thừa của f^{p_i}.

Điều đó chứng tỏ $f^p = \mathrm{Id}_E$.

7.3.4 Vì $f \circ (g + h) = f \circ g + f \circ h = e$, nên f khả nghịch phải đối với $\circ$ trong $\mathcal{L}(E)$. Vì E là hữu hạn chiều, nên theo 7.3.1, Định lý 2, ta có $(g + h) \circ f = e$, vậy :

$$g \circ f = e - h \circ f = f \circ g.$$

7.3.5 Tồn tại $p_1 \in L_1$ và $p_2 \in L_2$ sao cho $e = p_1 + p_2$.

Ta có $\begin{cases} p_1 = (p_1 \circ p_2) \circ p_1 = p_1 \circ p_1 + p_2 \circ p_1 \\ p_1 = p_1 \circ (p_1 + p_2) = p_1 \circ p_1 + p_1 \circ p_2 \end{cases}$, suy ra $2p_1 = 2p_1 \circ p_1 + (p_1 \circ p_2 + p_2 \circ p_1) = 2p_1 \circ p_1$,

và vì vậy $p_1 \circ p_1 = p_1$. Tương tự $p_2 \circ p_2 = p_2$.

Như vậy, p_1, p_2 là hai phép chiếu liên kết.

Ký hiệu $E_1 = \mathrm{Im}(p_1) = \mathrm{Ker}(p_2)$, $E_2 = \mathrm{Im}(p_2) = \mathrm{Ker}(p_1)$; ta có: $E_1 \oplus E_2 = E$.

• Giả sử $f_1 \in I_1$.

Ta có: $\forall x \in E_1,\ p_2(f_1(x)) = -(f_1 \circ p_2)(x) = -f_1(0) = 0$, vậy: $\forall x \in E_1, f_1(x) \in \mathrm{Ker}(p_2) = E_1$.

Điều đó chứng tỏ rằng: $f_1(E_1) \subset E_1$.

Cho $x \in E_2$. Ta có: $f_1(x) = f_1(p_2(x)) = -p_2 \circ f_1)(x)$, rồi bằng cách hợp với p_2:

$p_2(f_1(x)) = -(p_2 \circ p_2 \circ f_1)(x) = -(p_2 \circ f_1)(x)$; vậy: $p_2(f_1(x)) = 0$, nên $f_1(x) = 0$.

Điều đó chứng tỏ: $f_1(E_2) = \{0\}$.

• Vậy với $f_1 \in I_1$ ta có thể xét tự đồng cấu cảm sinh $f'_1 : \begin{matrix} E_1 \to E_1 \\ x \mapsto f_1(x) \end{matrix}$.

Hiển nhiên là ánh xạ $\theta_1 : \begin{matrix} I_1 \to \mathcal{L}(E_1) \\ f_1 \mapsto f'_1 \end{matrix}$ tuyến tính. Hơn nữa, với mọi f_1 thuộc $\mathrm{Ker}(\theta_1)$, ta có $f_1(E_1) = \{0\}$ và $f_1(E_2) = \{0\}$, vì vậy $f_1 = 0$, điều đó chứng tỏ θ_1 là đơn ánh.

• Từ đó suy ra: $\dim(I_1) \le \dim(\mathcal{L}(E_1)) = (\dim(E_1))^2$.

Vì trong giả thiết I_1, I_2 có vai trò đối xứng, nên ta cũng có: $\dim(I_2) \le (\dim(E_2))^2$.

Mặt khác: $(\dim(E_1))^2 = \dim(\mathcal{L}(E)) = \dim(I_1 \oplus I_2) = \dim(I_1) + \dim(I_2)$.

Ta được: $(\dim(E_1) + \dim(E_2))^2 \le (\dim(E_1))^2 + (\dim(E_2))^2$, từ đó suy ra: $2\dim(E_1)\dim(E_2) \le 0$, vì vậy: $\dim(E_1)$ hoặc $\dim(E_2) = 0$, nghĩa là $E_1 = \{0\}$ hoặc $E_2 = \{0\}$, và cuối cùng:

$$I_1 = \{0\} \text{ hoặc } I_2 = \{0\}.$$

7.3.6 Trước hết, rõ ràng là: $\mathrm{Ker}(f) \subset \mathrm{Ker}(f^2)$.

Với ký hiệu $p = \dim(\mathrm{Ker}(f))$, $q = \dim(\mathrm{Ker}(f^2)) - \dim(\mathrm{Ker}(f))$, thì tồn tại $u_1, \ldots, u_p, v_1, \ldots, v_q \in E$ sao cho :

$$\begin{cases} (u_1, \ldots, u_p) \text{ là một cơ sở } \mathrm{Ker}(f) \\ (u_1, \ldots, u_p, v_1, \ldots, v_q) \text{ là một cơ sở của } \mathrm{Ker}(f^2). \end{cases}$$

Giả sử $(\lambda_1, \ldots, \lambda_q) \in K^q$ sao cho $\sum_{j=1}^{q} \lambda_j f(v_j) = 0$. Khi đó $\sum_{j=1}^{q} \lambda_j v_j \in \mathrm{Ker}(f)$ và vì vậy tồn tại $(\alpha_1, \ldots, \alpha_n) \in K^n$ sao cho $\sum_{j=1}^{q} \lambda_j v_j = \sum_{i=1}^{p} \alpha_i u_i$.

Vì $(u_1, \ldots, u_p, v_1, \ldots, v_q)$ độc lập tuyến tính nên : $\lambda_1 = \ldots = \lambda_q = 0$.

Điều này chứng tỏ : $\big(f(v_j)\big)_{1 \le j \le q}$ độc lập tuyến tính.

Vì: $\forall j \in \{1, \ldots, q\}, f(v_j) \in \mathrm{Ker}(f)$, nên ta có: $q \le \dim(\mathrm{Ker}(f)) = p$, từ đó suy ra:

$\dim(\mathrm{Ker}(f^2)) = p + q \le 2p = 2\dim(\mathrm{Ker}(f))$.

7.3.7 Giả sử $\lambda \neq 0$.

Với mọi x thuộc E, ta có $\begin{cases} (\lambda f)(x) = f(\lambda x) \in \mathrm{Im}(f) \\ f(x) = \lambda^{-1}(\lambda f)(x) \in \mathrm{Im}(f) \end{cases}$, nên $\mathrm{Im}(\lambda f) = \mathrm{Im}(f)$.

◇ **Trả lời** : $\mathrm{rank}(\lambda f) = \begin{cases} 0 & \text{nếu } \lambda = 0 \\ \mathrm{rank}(f) & \text{nếu } \lambda \neq 0 \end{cases}$.

7.3.8 • Dễ dàng chứng minh tính chất tuyến tính của φ :

$\varphi\big(\lambda(x_1, x_2) + (y_1, y_2)\big) = \varphi\big(\lambda x_1 + y_1, \lambda x_2 + y_2\big) = \big(f_1(\lambda x_1 + y_1), f_2(\lambda x_2 + y_2)\big) =$

$\big(\lambda f_1(x_1) + f_1(y_1), \lambda f_2(x_2) + f_2(y_2)\big) = \lambda\big(f_1(x_1), f_2(x_2)\big) + \big(f_1(y_1), f_2(y_2)\big) = \lambda\varphi(x_1, x_2) + \varphi(y_1, y_2)$.

• $\forall (x_1, x_2) \in E_1 \times E_2$, $\varphi(x_1, x_2) = \big(f_1(x_1), f_2(x_2)\big) \in \mathrm{Im}(f_1) \times \mathrm{Im}(f_2)$, do đó $\mathrm{Im}(\varphi) \subset \mathrm{Im}(f_1) \times \mathrm{Im}(f_2)$.

và ngược lại $\mathrm{Im}(f_1) \times \mathrm{Im}(f_2) \subset \mathrm{Im}(\varphi)$.

Thế thì : $\mathrm{rank}(\varphi) = \dim\big(\mathrm{Im}(\varphi)\big) = \dim\big(\mathrm{Im}(f_1)\big) + \dim\big(\mathrm{Im}(f_2)\big) = \mathrm{rank}(f_1) + \mathrm{rank}(f_2)$

7.3.9 • $E = \mathrm{Id}_E(E) = (f + g)(E) \subset f(E) + g(E)$, nên: $E = \mathrm{Im}(f) + \mathrm{Im}(g)$,

rồi : $\dim(E) \le \mathrm{rank}(f) + \mathrm{rank}(g) - \dim(\mathrm{Im}(f) \cap \mathrm{Im}(g))$.

Vì theo giả thiết: $\mathrm{rank}(f) + \mathrm{rank}(g) \le \dim(E)$, nên ta suy ra : $\dim(\mathrm{Im}(f) \cap \mathrm{Im}(g)) = 0$, nghĩa là :

$\mathrm{Im}(f) \cap \mathrm{Im}(g) = \{0\}$.

• Cho $x \in E$. Ta có $f(g(x)) \in \mathrm{Im}(f)$ và :

$$f\big(g(x)\big) = (f \circ (e - f))(x) = ((e - f) \circ f)(x) = g(f(x)) \in \mathrm{Im}(g)$$

trong đó $e = \mathrm{Id}_E$.

Do vậy: $f(g(x)) = g(f(x)) = 0$, nên $f(x) = (f \circ f)(x)$. Điều đó chứng tỏ f là một phép chiếu của E.

Cuối cùng, vì $g = e - f$, nên g là một phép chiếu liên kết với f.

7.3.10 Trước hết nhận xét: $\mathrm{Im}(f + g) \subset \mathrm{Im}(f) + \mathrm{Im}(g)$, suy ra :

$\mathrm{rank}(f + g) \le \dim(\mathrm{Im}(f) + \mathrm{Im}(g)) = \mathrm{rank}(f) + \mathrm{rank}(g) - \dim(\mathrm{Im}(f) \cap \mathrm{Im}(g))$.

1) Giả sử: $\mathrm{rank}(f + g) = \mathrm{rank}(f) + \mathrm{rank}(g)$.

Khi đó ta có: $\mathrm{Im}(f) \cap \mathrm{Im}(g) = \{0\}$ và: $\dim(\mathrm{Im}(f + g)) = \dim(\mathrm{Im}(f)) + \dim(\mathrm{Im}(g))$ nên :

$\mathrm{Im}(f + g) = \mathrm{Im}(f) + \mathrm{Im}(g)$.

Giả sử $x \in E$. Vì $\mathrm{Im}(f) \subset \mathrm{Im}(f + g)$, nên tồn tại $x \in E$ sao cho $f(x) = (f + g)(t)$.

Khi đó: $g(t) = f(x - t) \in \mathrm{Im}(f) \cap \mathrm{Im}(g) = \{0\}$, nên $t \in \mathrm{Ker}(g)$ và $x - t \in \mathrm{Ker}(f)$.

Như vậy : $x = (x - t) + t \in \mathrm{Ker}(f) + \mathrm{Ker}(g)$, và vì vậy $\mathrm{Ker}(f) + \mathrm{Ker}(g) = E$.

2) Ngược lại, giả sử $\begin{cases} \mathrm{Im}(f) \cap \mathrm{Im}(g) = \{0\} \\ \mathrm{Ker}(f) + \mathrm{Ker}(g) = E \end{cases}$

Giả sử $y \in \mathrm{Im}(f)$. Tồn tại $x \in E$ sao cho $y = f(x)$, rồi tồn tại $(u, v) \in \mathrm{Ker}(f) \times \mathrm{Ker}(g)$ sao cho $x = u + v$. Ta có: $y = f(u) + f(v) = f(v) = f(v) + g(v) = (f + g)(v) \in \mathrm{Im}(f + g)$.

Điều đó chứng tỏ $\mathrm{Im}(f) \subset \mathrm{Im}(f + g)$.

Vai trò đối xứng của f và g trong giả thiết cho phép ta suy ra: $\mathrm{Im}(f) \subset \mathrm{Im}(f + g)$, và do vậy.

$\mathrm{Im}(f) \oplus \mathrm{Im}(g) \subset \mathrm{Im}(f + g)$.

Do bao hàm thức kia đã được thỏa mãn, nên ta được $\mathrm{Im}(f + g) = \mathrm{Im}(f) \oplus \mathrm{Im}(g)$, do đó :

$$\mathrm{Rank}(f + g) = \mathrm{rank}(f) + \mathrm{rank}(g).$$

7.3.11 a) • Với mọi y thuộc $\mathrm{Ker}(g|_{\mathrm{Im}(f)})$, ta có $y \in \mathrm{Im}(f)$ và $g(y) = 0$, nên $y \in \mathrm{Ker}(g) \cap \mathrm{Im}(f)$.

• Ngược lại, với mọi y thuộc $\mathrm{Ker}(g) \cap \mathrm{Im}(f)$, ta có $y \in \mathrm{Ker}(g|_{\mathrm{Im}(f)})$.

b) Áp dụng định lý về hạng cho $g|_{\mathrm{Im}(f)} : \mathrm{Im}(f) \to G$:

$$\dim(\mathrm{Im}(g|_{\mathrm{Im}(f)}) = \dim(\mathrm{Im}(f)) - \dim(\mathrm{Ker}(g|_{\mathrm{Im}(f)})).$$

Vì $\mathrm{Im}(g|_{\mathrm{Im}(f)} = g(\mathrm{Im}(f)) = (g \circ f)(E) = \mathrm{Im}(g \circ f)$ nên từ a) suy ra:

$$\mathrm{rank}(g \circ f) = \mathrm{rank}(f) - \dim(\mathrm{Ker}(g) \cap \mathrm{Im}(f)).$$

c) $\mathrm{Ker}(g) \cap \mathrm{Im}(f) \subset \mathrm{Ker}(g) \Rightarrow \dim(\mathrm{Ker}(g) \cap \mathrm{Im}(f)) \le \dim(\mathrm{Ker}(g)) = \dim(E) - \mathrm{rank}(g)$

$\Rightarrow \mathrm{rank}(f) - \mathrm{rank}(g \circ f) \le \dim(E) - \mathrm{rank}(g) \Rightarrow \mathrm{rank}(g \circ f) \ge \mathrm{rank}(f) + \mathrm{rank}(g) - \dim(E)$.

C7.1 1) • $\forall \sigma \in \mathfrak{S}_n$, $f_\sigma(s) = f_\sigma(\sum_{i=1}^{n} e_i) = \sum_{i=1}^{n} f_\sigma(e_i) = \sum_{i=1}^{n} e_{\sigma(i)} = s$,

vì vậy: $\forall \sigma \in \mathfrak{S}_n$, $f_\sigma(D) \subset D$, do đó : $D \in \mathfrak{F}$.

• Giả sử $x = \sum_{i=1}^{n} x_i e_i \in H$, $\sigma \in \mathfrak{S}_n$; ta có: $f_\sigma(x) = \sum_{i=1}^{n} x_i e_{\sigma(i)} = \sum_{k=1}^{n} x_{\sigma^{-1}(k)} e_k$

và $\sum_{k=1}^{n} x_{\sigma^{-1}(k)} = \sum_{i=1}^{n} x_i = 0$, nên $f_\sigma(x) \in H$.

Như vậy: $(\forall \sigma \in \mathfrak{S}_n, f_\sigma(H)) \subset H$, do vậy: $H \in \mathfrak{F}$.

2) • Giả sử $x = \sum_{i=1}^{n} x_i e_i \in D \cap H$. Khi đó $\begin{cases} x_1 = \cdots = x_n \\ x_1 + \cdots + x_n = 0 \end{cases}$, nên $x_1 = \ldots = x_n = 0$,

Như vậy $D \cap H = \{0\}$.

• $\dim(D \oplus H) = \dim(D) + \dim(H) = 1 + n - 1 = n$, do đó $D \oplus H = E$.

• Giả sử $x = \sum_{i=1}^{n} x_i e_i \in E$. Ta có :

$$\left(\frac{1}{n!}\sum_{\sigma \in \mathfrak{S}_n} f_\sigma\right)(x) = \frac{1}{n!}\sum_{\sigma \in \mathfrak{S}_n}\sum_{i=1}^{n} x_i e_{\sigma(i)} = \frac{1}{n!}\sum_{\sigma \in \mathfrak{S}_n}\sum_{k=1}^{n} x_{\sigma^{-1}(k)} e_k = \frac{1}{n!}\sum_{k=1}^{n}\left(\sum_{\sigma \in \mathfrak{S}_n} x_{\sigma^{-1}(k)}\right) e_k$$

$$= \frac{1}{n!}\sum_{k=1}^{n}\left((n-1)!\sum_{i=1}^{n} x_i\right) e_k = \sum_{k=1}^{n}\left(\frac{1}{n}\sum_{i=1}^{n} x_i\right) e_k .$$

vì vậy $\left(\frac{1}{n!}\sum_{\sigma \in \mathfrak{S}_n} f_\sigma\right)(x) \in D$.

Và vì $\sum_{i=1}^{n}\left(x_i - \frac{1}{n}\sum_{i=1}^{n} x_i\right) = 0$, nên ta có: $x - \left(\frac{1}{n!}\sum_{\sigma \in \mathfrak{S}_n} f_\sigma\right)(x) \in H$.

Như vậy, $p = \frac{1}{n!}\sum_{\sigma \in \mathfrak{S}_n} f_\sigma$ là phép chiếu lên D song song với H.

3) Vì $F \not\subset D$, nên tồn tại $x = \sum_{k=1}^{n} x_k e_k \in F$ sao cho $x \notin D$. Vì vậy tồn tại $(i, j) \in \{1, \ldots, n\}^2$ sao cho $i < j$ và $x_i \neq x_j$.

Giả sử $q \in \{2, \ldots, n\}$ tồn tại $\sigma \in \mathfrak{S}_n$ sao cho $\sigma(i) = 1$ và $\sigma(j) = q$. Vì $F \in \mathfrak{F}$ và $x \in F$, nên nếu đặt $x' = \sum_{k=1}^{n} x'_k e_k = f_\sigma(x)$, thì ta có $x' \in F$, $x'_1 = x_i \neq x_j = x'_q$

Vì $\tau_{1q} \in \mathfrak{S}_n$, ta cũng có $x'_q e_1 + x'_1 e_q + \sum_{\substack{2 \le k \le n \\ k \neq q}} x'_k e_k \in F$, do đó vì F là một kgvc nên khi lấy hiệu với x', ta sẽ được: $(x'_q - x'_1)(e_1 - e_q) \in F$.

Cuối cùng, vì F là một kgvc và $x'_q - x'_1 \neq 0$ nên: $e_1 - e_q \in F$.

Vì $(e_1 - e_2, \ldots, e_1 - e_n)$ là một cơ sở của H, ta kết luận: $H \subset F$.

4) • $\{0\}, D, H, E \in \mathfrak{F}$, xem 1)

• Giả sử $F \in \mathfrak{F}$.

Nếu $F \subset D$ thì $F = \{0\}$ hoặc $F = D$.

Nếu $F \not\subset D$ thì $H \subset F$ (xem 3)), vì vậy $F = H$ hoặc $F = E$

Chỉ dẫn và trả lời
các bài tập chương 8

8.1.1 Ta có : $E_{ij} = (\delta_{ui}\delta_{vj})_{u,v}$, $E_{kl} = (\delta_{sk}\delta_{tl})_{s,t}$, do đó: $E_{ij}E_{kl} = (a_{uv})_{u,v}$ trong đó :

$$a_{uv} = \sum_{r=1}^{p} \delta_{ui}\delta_{vj}\delta_{rk}\delta_{rl} = \delta_{ui}\delta_{jk}\delta_{vl} = \delta_{jk}(\delta_{ui}\delta_{vl})$$

Vì $E_{il} = (\delta_{ui}\ \delta_{vl})_{u,v}$, nên ta kết luận: $E_{ij}E_{kl} = \delta_{jk}E_{il}$.

8.1.2 Với $(i,j) \in \{1,\ldots,n\}^2$, đặt $A = (a_{ij})_{ij}$. Ta có:

$$E_{ij}A = \begin{pmatrix} & & \\ 1 & & \\ & & \end{pmatrix} \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ & & \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} = \begin{pmatrix} & 0 & \\ a_{j1} & \cdots & a_{jn} \\ & 0 & \end{pmatrix} \leftarrow \text{dòng thứ } i$$

như vậy, $(E_{ij}A)^2 = \begin{pmatrix} & 0 & \\ a_{j1}a_{j1} & \cdots & a_{jn}a_{jn} \\ & 0 & \end{pmatrix} \leftarrow$ dòng thứ i.

Như thế : $\forall i,j,k \in \{1,\ldots,n\}$, $a_{ji}a_{jk} = 0$.

Nói riêng: $\forall (i,j) \in \{1,\ldots,n\}^2$, $a_{ji}^2 = 0$, và do đó $A = 0$.

8.1.3 Đặt $I = I_n$, ta có $0 = AB + \alpha A + \beta B = (A + \beta I)(B + \alpha I) - \alpha\beta I$, nên :

$\frac{1}{\alpha\beta}(A + \beta I)(B + \alpha I) = I$.

Điều đó chứng tỏ $B + \alpha I$ khả nghịch trái, do đó khả nghịch (xem 8.1.5, Định lý) và có nghịch đảo là $\frac{1}{\alpha\beta}(A + \beta I)$.

Như vậy : $\frac{1}{\alpha\beta}(B + \alpha I)(A + \beta I) = I$, do đó $BA + \alpha A + \beta B = 0$, và cuối cùng $AB = BA$.

8.1.4 Đặt $Y = X - I_2$, ta có: $X^2 - 2X = \begin{pmatrix} -1 & 0 \\ 6 & 3 \end{pmatrix} \Leftrightarrow Y^2 = \begin{pmatrix} 0 & 0 \\ 6 & 4 \end{pmatrix}$.

Đặt $Y = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $Y^2 = \begin{pmatrix} 0 & 0 \\ 6 & 4 \end{pmatrix} \Leftrightarrow \begin{cases} a^2 + bc = 0 \\ b(a+d) = 0 \\ c(a+d) = 0 \\ bc + d^2 = 4 \end{cases} \Leftrightarrow \begin{cases} a = 0 \\ b = 0 \\ cd = 6 \\ d^2 = 4 \end{cases}$

◇ **Trả lời** : $\left\{\begin{pmatrix} 1 & 0 \\ 3 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -3 & -1 \end{pmatrix}\right\}$.

8.1.5 Vì $(XYX)Y = X(YXY)$, nên : $\begin{cases} XYX = \mathrm{I}_2 \\ YXY = \mathrm{I}_2 \end{cases} \Leftrightarrow \begin{cases} Y = X \\ X^3 = \mathrm{I}_2 \end{cases}$.

Đặt $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, ta được $X^3 = \mathrm{I}_2^2 \Leftrightarrow \begin{cases} a^3 + 2abc + bcd = 1 \\ b(a^2 + ad + bc + d^2) = 0 \\ c(a^2 + ad + bc + d^2) = 0 \\ abc + 2bcd + d^3 = 1 \end{cases}$.

Trường hợp $b = c = 0$ rất đơn giản.

Và : $\begin{cases} a^3 + 2abc + bcd = 1 \\ a^2 + ad + bc + d^2 = 0 \\ abc + 2bcd + d^3 = 1 \end{cases} \Leftrightarrow \begin{cases} bc = -(a^2 + ad + d^2) \\ a^3 - (2a + d)(a^2 + ad + d^2) = 1 \\ -(a + 2d)(a^2 + ad + d^2) + d^3 = 1 \end{cases}$

$\Leftrightarrow \begin{cases} bc = -(a^2 + ad + d^2) \\ (a + d)^3 = -1 \end{cases} \Leftrightarrow \begin{cases} d = -1 - a \\ bc = -1 - a - a^2 \end{cases}$

◇ **Trả lời:** $\{\mathrm{I}_2\} \cup \left\{ \begin{pmatrix} a & b \\ c & -1-a \end{pmatrix};\ a, b, c \in \mathbb{R}^3,\ bc = -1 - a - a^2 \right\}$.

8.1.6 Nhận xét rằng $U^2 = nU$, nên với mọi (a,b) thuộc $\mathbb{C}^2$: $(aU)(bU) = (nab)U$.

Hiển nhiên ánh xạ θ : $\underset{a \mapsto aU}{\mathbb{C} \to E}$ là song ánh và: $\begin{cases} \theta(1) = U \\ \forall a, b \in \mathbb{C}^2, \begin{cases} \theta(a+b) = \theta(a) + \theta(b) \\ \theta(ab) = \theta(a)\theta(b) \end{cases} \end{cases}$

Vì $\mathbb{C}$ là một thể, nên qua việc chuyển cấu trúc, E cũng là một thể đẳng cấu với $\mathbb{C}$.

Khi $n \geq 2$ thì vì $\mathrm{I}_n \notin E$, nên E không phải là một thể con của vành $\mathbf{M}_n(\mathbb{C})$. Điều đó cũng có thể suy ra từ nhận xét: các phần tử trung lập đối với phép nhân trong E và trong $\mathbf{M}_n(\mathbb{C})$ khác nhau, các phần tử đó tương ứng là $\frac{1}{n}U$ và I_n.

8.1.7 a) Rõ ràng phép cộng và phép nhân là các luật hợp thành trong trong E và: $\forall A \in E,\ A \in E$.

b) $\mathrm{I}_2 \notin E$. Các phần tử trung lập của phép nhân trong E và trong $\mathbf{M}_2(K)$ khác nhau: $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ và I_2.

◇ **Trả lời:** Không.

8.1.8 a) • E là kgvc của $\mathbf{M}_4(\mathbb{C})$ sinh bởi (I, J, K), trong đó

$I = \mathrm{I}_4$, $J = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$, $K = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$. Hơn nữa, hiển nhiên (I,J,K) độc lập tuyến tính.

