

**BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC SƯ PHẠM TP. HỒ CHÍ MINH**

LƯU THỊ THANH HÀ

**THUẬT TOÁN TÌM CƠ SỞ CỦA CÁC
MÔĐUN CON CỦA MÔĐUN TỰ DO HỮU
HẠN SINH TRÊN VÀNH CHÍNH**

Chuyên ngành: **Đại số và lý thuyết số**

Mã số: **60 46 05**

LUẬN VĂN THẠC SĨ TOÁN HỌC

**NGƯỜI HƯỚNG DẪN KHOA HỌC:
TS. TRẦN HUYỀN**

Thành phố Hồ Chí Minh - 2010

LỜI CẢM ƠN

Khi thầy Huyền nói với tôi về ý tưởng của đề tài này,
thầy đã có cái nhìn gần như hoàn chỉnh về mọi mặt của đề tài.
Thầy gọi tôi lại, chỉ nêu những ý chính và để tôi tự chứng minh, tìm thuật toán.
Thầy tìm người học trò để hướng dẫn nghiên cứu.
Tôi muốn cảm ơn thầy vì sự tin tưởng và tấm lòng thầy dạy dỗ.
Tôi cảm ơn các thầy cô đã dạy dỗ tôi trong suốt những năm tháng qua, giúp tôi
đạt được kết quả hôm nay.
Sự quan tâm của các thầy cô là nguồn động viên rất lớn của tôi.

Chương 1

MỞ ĐẦU

Đối tượng nghiên cứu của luận văn là cơ sở của các môđun tự do hữu hạn sinh trên vành chính. Nói về môđun tự do hữu hạn sinh trên vành chính, lý thuyết môđun đã có những kết quả rất phong phú và sâu sắc. Ta có thể nêu hai kết quả sau đây:

Định lý: Trên vành chính, môđun con của môđun tự do lại là tự do.

Định lý: Nếu F là môđun tự do trên vành chính R và M là môđun con hữu hạn sinh $\neq 0$ của F ; khi đó tồn tại một cơ sở $\mathcal{B}$ của F và các phần tử $e_1, e_2, \dots, e_m$ trong cơ sở đó và các phần tử khác không $a_1, a_2, \dots, a_m \in R$ sao cho:

1. Các phần tử $a_1e_1, a_2e_2, \dots, a_me_m$ là cơ sở của M trên R .
2. Ta có $a_i | a_{i+1}$ với $i = 1, \dots, m-1$.

Dãy các idêan $(a_1), (a_2), \dots, (a_m)$ là xác định duy nhất theo các điều kiện trên.

Tuy nhiên các kết quả nêu trên chỉ nói lên sự *tồn tại* của các phần tử cơ sở, cho nên còn mang nặng tính lý thuyết. Mục đích của chúng tôi trong đề tài này là xây dựng thuật toán tìm cơ sở của môđun con của một môđun. Đặc biệt chúng tôi muốn xây dựng thuật toán tìm giao và tổng hai môđun con có cơ sở cho trước.

Thuật toán có thể ứng dụng để tìm cơ sở của các nhóm con của nhóm aben tự do hữu hạn sinh (vốn là các $\mathbb{Z}$ -môđun), môđun tự do hữu hạn sinh trên vành đa thức trên trường, môđun tự do hữu hạn sinh trên vành số nguyên Gauss,...

TỔNG QUAN VỀ ĐỀ TÀI

Trong đề tài này, chúng tôi đưa ra một khái niệm mới “đơn tử”, xem xét tính đơn tử của các phần tử cơ sở. Chúng tôi khẳng định một đơn tử luôn có thể bổ sung thành cơ sở. Từ đó xây dựng nên một thuật toán tìm cơ sở của môđun. Nghiên cứu thuật toán trong những trường hợp cụ thể chúng tôi đưa ra các thuật toán tìm giao của hai môđun con có cơ sở cho trước và thuật toán tìm cơ sở của môđun con cho bởi một hệ sinh.