• Tính : $J^2 = 2I + 2K$, $JK = K$, $KJ = K$, $K^2 = I$. Vậy phép nhân là luật hợp thành trong E, giao hoán trong E và I là phần tử trung lập.

b) Đặt $X = aI + bJ + cK$, $(a,b,c) \in \mathbb{C}^3$. Ta có:

$$X^2 = I \Leftrightarrow a^2 I + b^2(2I + 2K) + c^2 I + 2abJ + 2acK + 2bcK = I$$

$$\Leftrightarrow \begin{cases} a^2 + 2b^2 + c^2 = 1 \\ 2ab = 0 \\ 2b^2 + 2ac + 2bc = 0 \end{cases} \Leftrightarrow \left(\begin{cases} a = 0 \\ 2b^2 + c^2 = 1 \\ b(b + c) = 0 \end{cases} \text{ hoặc } \begin{cases} b = 0 \\ a^2 + c^2 = 1 \\ ac = 0 \end{cases} \right)$$

$$\Leftrightarrow \left\{ \begin{cases} a=0 \\ b=0 \\ c^2=1 \end{cases} \text{ hoặc } \begin{cases} a=0 \\ 3b^2=1 \\ c=-b \end{cases} \text{ hoặc } \begin{cases} b=0 \\ c=0 \\ a^2=1 \end{cases} \right.$$

◇ **Trả lời:** $\left\{K,-K,\frac{1}{\sqrt{3}}(J-K),-\frac{1}{\sqrt{3}}(J-K),I,-I\right\}$.

8.1.9 Đặt $U=\begin{pmatrix} 1 & & 1 \\ & 1 & \\ 1 & & 1 \end{pmatrix} \in \mathbf{M}_n(\mathbb{C})$, ta có: $\mathbf{M}_{a,b}=(a-b)\mathbf{I}_n+bU$.

Vì I_n và U giao hoán được với nhau, nên theo công thức nhị thức Newton: $M_{ab}^k=\sum_{i=0}^{k} C_k^i (a-b)^{k-i} b^i U^i$.

Mặt khác $U^2=nU$, nên bằng quy nạp dễ dàng suy ra: $\forall i \in \mathbb{N}^*,\ U^i=n^{i-1}U$.

Do đó: $M_{ab}^k=(a-b)^k \mathrm{I}_n+\sum_{i=0}^{k} C_k^i (a-b)^{k-i} b^i n^{i-1} U=(a-b)^k 1_n+\frac{1}{n}(\sum_{i=0}^{k} C_k^i (a-b)^{k-i}(nb)^i)U$

$$=(a-b)^k 1_n+\frac{1}{n}((a-b+nb)^k-(a-b)^k)U .$$

◇ **Trả lời:** $M_{a,b}^k=(a-b)^k I_n+\frac{1}{n}((a+(n-1)b)^k-(a-b)^k)U$, trong đó $U=\begin{pmatrix} 1 & & 1 \\ & 1 & \\ 1 & & 1 \end{pmatrix}$.

8.1.10 Trước hết, ta có: $A^2=\begin{pmatrix} 1 & 2 & \cdots & n \\ & & \ddots & 2 \\ & 0 & & 1 \end{pmatrix}$, $A^3=\begin{pmatrix} 1 & 3 & 6 & \cdots & \frac{n(n+1)}{2} \\ & & & \ddots & 6 \\ & & 0 & & 3 \\ & & & & 1 \end{pmatrix}$

Ta chứng minh bằng quy nạp theo k: $A^k=(a_{k;i,j})_{1\le i,j\le n}$ trong đó $a_{k;i,j}=\begin{cases} C_j^{k\ i\ i-k\ 1} & \text{nếu } i\le j \\ 0 & \text{nếu } i>j \end{cases}$.

Với $k=1$, công thức là hiển nhiên. Giả sử công thức đúng cho k, và đặt $A^{k+1}=(a_{k+1;i,j})_{ij}$.

Hiển nhiên, với $i>j$, $a_{k+1;i,j}=0$ (xem thêm 8.3.2, Mệnh đề 2).

Cho $(i,j)\in\{1,\dots,n\}^2$ sao cho $i\le j$. Ta có:

$$a_{k+1;i,j}=\sum_{q=1}^{n} a_{k;i,j}a_{1;q,j}=\sum_{q=1}^{j} C_q^{k\ 1\ i+k-1}=\sum_{r=0}^{j-i} C_{r\ k-1}^{k\ 1} .$$

Chứng minh bằng quy nạp theo s: $\forall s\in\mathbb{N}$, $\sum_{r=0}^{s} C_{r+k-1}^{k-1}=C_{s+k}^{k}$.

Kết luận: $a_{k+1;i,j}=C_{j-i+k}^{k}$.

◇ **Trả lời:** $A^k=\begin{pmatrix} 1 & C_k^{k\ 1} & \cdots & C_{n+k\ 2}^{k\ 1} \\ & & & \vdots \\ & 0 & & C_k^{k-1} \\ & & & 1 \end{pmatrix}$.

8.1.11 1) Giả sử $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ thích hợp.

Từ $A^2=\begin{pmatrix} a^2 & b^2 \\ c^2 & d^2 \end{pmatrix}$, suy ra $\begin{cases} bc=0 \\ (a+d-b)b=0 \\ (a+d-c)c=0 \end{cases}$.

• Giả sử $c \neq 0$.

Khi đó $b = 0$ và $a + d = c$. Từ $A^3=\begin{pmatrix} a^3 & 0 \\ c^3 & d^3 \end{pmatrix}$ suy ra $c(a^2 + ad + d^2) = c^3$, sau đó $ad = 0$.

Như vậy A có dạng $\begin{pmatrix} 0 & 0 \\ c & c \end{pmatrix}$ hoặc $\begin{pmatrix} a & 0 \\ a & 0 \end{pmatrix}$.

• Tương tự, nếu $b = 0$ thì A sẽ có dạng $\begin{pmatrix} 0 & b \\ 0 & b \end{pmatrix}$ hoặc $\begin{pmatrix} a & a \\ 0 & 0 \end{pmatrix}$.

• Nếu $b = c = 0$, thì $A=\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$.

◇ **Trả lời:**

$$\left\{\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}; (a,d) \in \mathbf{R}^2\right\} \cup \mathbf{R}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \cup \mathbf{R}\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \cup \mathbf{R}\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \cup \mathbf{R}\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}.$$

8.1.12 1) •E là kgvc của $M_2(\mathbb{R})$ sinh bởi $\mathbf{I}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ và $J=\begin{pmatrix} 1 & 3 \\ -3 & -1 \end{pmatrix}$. Hiển nhiên (I, J) độc lập tuyến tính.

• $J^2=\begin{pmatrix} -2 & 0 \\ 0 & -2 \end{pmatrix}=-2\mathbf{I}$, nên:

$$\forall x, y, x', y' \in \mathbb{R},\ (x\mathbf{I} + yJ)(x'\mathbf{I} + y'J) = (xx' - 2yy')\mathbf{I} + (xy' + yx')J \in E.$$

• $\mathbf{I}_2 \in E$.

• Giả sử $M \in E - \{0\}$. Tồn tại $(x,y) \in \mathbb{R}^2 - \{(0,0)\}$ duy nhất sao cho $M = x\mathbf{I} + yJ$.

Giả sử $x', y' \in \mathbb{R}$, $M' = x'\mathbf{I} + y'J$. Ta có: $MM' = \mathbf{I}_2 \Leftrightarrow \begin{cases} xx'-2yy'=1 \\ yx'+xy'=0 \end{cases} \Leftrightarrow \begin{cases} x'=\dfrac{x}{x^2+2y^2} \\ y'=\dfrac{-y}{x^2+2y^2} \end{cases}$,

vì $x^2 + 2y^2 > 0$. Như vậy M có nghịch đảo trong E.

Điều đó chứng tỏ E là một thể con của vành $\mathbf{M}_2(\mathbb{R})$.

2) Ánh xạ θ: $E \to \mathbb{C}$, $(x,y) \in \mathbb{R}^2$, là một đẳng cấu thể:

$$x\mathbf{I} + yJ \mapsto x + y\sqrt{2}\,\mathrm{i}$$

• $\theta((x\mathbf{I} + yJ) + (x'\mathbf{I} + y'J)) = (x + x') + (y + y')\sqrt{2}\,\mathrm{i} = (x + y\sqrt{2}\,\mathrm{i}) + (x' + y'\sqrt{2}\,\mathrm{i}) = \theta(x\mathbf{I} + yJ) + \theta(x'\mathbf{I} + y'J)$.

• $\theta((x\mathbf{I} + yJ)(x'\mathbf{I} + y'J)) = xx' - 2yy' + (xy' + yx')\sqrt{2}\,\mathrm{i} = (x + y\sqrt{2}\,\mathrm{i})(x' + y'\sqrt{2}\,\mathrm{i}) = \theta(x\mathbf{I} + yJ)\theta(x'\mathbf{I} + y'J)$.

• $\theta(\mathbf{I}) = 1$

• θ là song ánh.

8.1.13 a) • E_α là kgvc của $M_2(\mathbb{R})$ sinh bởi $\mathbf{I}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ và $J=\begin{pmatrix} 0 & \alpha \\ 1 & 0 \end{pmatrix}$.

• Vì $J^2 = \alpha \mathrm{I}$, ta có:

$$\forall x, y, x', y' \in \mathbb{R}, \quad (x\mathrm{I} + yJ)(x'\mathrm{I} + y'J) = (xx' + \alpha yy')\mathrm{I} + (xy' + yx')J \in E_\alpha .$$

• Công thức trên chứng tỏ phép nhân giao hoán trong E_α.

• $I_2 \in E$.

b) • Nếu $\alpha < 0$, ánh xạ θ: $\quad E \to \mathbb{C}$ $\quad x\mathrm{I} + yJ \mapsto x + \sqrt{-\alpha}\,\mathrm{i}$, $(x, y) \in \mathbb{R}^2$, là một đẳng cấu đối với các luật + và ×,

do vậy, qua việc chuyển cấu trúc, E_α là một thể, đẳng cấu với $\mathbb{C}$.

• Nếu $\alpha \geq 0$, E_α là một vành (xem a)), không nguyên vì $\begin{cases} \sqrt{\alpha}\mathrm{I} + J \neq 0,\ \sqrt{\alpha}\mathrm{I} - J \neq 0 \\ (\sqrt{\alpha}\mathrm{I} + J)(\sqrt{\alpha}\mathrm{I} - J) = 0 \end{cases}$.

8.1.14 a) Giả sử $(e_1,...,e_n)$ là cơ sở chính tắc của $\mathbf{M}_{n,1}(\mathbb{R})$ và $(f_1,..., f_n)$ là họ vectơ thuộc $\mathbf{M}_{n,1}(\mathbb{R})$ xác định bởi $A = \mathrm{Mat}_{(e_1,...,e_n)}(f_1,..., f_n)$.

Hệ phương trình:

$$\begin{cases} f_1 = e_1 \\ f_2 = e_2 + e_1 = e_2 + f_1 \\ f_3 = e_3 + e_2 = e_3 + f_2 - f_1 \\ \vdots \\ f_n = e_n + e_{n-1} = e_n + f_{n-1} - f_{n-2} + ... + (-1)^n f_1 \end{cases} \quad \text{cho ta} \quad \begin{cases} e_1 = f_1 \\ e_2 = f_2 - f_1 \\ \vdots \\ e_n = f_n - f_{n-1} + \cdots + (-1)^{n-1} f_1 \end{cases}$$

◇ **Trả lời:** $A^{-1} = \begin{pmatrix} 1 & -1 & \cdots & (-1)^{n-1} \\ & & & \vdots \\ 0 & & & -1 \\ & & & 1 \end{pmatrix}$.

b) Tương tự như a).

◇ **Trả lời:** $A^{-1} = \begin{pmatrix} 1 & -1 & 0 \\ & & -1 \\ 0 & & 1 \end{pmatrix}$.

c) Tương tự như a). Cũng có thể nhận xét rằng đó chính là bình phương ma trận A ở a).

◇ **Trả lời:** $A^{-1} = \begin{pmatrix} 1 & -2 & 1 & & 0 \\ & & & & 1 \\ & & & & -2 \\ 0 & & & & 1 \end{pmatrix}$.

8.1.15 Ký hiệu $\gamma_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$ là hạng tử tổng quát của AB. Rõ ràng, nếu $i > j$ thì $\gamma_{ij} = 0$

(cũng có thể xem 8.3.2, Mệnh đề 2). Giả sử $i \geq j$. Ta có :

$$\gamma_{ij} = \sum_{k=i}^{j} t^{k-i} \mathrm{C}_k^i (-1)^{j+k} t^{j-k} \mathrm{C}_j^k = (-1)^j t^{j-i} \sum_{k=i}^{j} (-1)^k \mathrm{C}_k^i \mathrm{C}_j^k$$

$$= (-1)^j t^{j-i} \sum_{k=i}^{j} (-1)^k \frac{j!}{i!(k-i)!(j-k)!} = (-1)^j t^{j-i} \frac{j!}{i!(j-i)!} \sum_{k=i}^{j} (-1)^k \frac{(j-i)!}{(k-i)!(j-k)!}$$

$$= (-1)^{j+i} t^{j-i} \mathrm{C}_j^i \sum_{p=0}^{j-i} (-1)^p \mathrm{C}_{j-i}^p = (-1)^{j+i} t^{j-i} \mathrm{C}_j^i (1 + (-1))^{j-i} = \begin{cases} 1 & \text{nếu } i = j \\ 0 & \text{nếu } i < j \end{cases}$$

8.1.16 $\begin{cases} AX + BY = 0 \\ BX - AY = I_n \end{cases} \Leftrightarrow \begin{cases} Y = -B^{-1}AX \\ (B - AB^{-1}A)X = I_n \end{cases}$

◇ **Trả lời:** $\{((B - AB^{-1}A)^{-1}, -B^{-1}A(B - AB^{-1}A)^{-1})\}$.

8.1.17 Đặt $A = \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}$, $B = \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix}$, $C = \begin{pmatrix} 2 & 0 \\ 2 & 0 \end{pmatrix}$.

Nếu (X, Y, Z) thích hợp thì: $AC = (XY)(ZX) = X(YZ)X = XBX$.

Đặt $X = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$ ta có

$$AC = XBX \Leftrightarrow \begin{cases} (2x + y)(x + z) = 2 \\ (2x + y)(y + t) = 0 \\ (2z + t)(x + z) = 6 \\ (2z + t)(y + t) = 0 \end{cases} \Leftrightarrow \begin{cases} y + t = 0 \\ (2x + y)(x + z) = 2 \\ (2z + t)(x + z) = 6 \end{cases}$$

$$\Leftrightarrow \begin{cases} y + t = 0 \\ (2x + y)(x + z) = 2 \\ 2(x + z)^2 = 8 \end{cases} \Leftrightarrow \begin{cases} t = -y \\ x + z = 2\varepsilon \\ 2x + y = \varepsilon \end{cases},$$

trong đó $\varepsilon = 1$ hoặc -1.

Như vậy: $X = \begin{pmatrix} x & \varepsilon - 2x \\ 2\varepsilon - x & -\varepsilon + 2x \end{pmatrix}$

Chứng tỏ rằng X khả nghịch khi và chỉ khi $4\varepsilon x - 2 \neq 0$, và khi $4\varepsilon x - 2 \neq 0$ thì

$$X^{-1} = \frac{1}{4\varepsilon x - 2}\begin{pmatrix} -\varepsilon + 2x & -\varepsilon + 2x \\ -2\varepsilon + x & x \end{pmatrix}.$$

◇ **Trả lời:** $\left\{\left(\begin{pmatrix} x & \varepsilon - 2x \\ 2\varepsilon - x & -x + 2x \end{pmatrix}, \frac{1}{2\varepsilon x - 1}\begin{pmatrix} -\varepsilon + 2x & -\varepsilon + 2x \\ -\varepsilon + x & x \end{pmatrix}\right)\right.$;

$\left.(\varepsilon, x) \in \{-1, 1\} \times \mathbb{R} \text{ và } 2\varepsilon x - 1 \neq 0\right\}$.

8.1.18 a) Rõ ràng ánh xạ $f: \mathbf{M}_n(K) \to \mathbf{M}_n(K)$, $M \mapsto MS$ tuyến tính và $E = \mathrm{Ker}(f)$, do vậy E là một kgvc của $\mathbf{M}_n(K)$.

b) α) Nhận xét: $\forall A \in \mathbf{M}_n(K)$, $(A \in F \Leftrightarrow AS = S)$.

Giả sử $(A,B) \in F^2$. Thế thì $AS = S$ và $BS = S$, nên: $(AB)S = A(BS) = AS = S$, và do vậy $AB \in F$.

β) Giả sử $A \in F \cap \mathbf{GL}_n(K)$. Ta có: $A^{-1}S = A^{-1}(AS) = (A^{-1}A)S = S$, nên $A^{-1} \in F$.

8.1.19 a) $(I_n + E_{ij})(I_n - E_{ij}) = I_n - E_{ij}^2 = I_n$, xem bài tập 8.1.1. Vì vậy $I_n + E_{ij}$ khả nghịch và $(I_n + E_{ij})^{-1} = I_n - E_{ij}$, xem thêm 8.1.7.

b) Cho $A \in \mathbf{M}_n(K)$ sao cho: $\forall x \in \mathbf{GL}_n(K)$, $AX = XA$.

Nói riêng, với mọi (i, j) thuộc $\{1,\ldots,n\}^2$ sao cho $i \neq j$: $A(I_n + E_{ij}) = (I_n - E_{ij})A$.

và vì vậy $AE_{ij} = E_{ij}A$.

Đặt $A = (a_{kl})_{kl}$, ta có:

$$AE_{ij} = \begin{pmatrix} & a_{1i} & \\ 0 & \vdots & 0 \\ & a_{mi} & \end{pmatrix} \quad (\text{cột thứ } j), \qquad E_{ij}A = \begin{pmatrix} & 0 & \\ a_{j1} & \cdots & a_{jn} \\ & 0 & \end{pmatrix} \leftarrow \text{hàng thứ } i.$$

Suy ra $a_{ii} = a_{jj}$ và $a_{ik} = 0$, và do vậy $A = a_{11}\mathbf{I}_n$.

- Dễ dàng suy ra phần đảo.

◇ **Trả lời**: $K\mathbf{I}_n$.

8.1.20 Xác định $\mathrm{Ker}(M_{a,b})$. Cho $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in Mg_{n,1}(\mathbb{C})$. Ta có:

$$X \in \mathrm{Ker}(M_{a,b}) \Leftrightarrow \begin{cases} ax_1 + bx_2 + \cdots + bx_n = 0 \\ \vdots \\ bx_1 + bx_2 + \cdots + ax_n = 0 \end{cases} \Leftrightarrow \begin{cases} (a-b)x_1 + b(x_1 + \cdots + x_n) = 0 \\ \vdots \\ (a-b)x_n + b(x_1 + \cdots + x_n) = 0 \end{cases}$$

Trường hợp $a = b$ có thể xét dễ dàng.

Giả thiết $a \neq b$. Ta có $X \in \mathrm{Ker}(M_{a,b}) \Leftrightarrow \begin{cases} x_1 = \cdots = x_n \\ (a-b+nb)(x_1 + \cdots + x_n) = 0 \end{cases}$

- Nếu $a + (n-1)b \neq 0$ thì : $X \in \mathrm{Ker}(M_{a,b}) \Leftrightarrow \begin{cases} x_1 = \cdots = x_n \\ x_1 + \cdots + x_n = 0 \end{cases} \Leftrightarrow x_1 = \ldots = x_n = 0$, nên $\mathrm{Ker}(M_{a,b}) = \{0\}$, do đó $\mathrm{rank}(M_{a,b}) = n$.

- Nếu $a + (n-1)b = 0$ thì : $X \in \mathrm{Ker}(M_{a,b}) \Leftrightarrow x_1 = \ldots = x_n$, vì vậy $\dim(\mathrm{Ker}(M_{a,b})) = 1$, nên (theo định lý về hạng) : $\mathrm{rank}(M_{a,b}) = n - 1$.

◇ **Trả lời**: $\mathrm{rank}(M_{a,b}) = \begin{cases} n & \text{nếu } a \neq b \text{ và } a+(n-1)b \neq 0 \\ n-1 & \text{nếu } a \neq b \text{ và } a+(n-1)b = 0 \\ 1 & \text{nếu } a = b \neq 0 \\ 0 & \text{nếu } a = b = 0 \end{cases}$

8.1.21 a) $\mathrm{rank}(A) = n \Leftrightarrow \mathrm{rank}(C'_1, \ldots, C'_p) = \dim(\mathbf{M}_{n,1}(K))$

$\Leftrightarrow \mathrm{Vect}(C'_1, \ldots, C'_p) = \mathbf{M}_{n,1}(K) \Leftrightarrow (C'_1, \ldots, C'_p)$ sinh ra $\mathbf{M}_{n,1}(K)$.

b) $\mathrm{rank}(A) = p \Leftrightarrow \mathrm{rank}(C'_1, \ldots, C'_p) = p \Leftrightarrow (C'_1, \ldots, C'_p)$ độc lập tuyến tính).

8.1.22 a) $\mathrm{rank}(A) = n \Leftrightarrow \mathrm{rank}(f) = n \Leftrightarrow \dim(\mathrm{Im}(f)) = \dim(F)$

$\Leftrightarrow \mathrm{Im}(f) = F \Leftrightarrow f$ là toàn ánh.

b) $\mathrm{rank}(A) = p \Leftrightarrow \mathrm{rank}(f) = p \Leftrightarrow \dim(\mathrm{Ker}(f)) = 0 \Leftrightarrow \mathrm{Ker}(f) = \{0\} \Leftrightarrow f$ là đơn ánh.

Ta cũng có thể sử dụng bài tập 8.1.21.

8.1.23 1) Đặt $r = \mathrm{rank}(A)$ và giả thiết $r \leq s$.

Theo định lý về hạng, $\dim(\mathrm{Ker}(A)) \geq p - s$. Nếu $s = p$, ta có thể chọn $q = 1$ và $B = 0$.

Giả sử $s < p$. Tồn tại một cơ sở $V_1, ..., V_{p-r}$ của $\mathrm{Ker}(A)$. Đặt $q = p - r$ và B là ma trận của $\mathbf{M}_{p,q}(K)$ có các cột là $V_1, ..., V_{p-r}$, ta có $\mathrm{rank}(B) = p - r \geq p - s$ và $AB = 0$ vì $AV_1 = ... = AV_{p-r} = 0$.

2) Ngược lại, giả sử tồn tại $q \in \mathbb{N}^*$, $B \in \mathbf{M}_{p,q}(K)$ sao cho $AB = 0$ và $\mathrm{rank}(B) \geq p - s$. Thế thì tồn tại $p - s$ cột của B tạo thành một họ độc lập tuyến tính, và những cột này thuộc $\mathrm{Ker}(A)$ (vì $AB = 0$). Do vậy $\dim(\mathrm{Ker}(A) \geq p - s$, do đó theo định lý về hạng, có $\mathrm{rank}(A) \leq s$.

8.1.24 • $\mathrm{Ker}(B) \subset \mathrm{Ker}(AB)$ vì: $\forall X \in \mathbf{M}_{n,1}(K)$, $(BX = 0 \Rightarrow (AB)X = A(BX) = 0)$.

• Mặt khác, theo định lý về hạng: $\dim(\mathrm{Ker}(B)) = q - \mathrm{rank}(B) = q - \mathrm{rank}(AB) = \dim(\mathrm{Ker}(AB))$. Ta suy ra: $\mathrm{Ker}(B) = \mathrm{Ker}(AB)$.

• Tương tự như trên : $\mathrm{Ker}(BC) \subset \mathrm{Ker}(ABC)$.

• Với mọi X thuộc $\mathbf{M}_{r,1}(K)$:

$X \in \mathrm{Ker}(ABC) \Leftrightarrow CX \in \mathrm{Ker}(AB) \Leftrightarrow CX \in \mathrm{Ker}(B) \Rightarrow X \in \mathrm{Ker}(BC)$.

Như vậy: $\mathrm{Ker}(ABC) = \mathrm{Ker}(BC)$, nên theo định lý về hạng:

$\mathrm{rank}(ABC) = r - \dim(\mathrm{Ker}(ABC)) = r - \dim(\mathrm{Ker}(BC)) = \mathrm{rank}(BC)$.

8.1.25 Đặt $M = \begin{pmatrix} 0 & -1 & -1 \\ -1 & 0 & -1 \\ 1 & 1 & 2 \end{pmatrix}$, kiểm chứng rằng $M^2 = M$.

Ta suy ra: $ABC = M = M^2 = (ABC)^2$.

Chứng tỏ rằng $\mathrm{rank}(M) = 2$, từ đó suy ra: $2 = \mathrm{rank}(ABC) = \mathrm{rank}((ABC)^2) = \mathrm{rank}(AB(CAB)C) \leq \mathrm{rank}(ABC)$ (xem 8.1.66, Nhận xét).

Nhưng $CAB \in \mathbf{M}_2(\mathbb{R})$ nên $\mathrm{rank}(CAB) \leq 2$.

Ta nhận được $\mathrm{rank}(CAB) = 2$, nghĩa là $CAB \in \mathbf{GL}_2(\mathbb{R})$.

Sau đó: $(CAB)^2 = C(ABC)AB = C(ABC)^2AB = (CAB)^3$, do đó vì CAB khả nghịch, nên $CAB = \mathbf{I}_2$.

Cuối cùng: $(BCA)^2 = B(CAB)CA = B\mathbf{I}_2CA = BCA$.

8.1.26 a) Trước hết nhận xét $\mathrm{Im}(AB) \subset \mathrm{Im}(B)$; mặt khác, dễ dàng chứng minh bằng quy nạp:

$$\forall k \in \mathbb{N}^*, A^kB = BA^k.$$

Giả sử $\mathrm{Im}(BA) = \mathrm{Im}(B)$.

• Chứng minh bằng quy nạp theo k: $\forall k \in \mathbb{N}^*, \mathrm{Im}(BA^k) = \mathrm{Im}(B)$.

Theo giả thiết, tính chất đúng cho $k = 1$. Giả sử nó đúng cho một k thuộc $\mathbb{N}^*$.

Đặt $E = \mathbf{M}_{n,1}(K)$. Ta có:

$$\begin{aligned}\mathrm{Im}(BA^{k+1}) &= (BA^{k+1})(E) = (A^{k+1}B)(E) = A((A^kB)(E)) = A(B(E)) = (AB)(E) = (BA)(E) \\ &= \mathrm{Im}(BA) = \mathrm{Im}(B).\end{aligned}$$

• Vì A là lũy linh, nên tồn tại $k \in \mathbb{N}^*$ sao cho $A^k = 0$. Khi đó ta có: $\mathrm{Im}(B) = \mathrm{Im}(BA^k) = \{0\}$, nên $B = 0$, trường hợp này bị loại.

Điều đó chứng tỏ: $\mathrm{Im}(BA) \subsetneq \mathrm{Im}(B)$, và do vậy : $\mathrm{rank}(AB) = \mathrm{rank}(BA) < \mathrm{rank}(B)$.

b) Quy nạp theo p

Tính chất đúng cho $p = 1$ vì A_1 lũy linh nên không khả nghịch, do đó $\text{rank}(A_1) \leq n - 1 = (n-1)^+$.

Giả thiết tính chất đúng cho một p thuộc $\mathbb{N}^*$, và giả thiết $A_1, ..., A_{p+1} \in \mathbf{M}_n(K)$ lũy linh và giao hoán với nhau từng đôi một. Đặt $B = \prod_{i=1}^{p} A_i$.

Chứng tỏ rằng B lũy linh và giao hoán với A. Nếu $B = 0$, tính chất là tầm thường. Giả sử $B \neq 0$. Theo a):

$\text{rank}(A_{p+1}B) \leq \text{rank}(B) - 1$ nên $A_{p+1}B = 0$ hoặc $\text{rank}(A_{p+1}B) \leq (n-p) - 1 = n - c(p+1)$.

c) $\text{rank}\left(\prod_{i=1}^{n} A_i\right) \leq (n-n)^+ = 0$, vì vậy $\prod_{i=1}^{n} A_i = 0$.

8.1.27 Đặt $H = U^tV = \begin{pmatrix} 1 \\ \frac{1}{a} \\ \vdots \\ \frac{1}{a^{n-1}} \end{pmatrix} (1\ a \cdots a^{n-1}) = \begin{pmatrix} 1 & a & \cdots & a^{n-1} \\ \frac{1}{a} & & & \vdots \\ \vdots & & & a \\ \frac{1}{a^{n-1}} & \cdots & \frac{1}{a} & 1 \end{pmatrix}$,

hiển nhiên $A = H - \mathbf{I}_n$.

a) Vì H và $\mathbf{I}_n$ giao hoán với nhau, nên theo công thức nhị thức Newton: $A^k = \sum_{i=0}^{k} C_k^i (-1)^{k-i} H^i$.

Vì : $H^2 = (U^tV)(U^tV) = U({}^tVU)^tV = ({}^tVU)U^tV = nH$ (vì ${}^tVU \in \mathbb{R}$), ta được:

$$A^k = (-1)^k \mathbf{I}_n + \sum_{i=1}^{k} C_k^i (-1)^{k-i} n^{i-1} H = (-1)^k \mathbf{I}_n + \frac{1}{n}((n-1)^k - (-1)^k)H$$

◇ **Trả lời :** $A^k = \begin{pmatrix} (-1)^k + \alpha_k & \alpha_k a & \cdots & \alpha_k a^{n-1} \\ \frac{\alpha_k}{a} & & & \vdots \\ \vdots & & & \alpha_k a \\ \frac{\alpha_k}{a^{n-1}} & \cdots & \frac{\alpha_k}{a} & (-1)^k + \alpha_k \end{pmatrix}$.

trong đó $\alpha_k = \frac{1}{n}\left((n-1)^k - (-1)^k\right)$.

b) Theo câu a): $A^2 = \mathbf{I}_n + (n-2)H = (n-2)A + (n-1)\mathbf{I}_n$, nên $A\left(\frac{1}{n-1}(A - (n-2)\mathbf{I}_n)\right) = \mathbf{I}_n$.

Điều đó chứng tỏ A khả nghịch và cho ta A^{-1}.

◇ **Trả lời:** $A^{-1} = \frac{1}{n-1}(A - (n-2)\mathbf{I}_n) = \frac{1}{n-1}\begin{pmatrix} -(n-2) & a & \cdots & a^{n-1} \\ \frac{1}{a} & & & \\ \vdots & & & a \\ \frac{1}{a^{n-1}} & \cdots & \frac{1}{a} & -n-2 \end{pmatrix}$

c) Thác triển ký hiệu $\alpha_k = \frac{1}{n}((n-1)^k - (-1)^k)$, đã được đưa vào trong lời giải của a), cho trường hợp $k \in \mathbb{Z}^*_-$, ta có $\alpha_{-1} = \frac{1}{n-1}$, và công thức của a) về A^k sẽ đúng cho $k = -1$.

Giả sử với một k thuộc $\mathbb{Z}_-$: $A_k = (-1)^k I_n + \alpha_k H$.

Khi đó: $A^{k-1} = ((-1)^k I_n + \alpha_k H)(-I_n + \frac{1}{n-1} H = (-1)^{k+1} I_n + \left(\frac{(-1)^k}{n-1} - \alpha_k + \frac{n\alpha_k}{n-1}\right) H$.

Kiểm chứng lại: $\alpha_{k-1} = \frac{(-1)^k}{n-1} - \alpha_k + \frac{n\alpha_k}{n-1}$.

◇ **Trả lời**: Cùng công thức như trong a).

8.1.28 Giả sử $(A, B, C) \in (\mathbf{M}_2(K))^3$.

Vì $\mathrm{tr}(AB - BA) = \mathrm{tr}(AB) - \mathrm{tr}(BA) = 0$, nên tồn tại $(\alpha, \beta, \gamma \in K^3$, sao cho $AB - BA = \begin{pmatrix} \alpha & \beta \\ \gamma & -\alpha \end{pmatrix}$.

Khi đó: $(AB - BA)^2 = \begin{pmatrix} \alpha & \beta \\ \gamma & -\alpha \end{pmatrix}^2 = \begin{pmatrix} \alpha^2 + \beta\gamma & 0 \\ 0 & \alpha^2 + \beta\gamma \end{pmatrix} = (\alpha^2 + \beta\gamma) I_2$.

Vì I_2 giao hoán với C nên kết luận ta có công thức muốn chứng minh.

8.1.29 Giả sử tại (A, B, C, D) thích hợp. Khi đó

$\begin{cases} n = \mathrm{tr}(I_n) = \mathrm{tr}(AC + DB = \mathrm{tr}(AC) + \mathrm{tr}(DB) \\ 0 = \mathrm{tr}(CA + BD) = \mathrm{tr}(CA) + \mathrm{tr}(BD) = \mathrm{tr}(AC) + \mathrm{tr}(DB) \end{cases}$, mâu thuẫn.

8.1.30 Nếu (X, Y) thích hợp, thì $\mathrm{tr}(\mathrm{tr}(X)Y) + \mathrm{tr}((Y)X) = \mathrm{tr}\begin{pmatrix} 4 & 8 \\ 4 & -4 \end{pmatrix} = 0$, do đó $\mathrm{tr}(X).\mathrm{tr}(Y) = 0$.

1) Giả sử $\mathrm{tr}(X) = 0$.

Thế thì tồn tại $\lambda \in \mathbb{K}^*$ sao cho $X = \lambda \begin{pmatrix} 4 & 8 \\ 4 & -4 \end{pmatrix}$. Khi đó

$$(S) \Leftrightarrow \begin{cases} \mathrm{tr}(Y) = \frac{1}{\lambda} \\ 4\lambda \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix} Y = \begin{pmatrix} 1 & 1 \\ 4 & -2 \end{pmatrix} \end{cases} \Leftrightarrow \begin{cases} \mathrm{tr}(Y) = \frac{1}{\lambda} \\ Y = \frac{1}{4\lambda} \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 1 \\ 4 & -2 \end{pmatrix} \end{cases}$$

$$\Leftrightarrow Y = \frac{1}{4\lambda} \begin{pmatrix} 3 & -1 \\ -1 & 1 \end{pmatrix}.$$

2) Giả sử $\mathrm{tr}(Y) = 0$.

Thế thì tồn tại $\mu \in \mathbb{K}^*$ sao cho $Y = \mu \begin{pmatrix} 4 & 8 \\ 4 & -4 \end{pmatrix}$. Khi đó:

$$(S) \Leftrightarrow \begin{cases} \mathrm{tr}(X) = \frac{1}{\mu} \\ 4\mu X \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 4 & -2 \end{pmatrix} \end{cases} \Leftrightarrow \begin{cases} \mathrm{tr}(X) = \frac{1}{\mu} \\ X = \frac{1}{4\mu} \begin{pmatrix} 1 & 1 \\ 4 & -2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}^{-1} \end{cases}$$

$$\Leftrightarrow X = \frac{1}{12\mu} \begin{pmatrix} 2 & 1 \\ 2 & 10 \end{pmatrix}$$

◇ **Trả lời:**

$$\left\{\left(\alpha\begin{pmatrix}1 & 2\\ 1 & -1\end{pmatrix},\ \frac{1}{\alpha}\begin{pmatrix}3 & -1\\ -1 & 1\end{pmatrix}\right);\ \alpha\in\mathbf{R}^*\right\}\cup\left\{\left(\frac{1}{3\beta}\begin{pmatrix}2 & 1\\ 2 & 10\end{pmatrix},\ \beta\begin{pmatrix}1 & 2\\ 1 & -1\end{pmatrix}\right);\ \beta\in\mathbf{R}^*\right\}$$

8.1.31 a) Vì $\operatorname{rank}(H)\le 1$ nên tồn tại $U=\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}\in\mathbf{M}_{n,1}(K)$ sao cho các cột của H đồng phương với U ; vì vậy tồn tại $v_1,\dots,v_n\in K$ sao cho các cột của H là $v_1U,\dots,v_nU$, từ đó suy ra:

$$H=\begin{pmatrix}u_1v_1 & \cdots & u_1v_n\\ \vdots & & \vdots\\ u_nv_1 & \cdots & u_nv_n\end{pmatrix}=\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}(v_1,\cdots,v_n)=U{}^tV\ ,\ \text{trong đó ta đã đặt}\ \ V=\begin{pmatrix}v_1\\ \vdots\\ v_n\end{pmatrix},$$

Hơn nữa, $\operatorname{tr}(H)=\sum_{i=1}^{n}u_iv_i=(u_1,\cdots,u_n)\begin{pmatrix}v_1\\ \vdots\\ v_n\end{pmatrix}={}^tUV$.

b) $H^2=(U{}^tV)(U{}^tV)=U({}^tVU){}^tV=({}^tVU)U{}^tV=\operatorname{tr}(H)H$ (vì ${}^tVU\in\mathbb{K}$).

8.1.32 1) Giả sử $A^2=0$. Thế thì $\operatorname{Im}(A)\subset\operatorname{Ker}(A)$, nên $\operatorname{rank}(A)\le\dim(\operatorname{Ker}(A))=3-\operatorname{rank}(A)$, vì vậy $\operatorname{rank}(A)\le 1$. Theo bài tập 8.1.31, $A^2=\operatorname{tr}(A)A$, nên $\operatorname{tr}(A)=0$, hoặc $A=0$, do đó $\operatorname{tr}(A)=0$.

2) Ngược lại, nếu $\operatorname{rank}(A)\le 1$ và $\operatorname{tr}(A)=0$, thì theo bài tập 8.1.31: $A^2=\operatorname{tr}(A)A=0$.

8.1.33 Trước hết nhận xét: $\forall X\in\mathbf{M}_n(K)$, $\operatorname{tr}(AXB)=\operatorname{tr}(XBA)$.

1) Ta chứng minh dễ dàng phép suy diễn $\Leftarrow$.

2) Giả sử: $\forall X\in\mathbf{M}_{p,q}(K)$, $\operatorname{tr}(XBA)=0$.

Nói riêng, với $X=\mathrm{E}_{ij}$, $(i,j)\in\{1,\dots,p\}\times\{1,\dots,q\}$, đặt $BA=(c_{vw})_{vw}$, ta được:

$$0=\operatorname{tr}(XBA)=\sum_{u=1}^{p}\sum_{v=1}^{q}\delta_{ui}\delta_{vj}c_{vu}=c_{ji}\ ,$$

và vì vậy $BA=0$.

8.1.34 a) 1) Giả sử f thích hợp. Với mọi i,j,k,l thuộc $\{1,\dots,n\}$, ta có: $f(\mathrm{E}_{ij}\mathrm{E}_{kl})=f(\mathrm{E}_{kl}\mathrm{E}_{ij})$, vì vậy (xem bài tập 8.1.1): $\delta_{jk}f(\mathrm{E}_{il})=\delta_{li}f(\mathrm{E}_{kj})$.

Với (i,l) cố định, chọn $k=j=1$, ta nhận được: $f(\mathrm{E}_{il})=\delta_{li}f(\mathrm{E}_{11})$.

Khi đó, với mọi $A=(a_{ij})_{ij}$ thuộc $\mathbf{M}_n(K)$:

$$f(A)=f\left(\sum_{i,j}a_{ij}\mathrm{E}_{ij}\right)=\sum_{i,j}a_{ij}\delta_{ji}f(\mathrm{E}_{11})=\left(\sum_{i=1}^{n}a_{ii}\right)f(\mathrm{E}_{11})=\operatorname{tr}(A)f(\mathrm{E}_{11})\ .$$

Điều đó chứng tỏ tồn tại $F\in\mathbf{M}_n(K)$ sao cho $\forall A\in\mathbf{M}_n(K)$, $f(A)=\operatorname{tr}(A)F$.

2) Ngược lại, giả sử $F\in\mathbf{M}_n(K)$ và $f:\ \begin{matrix}\mathbf{M}_n(K)\to\mathbf{M}_n(K)\\ A\mapsto\operatorname{tr}(A)F\end{matrix}$.

Hiển nhiên f tuyến tính và với mọi (A,B) thuộc $(\mathbf{M}_n(K))^2$:

$$f(AB)=\operatorname{tr}(AB)F=\operatorname{tr}(BA)F=f(BA).$$

◇ **Trả lời:** $\left\{\begin{matrix}\mathbf{M}_n(K)\to\mathbf{M}_n(K)\\ A\mapsto\operatorname{tr}(A)F\end{matrix}\ ;\ F\in\mathbf{M}_n(K)\right\}$

b) 1) Giả sử f thích hợp. Theo a), tồn tại $F \in \mathbf{M}_n(K)$ sao cho: $\forall A \in \mathbf{M}_n(K)$, $f(A) = \mathrm{tr}(A)F$. Do vậy: $\forall A, B, C \in \mathbf{M}_n(K)$, $\mathrm{tr}(ABC)F = \mathrm{tr}(BAC)F$.

Nếu $F \neq 0$, nói riêng ta suy ra (nếu $n \geq 2$): $1 = \mathrm{tr}(E_{11}E_{12}E_{21}) = \mathrm{tr}(E_{12}E_{11}E_{21}) = 0$, mâu thuẫn.

2) Dễ dàng chứng minh phần đảo.

◇ **Trả lời:** • $\{0\}$ nếu $n \geq 2$

• $\angle(\mathbf{M}_1(K))$ nếu $n = 1$.

8.2.1 Theo 8.2.3 2), Mệnh đề 2, tồn tại $P \in \mathbf{GL}_p(K)$, $Q \in \mathbf{GL}_n(K)$ sao cho: $A = Q^{-1}\mathrm{J}_{n,p,r}P$.

Đặt $A_k = Q^{-1}E_{kk}P$ với $k = \{1, \ldots, r\}$, ta có: $\begin{cases} A = Q^{-1}\left(\sum_{k=1}^{r} \mathrm{E}_{kk}\right)P = \sum_{k=1}^{r} A_k \\ \forall k \in \{1, \cdots, r\},\ \mathrm{rank}(A_k) = 1 \end{cases}$.

8.2.2 Giả sử $A \in \mathbf{M}_n(\mathbb{C})$; đặt $r = \mathrm{rank}(A)$.

Theo 8.2.3.2), Mệnh đề 2, tồn tại P, $Q \in \mathbf{GL}_n(K)$ sao cho $A = Q^{-1}\mathrm{J}_{n,n,r}P$.

Đặt $U = \frac{1}{2}\mathbf{I}_n$, $V = \mathrm{J}_{n,n,r} - U = \begin{pmatrix} \frac{1}{2} & & & & & \\ & \ddots & & & 0 & \\ & & \frac{1}{2} & & & \\ & 0 & & -\frac{1}{2} & & \\ & & & & \ddots & \\ & & & & & -\frac{1}{2} \end{pmatrix}$, $B = Q^{-1}UP$, $C = Q^{-1}VP$.

Ta có: $\begin{cases} A = Q^{-1}(U+V)P = B + C \\ (B, C) \in (\mathbf{GL}_n(\mathbb{C}))^2 \end{cases}$.

8.2.3 1) Đặt $s = \mathrm{rank}(A)$ và giả sử $s \leq r$. Theo 8.2.3, Mệnh đề 2, tồn tại $P \in \mathbf{GL}_p(K)$, $Q \in \mathbf{GL}_n(K)$ sao cho: $A = Q^{-1}\mathrm{J}_{n,p,s}P$.

Nhận xét rằng: $\mathrm{J}_{n,r,s}\mathrm{J}_{n,p,s} = \mathrm{J}_{n,p,s}$, do đó nếu đặt $B = Q^{-1}\mathrm{J}_{n,r,s}$ và $C = \mathrm{J}_{r,p,s}P$ thì:

$B \in \mathbf{M}_{n,r}(K)$, $C \in \mathbf{M}_{r,p}(K)$, $A = BC$.

2) Ngược lại, giả sử tồn tại $(B, C) \in \mathbf{M}_{n,r}(K) \times \mathbf{M}_{r,p}(K)$ sao cho $A = BC$.

Khi đó $\mathrm{Im}(A) = \mathrm{Im}(BC) \subset \mathrm{Im}(B)$, vì vậy $\mathrm{rank}(A) \leq \mathrm{rank}(B) \leq r$.

8.2.4 a) Nếu $A = 0$, tính chất là hiển nhiên.

Giả thiết $A \neq 0$. Bằng cách giao hoán các hàng và giao hoán các cột, ta quy về một ma trận $(\alpha_{ij})_{ij}$ có $\alpha_{11} \neq 0$.

Nhân cột thứ nhất với α_{11}^{-1}, sau đó thay thế mỗi cột C_j $(2 \leq j \leq p)$ bởi $C_j - \alpha_{11}^{-1}C_1$, ta quy về một ma trận dạng: $\begin{pmatrix} 1 & 0 & \cdots & 0 \\ \vdots & & A_1 & \end{pmatrix}$, trong đó $A_1 \in \mathbf{M}_{n-1,p-1}(K)$ và $\mathrm{rank}(A_1) = r - 1$.

Lặp lại đối với A_1.

Như vậy, tồn tại một dãy hữu hạn những phép biến đổi sơ cấp trên các hàng và các cột quy A về một ma trận T có dạng : $T = \begin{pmatrix} 1 & 0 & \\ & \ddots & 0 \\ & \cdots & 1 \\ & \cdots & 0 \end{pmatrix}$.

Bằng các phép biến đổi sơ cấp trên hàng ($C_2 \leftarrow C_2 - t_{21}C_1, \ldots$), ta quy về

$$J_{n,p,r} = \begin{pmatrix} 1 & & 0 & \\ & \ddots & & 0 \\ 0 & & 1 & \\ & 0 & & 0 \end{pmatrix}.$$

Đặc biệt, ta gặp lại Mệnh đề 2 của 8.2.3, 2).

b) (i) $\Rightarrow$ (ii) :

Nếu $\text{rank}(A) = \text{rank}(B)$, theo a), ta có thể đưa A và B về $J_{n,p,r}$ bằng những phép biến đổi sơ cấp, do vậy có thể đưa A về B bằng những phép biến đổi sơ cấp.

(ii) $\Rightarrow$ (i): Xem 8.1.7, Mệnh đề.

c) Giả sử $A \in \mathbf{GL}_n(K)$. Vì $\text{rank}(A) = n$ nên theo b), có thể đưa A về $J_{n,n,n} = I_n$ bằng những phép biến đổi sơ cấp, do vậy A là một tích những ma trận của những phép biến đổi sơ cấp (và các nghịch đảo, chúng thuộc cùng loại).

8.2.5 Đặt $p = \dim(E)$, $n = \dim(F)$, $r = \text{rank}(f)$, $r' = \text{rank}(g)$.

a) Theo 8.2.3, 2), Mệnh đề 2, tồn tại các cơ sở $\mathcal{B}$, $\mathcal{B}'$ của E, và $\mathcal{C}$, $\mathcal{C}'$ của F sao cho:

$$\text{Mat}_{\mathcal{B},\mathcal{C}}(f) = J_{n,p,r}, \ \text{Mat}_{\mathcal{B}',\mathcal{C}'} = J_{n,p,r'}.$$

α) Xét $h \in \mathcal{L}(F)$, $k \in \mathcal{L}(E)$ xác định bởi: $\text{Mat}_{\mathcal{B}',\mathcal{B}}(k) = J_{p,p,r'}$, $\text{Mat}_{\mathcal{C},\mathcal{C}'}(h) = I_n$.

Ta có: $\text{Mat}_{\mathcal{B}',\mathcal{C}'}(h \circ g) = (\text{Mat}_{\mathcal{C},\mathcal{C}'}(h))(\text{Mat}_{\mathcal{B},\mathcal{C}}(g) = I_n J_{n,p,r} = J_{n,p,r'}$.

$\text{Mat}_{\mathcal{B}',\mathcal{C}'}(f \circ k) = (\text{Mat}_{\mathcal{B},\mathcal{C}}(f))(\text{Mat}_{\mathcal{B}',\mathcal{B}}(k) = J_{n,p,r} J_{n,p,r'}$.

Vì $r' \leq r$, ta có $J_{n,p,r} J_{n,p,r'} = J_{n,p,r'}$, do đó $\text{Mat}_{\mathcal{B}',\mathcal{C}'}(h \circ g) = \text{Mat}_{\mathcal{B}',\mathcal{C}'}(f \circ k)$ nên $h \circ g = f \circ k$.

Hơn nữa, rõ ràng $h \in \mathcal{GL}(F)$.

β) Tương tự như α).

b) Cũng phương pháp như trong lời giải của a) α), bằng cách lấy: $\text{Mat}_{\mathcal{B}',\mathcal{B}}(k) = I_p$, $\text{Mat}_{\mathcal{C},\mathcal{C}'}(h) = I_n$.

8.2.6 Nhận xét rằng $S(A) = \text{tr}(A)^2$, do đó:

$S(P^{-1}AP) = \text{tr}(P^{-1}AP)(P^{-1}AP)) = \text{tr}(P^{-1}A^2P) = \text{tr}(A^2) = S(A)$.

8.2.7 Nhận xét rằng: $A^2 \neq 0$ và $B^2 = 0$.

◇ **Trả lời**: Không.

8.3.1 Rõ ràng là $\forall P \in \mathbb{C}_n[X]$, $P[X] + P'\left(\frac{X}{2}\right) + \ldots + P^{(n)}\left(\frac{X}{2^n}\right) \in \mathbb{C}_n[X]$ và ánh xạ $f: \mathbb{C}_n[X] \to \mathbb{C}_n[X]$ xác định bởi: $\forall P \in \mathbb{C}_n[X]$, $f(P) = P(X) + \ldots + P^{(n)}\left(\frac{X}{2^n}\right)$ tuyến tính.

Hơn nữa, $\mathrm{Mat}_{(1,X,\ldots,X^n)}(f) = \begin{pmatrix} 1 & & \cdots \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ là tam giác trên với các hệ số chéo khác không, và khả nghịch.

Như vậy, f là song ánh, từ đó suy ra kết quả muốn chứng minh.

Xem thêm bài tập 7.3.1.

8.3.2 • Giả sử A lũy linh. Tồn tại $k \in \mathbb{N}^*$ sao cho $A^k = 0$. Vì các hạng tử chéo của A^k là $a_{ii}^k = 0$ $(1 \le i \le n)$, xem 8.3.2, Nhận xét 2, nên : $\forall i \in \{1, \ldots, n\}$, $a_{ii} = 0$.

• Ngược lại, giả sử: $\forall i \in \{1, \ldots, n\}$, $a_{ii} = 0$. Thế thì:

$$A = \begin{pmatrix} 0 & & \cdots \\ & \ddots & \\ 0 & & 0 \end{pmatrix}, A^2 = \begin{pmatrix} 0 & 0 & & \cdots \\ & 0 & & \\ & & \ddots & \\ & & & 0 \end{pmatrix}, \ldots, A^{n-1} = \begin{pmatrix} 0 & \cdots & 0 & * \\ & \ddots & & 0 \\ & & \ddots & \vdots \\ 0 & & & 0 \end{pmatrix}$$

$$A^n = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & 0 & \vdots \\ 0 & \cdots & 0 \end{pmatrix} = 0.$$

8.3.3 1) $\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & c+x & b+cx+y \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{pmatrix} \in G$.