Trong quá trình thực hiện đề tài, chúng tôi cũng chứng minh lại được một số kết quả của lý thuyết môđun. Việc làm này thể hiện một cách nhìn mới về lý thuyết môđun. Những kết quả của đề tài cũng mô tả rõ hơn về các phần tử cơ sở của môđun con, mối quan hệ giữa cơ sở môđun với môđun con của nó.

Để minh họa cho các thuật toán, chúng tôi nêu các ví dụ áp dụng cho từng thuật toán. Trong đó có các ví dụ trên nhóm aben tự do hạng hữu hạn, môđun tự do hữu hạn sinh trên vành đa thức trên trường (như $\mathbb{Z}_7[x], \mathbb{Q}[x], \dots$) và trên vành số nguyên Gauss $\mathbb{Z}[i]$.

Chương 2

MỘT SỐ KIẾN THỨC CHUẨN BỊ

2.1 Các kết quả về vành chính

2.1.1 Định nghĩa vành chính

Một miền nguyên được gọi là *vành chính* nếu mọi ideal của nó là ideal chính.

Miền nguyên là một vành có nhiều hơn một phần tử, giao hoán, có đơn vị, không có ước của 0 (sẽ định nghĩa dưới đây).

Idéal chính là ideal sinh ra bởi một phần tử.

2.1.2 Các tính chất số học trên vành chính

Tính chia hết

Giả sử R là một vành giao hoán. Ta nói phần tử $a \in R$ là *bội* của một phần tử $b \in R$ hay a *chia hết cho* b , kí hiệu $a : b$, nếu có $c \in R$ sao cho $a = bc$; ta còn nói rằng b là *ước* của a hay b *chia hết* a , kí hiệu $b \mid a$.

Như vậy, theo định nghĩa trên, mọi phần tử $x \in R$ là *ước của 0*; nhưng ta lại định nghĩa:

Một phần tử $a \neq 0$ được gọi là *ước của 0* nếu có $b \neq 0$ sao cho $ab = 0$.

Một số tính chất cơ bản về tính chia hết:

- $a \mid a$.

- $c \mid b$ và $b \mid a$ kéo theo $c \mid a$.
- u khả nghịch, $u \mid a$ với mọi a .
- Nếu $b \mid u$ với u khả nghịch, thì b khả nghịch.
- Quan hệ S xác định như sau: xx' khi $x' = ux$ với u khả nghịch, là một quan hệ tương đương; x và x' gọi là liên kết.

x và x' là liên kết khi và chỉ khi $x \mid x'$ và $x' \mid x$.

Kí hiệu: $Ra = \{xa, x \in R\}$, ta có: $a \mid b$ khi và chỉ khi $Ra \supset Rb$.

x và x' liên kết khi và chỉ khi $Rx = Rx'$. Đặc biệt: u khả nghịch khi và chỉ khi $Ru = R$.

Ta gọi các phần tử liên kết với x và các phần tử khả nghịch là các ước *các ước không thực sự* của x , còn các ước khác của x là các *ước thực sự* của x .

Giả sử x là một phần tử khác 0 và không khả nghịch của R ; x gọi là một *phần tử bất khả quy* của R nếu x không có ước thực sự.

Định nghĩa 1 Nếu $c \mid a$ và $c \mid b$ thì c gọi là ước chung của a và b . Phần tử c gọi là ước chung lớn nhất (ƯCLN) của a và b nếu c là ước chung của a và b , đồng thời mọi ước chung của a và b đều là ước của c .

Hai ước chung lớn nhất của a và b là liên kết với nhau, do đó có thể coi là bằng nhau nếu không kể nhân tử khả nghịch.

Tương tự ta định nghĩa ước chung lớn nhất của ba phần tử trở lên như sau:

Định nghĩa 2 Cho $a_1, a_2, \dots, a_n$ là những phần tử của vành chính R . Nếu $c \mid a_i$ với mọi $i = 1, 2, \dots, n$ thì ta nói c là ước chung của $a_1, a_2, \dots, a_n$.

c sẽ được gọi là ước chung lớn nhất của $a_1, a_2, \dots, a_n$ nếu c là ước chung của $a_1, a_2, \dots, a_n$ và mọi ước chung khác đều là ước của c .