2) $I_3 \in G$.

3) $\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$ khả nghịch và nghịch đảo của nó có dạng: $\begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}$, xem 8.3.2, Mệnh đề 4, nên thuộc G.

b) Cho $A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in G$. Ta có :

$$(\forall M \in G, AM = MA) \Leftrightarrow (\forall (x, y, z) \in K^3, b + cx + y = y + za + b)$$
$$\Leftrightarrow (\forall (x, y, z) \in K^3, cx = za) \Leftrightarrow a = c = 0.$$

◇ **Trả lời:** $\left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},\ b \in K \right\}$

8.3.4 1) Giả sử A thích hợp. Nói riêng: $\forall (i, j) \in \{1,...,n\}^2$, $(i \leq j \Rightarrow AE_{ij} = E_{ij}A)$. Đặt $A = (a_{kl})_{kl}$. Với mọi i, j, u, v sao cho $i \leq j$, ta có:

$$\sum_{l=1}^{n} a_{ul}\delta_{li}\delta_{vj} = \sum_{l=1}^{n} \delta_{ul}\delta_{lj}a_{iv} ,$$

nghĩa là $a_{ui}\delta_{vj} = \delta_{ui}a_{jv}$.

Cho $(u, v) \in \{1, ..., n\}^2$ sao cho $u \neq v$.

Lấy $i = j = v$, ta suy ra $a_{uv} = 0$. Nếu $u < v$, lấy $i = u, j = v$, ta suy $a_{uu} = a_{vv}$.

Như vậy tồn tại $\alpha \in K$ sao cho $A = \alpha I_n$.

2) Phần đảo là hiển nhiên.

◇ **Trả lời**: $K\mathbf{I}_n$.

8.3.5 1) Giả sử A thích hợp. Nói riêng: $\forall i \in \{1,...,n\}$, $AE_{ii} = E_{ii}A$.

Đặt $A = (a_{kl})_{kl}$. Với mọi i, u, v thuộc $\{1,...,n\}$, ta có: $\sum_{l=1}^{n} a_{ul}\delta_{li}\delta_{vi} = \sum_{l=1}^{n} \delta_{ui}\delta_{li}a_{iv}$,

nghĩa là: $a_{ui}\,\delta_{vi} = \delta_{ui}a_{iv}$.

Giả sử $(u, v) \in \{1,...,n\}^2$ sao cho $u \neq v$.

Chọn $i = v$, suy ra $a_{uv} = 0$.

2) Ngược lại, nếu A là ma trận chéo, thì A giao hoán với mọi ma trận chéo (xem 8.3.3, Mệnh đề 1).

◇ **Trả lời**: $\mathbf{D}_n(K)$.

8.3.6 1) Giả sử $A = (a_{ij})_{ij}$ thích hợp. Thế thì ta có:

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}=\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix},$$

nghĩa là $\begin{pmatrix} a_{11}\lambda_1 & \cdots & a_{1n}\lambda_n \\ \vdots & & \vdots \\ a_{n1}\lambda_1 & \cdots & a_{nn}\lambda_n \end{pmatrix}=\begin{pmatrix} \lambda_1 a_{11} & \cdots & \lambda_1 a_{1n} \\ \vdots & & \vdots \\ \lambda_n a_{n1} & \cdots & \lambda_n a_{nn} \end{pmatrix}$

hoặc: $\forall (i, j) \in \{1,...,n\}^2$, $(\lambda_i - \lambda_j)a_{ij} = 0$.

Vì $\lambda_1,...,\lambda_n$ khác nhau từng đôi một, suy ra: $\forall i,j \in \{1,...,n\}^2$, $(i \neq j \Rightarrow a_{ij} = 0)$, và vì vậy A là ma trận chéo.

2) Ngược lại, mọi ma trận chéo giao hoán với D (xem 8.3.3, Mệnh đề 1).

◇ **Trả lời**: $\mathbf{D}_n(K)$.

C.8.1 I Giả sử $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbf{M}_{n,1}(\mathbf{R})$ sao cho $AX = 0$, nghĩa là:

$$\begin{cases} \alpha_1 x_1 + \beta x_2 + \cdots + \beta x_n = 0 \\ \vdots \\ \beta x_1 + \cdots + \beta x_{n-1} + \alpha_n x_n = 0 \end{cases}$$

Đặt $S = x_1 + ... + x_n$, suy ra $\beta S = (\beta - \alpha_1)x_1 = ... = (\beta - \alpha_n)x_n$.

• Nếu không tồn tại một i nào thuộc $\{1,..., n\}$ sao cho $\alpha_i = \beta$, thì: $\forall i \in \{1,..., n\}$, $\beta - \alpha_i < 0$, và vì vậy $x_1, ..., x_n$ có cùng dấu theo nghĩa rộng, nghĩa là: $(x_1, ..., x_n) \in (\mathbb{R}_+)^n$ hoặc $(x_1, ..., x_n) \in (\mathbb{R}_-)^n$.

Nhưng khi đó, trong trường hợp thứ nhất, ta sẽ có $S \geq 0$, rồi $x_1 = \dfrac{\beta S}{\beta - \alpha_1} \leq 0, \cdots, x_n = \dfrac{\beta S}{\beta - \alpha_n} \leq 0$, nên $x_1 = ... = x_n = 0$, $X = 0$. Tương tự đối với trường hợp thứ hai.

• Nếu tồn tại một và chỉ một chỉ số i_0 thuộc $\{1,...,n\}$ sao cho $\alpha_{i_0} = \beta$, thì $S = \dfrac{\beta - \alpha_{i_0}}{\beta} x_{i_0} = 0$, nên:

$$\forall i \in \{1,...,n\} - \{i_0\},\ x_i = \frac{\beta S}{\beta - \alpha_i} = 0,$$

rồi: $x_{i_0} = S - \sum_{\substack{1 \leq i \leq n \\ i \neq i_0}} x_i = 0$, và do vậy $X = 0$.

Điều đó chứng tỏ: $\forall X \in M_{n,1}(\mathbb{R})$, $(AX = 0 \Rightarrow X = 0)$, và do vậy: $A \in \mathbf{GL}_n(\mathbf{R})$.

II 1) • Đặt $A = (a_{ij})_{ij}$. Với mọi (i, j) thuộc $\{1,...,n\}^2$, ta có:

$$\begin{aligned} a_{ij} &= \sum_{k=1}^{p} b_{ki} b_{kj} = \mathrm{Card}\left\{k \in \{1,\ldots,p\}; b_{ki} = b_{kj} = 1\right. \\ &= \mathrm{Card}\{k \in \{1,...,p\};\ u_k \in A_i \text{ và } u_k \in A_j\} \\ &= \mathrm{Card}(A_i \cap A_j). \end{aligned}$$

• Theo giả thiết: $\begin{cases} \forall (i,j) \in \{1,\cdots,n\}^2, (i \neq j \Rightarrow a_{ij} = \mathrm{Card}(A_i \cap A_j) = \beta) \\ \forall (i,j) \in \{1,\cdots,n\}^2, a_{ii} = \mathrm{Card}(A_i) \geq \mathrm{Card}(A_i \cap A_j) = \beta \end{cases}$

Giả sử tồn tại ít nhất hai chỉ số i_1, i_2 thuộc $\{1,...,n\}$, khác nhau, sao cho $a_{i_1 i_1} = a_{i_2 i_2} = \beta$.

Khi đó ta có: $\mathrm{Card}(A_{i_1}) = \mathrm{Card}(A_{i_2}) = \mathrm{Card}(A_{i_1} \cap A_{i_2})$, do đó, vì A_{i_1} và A_{i_2} là hữu hạn, nên $A_{i_1} = A_{i_2}$, mâu thuẫn.

Như vậy, A thỏa mãn các thiết của I, do đó $A \in \mathbf{GL}_n(\mathbb{R})$.

2) Vì $A \in \mathbf{GL}_n(\mathbb{R})$: $n = \mathrm{rank}(A)$.

Mặt khác, vì $\mathrm{Im}(A) = \mathrm{Im}({}^tBB) \subset \mathrm{Im}({}^tB)$ (cũng có thể xem bài tập 7.2.9) ta có:

$$\mathrm{rank}(A) = \dim(\mathrm{Im}(A)) \leq \dim(\mathrm{Im}({}^tB)) = \mathrm{rank}({}^tB).$$

Và vì ${}^tB \in \mathbf{M}_{n,p}(\mathbb{R})$: $\mathrm{rank}({}^tB) \leq p$.

Như vậy: $n \leq p$.

Chỉ dẫn và trả lời
các bài tập chương 9

9.4.1 $$|\det(A)| = \left|\sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1)1}\cdots a_{\sigma(n)n}\right| \le \sum_{\sigma\in\mathfrak{S}_n} |a_{\sigma(1)1}|\cdots|a_{\sigma(n)n}|$$

$$\le \sum_{(i_1,\ldots,i_n)\in\{1,\ldots,n\}^n} |a_{i_1 1}|\cdots|a_{i_n n}| = \prod_{j=1}^{n}\left(\sum_{i=1}^{n}|a_{ij}|\right),$$

bằng cách khai triển tích của n tổng gồm n hạng tử.

9.4.2 a) $AB = -BA \Rightarrow \det(AB) = (-1)^n \det(AB) \Leftrightarrow \det(A)\det(B) = (-1)^n \det(B)\det(A)$

$\Leftrightarrow 1 = (-1)^n \Leftrightarrow n$ chẵn

b) ◇ **Trả lời:** $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; $B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

9.4.3 a) • $\mathbf{SL}_n(K) \subset \mathbf{GL}_n(K)$, vì $\det(A) = 1 \Rightarrow \det(A) \neq 0$

• Nếu $A, B \in \mathbf{SL}_n(K)$ thì $\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1$, vì vậy $AB \in \mathbf{SL}_n(K)$

• $\mathrm{I}_n \in \mathbf{SL}_n(K)$ vì $\det(\mathrm{I}_n) = 1$.

• Nếu $A \in \mathbf{SL}_n(K)$, thì $\det(A^{-1}) = (\det(A))^{-1} = 1^{-1} = 1$, vì vậy $A^{-1} \in \mathbf{SL}_n(K)$.

b) Giả sử $A \in \mathbf{GL}_n(K)$. Tồn tại $\alpha \in \mathbb{C}^*$ sao cho $\alpha^n = \det(A)$; đặt $B = \frac{1}{\alpha}A$, khi đó ta có:

$\det(B) = \frac{1}{\alpha^n}\det(A) = 1$, do vậy $B \in \mathbf{SL}_n(K)$.

9.4.4 Giả sử A thích hợp.

• Lấy $M = A$, ta có $2^n \det(A) = 2\det(A)$, do đó, vì $n \geq 2$ nên $\det(A) = 0$.

Như vậy ta có: $\forall M \in \mathbf{M}_n(\mathbb{C})$, $\det(A + M) = \det(M)$.

• Ký hiệu các cột của A là $C_1, \ldots, C_n$.

Giả sử $A \neq 0$; tồn tại $j \in \{1, \ldots, n\}$ sao cho $C_j \neq 0$. Theo định lý về cơ sở không đầy đủ, tồn tại các cột $V_1, \ldots, V_{j-1}, V_{j+1}, \ldots, V_n$ của $\mathbf{M}_{n,1}(C)$ sao cho $(V_1, \ldots, V_{j-1}, C_j, V_{j+1}, \ldots, V_n)$ là một cơ sở của $\mathbf{M}_{n,1}(\mathbb{C})$.

Gọi M là ma trận có các cột là $V_1, \ldots, V_{j-1}, -C_j, V_{j+1}, \ldots, V_n)$, khi đó ta có:

$$\begin{cases} \det(A + M) = 0 \quad \text{(vì cột thứ } j \text{ bằng không)} \\ \det(M) \neq 0 \end{cases}, \text{ mâu thuẫn}$$

Vậy $A = 0$.

Phần đảo là hiển nhiên.

◇ **Trả lời:** $\{0\}$.

9.4.5 a) Vì $AB = BA$, ta có $A^2 + B^2 = (A + iB)(A - iB)$, nên:

$$\det(A^2 + B^2) = \det(A + iB)\det(A - iB) = \det(A + iB)\overline{\det(A + iB)} = |\det(A + iB)|^2 \geq 0.$$

b) ◇ **Trả lời:** • Có, nếu $n = 1$

• không, nếu $n \geq 2$; chẳng hạn $A = \begin{pmatrix} 1 & -2 \\ 2 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}$.

9.4.6 Ánh xạ $P: \begin{array}{c} \mathbb{R} \to \mathbb{R} \\ x \mapsto \det(A + xB) \end{array}$ là ánh xạ đa thức, do vậy liên tục.

Vì $P(x) \underset{x \to 0}{\to} P(0) = \det(A) \neq 0$, nên tồn tại $\varepsilon > 0$ sao cho:

$$\forall x \in \mathbb{R},\ (|x| < \varepsilon \Rightarrow P(x) \neq 0 \Rightarrow A + xB \in \mathbf{GL}_n(\mathbb{R})).$$

9.4.7 a) Quy nạp theo k.

• Hiển nhiên với $k = 0$.

• Nếu $AB^k = B^k(A + kI_n)$, thì:

$$AB^{k+1} = AB^k B = B^k(A + kI_n)B = B^k(AB + kB) = B^k(BA + B + kB) = B^{k+1}(A + (k+1)I_n).$$

b) Lập luận phản chứng: Giả thiết $\det(B) \neq 0$, khi đó từ a) suy ra:

$$\forall k \in \mathbb{N},\ \det(A) = \det(A + kI_n).$$

Nhưng, sau khi khai triển, $\begin{array}{c} \mathbb{R} \to \mathbb{R} \\ x \mapsto \det(A + xI_n) \end{array}$ là một đa thức bậc n với hệ số của x^n là 1 (số hạng duy nhất chứa x^n xuất phát từ hạng tử của khai triển định thức ứng với hoán vị đồng nhất). Vì vậy $\det(A + kI_n) \underset{k \to \infty}{\to} \infty$, mâu thuẫn.

◇ **Trả lời:** $\operatorname{com}(A) = \begin{pmatrix} \det(M) & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \mathbf{0} & \\ 0 & & & \end{pmatrix}$.

9.5.2 Vì $A^p = I_n$ và $p \in \mathbb{N}^*$ nên A khả nghịch, do đó:

$$(\operatorname{com}(A))^p = (\det(A)\,{}^t(A^{-1}))^p = (\det(A))^p\,{}^t(A^{-1})^p = \det(A^p)\,{}^t(A^p)^{-1} = I_n.$$

9.5.3 Vì A khả nghịch nên:

$$\operatorname{com}(A^{-1}) = \det(A^{-1})\,{}^t(A^{-1})^{-1}) = (\det(A)\,{}^tA^{-1})^{-1} = (\operatorname{com}(A))^{-1}.$$

9.6.1 a) $\begin{vmatrix} 1^2 & 2^2 & 3^2 & \cdots & n^2 \\ 2^2 & 3^2 & 4^2 & \cdots & (n+1)^2 \\ \vdots & \vdots & \vdots & & \vdots \\ n^2 & (n+1)^2 & (n+2)^2 & \cdots & (2n-1)^2 \end{vmatrix} = \begin{vmatrix} 1^2 & 3 & 5 & \cdots & 2n-1 \\ 2^2 & 5 & 7 & \cdots & 2n+1 \\ \vdots & \vdots & \vdots & & \vdots \\ n^2 & 2n+1 & 2n+3 & \cdots & 4n-3 \end{vmatrix}$

bởi $C_j \leftarrow C_j - C_{j-1}$ với $j \geq 2$

$$= \begin{vmatrix} 1^2 & 3 & 2 & -2 \\ 2^2 & 5 & 2 & -2 \\ \vdots & \vdots & | & | \\ n^2 & 2n+1 & 2 & -2 \end{vmatrix}$$ bởi $C_j \leftarrow C_j - C_{j-1}$ với $j \geq 3$.

◇ **Trả lời :** $\begin{cases} 0 & \text{nếu } n \geq 3 \\ -7 & \text{nếu } n = 2 \\ 1 & \text{nếu } n = 1 \end{cases}$.

b) Thực hiện đồng thời: $C_2 \leftarrow C_2 - C_1$, $C_3 \leftarrow C_3 - C_2$, ..., $C_n \leftarrow C_n - C_{n-1}$ việc này quy về việc thực *liên tiếp* : $C_n \leftarrow C_n - C_{n-1}$,..., $C_3 \leftarrow C_3 - C_2$, $C_2 \leftarrow C_2 - C_1$:

$$\begin{vmatrix} S_1 & S_1 & S_1 & \cdots & S_1 \\ S_1 & S_2 & S_2 & \cdots & S_2 \\ S_1 & S_2 & S_3 & \cdots & S_3 \\ | & | & | & \ddots & \vdots \\ S_1 & S_2 & S_3 & \cdots & S_n \end{vmatrix} = \begin{vmatrix} S_1 & 0 & \cdots & 0 \\ | & S_2 - S_1 & \ddots & 0 \\ | & 1 & \ddots & \\ S_1 & S_2 - S_1 & \cdots & S_n - S_{n-1} \end{vmatrix}$$

◇ **Trả lời** : $n!$

c) Thực hiện đồng thời: $C_2 \leftarrow C_2 - C_1, C_3 \leftarrow C_3 - C_2, \ldots, C_n \leftarrow C_n - C_{n-1}$, sau đó khai triển theo dòng cuối cùng.

◇ **Trả lời** : $(-1)^{n+1} a_1 (a_2 - a_1)^{n-1}$.

d) Khai triển theo tính chất đa tuyến tính và thay phiên:

$$\begin{vmatrix} a_1 + b_1 & a_1 & \cdots & a_n \\ a_2 & a_2 + b_2 & \cdots & a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_n & a_n & \cdots & a_n + b_n \end{vmatrix} = \begin{vmatrix} b_1 & & & 0 \\ & \ddots & & \\ & & & \\ 0 & & & b_n \end{vmatrix} + \begin{vmatrix} a_1 & 0 & & \\ a_2 & b_2 & 0 & \\ \vdots & & \ddots & \\ a_n & 0 & & b_n \end{vmatrix} + \begin{vmatrix} b_1 & a_1 & 0 & \\ 0 & a_2 & 0 & \\ | & \vdots & b_3 & \ddots \\ | & | & \ddots & b_n \\ 0 & a_n & 0 & \end{vmatrix}$$

$$+ \ldots + \begin{vmatrix} b_1 & & & a_1 \\ & \ddots & 0 & \vdots \\ & 0 & b_{n-1} & \vdots \\ & & & a_n \end{vmatrix}$$

◇ **Trả lời** : $b_1 \ldots b_n + a_1 b_2 \ldots b_n + b_1 a_2 b_3 \ldots b_n + \ldots + b_1 \ldots b_{n-1} a_n$.

Nếu $b_1 \ldots b_n \neq 0$, có thể viết kết quả dưới dạng: $b_1 \ldots b_n \left(1 + \frac{a_1}{b_1} + \ldots + \frac{a_n}{b_n}\right)$.

e) Gọi Δ_n là định thức cần tính, thay C_n bởi $C_1 + ... + C_n$, ta được:

$$\Delta_n = \begin{vmatrix} a_1 & -a_1 & & & 0 \\ -a_1 & a_1+a_2 & & & \\ & & & -a_{n-2} & \\ 0 & & -a_{n-2} & a_{n-2}+a_{n-1} & 0 \\ & & 0 & -a_{n-1} & a_n \end{vmatrix} = a_n\Delta_{n-1}.$$

◇ **Trả lời:** $\prod_{k=1}^{n} a_k$.

f) Đặt $\Delta_n = \begin{vmatrix} a & b & & & 0 \\ c & a & b & & \\ & \ddots & \ddots & \ddots & \\ & & \ddots & a & b \\ 0 & & & c & a \end{vmatrix}_{[n]}$

Với $n \geq 3$, trước hết ta khai triển theo dòng thứ nhất để được:

$$\Delta_n = a\Delta_{n-1} - b\begin{vmatrix} c & b & & & \\ 0 & a & b & 0 & \\ & c & \ddots & \ddots & \\ & & \ddots & a & b \\ 0 & & 0 & c & a \end{vmatrix}_{[n-1]} = a\Delta_{n-1} - bc\Delta_{n-2}.$$

Xét các dãy truy hồi tuyến tính cấp 2 với hệ số hằng (tập 1, 3, 4, 2). Phương trình đặc trưng là $r^2 - ar + bc = 0$ với biệt thức $\delta = a^2 - 4bc$

Trường hợp thứ nhất: $\delta \neq 0$

Phương trình đặc trưng có hai nghiệm phân biệt r_1, r_2, và tồn tại $(\lambda_1, \lambda_2) \in \mathbb{C}^2$ sao cho:

$$\forall n \in \mathbb{N}^*, \Delta_n = \lambda_1 r_1^n + \lambda_2 r_2^n.$$

Ta chú ý là có thể đặt $\Delta_0 = 1$ để hệ thức $\Delta_n = n\Delta_{n-1} - bc\Delta_{n-2}$ cũng đúng cho $n = 2$. Khi đó:

$$\begin{cases} \Delta_0 = 1 \\ \Delta_1 = a \end{cases} \Leftrightarrow \begin{cases} \lambda_1 + \lambda_2 = 1 \\ \lambda_1 r_1 + \lambda_2 r_2 = a \end{cases} \Leftrightarrow \begin{cases} \lambda_1 = \dfrac{r_1}{r_2 - r_1} \\ \lambda_2 = \dfrac{r_2}{r_2 - r_1} \end{cases}.$$

Do đó: $\Delta_n = \dfrac{1}{r_1 - r_2}(r_1^{n+1} - r_2^{n+1})$.

Trường hợp thứ hai: $\delta = 0$

Phương trình đặc trưng có một nghiệm "kép" bằng $\dfrac{a}{2}$ và tồn tại $(\lambda, \mu) \in \mathbb{C}^2$ sao cho:

$$\forall n \in \mathbb{N}, \quad \Delta_n = (\lambda n + \mu)\left(\frac{a}{2}\right)^n.$$

Khi đó: $\begin{cases} \Delta_0 = 1 \\ \Delta_1 = a \end{cases} \Leftrightarrow \begin{cases} \mu = 1 \\ (\lambda + \mu)\dfrac{a}{2} = a \end{cases} \Leftrightarrow \lambda = \mu = 1$

◇ **Trả lời:** • Nếu $a^2 - 4bc \neq 0$ gọi r_1, r_2 là hai không điểm của $X^2 - aX + bc$ trong $\mathbb{C}$, ta có:

$$\forall n \in \mathbb{N}, \ \Delta_n = \frac{1}{r_1 - r_2}(r_1^{n+1} - r_2^{n+1}).$$

• Nếu $a^2 - 4bc = 0$, thì $\forall n \in \mathbb{N}, \Delta_n = (n+1)\left(\frac{a}{2}\right)^n$.

Có thể tổng hợp các đáp số của hai trường hợp dưới dạng: $\Delta_n = \sum_{k=0}^{n} r_1^k r_2^{n-k}$.

g) Gọi Δ_n là định thức cần tính:

$$\Delta_n = \begin{vmatrix} C_0^0 & 0 & \cdots & 0 \\ C_1^0 & C_1^1 & \cdots & C_n^n \\ C_2^0 & C_2^1 & \cdots & C_{n+1}^n \\ \vdots & \vdots & & \vdots \\ C_n^0 & C_n^1 & \cdots & C_{2n-1}^n \end{vmatrix} \quad \text{bởi } C_j \leftarrow C_j - C_{j-1} \text{ với } j \geq 2$$

$$= \begin{vmatrix} C_0^0 & 0 & \cdots & 0 \\ 0 & C_1^1 & \cdots & C_n^n \\ \vdots & C_1^0 & \cdots & C_n^{n-1} \\ & \vdots & & \vdots \\ 0 & C_{n-1}^0 & \cdots & C_{2n-2}^n \end{vmatrix} \quad \text{bởi } D_i \leftarrow D_i - D_{i-1} \text{ với } i \geq 2$$

$= \Delta_{n-1}$.

◇ **Trả lời** : 1

h) Gọi Δ_n là định thức cần tính. Khai triển theo dòng cuối cùng:

$$\Delta_n = \alpha\Delta_{n-1} + (-1)^{n+1} a_n \begin{vmatrix} -1 & 0 \\ \alpha & \\ 0 & \alpha - 1 \end{vmatrix} = \alpha\Delta_{n-1} + a_n.$$

◇ **Trả lời :** $\sum_{k=0}^{n} \alpha^k a_{n-k}$ (nếu đặt $a_0 = 1$).

i) Gọi Δ_n là định thức cần tính. Khai triển theo dòng cuối cùng ta có:

$$\Delta_n = b_n\Delta_{n-1} + (-1)^{n+2} a_n \begin{vmatrix} -a_1 & \cdots & \cdots & \cdots & -a_n \\ b_1 & 0 & & 0 & \\ & \ddots & & & \\ & 0 & \ddots & & \\ & & & b_{n-1} & 0 \end{vmatrix}_{(n)}$$

$$= b_n\Delta_{n-1} + (-1)^{n+2} a_n (-1)^{n+1} (-a_n) b_1 \ldots b_{n-1} a_n^2$$

Cộng lại sau khi đã nhân với các hệ số:

$$\begin{aligned} \Delta_n &= b_n \Delta_{n-1} + b_1 \ldots b_{n-1} a_n^2 && 1 \\ \Delta_{n-1} &= b_{n-1} \Delta_{n-2} + b_1 \ldots b_{n-2} a_{n-2}^2 && b_n \\ \Delta_{n-2} &= b_{n-2} \Delta_{n-3} + b_1 \ldots b_{n-3} a_{n-2}^2 && b_{n-1} b_n \\ &\vdots && \vdots \\ \Delta_1 &= b_1 + a_1^2 && b_2 \ldots b_n \end{aligned}$$

◇ **Trả lời :** $b_1 \ldots b_{n-1} a_n^2 + b_1 \ldots b_{n-2} a_{n-1}^2 b_n + \ldots + a_1^2 b_2 \ldots b_n + b_1 \ldots b_n$.

Nếu $b_1 \ldots b_n \neq 0$ có thể viết kết quả dưới dạng: $b_1 \ldots b_n \left(1 + \frac{a_1^2}{b_1} + \cdots + \frac{a_n^2}{b_n}\right)$.

j) Chứng minh hệ thức $\Delta_n = z\Delta_{n-1} - xyz^{n-2}$.

◇ **Trả lời :** $az^{n-1} - (n-1)xyz^{n-2}$.

k) Gọi Δ_n là định thức cần tính, ta có:

$$A_n = \begin{vmatrix} -(a+1) & 1 & & & 0 & -a \\ a & \ddots & \ddots & & & 0 \\ & \ddots & \ddots & & n-2 & \vdots \\ & & \ddots & a & -(a+n+1) & 0 \\ 0 & & & 0 & a & -n \end{vmatrix} \quad \text{bởi } C_n \leftarrow C_1 + \ldots + C_n$$

$= (-1)^{n+1}(-a)a^{n-1} - n\Delta_{n-1}$ bằng cách khai triển theo cột cuối cùng.

Đặt $D_n = \dfrac{(-1)^n}{n!}\Delta_n$, ta nhận được: $\forall n \in \mathbb{N} - \{0, 1\}$, $D_n = \dfrac{a^n}{n!} + D_{n-1}$ (và $D_1 = -(a+1)$).

◇ **Trả lời :** $(-1)^n n! \sum_{k=0}^{n} \dfrac{a^k}{k}$.

9.6.2 Đặt $I = \mathbf{I}_3$, $A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 0 \end{pmatrix}$. Vì $A^2 = \begin{pmatrix} 0 & 0 & 1 \\ 2 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}$, nên ta có:

$$E = \{(xI + yA + zA^2);\ (x, y, z) \in \mathbb{Q}^3\}$$

Do đó, rõ ràng E là kgvc của $\mathbf{M}_3(\mathbb{Q})$ sinh bởi (I, A, A^2).

Mặt khác, vì $A^3 = 2I$, tích của hai phần tử của E được phân tích $\mathbb{Q}$-tuyến tính trên I, A, A^2. Ta suy ra E là một vành con của $\mathbf{M}_3(\mathbb{Q})$.

Còn lại phải chứng minh rằng mọi phần tử khác không của E có một nghịch đảo trong E.

Trước hết ta chứng minh : $\forall M \in E$, $(\det(E) = 0 \Rightarrow M = 0)$.

Giả sử $(x, y, z) \in \mathbb{Q}^3$, $M = xI + yA + zA^2$ và giả sử $\det(M) = 0$, nghĩa là sau khi khai triển:

$$x^3 + 2y^3 + 4z^3 - 6xyz = 0.$$

Tồn tại $(\alpha, \beta, \gamma) \in \mathbb{Z}^3$ và $q \in \mathbb{N}^*$ sao cho $x = \dfrac{\alpha}{q}, y = \dfrac{\beta}{q}, z = \dfrac{\gamma}{q}$, do đó:

$$\alpha^3 + 2\beta^3 + 4\gamma^3 - 6\alpha\beta\gamma = 0$$

Bằng phương pháp đi xuống vô hạn, ta sẽ chứng minh rằng phương trình này chỉ có nghiệm (0,0,0).

Giả sử (α, β, γ) là một nghiệm.

Khi đó $2 | \alpha^3$, vì vậy $2 | \alpha$, và do vậy tồn tại $\alpha' \in \mathbb{Z}$ sao cho $\alpha = 2\alpha'$, từ đó suy ra:

$$4\alpha'^3 + \beta^3 + 2\gamma^3 - 6\alpha'\beta\gamma = 0.$$

Tương tự, $2 | \beta$, nên tồn tại $\beta' \in \mathbb{Z}$ sao cho $\beta = 2\beta'$, từ đó suy ra :

$$2\alpha'^3 + 4\beta'^3 + \gamma^3 - 6\alpha'\beta'\gamma = 0.$$

Lại có $2 | \gamma$ nên tồn tại $\gamma' \in \mathbb{Z}$ sao cho $\gamma = \gamma'$ nên:

$$\alpha'^3 + 2\beta'^3 + 4\gamma'^3 - 6\alpha'\beta'\gamma' = 0.$$

nghĩa là $(\alpha', \beta', \gamma')$ là nghiệm.

Như vậy, với mọi nghiệm (α, β, γ), ba số nguyên α, β, γ chia hết cho 2. Bằng cách lặp lại quá trình này, ta suy ra α, β, γ chia hết cho mọi lũy thừa $2^n (n \in \mathbb{N}^*)$ và do vậy $\alpha = \beta = \gamma = 0$.

Cho $M \in E - \{0\}$. Theo kết quả trên, $\det(M) \neq 0$ và do vậy $M \in \mathbf{GL}_3(\mathbb{C})$.

Ánh xạ $f : \begin{matrix} E \to E \\ N \mapsto MN \end{matrix}$ tuyến tính, là đơn ánh (vì M khả nghịch trong $\mathbf{GL}_3(\mathbb{C})$), và E hữu hạn chiều, do vậy f là song ánh. Vì $\mathbf{I}_3 \in E$ nên tồn tại $N \in E$ sao cho $MN = \mathbf{I}_3$, nghĩa là : $M^{-1} \in E$.

9.6.3 a) $\begin{cases} abc < 0 \\ def < 0 \\ ghk < 0 \end{cases} \Rightarrow abcdefghk < 0$, và $\begin{cases} adh > 0 \\ beh > 0 \\ cfk > 0 \end{cases} \Rightarrow abcdefghk > 0$.

b) $\begin{cases} aek > 0 \\ bfg > 0 \\ cdh > 0 \end{cases} \Rightarrow abcdefghk > 0$, và $\begin{cases} -ceg > 0 \\ -afh > 0 \\ -bdk > 0 \end{cases} \Rightarrow abcdefghk < 0$.

9.6.4 Trước hết ta chú ý là f tuyến tính.

Ta nhắc lại rằng $\mathbf{S}_n(\mathbb{R})$ (tập hợp các ma trận đối xứng thực cấp n) và $\mathbf{A}_n(\mathbb{R})$ (tập hợp các ma trận phản đối xứng thực cấp n) bù nhau trong $\mathbf{M}_n(\mathbb{R})$ (xem 8.3.1, Mệnh đề 2).

Trong một cơ sở của $\mathbf{M}_n(\mathbb{R})$ tạo thành bởi một cơ sở của $\mathbf{S}_n(\mathbb{R})$, kế tiếp là một cơ sở của $\mathbf{A}_n(\mathbb{R})$, ma trận của f là:

$$\begin{pmatrix} 1 & & & & \\ & 1 & & 0 & \\ & & -1 & & \\ & 0 & & & \\ & & & & -1 \end{pmatrix}$$, nên : $\det(f) = (-1)^{\dim(\mathbf{A}_n(\mathbb{R}))} = (-1)^{\frac{n(n-1)}{2}}$.

Ngay từ đầu, ta có thể nhận xét rằng, vì f là một phép đối hợp nên: $(\det(f))^2 = \det(f^2) = 1$.

◇ **Trả lời** : $(-1)^{\frac{n(n-1)}{2}}$.

9.6.5 a)

$$\varphi_p(x+1) - \varphi_p(x) = \begin{vmatrix} 1 & 0 & 0 & \cdots & \cdots & (1+x) - x \\ & 2 & 0 & \cdots & \cdots & (1+x)^2 - x^2 \\ & 3 & 3 & & & \vdots \\ & \vdots & \vdots & & C_p^{p-1} & (1+x)^p - x^p \\ 1 & C_{p-1}^1 & C_{p-1}^2 & \cdots & C_{p-1}^{p-1} & (1+x)^{p+1} - x^{p+1} \end{vmatrix}$$

Cột cuối cùng phân tích thành:

$$\begin{pmatrix} (1+x)-x \\ (1+x)^2-x^2 \\ \vdots \\ (1+x)^p-x^p \\ (1+x)^{p+1}-x^{p+1} \end{pmatrix} = \begin{pmatrix} 1 \\ 1+2x \\ 1+3x+3x^2 \\ \vdots \\ \sum_{k=0}^{p} C_{p+1}^k x^k \end{pmatrix} = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} + x\begin{pmatrix} 0 \\ 2 \\ 3 \\ \vdots \\ C_{p+1}^1 \end{pmatrix} + \cdots + x^{p-1}\begin{pmatrix} 0 \\ \vdots \\ 0 \\ C_p^{p-1} \\ C_{p+1}^{p-1} \end{pmatrix} + x^p \begin{pmatrix} 0 \\ \vdots \\ 0 \\ C_{p+1}^p \end{pmatrix}$$

nên do tính chất tuyến tính và thay phiên:

$$\varphi_p(x+1)-\varphi_p(x) = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ & 2 & 0 & & \\ & 3 & 3 & & \\ & \vdots & \vdots & & C_p^{p-1} \quad 0 \\ 1 & C_{p+1}^1 & C_{p+1}^2 & \cdots & C_{p+1}^{p-1} \quad C_{p+1}^p x^p \end{vmatrix} = 1.2.3\ldots p(p+1)x^p$$

◇ **Trả lời**: $(p+1)!x^p$.

b) $\varphi_p(n+1)-\varphi_p(n) = (p+1)!n^p$

$\varphi_p(n)-\varphi_p(n-1) = (p+1)!(n-1)^p$

$\vdots$

$\varphi_p(2)-\varphi_p(1) = (p+1)!1^p$

$\varphi_p(1) = 0$

$$\varphi_p(n+1) = (p+1)!\sum_{k=1}^{n} k^p$$

c) 1) $$\sum_{k=1}^{n} k = \frac{1}{2!}\varphi_1(n+1) = \frac{1}{2}\begin{vmatrix} 1 & n+1 \\ 1 & (n+1)^2 \end{vmatrix} = \frac{n(n+1)}{2}$$

2) $$\sum_{k=1}^{n} k^2 = \frac{1}{3!}\varphi_2(n+1) = \frac{1}{6}\begin{vmatrix} 1 & 0 & n+1 \\ 1 & 2 & (n+1)^2 \\ 1 & 3 & (n+1)^3 \end{vmatrix} = \frac{n+1}{6}\begin{vmatrix} 1 & 0 & 0 \\ 1 & 2 & n \\ 1 & 3 & n^2+2n \end{vmatrix} = \frac{n(n+1)(2n+1)}{6}$$

3) $$\sum_{k=1}^{n} k^3 = \frac{1}{4!}\varphi_3(n+1) = \frac{1}{24}\begin{vmatrix} 1 & 0 & 0 & n+1 \\ 1 & 2 & 0 & (n+1)^2 \\ 1 & 3 & 3 & (n+1)^3 \\ 1 & 4 & 6 & (n+1)^4 \end{vmatrix}$$

$$= \frac{n+1}{24}\begin{vmatrix} 1 & 0 & 0 & 0 \\ 1 & 2 & 0 & n \\ 1 & 3 & 3 & n^2+2n \\ 1 & 4 & 6 & n^3+3n^2+3n \end{vmatrix} = \frac{n(n+1)}{4}\begin{vmatrix} 2 & 0 & 1 \\ 3 & 3 & n+2 \\ 4 & 6 & n^2+3n+3 \end{vmatrix} = \frac{n^2(n+1)^2}{4}$$

◇ **Trả lời**: $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$, $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$, $\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$.

9.6.6 Khai triển theo tính chất đa tuyến và thay phiên (như trong lời giải của bài tập 9.6.1 *d*)), ta được:

$$\det(A) = x_1 \ldots x_n + x_2 \ldots x_n + x_1 x_3 \ldots x_n + \ldots + x_1 \ldots x_{n-1} = \sigma_n + \sigma_{n-1},$$

trong đó $\sigma_1,\ldots,\sigma_n$ là các hàm đối xứng sơ cấp của $x_1,\ldots,x_n$ (xem 5.3.2, Định nghĩa 2). Vì $x_1,\ldots,x_n$ là các không điểm của $X^n - X + 1$, ta có (xem 5.3.2 Mệnh đề): $\sigma_{n-1} = (-1)^n$ và $\sigma_n = (-1)^n$

◇ **Trả lời :** $2(-1)^n$.

9.6.7 Rõ ràng ánh xạ $\varphi : E^n \to K$ xác định bởi:

$$\forall (V_1,\ldots,V_n) \in E^n,\ \varphi(V_1,\ldots,V_n) = \sum_{j=1}^{n} \det_{\mathcal{B}}(V_1,\ldots,f(V_j),\ldots,V_n)$$

là một dạng n - tuyến tính thay phiên.

Theo 9.2.2. Mệnh đề 1, ta có: $\forall (V_1,\ldots,V_n) \in E^n,\ \varphi(V_1,\ldots,V_n) = \det_{\mathcal{B}}(V_1,\ldots,V_n)\,\varphi(\mathcal{B})$.

Mặt khác, nếu ký hiệu ma trận của f trong $\mathcal{B}$ là $A = (a_{ij})_n$ ta có:

$$\varphi(\mathcal{B}) = \sum_{j=1}^{n} \begin{vmatrix} 1 & & & 0 & a_{1j} & & \\ & \ddots & & & \vdots & & 0 \\ & & 1 & & a_{ij} & & \\ & 0 & & & \vdots & 1 & \\ & & & & a_{nj} & & \ddots \\ & & & & & & & 1 \end{vmatrix} = \sum_{j=1}^{n} a_{jj} = \operatorname{tr}(A) = \operatorname{tr}(f).$$

9.6.8 Vì $\det(A)$ được biểu diễn như là tổng những tích các phần tử của A, nên nếu chuyển qua modulo 2, ta được: $\det(A) \equiv \begin{vmatrix} 1 & & & \\ & \ddots & & 0 \\ & & \ddots & \\ & 0 & & 1 \end{vmatrix} = 1$, và do đó $\det(A) \neq 0$.

9.6.9 Cũng như lời giải của bài tập 9.6.8, nếu chuyển qua modulo 2, ta được:

$$\det(A) \equiv \begin{vmatrix} 0 & & & \\ & \ddots & 1 & \\ & 1 & \ddots & \\ & & & 0 \end{vmatrix}_{[n]}.$$

$$\text{Và} \quad \begin{vmatrix} 0 & & & \\ & \ddots & 1 & \\ & 1 & \ddots & \\ & & & 0 \end{vmatrix}_{[n]} = (n-1) \begin{vmatrix} 1 & 1 & \cdots & 1 \\ 0 & & & \\ & & 1 & \\ & & \ddots & \\ 1 & & & 0 \end{vmatrix} \quad \text{bởi } C_1 \leftarrow C_1 + \ldots + C_n$$

$$= (n-1) \begin{vmatrix} 1 & \cdots & 1 \\ 0 & -1 & \\ & & \ddots \\ 0 & & -1 \end{vmatrix} \quad \text{bởi } D_i \leftarrow D_i - D_1 \text{ với } i \geq 2$$

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

Vì n chẵn: $(n-1)(-1)^{n-1} \equiv 1\ [2]$.

Phương pháp khác: Chứng tỏ rằng có thể áp dụng bài tập 9.6.8 cho A^2, từ đó suy ra $\det(A)^2 \neq 0$ và sau đó $\det(A) \neq 0$.

9.8.1 1) Nếu $\text{rank}(A) \leq n - 2$, thì tất cả các phần phụ đại số của A đều bằng không, vì đó là những định thức của các ma trận vuông cấp $n - 1$ trích ra từ A, xem 9.8, Định lý.

2) Nếu $\text{rank}(A) = n$, thì $\det(A) \neq 0$, và vì $\left(\frac{1}{\det(A)}\ {}^tA\right)\text{com}(A) = I_n$ nên $\text{com}(A)$ khả nghịch, do đó $\text{rank}(\text{com}(A)) = n$.

3) Giả sử $\text{rank}(A) = n - 1$.

Vì ${}^tA({}^t\text{com}(A)) = \det(A)I_n = 0$ nên ta có $\text{Im}({}^t\text{com}(A)) \leq \dim(\text{Ker}(A))$ và do vậy:

$$\text{Rank}(\text{com}(A)) = \text{rank}({}^t\text{com}(A)) \leq \dim(\text{Ker}(A))$$

Nhưng, theo định lý về hạng, $\dim(\text{Ker}(A)) = n - \text{rank}(A) = 1$.

Mặt khác, theo 9.8, Định lý, tồn tại một ma trận vuông cấp $n - 1$ trích ra từ A và khả nghịch, và do vậy ít nhất một trong các phần phụ đại số của A là $\neq 0$, từ đó suy ra $\text{com}(A) \neq 0$.

Ta kết luận: $\text{rank}(\text{com}(A)) = 1$.

9.8.2 Với $p \in \mathbb{N}^*$, ký hiệu $\text{com}_p(A) = \text{com}(...(\text{com}(A))...)$, trong đó com được lặp lại p lần.

a) Ta bắt đầu bằng việc xác định $\text{com}_2(A)$.

1) Nếu $\text{rank}(A) \leq n - 2$, theo bài tập 9.8.1, $\text{com}(A) = 0$, vì vậy $\text{com}_2(A) = 0$.

2) Giả sử $\text{rank}(A) = n$. Khi đó: $\text{com}(A) = \det(A){}^tA^{-1}$, nên:

$\det(\text{com}(A)) = (\det(A))^n(\det(A))^{-1} = (\det(A))^{n-1} \neq 0$,

và vì vậy $\text{com}(A)$ khả nghịch (cũng có thể xem bài tập 9.5.3). Sau đó:

$$\text{com}_2(A) = \text{com}(\text{com}(A)) = \det(\text{com}(A))^{-1}(\text{com}(A))^{-1}$$

$$= (\det(A))^{n-1}(\det(A)^{-1}({}^tA^{-1})^{-1} = (\det(A))^{n-2}A.$$

3) Giả sử $\text{rank}(A) = n - 1$.

Theo bài tập 9.8.1, $\text{rank}(\text{com}(A)) = 1$, do vậy nếu $n \geq 3$, áp dụng bài tập 9.8.1 cho $\text{com}(A)$ thay vì A, ta sẽ có: $\text{com}_2(A) = 0$.

Nếu $n = 2$, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\det(A) = 0$, $\text{com}(A) = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$, $\text{com}_2(A) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = A = (\det(A))^{n-2}A$, vì $0^0 = 1$.

Như vậy ta đã chứng minh: $\forall A \in \mathbf{M}_n(K)$, $\text{com}_2(A) = (\det(A))^{n-2}A$.

b) Ta suy ra: $\text{com}_3(A) = \text{com}((\det(A))^{n-2}A) = (\det(A))^{(n-2)(n-1)}\text{com}(A)$, nhờ công thức hiển nhiên:

$$\forall \lambda \in K, \text{com}(\lambda A) = \lambda^{n-1}\text{com}(A).$$

Sau đó: $\text{com}_4(A) = (\det(A))^{(n-2)(n-1)^2}\text{com}_2(A) = (\det(A))^{(n-2)(1+(n-1)^2)}A$.

Chứng minh kết quả bằng quy nạp.

◇ **Trả lời:**

$(\det(A))^{(n-2)(n-1)(1+(n-1)^2+\cdots+(n-1)^{2k-2})}\operatorname{com}(A)$ nếu p lẻ ≥ 3, $p = 2k+1$, $k \in \mathbb{N}^*$.

$(\det(A))^{(n-2)(1+(n-1)^2+\cdots+(n-1)^{2k-2})}A$ nếu p chẵn, $p = 2k$, $k \in \mathbb{N}^*$.

9.8.3 Ta có $AB = 0 \Rightarrow \operatorname{Im}(B) \subset \operatorname{Ker}A \Rightarrow \operatorname{rank}(B) \leq \dim(\operatorname{Ker}(A)) = n - \operatorname{rank}(A) = 1$.

Nếu $B = 0$, thì $\gamma = 0$ là thích hợp.

Giả sử $B \neq 0$, vì $\operatorname{rank}(B) = 1$, theo bài tập 8.1.31 a), tồn tại $U, V \in M_{n,1}(K)$ sao cho $B = U{}^tV$.

Khi đó: $\begin{cases} AB = 0 \\ BA = 0 \end{cases} \Leftrightarrow \begin{cases} (AU){}^tV = 0 \\ U({}^tVA) = 0 \end{cases}$

Nếu một trong các phần tử của cột AU là $\neq 0$, vì dòng ${}^tV$ là $\neq 0$(nếu không: $B = 0$), thì có ít nhất một phần tử của ma trận vuông $(AU){}^tV$ khác không, mâu thuẫn.

Vì vậy $AU = 0$, tương tự ${}^tVA = 0$, do vậy ${}^tAV = 0$.

Vì $\dim(\operatorname{Ker}(A)) = 1$ và $\dim(\operatorname{Ker}({}^tA) = n\text{-}\operatorname{rank}({}^tA) = n - \operatorname{rank}(A) = 1$, nên ta suy ra rằng U (tương ứng: V) sinh ra $\operatorname{Ker}(A)$ (tương ứng: $\operatorname{Ker}({}^tA)$).

Áp dụng cùng lập luận này cho ${}^t\operatorname{com}(A)$ thay vì B.

Do vậy tồn tại $U_0, V_0 \in M_{n,1}(K)$, $\alpha, \beta \in K - \{0\}$ sao cho: ${}^t\operatorname{com}(A) = U_0{}^tV_0$, $U = \alpha U_0$, $V = \beta V_0$, và do vậy $B = \alpha\beta U_0{}^tV_0 = \alpha\beta\,{}^t\operatorname{com}(A)$.

9.8.4 1) Tính $\operatorname{rank}(A)$

Trước hết ta nhận thấy tổng các cột của A bằng 0, nên $\det(A) = 0$.

Với mọi $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ thuộc $\mathbf{M}_{n,1}(K)$:

$$X \in \operatorname{Ker}(A) \Leftrightarrow \begin{cases} (1-n)x_1 + x_2 + \cdots + x_n = 0 \\ \vdots \\ x_1 + \cdots + x_{n-1} + (1-n)x_n = 0 \end{cases} \Leftrightarrow \begin{cases} x_1 + \cdots + x_n = nx_1 \\ \vdots \\ x_1 + \cdots + x_n = nx_n \end{cases} \Leftrightarrow x_1 = \ldots = x_n$$

Vì vậy, $\dim(\operatorname{Ker}(A)) = 1$, $\operatorname{rank}(A) = n - 1$.

2) Theo bài tập 9.8.1, ta có $\operatorname{rank}(\operatorname{com}(A)) = 1$.

Đặt $B = \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & 1 & \vdots \\ 1 & \cdots & 1 \end{pmatrix} \in \mathbf{M}_n(K)$ rõ ràng ta có $AB = BA = 0$.

Theo bài tập 9.8.3, tồn tại $\delta \in K$ sao cho ${}^t\operatorname{com}(A) = \delta B$. Nói cách khác, tất cả các hạng tử của $\operatorname{com}(A)$ đều bằng nhau. Hạng tử thứ (1,1) của $\operatorname{com}(A)$ là:

$$\begin{vmatrix} 1-n & 1 & \\ 1 & \ddots & \\ & & 1-n \end{vmatrix}_{[n-1]} = \begin{vmatrix} -1 & 1 & \cdots & 1 \\ \vdots & n-1 & 1 & \\ -1 & 1 & \ddots & \\ & & & 1-n \end{vmatrix}_{[n-1]} \quad \text{bởi } C_1 \leftarrow C_1 + \ldots + C_{n-1}$$

$$= \begin{vmatrix} -1 & 1 & \cdots & 1 \\ 0 & -n & 0 & \\ \vdots & & \ddots & \\ 0 & 0 & & -n \end{vmatrix}_{[n-1]} \quad \text{bởi } D_i \leftarrow D_i - D_1 \text{ với } i \geq 2$$

$$= (-1)^{n-1}n^{n-2}.$$

◇ **Trả lời:** $\operatorname{com}(A) = (-1)^{n-1}n^{n-2}\begin{pmatrix} 1 & \cdots & 1 \\ \vdots & 1 & \vdots \\ 1 & \cdots & 1 \end{pmatrix}$.

9.8.5 Khai triển theo dòng thứ nhất, ta có:

$$\begin{vmatrix} A_{11} & 0 & \cdots & 0 & A_{1n} \\ A_{21} & 1 & & & A_{2n} \\ \vdots & & \ddots & & \vdots \\ A_{n-11} & & 0 & 1 & A_{n-1n} \\ A_{n1} & 0 & \cdots & 0 & A_{nn} \end{vmatrix}$$

$$= A_{11}\begin{vmatrix} 1 & & & A_{2n} \\ & \ddots & & \vdots \\ & 0 & 1 & A_{n-1n} \\ 0 & \cdots & 0 & A_{nn} \end{vmatrix} + (-1)^{n+1} A_{1n}\begin{vmatrix} A_{21} & 1 & & \\ \vdots & & \ddots & 0 \\ & & 0 & \\ A_{n-11} & & & 1 \\ A_{n1} & 0 & \cdots & 0 \end{vmatrix}$$

$$= A_{11}A_{nn} + (-1)^{n+1}A_{1n}(-1)^n A_{n1} = A_{11}A_{nn} - A_{1n}A_{n1}.$$

Mặt khác:

$$\det\left(\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}\begin{pmatrix} A_{11} & & 1 & & 0 & A_{1n} \\ \vdots & & & \ddots & & \vdots \\ A_{n1} & & 0 & & 1 & A_{nn} \end{pmatrix}\right)$$

$$= \begin{vmatrix} \sum_{i=1}^{n} a_{1i}A_{i1} & a_{12} & \cdots & a_{1n-1} & \sum_{i=1}^{n} a_{1i}A_{in} \\ \vdots & \vdots & & \vdots & \vdots \\ \sum_{i=1}^{n} a_{ni}A_{i1} & a_{n2} & \cdots & a_{nn-1} & \sum_{i=1}^{n} a_{ni}A_{in} \end{vmatrix} = \begin{vmatrix} \det(A) & a_{12} & \cdots & a_{1n-1} & 0 \\ 0 & a_{22} & \cdots & a_{2n-1} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & a_{n-12} & \cdots & a_{n-1n-1} & 0 \\ 0 & a_{n2} & & a_{nn-1} & \det(A) \end{vmatrix}$$

$$= \det(A)\det(B)\det(A)$$

Như vậy ta nhận được: $\det(A)(A_{11}A_{nn} - A_{1n}A_{n1}) = (\det(A))^2\det(B)$.

- Nếu $\det(A) \neq 0$, ta suy ra : $\begin{vmatrix} A_{11} & A_{1n} \\ A_{n1} & A_{nn} \end{vmatrix} = \det(A)\det(B)$.
- Nếu $\det(A) = 0$, thì $\text{rank}(\text{com}(A)) \leq 1$ (xem bài tập 9.8.1)), và vì vậy $\begin{vmatrix} A_{11} & A_{1n} \\ A_{n1} & A_{nn} \end{vmatrix} = 0$.

9.9.1 a) Chẳng hạn, rút z từ phương trình thứ nhất và thế vào, hệ phương trình tương đương với:

$$\begin{cases} z = 2x + 3y + 1 \\ 7x + 11y + 1 = 0 \end{cases}$$

◇ **Trả lời:** $\left\{\left(x, -\frac{7x+1}{11}, \frac{x+8}{11}\right);\ x \in \mathbb{C}\right\}$.

b) Rút z từ phương trình thứ hai, hệ phương trình được quy về :

$$\begin{cases} z = -mx - y + 1 \\ (m-1)((2m+1)x + 2(m-1)y - 2(m-1)) = 0 \\ (1-m)x + (m-1)y - 3m - 2 = 0 \end{cases}$$

Nếu $m \neq 1$, rút $y = \frac{(-2m-1)x + 2}{2}$ và đưa vào phương trình thứ ba.

◇ **Trả lời:**
$$\begin{cases} \left\{\left(-\frac{2}{m-1}, \frac{3m}{m-1}, -\frac{1}{m-1}\right)\right\} & \text{nếu } m \neq -\frac{3}{2} \text{ và } m \neq 1 \\ \left\{\left(x, x+1, \frac{x}{2}\right); x \in \mathbb{C}\right\} & \text{nếu } m = -\frac{3}{2} \\ \varnothing & \text{nếu } m = 1. \end{cases}$$

c) Từ hiệu giữa các phương trình thứ nhất và thứ ba, suy ra: $m(x + 2y + z) = 0$

Nếu $m \neq 0$, hệ phương trình được quy về : $\begin{cases} z = -x - 2y \\ (2m + 5)x + (m + 3)y = m - 1 \\ x + y = -m - 1 \end{cases}$

Rút y và thế vào.

◇ **Trả lời:**
$$\begin{cases} \left\{\left(\frac{m^2+5m+2}{m+2}, -\frac{2m^2+8m+4}{m+2}, \frac{3m^2+11m+6}{m+2}\right)\right\} & \text{nếu } m \neq 0 \text{ và } m \neq 2 \\ \varnothing & \text{nếu } m = -2 \\ \left\{\left(x, -x-1, \frac{7x+8}{5}\right); x \in \mathbb{C}\right\} & \text{nếu } m = 0 \end{cases}$$

d) ◇ **Trả lời:**
$$\begin{cases} \left\{\left(m, 1, \frac{1}{m}\right)\right\} & \text{nếu } m \notin \{-1, 0, 1, -i, i\} \\ \{(-1, y, -y); y \in \mathbb{C}\} & \text{nếu } m = -1 \\ \varnothing & \text{nếu } m = 0 \\ \{(1, y, y); y \in \mathbb{C}\} & \text{nếu } m = 1 \\ \{(x, -ix, -i); x \in \mathbb{C}\} & \text{nếu } m = i \\ \{(x, ix, i); x \in \mathbb{C}\} & \text{nếu } m = -i. \end{cases}$$

e) ◇ **Trả lời:**
$$\begin{cases} \varnothing & \text{nếu } a + b \neq 3 \\ \{(2 - a, y, y + 5 - 3a); y \in \mathbb{C}\} & \text{nếu } a + b = 3 \end{cases}$$

f) Bằng phép trừ các phương trình, hệ được quy về: $\begin{cases} ax + (b-1)y + 2z = 1 \\ (b-2)y + z = 0 \\ bz = 2b - 4 \end{cases}$

◇ **Trả lời:**
$$\begin{cases} \left\{\left(-\frac{b-6}{ab}, -\frac{2}{b}, \frac{2b-4}{b}\right)\right\} & \text{nếu } b \neq 0, b \neq 2, a \neq 0 \\ \{(x, 1 - ax, 0); x \in \mathbb{C}\} & \text{nếu } b = 2 \\ \left\{\left(x, -\frac{1}{3}, \frac{4}{3}\right); x \in \mathbb{C}\right\} & \text{nếu } a = 0, b = 6 \\ \varnothing & \text{trong các trường hợp còn lại.} \end{cases}$$

g) Hệ tạo bởi 3 phương trình đầu có một nghiệm và chỉ một $(2, 2a - 2, 2a)$. Thế vào phương trình thứ 4.

◇ **Trả lời:**
$$\begin{cases} \varnothing & \text{nếu } a \neq b \\ \{(2, 2a - 2, 2a)\} & \text{nếu } a = b \end{cases}$$

9.9.2 Ba mặt phẳng đang xét chứa cùng một đường thẳng vectơ khi và chỉ khi hệ phương trình tuyến tính $\begin{cases} (1-m)x - 2y + z = 0 \\ 3x - (1+m)y - 2z = 0 \\ 3x - 2y - (1+m)z = 0 \end{cases}$ có ít nhất một nghiệm ngoài nghiệm $(0,0,0)$, điều đó (xem 9.9.2, 4), Mệnh đề) tương đương với: $\begin{vmatrix} 1-m & -2 & 1 \\ 3 & -1-m & -2 \\ 3 & -2 & -1-m \end{vmatrix} = 0.$

9.9.3 a) $\begin{cases} 3x+4y+z+2t=3 \\ 2(3x+4y+z)+6t=7 \\ 2(3x+4y+z)+10t=0 \end{cases} \Leftrightarrow \begin{cases} 3x+4y+z=2 \\ 2t=1 \\ 11=0 \end{cases}$

◇ **Trả lời:** ∅.

b) ◇ **Trả lời:** $\begin{cases} \left\{\left(x, y, \dfrac{-7x+6y+2}{5}, \dfrac{-3x-y+3}{5}\right) : (x,y) \in \mathbb{C}^2\right\} & \text{nếu } m=5 \\ \varnothing & \text{nếu } m \neq 5 \end{cases}$

c) ◇ **Trả lời:** $\begin{cases} \left\{\left(x, x+1, x+\dfrac{m}{m-1}, -(m+2)x-\dfrac{m}{m-1}\right) : (x,y) \in \mathbb{C}^2\right\} & \text{nếu } m \neq 1 \\ \varnothing & \text{nếu } m=1 \end{cases}$

d) Cộng bốn phương trình đầu tiên: $x+y+z+t=2$. Như vậy, hệ tạo bởi bốn phương trình đầu tiên có một nghiệm và chỉ một: $x=1, y=-1, z=0, t=2$.

◇ **Trả lời:** $\begin{cases} \{(1,-1,0,2)\} & \text{nếu } a=b=-1 \\ \varnothing & \text{nếu không} \end{cases}$.

e) Cộng lại, ta suy ra: $(a+3)(x+y+z+t)=1+b+b^2+b^3$.

◇ **Trả lời:**

$\begin{cases} \left\{\left(\dfrac{1}{a-1}(1-c), \dfrac{1}{a-1}(b-c), \dfrac{1}{a-1}(b^2-c), \dfrac{1}{a-1}(b^3-c)\right)\right\} & \text{nếu } a \neq 1, \text{và } a \neq 3, \text{và đặt} \\ & c=\dfrac{1+b+b^2+b^3}{a+3} \\ \{(x,y,z,1-x-y-z) : (x,y,z) \in \mathbb{C}^3\} & \text{nếu } a=b=1 \\ \left\{\left(x, x+\dfrac{1-b}{4}, x+\dfrac{1-b^2}{4}, x+\dfrac{1-b^3}{4}\right) : x \in \mathbb{C}\right\} & \text{nếu } a=-3 \text{ và } 1+b+b^2+b^3=0 \\ \varnothing & \text{nếu không} \end{cases}$

9.9.4 Lần lượt tính $x_2, x_3, \ldots, x_n$ theo x_1 và thế vào phương trình cuối cùng; tách các trường hợp theo tính chẵn lẻ của n

◇ **Trả lời:**

1) Nếu n là chẵn, $n=2p$ $(p \in \mathbb{N}^*)$:

- $S=\varnothing$ nếu $a_{2p}-a_{2p-1}+\ldots+a_2-a_1 \neq 0$
- $S=\{(x_1, 2a_1-x_1, 2a_2-2a_1+x_1, \ldots, 2a_{2p-1}-2a_{2p-2}+\ldots+2a_1-x_1) : x_1 \in \mathbb{C}\}$ nếu $a_{2p}-a_{2p-1}+\ldots+a_2-a_1=0$

Nếu n chẵn, $n=2p+1$ $(p \in \mathbb{N}^*)$: $S=\{(x_1, x_2, \ldots, x_{2p+1})\}$, trong đó:

$$x_1 = a_{2p+1}-a_{2p}+\ldots-a_2+a_1,$$
$$x_{2k+1} = a_{2p+1}-a_{2p}+\ldots-a_{2k+2}+a_{2k+1}+a_{2k}+a_{2k-1}+\ldots-a_1, k \in \{1,\ldots,p\},$$
$$x_{2k} = -a_{2p-1}+a_{2p}-\ldots+a_{2k}+a_{2k-1}-a_{2k-2}+\ldots-a_2+a_1, k \in \{1,\ldots,p\}.$$

Chẳng hạn, với $p=2$ $(n=5)$, ta có: $\begin{cases} x_1=a_5-a_4+a_3-a_2+a_1 \\ x_2=-a_5+a_4-a_3+a_2+a_1 \\ x_3=a_5-a_4+a_3+a_2-a_1 \\ x_4=-a_5+a_4+a_3-a_2+a_1 \\ x_1=a_5+a_4-a_3+a_2-a_1 \end{cases}$.

Chỉ dẫn và trả lời
các bài tập chương 10

10.1.1 Khai triển bằng tích vô hướng, tất các hạng tử sẽ được giản ước.

Cách khác

Đặt $u = b - a$, $v = c - a$, $w = d - a$. Áp dụng đẳng thức hình bình hành:

$2(\|u\|^2 + \|v - u\|^2 + \|w - v\|^2 + \|w\|^2) = 2(\|u\|^2 + \|w - v\|^2) + 2(\|v - u\|^2 + \|w\|^2)$

$= \|u + w - v\|^2 + \|u - w + v\|^2 + \|v - u + w\|^2 + \|v - u - w\|^2$

và $2(\|v\|^2 + \|w - u\|^2 + \|v - w - u\|^2) = \|v + w - u\|^2 + \|v - w + u\|^2 + 2\|u - w - u\|^2)$,

từ đó suy ra đẳng thức cần chứng minh.

10.1.2 Cho $X \in \mathbf{M}_{n,1}(\mathbb{R})$ sao cho $(I_n + A)X = 0$, nghĩa là $AX = -X$. Lấy chuyển vị, và vì A là phản đối xứng, ta được: ${}^tXA = {}^tX$, do đó : $\begin{cases} {}^tXAX = {}^tX(AX) = -{}^tXX \\ {}^tXAX = ({}^tXA)X = {}^tXX \end{cases}$,

nên ${}^tXX = 0$, và cuối cùng $X = 0$.

10.1.3 Sử dụng bất đẳng thức tam giác trong E, sau đó là bất đẳng thức Cauchy - Schwarz trong $\mathbb{R}^n$ thông thường áp dụng cho $(1,...,1)$ và $(\|x_1\|,...,\|x_n\|)$, ta được:

$$\left\| \sum_{k=1}^{n} x_k \right\|^2 \le \left(\sum_{k=1}^{n} \| x_k \| \right)^2 \le \left(\sum_{k=1}^{n} 1^2 \right) \left(\sum_{k=1}^{n} \| x_k \|^2 \right) = n \sum_{k=1}^{n} \| x_k \|^2 .$$

10.1.4 Theo đẳng thức hình bình hành:

$$2(\|x - y\|^2 + \|y - z\|^2) = \|x - z\|^2 + \|x - 2y + z\|^2 \ge \|x - z\|^2.$$

Nhận xét: Tổng quát hơn, bất đẳng thức đúng trong một kgv trực chuẩn vì

$$\|x - z\|^2 \le \|x - y\|^2 + \|y - z\|^2 + 2\|x - y\| \, \|y - z\| \le 2(\|x - y\|^2 + \|y - z\|^2),$$

do: $\forall (\alpha, \beta) \in \mathbf{R}_+^2$, $2\alpha\beta \le \alpha^2 + \beta^2$.

10.1.5 Áp dụng bất đẳng thức Cauchy - Schwarz cho $(1, 1, 1, 1)$ và $(1 - x, x - y, y - z, z)$ trong $\mathbb{R}^4$ thông thường:

$$1^2 = ((1 - x) + (x - y) + (y - z) + z)^2 \le 4((1 - x)^2 + (x - y)^2 + (y - z)^2 + z^2).$$

Theo 10.1.2, Mệnh đề 1, ta có đẳng thức khi và chỉ khi $(1 - x, x - y, y - z, z)$ cộng tuyến với $(1, 1, 1, 1)$, nghĩa là: $1 - x = x - y = y - z = z$.

◇ **Trả lời :** $\left\{ \left(\frac{3}{4}, \frac{1}{2}, \frac{1}{4} \right) \right\}$.

10.1.6 Bất đẳng thức cần chứng minh suy từ bất đẳng thức Cauchy-Schwarz trong $\mathbb{R}^n$ thông thường, áp dụng cho $u = (\sqrt{x_1},...,\sqrt{x_n})$ và $v = \left(\frac{1}{\sqrt{x_1}},...,\frac{1}{\sqrt{x_n}}\right)$.

Theo 10.1.2 , Mệnh đề 1, ta có đẳng thức khi và chỉ khi (u, v) phụ thuộc tuyến tính.

◇ **Trả lời:** Có đẳng thức khi và chỉ khi $x_1 = ... = x_n = \frac{1}{n}$.

10.1.7 Giả sử $\sum_{i\neq j} a_i b_j = 0$, thế thì $\left(\sum_i a_i\right)\left(\sum_i b_i\right) = \sum_i a_i b_i$.

Vì các $a_i > 0$, ta suy ra : $\sum_i b_i = \frac{\sum_i a_i b_i}{\sum_i a_i}$.

Theo bất đẳng thức Cauchy-Schwarz : $\left(\sum_i a_i b_i\right)^2 \leq \left(\sum_i a_i^2\right)\left(\sum_i b_i^2\right)$,

và vì $a_i > 0$ nên: $\sum_i a_i^2 \leq \left(\sum_i a_i\right)^2$.

Ta suy ra: $$\sum_{i\neq j} b_i b_j = \left(\sum_i b_i\right)^2 - \sum_i b_i^2 = \left(\frac{\sum_i a_i b_i}{\sum_i a_i}\right)^2 - \sum_i b_i^2$$

$$= \frac{1}{\left(\sum_i a_i\right)^2}\left(\left(\sum_i a_i b_i\right)^2 - \left(\sum_i a_i\right)^2\left(\sum_i b_i^2\right)\right) \leq 0.$$

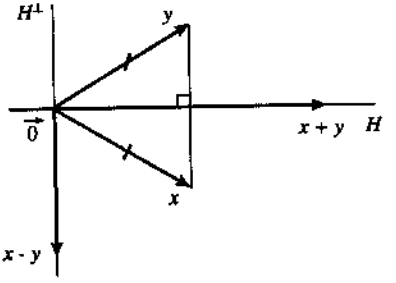
10.2.1 Trường hợp $x = y$ có thể khảo sát dễ dàng.

a) Đặt $H = (x - y)^\perp$.

Vì $< x + y, x - y > = \|x\|^2 - \|y\|^2 = 0$,

nên ta có $x + y \in H$.

Vì $\begin{cases} y + x \in H \\ y - x \in H^\perp \end{cases}$, ta suy ra $y = s_H(x)$.

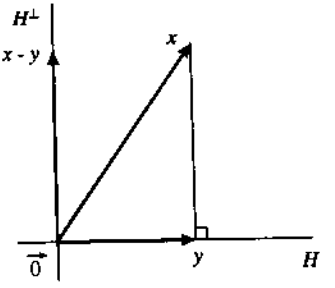


b) Đặt $H = (x - y)^\perp$.

Vì $< x - y, y > = < x, y > - \|y\|^2 = 0$,

nên ta có: $y \in H$.

Vì $\begin{cases} y \in H \\ y - x \in H^\perp \end{cases}$, ta suy ra $y = p_H(x)$.



10.3.1 Đặt $A = (a_{ij})_{ij}$, với mọi j thuộc $\{1,...,n\}$ ta có $C_j {}^tC_j = (a_{ij}a_{kj})_{i,k}$,

do đó : $\sum_{j=1}^{n} C_j {}^tC_j = \left(\sum_{j=1}^{n} a_{ij}a_{kj}\right)_{i,k} = A\,{}^tA$.

10.3.2 • ${}^tS = I_n - \frac{2}{{}^tCC}{}^t(C^tC) = I_n - \frac{2}{{}^tCC}C^tC = S$

• ${}^tSS = S^2 = I_n - \frac{4}{{}^tCC}C^tC + \frac{4}{({}^tCC)^2}C^tCC^tC = I_n - \frac{4}{{}^tCC}C^tC + \frac{4}{({}^tCC)^2}({}^tCC)C^tC = S$

• $SC = C - \frac{2}{{}^tCC}C^tCC = C - 2C = -C$

• $\forall X \in C^{\perp}$, $SX = X - \frac{2}{{}^tCC}C^tCX = X$

10.3.3 Đặt $U = \begin{pmatrix}1\\1\\\vdots\\1\end{pmatrix} \in \mathbf{M}_{n,1}(\mathbb{R})$, ta có: $AU = \begin{pmatrix}\sum_{j=1}^{n} a_{1j}\\\vdots\\\sum_{j=1}^{n} a_{nj}\end{pmatrix}$.

Theo bất đẳng thức Cauchy-Schwarz trong $\mathbf{M}_{n,1}(\mathbb{R})$ được trang bị tích vô hướng chính tắc:
$|\langle AU, U\rangle| \le \|AU\|\,\|U\|$, và $\|AU\| = \|U\|$ vì $A \in \mathbf{O}_n(\mathbb{R})$, vậy

$$\left|\sum_{1\le i,j\le n} a_{ij}\right| = \left|\sum_{i=1}^{n}\left(\sum_{j=1}^{n} a_{ij}\right)\right| \le \|U\|^2 = n.$$

Khảo sát trường hợp đẳng thức

Theo 10.1.2, Mệnh đề 1, có đẳng thức khi và chỉ khi (AV, U) phụ thuộc tuyến tính.

◇ **Trả lời**: Có đẳng thức khi và chỉ khi $AU = U$ hoặc $AU = -U$, trong đó $U = \begin{pmatrix}1\\1\\\vdots\\1\end{pmatrix}$.

10.3.4 a) Nếu $(V_1,...,V_n)$ phụ thuộc tuyến tính, thì bất đẳng thức là hiển nhiên.

Giả thiết $(V_1,...,V_n)$ độc lập tuyến tính.

Theo thủ tục trực giao hóa Schmidt, tồn tại $W_1,...,W_n \in E$ sao cho:

$$\begin{cases}(W_1,...,W_n) & \text{là một họ trực giao}\\ \forall i \in \{1,...,n\}, & W_i \neq 0\\ \forall i \in \{2,...,n\}, & W_i \in \mathrm{Vect}(V_1, W_1,...,W_{i-1}).\end{cases}$$

Với $i \in \{1,...,n\}$, đặt $e_i = \frac{W_i}{\|W_i\|}$.

Theo 9.2.2, Hệ quả (hệ thức Chasles đối với định thức):

$$|\det_{\mathcal{B}}(V_1,...,V_n)| = |\det_{\mathcal{B}}(e_1,...,e_n)|\;|\det_{(e_1,...,e_n)}(w_1,...,w_n)|\;|\det_{(W_1,...,W_n)}(V_1,...,V_n)|.$$

• $|\det_{\mathcal{B}}(e_1,...,e_n)| = 1$ vì $\mathcal{B}$ và $(e_1,...,e_n)$ là những c.s.t.c. của E (xem 10.3.2, Mệnh đề 3 và 4).

• $|\det_{(e_1,...,e_n)}(w_1,...,w_n)| = \prod_{i=1}^{n}\|W_i\|$, theo định nghĩa của các e_i.

• $\det_{(u_1,\dots,u_n)}(V_1,\dots,V_n) = 1$, vì ma trận chuyển từ $(V_1,\dots,V_n)$ sang $(W_1,\dots,W_n)$ là ma trận tam giác trên với các hạng tử chéo bằng 1.

Ta được: $|\det_B(V_1,\dots,V_n)| = \prod_{i=1}^{n} \|W_i\|$.

Cuối cùng, vì $W_i = V_i + U_i$, trong đó $U_i \in \text{Vect}(V_1,\dots,V_{i-1}) = \text{Vect}(W_1,\dots,W_{i-1})$, do đó $U_i \perp W_i$; nên theo định lý Pythagore ta có : $\|V_i\|^2 = \|W_i\|^2 + \|U_i\|^2 \geq \|W_i\|^2$

Ta kết luận: $|\det_B(V_1,\dots,V_n)| \leq \prod_{i=1}^{n} \|V_i\|$.

b) Khảo sát trường hợp đẳng thức khi $(V_1,\dots V_n)$ độc lập tuyến tính

Giả sử có đẳng thức: $|\det_B(V_1,\dots,V_n)| = \prod_{i=1}^{n} \|V_i\|$.

Vì $\begin{cases} \prod_{i=1}^{n} \|W_i\| = \prod_{i=1}^{n} \|V_i\| \\ \forall i \in \{1,\dots,n\},\ 0 < \|W_i\| \leq \|V_i\| \end{cases}$, ta suy ra $\forall i \in \{1,\dots,n\}$, $\|W_i\| =$

rồi với các ký hiệu trên : $\forall i \in \{1,\dots,n\}$, $U_i = 0$, nghĩa là $\forall i \in \{1,\dots,n\}$, $W_i = V_i$. Từ đó suy ra rằng $(V_1,\dots,V_n)$ là một họ trực giao.

◇ **Trả lời**: Có đẳng thức khi và chỉ khi: $\begin{cases} (V_1,\dots,V_n) \text{ trực giao} \\ \text{hoặc} \\ (\exists\, i \in \{1,\dots,n\},\ V_i = 0) \end{cases}$

10.3.5 Vì f là song ánh, nên $\dim(f(F)) = \dim(F)$. Vậy từ bao hàm thức $f(F) \subset F$, ta suy ra đẳng thức $f(F) = F$. Hơn nữa: $f^{-1}(F) = f^{-1}(f(F)) = F$.

• Giả sử $y \in f(F^\perp)$; tồn tại $x \in F^\perp$ sao cho $y = f(x)$.

Với mọi z thuộc F, ta có : $< y, z > = < f(x), z > = < x, f^{-1}(z) > \geq 0$, vì $f^{-1}(z) \in F$.

Do đó $y \in F^\perp$, và như vậy $f(F^\perp) \subset F^\perp$.

• Như phần đầu, ta được $f(F^\perp) \subset F^\perp$.

Dễ dàng suy ra các tính chất $f|_F \in \mathcal{O}(F)$, $f|_{F^\perp} \in \mathcal{O}(F^\perp)$.

10.3.6 • Rõ ràng f tuyến tính

• Cho $x \in E$. Vì $u(p_F(x)) \in F$ và $v(p_{F^\perp}(x)) \in F^\perp$, ta có:

$$\|f(x)\|^2 = \|u(p_F(x))\|^2 + \|v(p_{F^\perp}(x))\|^2 = \|p_F(x)\|^2 + \|p_{F^\perp}(x)\|^2 = \|x\|^2.$$

Điều đó chứng tỏ : $f \in \mathcal{O}(E)$.

10.3.7 Quy nạp theo n .

Nếu $n = 1$, thì f là ánh xạ đồng nhất hoặc là phép phản chiếu $-\text{Id}_E$.

Giả sử tính chất đúng đối với mọi kgv Euclide n chiều, và E là một kgv Euclide $n+1$ chiều và $f \in \mathcal{O}(E)$.

Kgv Euclide E có ít nhất một c.s.t.c $(e_1,\dots,e_{n+1})$. Theo bài tập 10.2.1, *a*), tồn tại một phép phản chiếu s của E sao cho $s(f(e_{n+1})) = e_{n+1}$.

Vì đường thẳng vectơ $\mathbb{R}e_{n+1}$ ổn định đối với tự đẳng cấu trực giao $s \circ f$, nên theo bài tập 10.3.5, $(\mathbb{R}e_{n+1})^\perp$, tức là $\text{Vect}(e_1,\dots,e_n)$ cũng ổn định đối với $s \circ f$.

Ta ký hiệu $F = \text{Vect}(e_1,...,e_n)$ và f' là tự đồng cấu cảm sinh bởi $s \circ f$ trên F. Vì $f' \in \mathcal{O}(F)$ (xem bài tập 10.3.5), theo giả thiết quy nạp, nên tồn tại $s'_2,...,s'_{n+1}$ (là những phép phản chiếu hoặc đồng nhất của F) sao cho $f' = s'_2 \circ ... \circ s'_{n+1}$. Với $2 \leq i \leq n+1$, gọi s_i là tự đồng cấu trực giao nhận được bởi phép dán s_i trên F' và phép đồng nhất trên $\mathbb{R}e_{n+1}$ (xem bài tập 10.3.6), rõ ràng $s_2,...,s_{n+1}$ là những phép phản chiếu hoặc đồng nhất, và $s \circ f = s_2 \circ ... \circ s_{n+1}$, do đó $f = s \circ s_2 \circ ... \circ s_{n+1}$.

Có thể so sánh lời giải này với phép chứng minh ở 3.4.2, Định lý 1, đối với việc phân tích một hoán vị thành một tích những chuyển vị.

10.4.1 ◇ **Trả lời :** $R_\theta R_\theta = R_{\theta+\theta'}$, $R_\theta S_\varphi = S_{\theta+\varphi}$, $S_\varphi R_\theta = S_{\varphi-\theta}$, $S_\varphi S_{\varphi'} = R_{\varphi-\varphi'}$.

10.4.2 *Phương pháp thứ nhất*

Vì $r \circ s$ là một tự đồng cấu trực giao nghịch của E_2, đó là một phép phản chiếu, do vậy $(r \circ s)^2 = e$ (trong đó $e = \text{Id}_E$), nghĩa là $r \circ s \circ r \circ s = e$, suy ra $s \circ r \circ s = r^{-1}$ và $r \circ s \circ r = s^{-1} = s$.

Phương pháp thứ hai

Sử dụng kết quả của bài tập 10.4.1 :

$S_\varphi R_\theta S_\varphi = S_{\varphi-\theta}S_\varphi = R_{-\theta} = R_\theta^{-1}$ và $R_\theta S_\varphi R_\theta = S_{\theta+\varphi}R_\theta = S_\varphi$.

◇ **Trả lời :** $s \circ r \circ s = r^{-1}$, $r \circ s \circ r = s$.

10.4.3 Sử dụng $u.v = \|u\|\,\|v\| \cos(\widehat{u, v})$ và $\det_{i,j}(u, v) = \begin{vmatrix} -2 & 1 \\ 1 & 3 \end{vmatrix} = -7 < 0$

◇ **Trả lời :** $-\text{Arccos}\left(\dfrac{\sqrt{2}}{10}\right)$ $[2\pi]$.

10.4.4 a) • Nếu $b^2 - ac < 0$: $ax^2 + 2bxy + cy^2 = 0 \Leftrightarrow x = y = 0$

• Nếu $b^2 - ac \geq 0$ và $c \neq 0$, tam thức thực $a + 2bX + cX^2$ có hai không điểm thực (có thể trùng nhau) m, m' và: $ax^2 + 2bxy + cy^2 = 0 \Leftrightarrow (y = mx$ hoặc $y = m'x)$.

• Nếu $c = 0$: $ax^2 + 2bxy + cy^2 = 0 \Leftrightarrow (x = 0$ hoặc $ax + 2by = 0)$.

◇ **Trả lời:** $b^2 - ac \geq 0$.

b) Giả sử $b^2 - ac \geq 0$ và $c \neq 0$.

Cho $V\begin{pmatrix}1\\m\end{pmatrix}, V'\begin{pmatrix}1\\m'\end{pmatrix}$ tương ứng là các vectơ chỉ phương của D, D', trong đó có m, m' là các không điểm thực của $a + 2bX + cX^2$. Ta có:

$$\cos(\widehat{v,v'}) = \frac{V \cdot V'}{\|V\| \cdot \|V'\|} = \frac{1 + mm'}{\sqrt{(1+m^2)(1+m'^2)}}.$$

Vì $m + m' = -\dfrac{2b}{c}$ và $mm' = \dfrac{a}{c}$, ta được :

$$\cos(\widehat{V, V'}) = \frac{a+c}{\sqrt{(a-c)^2 + 4b^2}}.$$

Nếu $c = 0$, thì ta lấy $V\begin{pmatrix}0\\1\end{pmatrix}, V'\begin{pmatrix}-2b\\a\end{pmatrix}$, nên $\cos(\widehat{V, V'}) = \dfrac{a}{\sqrt{a^2 + 4b^2}}$.

◇ **Trả lời :** $|(\widehat{D, D'})| = \text{Arccos}\dfrac{|a+c|}{\sqrt{(a-c)^2 + 4b^2}}$.

c) Bó toàn phương các phân giác của D và D', tức là hợp của các phân giác của D, D', là tập hợp các $W\begin{pmatrix}x\\y\end{pmatrix}$ của E_2 sao cho $d(W, D) = d(W, D')$.

• Giả sử $c \neq 0$. Vì $d(W, D) = \dfrac{|y - mx|}{\sqrt{1+m^2}}$ và $d(W, D') = \dfrac{|y - m'x|}{\sqrt{1+m'^2}}$, ta có:

$d(W, D) = d(W, D') \Leftrightarrow (1 + m'^2)(y - mx)^2 - (1 + m^2)(y - m'x)^2 = 0$

$\Leftrightarrow (m + m')x^2 - 2(1 - mm')xy - (m + m')y^2 = 0$ nếu $m \neq m'$

$\Leftrightarrow -\dfrac{2b}{c}x^2 - 2\left(1 - \dfrac{a}{c}\right)xy + \dfrac{2b}{c}y^2 = 0$.

• Khảo sát trường hợp $c = 0$.

◇ **Trả lời**: $bx^2 + (c - a)xy - by^2 = 0$.

10.5.1 a) ◇ **Trả lời**: f là phép quay với trục định phương và định hướng bởi $7i + 7j - 3k$, với góc quay $\text{Arccos}\left(-\dfrac{53}{54}\right)$ [2π].

b) ◇ **Trả lời**: f là phép lật quanh đường thẳng vectơ sinh bởi $i + 2j - 2k$.

c) ◇ **Trả lời**: f là phép phản chiếu qua mặt phẳng có phương trình $x - 2y - 2z = 0$.

d) ◇ **Trả lời**: f là tích giao hoán của phép quay có trục định phương và định hướng bởi $i - 4k$ và có góc $-\text{Arccos}\left(\dfrac{8}{9}\right)$ [2π], và phép phản chiếu qua mặt phẳng có phương trình $x - 4z = 0$.

e) Đặt $u = ai + bj + ck$, nhận xét rằng : $\forall x \in E_3, f(x) = (u.x)u + u \wedge x$.

◇ **Trả lời**: f là phép quay có trục định phương và định hướng bởi $ai + bj + ck$ và có góc quay $\dfrac{\pi}{2}[\pi]$.

10.5.2 Đặt $u = \dfrac{1}{\sqrt{3}}(i + j + k)$, $v = \dfrac{1}{\sqrt{2}}(i - j)$ là vectơ chuẩn hóa và trực giao với u, $w = u \wedge v = \dfrac{1}{\sqrt{6}}(i + j - 2k)$, $\mathcal{B}' = (u, v, w)$ là một c.s.t.c.t. $\Omega_1 = \text{Mat}_{\mathcal{B}'}(f) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \dfrac{1}{2} & -\dfrac{\sqrt{3}}{2} \\ 0 & \dfrac{\sqrt{3}}{2} & \dfrac{1}{2} \end{pmatrix}$,

$P = \text{Pass}(\mathcal{B}, \mathcal{B}') = \begin{pmatrix} \dfrac{1}{\sqrt{3}} & \dfrac{1}{\sqrt{2}} & \dfrac{1}{\sqrt{6}} \\ \dfrac{1}{\sqrt{3}} & -\dfrac{1}{\sqrt{2}} & \dfrac{1}{\sqrt{6}} \\ \dfrac{1}{\sqrt{3}} & 0 & -\dfrac{2}{\sqrt{6}} \end{pmatrix}$.

Tính: $\Omega = P\Omega_1 P^{-1} = P\Omega_1 {}^tP$.

◇ **Trả lời**: $\Omega = \dfrac{1}{3}\begin{pmatrix} 2 & -1 & 2 \\ 2 & 2 & -1 \\ -1 & 2 & 2 \end{pmatrix}$.

10.5.3 Ký hiệu $\vec{\Delta}$ là trục của f, u là *vectơ* chuẩn hoá chỉ phương và chỉ hướng của $\vec{\Delta}$, θ là góc của f, và tương tự với $\vec{\Delta}$, u', θ' của g.

1) Giả sử $f \circ g = g \circ f$.

Ta có: $f(g(u)) = g(f(u)) = g(u)$.

Vì f là một phép quay không trùng với Id_{E_3}, ta suy ra $g(u) \in \mathbb{D}u$.

Hơn nữa, $\|g(u)\| = \|u\|$, do vậy $g(u) = u$ hoặc $g(u) = -u$.

Tương tự, $f(u') = u'$ hoặc $f(u') = -u'$.

Trường hợp thứ nhất: $g(u) = u$ hoặc $f(u') = u'$.

Khi đó $u' = u$ hoặc $u' = -u$, vậy f và g có cùng trục.

Trường hợp thứ hai: $g(u) = -u$ và $f(u') = -u'$.

Khi đó: $u.u' = f(u).f(u') = u.(-u')$, do vậy $u \perp u'$. Đặt $w = u \wedge u'$, $\mathcal{B}' = (u, u', w)$ là một c.s.t.c.t. của E_3. Ma trận của f trong cơ sở $\mathcal{B}'$ có dạng: $\begin{pmatrix} 1 & 0 & \alpha \\ 0 & -1 & \beta \\ 0 & 0 & \gamma \end{pmatrix}$, $(\alpha, \beta, \gamma) \in \mathbb{R}^3$.

Vì $f \in \mathcal{O}(E_3)$, ta có $\gamma^2 = 1$, sau đó $\alpha = \beta = 0$, và cuối cùng, vì $f \in \mathcal{SO}(E_3)$, $\gamma = -1$.

Tương tự: $\mathrm{Mat}_{\mathcal{B}'}(g) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$.

Như vậy f và g là hai phép lật theo hai trục trực giao.

2) *Phần đảo*

α) Nếu $\vec{\Delta}' = \vec{\Delta}$, thì rõ ràng $f \circ g = g \circ f = \mathrm{Rot}_{\vec{\Delta}, \theta+\theta'}$.

β) Nếu f và g là hai phép lật sao cho $\Delta \perp \Delta'$, thì trong c.s.t.c.t $(u, u', u \wedge u')$, các ma trận của f và g là $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ và $\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$, chúng giao hoán vì cả hai đều là ma trận chéo.

10.5.4 Giả sử f là một phép quay của E_3, $\vec{\Delta}$ là trục của f, θ là góc của f, I là vectơ chuẩn hóa chỉ phương và chỉ hướng của $\vec{\Delta}$, J là vectơ chuẩn hóa vuông góc với I (tồn tại ít nhất một), $K = I \wedge J$. Thế thì $\mathcal{B} = (I, J, K)$ là một c.s.t.c.t của E_3 và :

$$\Omega = \mathrm{Mat}_{\mathcal{B}}(f) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}.$$

Rõ ràng $\Omega = \Omega_1\Omega_2$, trong đó $\Omega_1 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$, $\Omega_2 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & -\sin\theta & -\cos\theta \end{pmatrix}$.

Vì Ω_1, Ω_2 trực giao, đối xứng, có định thức bằng 1, khác I_3, nên ta suy ra rằng Ω_1, Ω_2 là các ma trận trong $\mathcal{B}$ của hai phép lật.

Như vậy ta cũng có thể nhận xét rằng, với mọi đường thẳng D_1 trực giao với Δ, tồn tại một đường thẳng D_2 duy nhất sao cho $f = \mathrm{Ret}_{D_1} \circ \mathrm{Ret}_{D_2}$ trong đó Ret_{D_1} (tương ứng: Ret_{D_2}) là phép lật quanh D_1 (tương ứng: D_2).

10.5.5 Vì $\forall x \in E_3$, $a \wedge x \perp a$, nếu $a.b \neq 0$, nên phương trình (1) $a \wedge x = b$ không có nghiệm
$x \in E_3$.

Do vậy, ta giả thiết $a.b = 0$.

Nếu ($a = 0$ và $b \neq 0$), (1) không có nghiệm.

Nếu ($a \neq 0$ và $b = 0$) , tập hợp các nghiệm của (1) là $\mathbb{R}a$.

Giả thiết $a \neq 0$ và $b \neq 0$.

Khi đó $(a, b, a \wedge b)$ là một cơ sở của E_3; gọi (α, β, γ) là các thành phần của x trong cơ sở này, ta có:

$$a \wedge x = b \Leftrightarrow \beta a \wedge b + \gamma a \wedge (a \wedge b) = b \Leftrightarrow \beta a \wedge b - \gamma \|a\|^2 b = b \Leftrightarrow (\beta = 0 \text{ và } \gamma = -\frac{1}{\|a\|^2}).$$

◇ **Trả lời:**
$$\begin{cases} \varnothing & \text{nếu } a.b = 0 \\ \left\{ -\frac{1}{\|a^2\|} a \wedge b + \alpha a ; \alpha \in \mathbb{R} \right\} & \text{nếu } (a.b = 0 \text{ và } a \neq 0) \\ \varnothing & \text{nếu } (a = 0 \text{ và } b \neq 0) \\ E_3 & \text{nếu } a = b = 0 \end{cases}$$

10.5.6 Lập luận phản chứng: Giả sử tồn tại $c \in E_3$ sao cho:

$$\forall x \in E_3, a \wedge (b \wedge x) = c \wedge x.$$

Đặc biệt khi thay x bởi b: $c \wedge b = 0$. Do vậy tồn tại $\alpha \in \mathbb{R}$ sao cho $c = \alpha b$. Sau đó, thay x bởi a: $a \wedge (b \wedge a) = \alpha b \wedge a$. Nhưng $a \wedge (b \wedge a)$ khác không và trực giao với $b \wedge a$, từ đó suy ra mâu thuẫn.

10.5.7 Suy ra: $a - x = a \wedge y = a \wedge (a - a \wedge x) = -a \wedge (a \wedge x) = -(a.x)a + \|a\|^2 x$, do đó: $(1 + \|a\|^2)x = (1 + a.x)a$.

Do vậy tồn tại $\lambda \in \mathbb{R}$ sao cho $x = \lambda a$. Khi đó: $\begin{cases} a \wedge x + y = a \\ a \wedge y + x = a \end{cases} \Leftrightarrow \begin{cases} y = a \\ x = a \end{cases}$.

◇ **Trả lời:** $\{(a,a)\}$.

10.5.8 $(a \wedge x) \wedge b = a \wedge (x \wedge b) \Leftrightarrow -(b.x)a + (b.a)x = (a.b)x - (a.x)b \Leftrightarrow a.x = b.x = 0$.

◇ **Trả lời:** $\mathbb{R}(a \wedge b)$.

10.5.9 $(S) \Rightarrow \begin{cases} a \wedge (x - y) = b \wedge (y - x) \\ a \wedge (x + y) = b \wedge (y + x) \end{cases} \Leftrightarrow \begin{cases} (a + b) \wedge (x - y) = 0 \\ (a - b) \wedge (x + y) = 0 \end{cases}$.

Do đó tồn tại $(\alpha, \beta) \in \mathbb{R}^2$ sao cho $\begin{cases} x - y = 2\alpha (a + b) \\ x + y = 2\beta (a - b) \end{cases}$, từ đó suy ra : $\begin{cases} x = (\alpha + \beta)a + (\alpha - \beta)b \\ y = (\beta - \alpha)a - (\alpha + \beta)b \end{cases}$.

Khi đó $(S) \Leftrightarrow -(\alpha + \beta)^2 a \wedge b - (\alpha - \beta)^2 b \wedge a = a \wedge b \Leftrightarrow -(\alpha + \beta)^2 b + (\alpha - \beta)^2 = 1$.

◇ **Trả lời:** $\{((\alpha + \beta)a + (\alpha - \beta)b, (\beta - \alpha)a - (\alpha + \beta)b); (\alpha, \beta) \in \mathbb{R}^2, -4\alpha\beta = 1\}$.

10.5.10 • $[x \wedge u, y \wedge v, z \wedge w] = (x \wedge u) \cdot ((y \wedge v) \wedge (z \wedge w))$

$= (x \wedge u)(((y \wedge v).w)z - ((y \wedge v).z)w) = [x, u, z][y, v, w] - [x, u, w][y, v, z]$

• $[x \wedge v, y \wedge w, z \wedge u] = [y \wedge w, z \wedge u, x \wedge v] = (y \wedge w).((z \wedge u) \wedge (x \wedge v))$

$= (y \wedge w)(((z \wedge u) \cdot v)x - ((z \wedge u) \cdot x)v) = [y, w, x][z, u, v] - [y, w, v][z, u, x]$

• $[x \wedge w, y \wedge u, z \wedge v] = [z \wedge v, x \wedge w, y \wedge u] = (z \wedge v) \cdot ((x \wedge w) \wedge (y \wedge u))$

$= (z \wedge v) \cdot (((x \wedge w) \quad u) \cdot y - ((x \wedge w).y).u) = [z, v, y][x, w, u] - [z, v, u][x, w, y]$.

10.5.11 a) Dễ dàng suy ra các công thức cần chứng minh.

b) Giả sử $x \cdot y = 0$. Khi đó ta có $f_a(x,y) = -(y \cdot x)a + (y \cdot a)x - (x \cdot y)a + (x \cdot a)y = (y \cdot a)x + (x.a)y$.

Vì $(x \neq 0, y \neq 0, x.y = 0)$, nên (x, y) độc lập tuyến tính, và do vậy:

$$f_a(x, y) = 0 \Leftrightarrow x \cdot a = y \cdot a = 0 \Leftrightarrow a \in \mathbb{R}(x \wedge y).$$

10.5.12 $f^2(x) = (x \wedge u) \wedge u = -x + (u.x)u$, $f^3(x) = (-x + (u \cdot x)u) \wedge u = -x \wedge u = -f(x)$.

10.5.13 1) Trước hết tìm một điều kiện cần và đủ để f là một tự đồng cấu trực giao .

Trước hết, rõ ràng f tuyến tính.

Với mọi x thuộc E_3 ta có:

$$\|f(x)\|^2 = \alpha^2 \|x\|^2 + \beta^2(u \cdot x)^2 + \gamma^2 \|u \wedge x\|^2 + 2\alpha\beta(u \cdot x)^2$$

$$= (\alpha^2 + \beta^2)\|x\|^2 + (2\alpha\beta + \beta^2 - \gamma^2)(u \cdot x)^2.$$

Sau đó: $\forall x \in E_3, \|f(x)\| = \|x\| \Leftrightarrow \forall x \in E_3, (\alpha^2 + \gamma^2 - 1)\|x\|^2 + (2\alpha\beta + \beta^2 - \gamma^2)(u \cdot x)^2 = 0$

$$\Leftrightarrow \begin{cases} \alpha^2 + \gamma^2 - 1 = 0 \\ 2\alpha\beta + \beta^2 - \gamma^2 = 0 \end{cases} \Leftrightarrow \begin{cases} \alpha^2 + \gamma^2 = 1 \\ \alpha + \beta \in \{-1, 1\} \end{cases}$$

Ta cũng có thể nhận xét rằng $f(u) = (\alpha + \beta)u$ và, với mọi vectơ y chuẩn hóa trực giao với u, $\|f(y)\|^2 = \alpha^2 + \gamma^2$.

2) Giả sử điều kiện cuối cùng được thực hiện. Nói riêng, tồn tại $\theta \in \mathbb{R}$ sao cho:

$$\alpha = \cos\theta \text{ và } \gamma = \sin\theta.$$

Tồn tại $v, w \in E_3$ sao cho (u, v, w) là một c.s.t.c.t. của E_3. Ta có: $\begin{cases} f(u) = \alpha u + \beta u = (\alpha + \beta)u \\ f(v) = \alpha v + \gamma u \wedge v = \alpha v + \gamma w \\ f(w) = \alpha w + \gamma u \wedge w = -\gamma v + \alpha w \end{cases}$

Như vậy, $\mathrm{Mat}_{(u,v,w)}(f) = \begin{pmatrix} \alpha + \beta & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$

Do đó f là một phép quay khi và chỉ khi $\alpha + \beta = 1$.

◇ **Trả lời**: • $\alpha^2 + \gamma^2 = 1$ và $\alpha + \beta = 1$

• Trong trường hợp này, f là phép quay có trục được định phương và định hướng bởi u, có góc θ xác định bởi:

$$\begin{cases} \cos\theta = \alpha \\ \sin\theta = \gamma \end{cases}$$

C.10.1 *I* 1) • Xem 10.1.1, Ví dụ 3).

• $< PQ, R > = \int_{-1}^{1} (P(x)Q(x))R(x)dx = \int_{-1}^{1} P(x)(Q(x)R(x))dx = < P, QR >$.

2) **Tồn tại**

Quy nạp mạnh theo n.

Đặt $P_0 = \frac{1}{\sqrt{2}}$; như vậy P_0 có bậc 0, có hệ tử cao nhất > 0 , và $\|P_0\|^2 = \int_{-1}^{1} \left(\frac{1}{\sqrt{2}}\right)^2 dx = 1$.

Giả sử đã xác định $P_0,...,P_n$ thích hợp, nghĩa là sao cho:

$$\begin{cases} \forall (k, l) \in \{0, ..., n\}^2, < P_k, P_l > = \begin{cases} 1 & \text{nếu } k = l \\ 0 & \text{nếu } k \neq l \end{cases} \\ \text{Với mọi } k \text{ thuộc } \{0, ..., n\}, P_k \text{ có bậc } k \text{ và có hệ tử cao nhất} > 0. \end{cases}$$

Vì: $\forall k \in \{0,...,n\}$, $\deg(P_k) = k$, nên $(P_0,...,P_n)$ là một cơ sở của E_n (xem 5.1.4, Nhận xét).

Mặt khác, E_n là một kgvc của E_{n+1} và $\dim(E_{n+1}) = n + 2 = \dim(E_n) + 1$. Do vậy tập trực giao của E_n trong E_{n+1} là một đường thẳng vectơ. Tồn tại $V_{n+1} \in E_{n+1} - \{0\}$ sao cho: $\forall P \in E_n, < P, V_{n+1} > = 0$.

Rõ ràng $V_{n+1} \notin E_n$ (nếu không: $\|V_{n+1}\|^2 = 0$), do vậy $\deg(V_{n+1}) = n + 1$.

Nếu cần ta có thể thay V_{n+1} bởi $- V_{n+1}$, ta có thể giả thiết rằng hệ tử cao nhất của V_{n+1} là > 0.

Khi đó rõ ràng đa thức P_{n+1} xác định bởi $P_{n+1} = \frac{1}{\|V_{n+1}\|} V_{n+1}$ thích hợp.

Nhận xét: Cũng có thể xây dựng $(P_n)_{n \in \mathbb{N}}$ bằng cách trực giao hóa (sau đó trực chuẩn hóa) $(X^n)_{n \in \mathbb{N}}$ bằng cách sử dụng thủ tục Schmidt (xem 10.2.1), dưới dạng áp dụng cho một họ được chỉ số hóa bởi $\mathbb{N}$.

Tính duy nhất

Giả sử có hai dãy $(P_n)_{n \in \mathbb{N}}$, $(Q_n)_{n \in \mathbb{N}}$ thích hợp.

Trước hết rõ ràng $P_0 = Q_0 = \frac{1}{\sqrt{2}}$.

Cho $n \in \mathbb{N}^*$, ta ký hiệu p_n (tương ứng : q_n) là hệ tử cao nhất của P_n (tương ứng : Q_n), và nhận xét rằng $p_nQ_n - q_nP_n$ có bậc $\leq n - 1$ (các hệ số bậc n triệt tiêu lẫn nhau).

Mặt khác P_n và Q_n trực giao với E_{n-1} , vì $(P_0,...,P_{n-1})$ và $(Q_0,...,Q_{n-1})$ đều sinh ra E_{n-1}. Do vậy $p_nQ_n - q_nP_n$ trực giao với E_{n-1}.

Từ đó suy ra : $p_nQ_n - q_nP_n = 0$.

Vì $\|P_n\| = \|Q\| = 1$ và $p_n > 0$ và $q_n > 0$, ta suy ra $p_n = q_n$, $P_n = Q_n$.

3) Cho $n \in \mathbb{N}^*$. Vì : $\forall k \in \{0,..., n - 1\}$, $\deg(P_k) = k$, $(P_0,...,P_{n-1})$ là một cơ sở của E_{n-1} . Vì P_n trực giao với $P_0,..., P_{n-1}$, ta được: $P_n \in E_{n-1}^{\perp}$. Vả lại , tính chất này đã xuất hiện trong lời giải của 2) trên đây.

II 1) a) Cho $n \in \mathbb{N}$. Vì $(X^2 - 1)^n$ chẵn, nên rõ ràng đạo hàm cấp n của nó chẵn nếu n chẵn, lẻ nếu n lẻ.

b) Cho $n \in \mathbb{N}$. Ta có: $\deg(U_n) = \deg(((X^2 - 1)^n)^{(n)}) - n = 2n - n = n$.

Hơn nữa, hạng tử chứa X^n của U_n là $(X^{2n})^{(n)}$, nghĩa là $\frac{(2n)!}{n!} X^n$.

◇ **Trả lời**: Hệ tử cao nhất của U_n là $\frac{(2n)!}{n!}$.

2) Với $(p, q) \in \mathbb{N}^2$, đặt $H_{p,q} = ((x^2 - 1)^p)^{(q)}$. Rõ ràng là :

$$\begin{cases} \forall p \in \mathbb{N}, \quad H_{p,p} = U_p \\ \forall (p,q) \in \mathbb{N}^2, \quad H'_{p,q} = H_{p,q+1} \\ \forall (p,q) \in \mathbb{N}^2, \quad (p > q \Rightarrow H_{p,q}(1) = H_{p,q}(-1) = 0). \end{cases}$$

Cho $(m, n) \in \mathbb{N}^2$ sao cho $m \neq n$; ta có thể giả thiết, chẳng hạn, $m > n$. Bằng một phép tích phân từng phần:

$$< U_m, U_n > = \int_{-1}^{1} H_{m,m}(x) H_{n,n}(x)\,dx = \left[H_{m,m-1}(x) H_{n,n}(x)\right]_{-1}^{1} - \int_{1}^{1} H_{m,m-1}(x) H_{n,n+1}(x)\,dx$$

$$= - < H_{m,m-1}, H_{n,n+1} >$$

Lặp lại (hoặc bằng quy nạp), ta có :

$$< U_m, U_n > = - < H_{m,m-1}, H_{n,n+1} > = < H_{m,m-2}, H_{n,n+2} > = \ldots = (-1)^m < H_{m,0}, H_{n,n+m} >.$$

Vì $n + m > 2n$, ta có $H_{n,n+m} = 0$, và do đó $< U_m, U_n > = 0$.

b) • Với cùng ký hiệu như ở a): $\|U_n\|^2 = < U_n, U_n > = (-1)^n < H_{n,0}, H_{n,2n} >$.

Nhưng $H_{n,0} = (X^2 - 1)^n$ và $H_{n,2n} = ((X^2 - 1)^n)^{(2n)} = (2n)!$, do đó: $\|U_n\|^2 = (2n)! \int_{-1}^{1} (1 - x^2)^n\,dx$.

• Với $(p, q) \in \mathbb{N}^2$, đặt $I_{p,q} = \int_{-1}^{1} (1 - x)^p (1 + x)^q\,dx$, do đó : $\|U_n\|^2 = (2n)!\, I_{n,n}$. Một phép tích phân từng phần (với $q \geq 1$) cho ta:

$$I_{p,q} = \left[-\frac{(1-x)^{p+1}}{p+1} (1+x)^q \right]_{-1}^{1} + \int_{-1}^{1} \frac{(1-x)^{p+1}}{p+1} q (1+x)^{q-1}\,dx = \frac{q}{p+1} I_{p+1,q-1},$$

do đó, bằng quy nạp dễ dàng suy ra: $I_{p,q} = \frac{q}{p+1} \frac{q-1}{p+2} \cdots \frac{1}{p+q} I_{p+q,0}$.

Và : $I_{p+q,0} = \int_{-1}^{1} (1-x)^{p+q}\,dx = \frac{2^{p+q+1}}{p+q+1}$. Do đó: $I_{p,q} = \frac{p!\,q!}{(p+q+1)!} 2^{p+q+1}$.

Ta suy ra: $\|U_n\|^2 = \frac{(n!)^2}{2n+1} 2^{2n+1}$.

◇ **Trả lời**: $\forall n \in \mathbb{N}, \|U_n\| = \sqrt{\frac{2}{2n+1}}\, 2^n n!$.

c) Theo II) 2) *a*) và *b*), dãy $\left(\frac{1}{2^n n!} \sqrt{\frac{2n+1}{2}} U_n \right)$ thỏa mãn các điều kiện của ***I*** 2).

Do tính duy nhất của $(P_n)_{n \in \mathbb{N}}$, ta suy ra: $\forall n \in \mathbb{N}, P_n = \frac{1}{2^n n!} \sqrt{\frac{2n+1}{2}}\, U_n$.

d) Dùng II *1*) *b*) và II 2) *c*).

◇ **Trả lời**: Hệ số cao nhất của P_n là $\frac{(2n)!}{2^n (n!)^2} \sqrt{\frac{2n+1}{2}}$, hoặc $\frac{C_{2n}^n}{2} \sqrt{\frac{2n+1}{2}}$.

3) Cho $n \in \mathbb{N}$. Rõ ràng: $(X^2 - 1) M_n' = 2nX(X^2 - 1)^n = 2nXM_n$.

Tính các đạo hàm cấp $n + 1$ và sử dụng công thức Leibniz, ta được:

$$(X^2 - 1) M_n^{(n+2)} + C_{n+1}^1 2X M_n^{(n+1)} + 2 C_{n+1}^2 M_n^{(n)} = 2n \left(XM_n^{(n+1)} + C_{n+1}^1 M_n^{(n)} \right),$$

do đó, vì $M_n^{(n)} = U_n$:

$$(X^2 - 1)U_n'' + (2C_{n+1}^1 - 2n)XU_n' + (2C_{n+1}^1 - 2nC_{n+1}^1)U_n = 0$$

tức là: $(X^2 - 1)U''_n + 2XU'_n - n(n+1)U_n = 0$.

Vì với n cố định L_n đồng phương với U_n, nên ta kết luận: $(1 - X^2)L''_n - 2XL'_n + n(n+1)L_n = 0$.

4) a) Với mọi k thuộc $\mathbb{N}$, gọi c_k là hệ số cao nhất của L_k.

Cho $n \in \mathbb{N}^*$. Đa thức $D_n = c_n L_{n+1} - c_{n+1} X L_n$ có bậc $\leq n$ (các hạng tử chứa X^{n+1} triệt tiêu lẫn nhau), và do vậy $D_n \in \text{Vect}(L_0,...,L_n)$.

• Với mọi k thuộc $\{0,...,n-2\}$, ta có : $< D_n, L_k > = = c_n < L_{n+1}, L_k > - c_{n+1} < L_n, XL_k > = 0$,

vì $< L_{n+1}, L_k > = 0$ $(n+1 \neq k)$ và $< L_n, XL_k > = 0$ ($L_n \in E_{n-1}^{\perp}$ và $XL_k \in E_{n-1}$).

Và : $< D_n, L_n > = c_n < L_{n+1}, L_n > - c_{n+1} < XL_n, L_n > = 0$.

vì $< L_{n+1}, L_n > = 0$ và $< XL_n, L_n > = \int_{-1}^{1} x(L_n(x))^2 dx = 0$ do XL_n^2 lẻ.

Điều đó chứng tỏ D_n trực giao với $L_0,...L_{n-2}, L_n$, do vậy đồng phương với L_{n-1}; tồn tại $\gamma_n \in \mathbb{R}$, sao cho $D_n = \gamma_n L_{n-1}$

• Tồn tại $R_{n-1}, R_{n-2} \in \mathbb{R}[X]$ sao cho : $\begin{cases} L_n = c_n X^n + R_{n-1} \text{ và } \deg(R_{n-1}) \leq n-1 \\ L_{n-1} = c_{n-1} X^{n-1} + R_{n-2} \text{ và } \deg(R_{n-2}) \leq n-2 \end{cases}$

Vì $L_{n-1} = \sqrt{\frac{2}{2n-1}} P_{n-1}$ (xem 2) c)) và $\|P_{n-1}\| = 1$, ta có: $\|L_{n-1}\| = \sqrt{\frac{2}{2n-1}}$. Do đó:

$$\frac{2}{2n-1}\gamma_n = \gamma_n \|L_{n-1}\|^2 = < \gamma_n L_{n-1}, L_{n-1} > = < c_n L_{n+1} - c_{n+1} X L_n, L_{n-1} > = -c_{n+1} < L_n, X L_{n-1} >$$

$$= -c_{n+1} < L_n, c_{n-1} X^n + XR_{n-2} > = -c_{n+1} c_{n-1} < L_n, X^n >,$$

vì $L_n \in E_{n-1}^{\perp}$ và $XR_{n-2} \in E_{n-1}$. Sau đó: $< L_n, c_n X^n > = < L_n, L_n - R_{n-1} > = \|L_n\|^2 = \frac{2}{2n+1}$.

Do đó : $\gamma_n = -\frac{(2n-1)c_{n+1}c_{n-1}}{(2n+1)c_n}$, và do vậy: $c_n L_{n+1} - c_{n+1} X L_n + \frac{(2n-1)c_{n+1}c_{n-1}}{(2n+1)c_n} L_{n-1} = 0$.

Ta đã thấy (/) b)): $\forall k \in \mathbb{N}$, $c_k = \frac{(2k)!}{2^k (k!)^2}$.

Một phép tính sơ cấp cho ta: $(n+1)L_{n+1} - (2n+1)XL_n + nL_{n-1} = 0$.

• Ta có $\begin{cases} U_0 = 1 \text{, do vậy } L_0 = 1 \\ U_1 = (X^2 - 1)' = 2X \text{, do vậy } L_1 = X \end{cases}$

Sau đó áp dụng công thức truy hồi trên, ta suy ra $L_2, L_3, ..., L_6$.

b) ◇ **Trả lời**:

$L_0 = 1$

$L_1 = X$

$L_2 = \frac{1}{2}(3X^2 - 1)$

$L_3 = \frac{1}{2}(5X^3 - 3X)$

$L_4 = \frac{1}{8}(35X^4 - 10X^2 + 3)$

$L_5 = \frac{1}{8}(63X^5 - 70X^3 + 15X)$

$L_6 = \frac{1}{16}(231X^6 - 315X^4 + 105X^2 - 5)$.

c) • *Tính* $L_n(1)$

Quy nạp theo n (hai bước):

• $L_0(1) = L_1(1) = 1$

• Nếu , với n cố định ($n \geq 1$), $L_{n-1}(1) = L_n(1) = 1$, thì :

$(n+1)L_{n+1}(1) = (2n+1)L_n(1) - nL_{n-1}(1) = n+1$, do vậy $L_{n+1} = 1$.

• Tính $L'_n(1)$

Sử dụng 3).

◇ **Trả lời** : Với mọi n thuộc $\mathbb{N}$: $L_n(1) = 1$, $L'_n(1) = \dfrac{n(n+1)}{2}$.

III 1) Cho $n \in \mathbb{N}$, $(x, y) \in \mathbb{R}^2$.

Theo II 4), với mọi k thuộc $\{0,...,n\}$, ta có (vẫn đặt $L_{-1} = 0$):

$$(k+1)L_{k+1} = (2k+1)XL_k - kL_{k-1},$$

do đó: $(k+1)(L_{k+1}(x)L_k(y) - L_k(x)L_{k+1}(y))$

$= ((2k+1)xL_k(x) - kL_{k-1}(x)L_k(y) - L_k(x)((2k+1)yL_k(y) - kL_{k-1}(y))$

$= (2k+1)(x-y)L_k(x)L_k(y) + k(L_k(x)L_{k-1}(y) - L_{k-1}(x)L_k(y))$,

tức là:

$(x-y)(2k+1)L_k(x)L_k(y) = (k+1)(L_{k+1}(x)L_k(y) - L_k(x)L_{k+1}(y)) - k(L_k(x)L_{k-1}(y) - L_{k-1}(x)L_k(y))$.

Cộng các đẳng thức đó từ k tới n, ta được:

$$(x-y)\sum_{k=0}^{n}(2k+1)L_k(x)L_k(y) = (n+1)(L_{n+1}(x)L_n(y) - L_n(x)L_{n+1}(y)),$$

vì $L_{-1} = 0$.

2) Cho $n \in \mathbb{N}^*$. Gọi $\alpha_1,...,\alpha_p$ là các không điểm của L_n có cấp lẻ và thuộc khoảng $]-1, 1[$, sắp xếp sao cho: $-1 < \alpha_1 < ... < \alpha_p < 1$ (như vậy ta có $0 \leq p \leq n$).

Giả sử $p < n$ và xét đa thức $V = \prod_{i=1}^{p}(X - \alpha_i)$. Khi đó $V \in E_{n-1}$, nên $\langle L_n, V \rangle = 0$, nghĩa là

$$\int_{-1}^{1} L_n(x)V(x)dx = 0,$$

Nhưng, theo cách chọn V, đa thức L_nV có dấu cố định (theo nghĩa rộng) trên $]-1, 1[$. Do đó, vì hơn nữa L_nV liên tục, nên ta suy ra: $\forall x \in [-1, 1]$, $(L_nV)(x) = 0$, nên $L_nV = 0$ (đa thức), $L_n = 0$ hoặc $V = 0$, mâu thuẫn.

Điều đó chứng tỏ $p \geq n$, và do đó $p = n$ (vì $\deg(L_n) = n$).

Như vậy, trong $]-1, 1[$, L_n có đúng n không điểm.

Vì $\deg(L_n) = n$, ta kết luận L_n tách được trên $\mathbb{R}$, với các không điểm đều là đơn và đều thuộc $]-1, 1[$.

3) a) Cho $n \in \mathbb{N}$, $x \in \mathbb{R}$. Theo *I*):

$$\forall y \in \mathbb{R} - \{x\}, \quad \frac{1}{n+1}\sum_{k=0}^{n}(2k+1)L_k(x)L_k(y) = \frac{L_{n+1}(x)L_n(y) - L_n(x)L_{n+1}(y)}{x-y}$$

$$= \frac{L_{n+1}(x) - L_{n+1}(y)}{x-y}L_n(y) - \frac{L_n(x) - L_n(y)}{x-y}L_{n+1}(y),$$

Cho y dần tới x và vì L_n và L_{n+1} khả vi (do vậy liên tục), ta được:

$$\frac{1}{n+1}\sum_{k=0}^{n}(2k+1)(L_k(x))^2 = L'_{n+1}(x)L_n(x) - L'_n(x)L_{n+1}(x).$$

b) Theo 2), L_{n+1} tách được trên $\mathbb{R}$ và có các không điểm đều là đơn, ở đây được ký hiệu là $\xi_1, \ldots, \xi_{n+1}$. Hơn nữa, $\deg(L_n) < \deg(L_{n+1})$. Theo định lý về sự phân tích thành các phân tử đơn giản, tồn tại $\lambda_1, \ldots \lambda_{n+1}$ sao cho: $F_n = \dfrac{L_n}{L_{n+1}} = \sum_{i=1}^{n+1} \dfrac{\lambda_i}{X - \xi_i}$.

Ta biết (xem 5.4.2, 2) *a*), Mệnh đề 2): $\forall i \in \{1, \ldots, n+1\}$, $\lambda_i = \dfrac{L_n(\xi_i)}{L'_{n+1}(\xi_i)}$.

Mặt khác, theo *a*) áp dụng tại $x = \xi_i$: $\dfrac{1}{n+1} \sum_{k=0}^{n} (2k+1)\big(L_k(\xi_i)\big)^2 = L'_{n+1}(\xi_i) L_n(\xi_i)$

Vì $L_0 = 1$ và $n \in \mathbb{N}^*$, rõ ràng $\sum_{k=0}^{n} (2k+1)\big(L_k(\xi_i)\big)^2 \geq 1 > 0$, và vì vậy: $\lambda_i > 0$.

4) Giữ lại các ký hiệu của 3) *b*): $F_n = \dfrac{L_n}{L_{n+1}} = \sum_{i=1}^{n+1} \dfrac{\lambda_i}{X - \xi_{n+1,i}}$, do đó: $F'_n = -\sum_{i=1}^{n+1} \dfrac{\lambda_i}{(X - \xi_{n+1,i})^2}$.

Từ đó ta suy ra sự biến thiên của hàm hữu tỷ F_n trên $\mathbb{R}$:

x	$-\infty$		$\xi_{n+1,1}$	$\cdots$	$\xi_{n+1,i}$		$\xi_{n+1,i+1}$	$\cdots$	$\xi_{n+1,n+1}$		$+\infty$
$F_n(x)$	0	$\searrow$	$+\infty$	$\cdots$	$+\infty$	$\searrow$	$+\infty$	$\cdots$	$+\infty$	$\searrow$	0
			$-\infty$		$-\infty$						

Theo định lý về giá trị trung gian, F_n có ít nhất n không điểm thực $x_1, \ldots, x_n$ sao cho:

$$\xi_{n+1,1} < x_1 < \xi_{n+1,2} < \ldots < \xi_{n+1,i} < x_i < \xi_{n+1,i+1} < \ldots < \xi_{n+1,n} < x_n < \xi_{n+1,n+1}$$

Vì $F_n = \dfrac{L_n}{L_{n-1}}$, rõ ràng: $\forall i \in \{1, \ldots, n\}$, $\xi_{n,i} = x_i$

5) Trường hợp $c = 0$ đã gặp ở 2). Giả sử $c \neq 0$ và đặt $A_n = L_n + cL_{n-1}$

Cho $i \in \{1, \ldots, n-1\}$

Theo 4): $L_{n-1}(\xi_{n,i}) L_{n-1}(\xi_{n,i+1}) < 0$, vì trong $]\xi_{n,i}; \xi_{n,i+1}[$ L_{n-1} có một không điểm và chỉ một, và đó là một không điểm đơn.

Do đó: $A_n(\xi_{n,i})\, A_n(\xi_{n,i+1}) = c^2 L_{n-1}(\xi_{n,i}) L_{n-1}(\xi_{n,i+1}) < 0$.

Theo định lý về giá trị trung gian, A_n có ít nhất một không điểm, ký hiệu là u_i, trong khoảng $]\xi_{n,i}; \xi_{n,i+1}[$.

Ta chứng tỏ rằng u_i là không điểm đơn của A_n. Lập luận phản chứng: giả sử u_i là không điểm cấp bội ít nhất 2 của A_n

Khi đó: $A_n(u_i) = A'_n(u_i) = 0$, nên: $L_n(x_i) = -cL_{n-1}(u_i)$ và $L'_n(u_i) = -cL'_{n-1}(u_i)$, và do đó:

$$L'_n(u_i) L_{n-1}(u_i) - L'_{n-1}(u_i) L_n(u_i) = 0.$$

Nhưng khi đó (xem 3) *a*)): $\sum_{k=0}^{n-1} (2k+1)\big(L_k(u_i)\big)^2 = 0$;

mâu thuẫn, vì $\sum_{k=0}^{n-1} (2k+1)\big(L_k(u_i)\big)^2 \geq \big(L_0(u_i)\big)^2 = 1$.

Như vậy, A_n có ít nhất $n-1$ không điểm $u_1, \ldots, u_{n-1}$, tất cả đều là đơn và thuộc khoảng $]-1; 1[$. Vì $\deg(A_n) = n$, nên khi đó rõ ràng A_n có đúng n không điểm thực và tất cả đều là đơn ($n-1$ trong số chúng thuộc khoảng $]-1; 1[$).

Bảng ký hiệu

$P \circ Q$, $P(Q)$,147
P', $P^{(K)}$, 147
$\widetilde{P}$, 148
$\widetilde{P}(f)$, $\widetilde{P}(A)$, 149
$A[X]$, $K[X,Y]$, $K[X_1, \ldots, X_n]$, 152
$A \mid P$, 154
$P \circ K[X]$, 158
UCLN, UCLN$(P_1,\ldots,P_n)$, UCLN$((P_i)_{1\le i\le n})$, BCNN, BCNN$(P_1,\ldots,P_n)$, BCNN$((P_i)_{1\le i\le n})$ 160
$P \wedge Q$, $P \vee Q$, 161
PTNT, 166
$\sigma_1, \sigma_2, \ldots, \sigma_n$, 172
$K(X)$, $\frac{A}{S}$, 186
deg (F), 188
F',189
$F^{(n)}$, $\widetilde{F}$, 190
0, 0_K, 0_E, 208
$\sum$, $\sum_{i=1}^{n}$, 209
kgvc, K-kgvc, 211
$F_1 + F_2$, $V(E)$, $F_1 \oplus F_2$, 212
Vect(A), 219
Vect$((x_i)_{i\in I})$, 220
$F_1 + F_2 + \ldots + F_n$, $\sum_{i=1}^{n} F_i$, $F_1 \oplus \ldots \oplus F_n$, $\bigoplus_{i=1}^{n} F_i$, 221
$\dim_K(E)$, $\dim(E)$, 228
rank$(\mathcal{F})$, 234
$\mathcal{L}(E,F)$, $\mathcal{L}_K(E,F)$, $\mathcal{L}_K(E)$, $\mathcal{GL}(E)$, $\mathcal{GL}_K(E)$, 237
E^*, 238
h_α, 239
Ker(f), Im(f), 242
rank(f) 254
δ_{ij}, 258
$(a_{ij})_{1\le i\le n}$, $a(i,j)_{1\le i\le n,1\le j\le p}$, $a(i,j)_{i,j}$, $_{1\le j\le p}$
$\begin{pmatrix} a_{11} & \cdots & a_{1p} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{np} \end{pmatrix}$, 261
$\mathbf{M}_{n,p}(K)$, $\mathbf{M}_n(K)$, Mat$_{\mathcal{B}}(x)$, Mat$_{\mathcal{B}}(\mathcal{F})$, 262
Mat$_{\mathcal{B},\mathcal{C}}(f)$, Mat$_{\mathcal{B}}(f)$, 263
$A + B$, αA, 264
$0_{n,p}$, 0, 0, $E_{i,j}$, 265
AB, 266
I_n, 269
$\nu(A)$, Ker(A), Im(A), 270
A^{-1}, $\mathbf{GL}_n(K)$, 272
rank(A), 276
$P_{i,j}$, 279
$D_{i,\alpha}$, $T_{i,j,\alpha}$, 280
^tA, 283
tr(A), 284
Pass $(\mathcal{B},\mathcal{B}')$, 286
A id B, $J_{n,p,r}$, 288
$A \sim B$, 291
tr(f), 292
$\mathbf{S}_n(K)$, 293
$\mathbf{A}_n(K)$, 294
$\mathbf{T}_{n,s}(K)$, $\mathbf{T}_{n,i}(K)$, 295
$\mathbf{D}_n(K)$, diag$(\lambda_1, \ldots, \lambda_n)$, 298
$\mathcal{L}_p(E_1, \ldots, E_n; F)$, 302
$A_n(E)$, $\det_{\mathcal{B}}$, $\det_{\mathcal{B}}(V_1, \ldots, V_n)$, 305
$\beta(E)$, 306
det (f), 307
det(A), $\begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix}$, $\begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix}_{[n]}$ 309
$\mathbf{SL}_n(K)$, 311
Δ_{ij}, 314
A_{ij}, 345
com(A), 316
$V(x_1, \ldots x_n)$, 322
$\mathcal{R}$, 327
φ, $\varphi(x,y)$, $(x \mid y)$, $< x,y >$, $x \cdot y$, 339
ϕ, 341
$\| . \|$, $\| x \|$, d, $d(x, y)$, 343
$x \perp y$, $x \perp A$, $A^\perp$, 345
c.s.t.c., 350
p_F, $d(x,F)$, 352
s_F, 353
$\mathcal{O}(E, <\cdot,\cdot>)$, $\mathcal{O}(E)$, 356
$\mathbf{O}_n(\mathbb{R})$, 358
$\mathcal{SO}(E)$, $\mathbf{SO}_n(\mathbb{R})$, c.s.t.c.t., $[V_1,\ldots, V_n]$, 360
Rot$_\theta$, 362
(u,v), 363
Rot$_{\vec{\Lambda},\theta}$, 368
$[u,v,w]$, $u \wedge v$, $u \times v$, 375

Bảng thuật ngữ

A

B

C

D

Đ

E

F

G

H

I

K

L

M

N

O

P

Q, R

S

T

Ư

V

W

Chịu trách nhiệm xuất bản :
Chủ tịch HĐQT kiêm Tổng Giám đốc NGÔ TRẦN ÁI
Phó Tổng Giám đốc kiêm Tổng biên tập NGUYỄN QUÝ THAO

Biên tập :
NGUYỄN VĂN THƯỜNG
Biên tập tái bản :
TRẦN PHƯƠNG DUNG
Sửa bản in :
NGUYỄN VĂN THƯỜNG
Sắp chữ :
PHÒNG CHẾ BẢN (NXB GIÁO DỤC)

GIÁO TRÌNH TOÁN - TẬP 5
ĐẠI SỐ 1

In 1500 bản, khổ 16x24cm, tại Trung tâm Công nghệ Thông tin Chế bản và In Nhà xuất bản Thế Giới. Giấy chấp nhận đăng ký kế hoạch xuất bản: 194-2006/CXB/3-323/GD cấp ngày 22-3-2006.
In xong và nộp lưu chiểu quý II năm 2006.

Jean-Marie Monier

ĐẠI SỐ 1

Giáo trình và 600 bài tập có lời giải

Giáo trình Toán - Tập 5

Mục tiêu của bộ giáo trình Toán này là cung cấp cho sinh viên những năm đầu của các trường đại học khoa học và kỹ thuật một tài liệu học tập, tra cứu thông dụng và có hiệu quả. Với nhiều bài tập có lời giải, đa dạng, bao quát mọi khía cạnh của lý thuyết, cuốn sách còn nhằm giúp cho người học rèn luyện năng lực vận dụng lý thuyết được học.

8 934980 640203

Tập 5 đề cập việc khảo sát cấu trúc đại số, số học các số nguyên, số hữu tỷ, đa thức và phân thức hữu tỷ, các không gian vecto và các ánh xạ tuyến tính, ma trận, định thức và các không gian Euclide.

Giá: 56.000đ