Trong các kết quả dưới đây chúng ta luôn xét R là vành chính và các phần tử là thuộc vành chính R

Định lý 1 Với R là vành chính thì ước chung lớn nhất của hai phần tử a, b bất kỳ luôn tồn tại.

Chứng minh

Gọi I là ideal sinh ra bởi a và b . Các phần tử thuộc I có dạng $ax + by$ với $x, y \in R$.

Mặt khác vì R là vành chính nên I sinh ra bởi một phần tử d nào đó, phần tử d cũng thuộc I nên d có dạng

$$d = ax + by, \quad x, y \in R \quad (1)$$

Ta sẽ chứng minh d là ước chung của a và b . Thật vậy: vì $a, b \in I = Rd$ nên $a = a'd$ và $b = b'd$ với $a', b' \in R$. Vậy d là ước chung của a và b .

Nếu c là một ước chung khác của a và b thì ta có $a = ca''$ và $b = cb''$ với $a'', b'' \in R$.

Lúc bấy giờ (1) sẽ trở thành: $d = c(a''x + b''y)$.

Suy ra c là ước của d .

Vậy d là ước chung lớn nhất của a và b .

□

Hệ quả 1 Nếu e là một ước chung lớn nhất của a và b , thì có $r, s \in R$ sao cho

$$e = ra + sb$$

Hai phần tử a, b được gọi là *nguyên tố cùng nhau* nếu chúng nhận 1 làm ước chung lớn nhất.

Theo hệ quả trên: nếu a, b nguyên tố cùng nhau thì tồn tại $r, s \in R$ sao cho

$$1 = ra + sb$$

Các kết quả trên đều có thể dễ dàng mở rộng cho n phần tử, với $n \geq 2$:

Nếu R là vành chính thì ước chung lớn nhất của n ($n \geq 2$) phần tử bất kỳ $a_1, a_2, \dots, a_n \in R$ luôn tồn tại.

Nếu d là ước chung lớn nhất của $a_1, a_2, \dots, a_n \in R$ thì tồn tại $r_1, r_2, \dots, r_n \in R$ sao cho:

$$d = r_1 a_1 + r_2 a_2 + \dots + r_n a_n$$

Hệ quả 2 Nếu $c \mid ab$ và c, a nguyên tố cùng nhau, thì $c \mid b$.

Chứng minh

Vì a, c nguyên tố cùng nhau nên từ hệ quả vừa nêu trên ta có $r, s \in R$ sao cho

$$1 = ar + cs$$

Nhân 2 vế đẳng thức với b :

$$b = abr + bcs$$

Vì $c \mid ab$ nên có $q \in R$ sao cho $ab = cq$. Do đó

$$b = c(qr + bs)$$

tức là $c \mid b$.

□

Tính chất Nếu d là ước chung lớn nhất của a, b , thì $a = da', b = db'$ với $a', b' \in R$ và a', b' nguyên tố cùng nhau.

Thật vậy:

Vì d là ước chung của a và b nên $a = da'$ và $b = db'$ với $a', b' \in R$.

Gọi e là ước chung lớn nhất của a' và b' , ta có $a' = ea_1, b' = eb_1$. Từ đây suy ra:

$$a = dea_1, \quad b = deb_1$$

Tức là de là ước chung của a và b . Vì d là ước chung lớn nhất nên $de \mid d$, do đó $e \mid 1$. Như vậy ước chung lớn nhất của a', b' là 1 hay a', b' nguyên tố cùng nhau.

2.2 Các kết quả về môđun

2.2.1 Định nghĩa môđun và môđun con

Cho vành R có đơn vị (đơn vị của R kí hiệu là 1). Nhóm cộng aben $(X, +)$ sẽ được gọi là *môđun trái trên vành R* nếu trên X ta đã xác định được một tác động

trái từ R , tức là có ánh xạ $\mu : R \rightarrow X$, ta kí hiệu $\mu(r, x) = rx$ và gọi là tích của hệ tử r với phần tử x . Ngoài ra các tiên đề sau cần được thỏa mãn với mọi $x, y \in X$ và $r, s \in R$:

1. $1.x = x$,
2. $(rs)x = r(sx)$,
3. $r(x + y) = rx + ry$,
4. $(r + s)x = rx + sx$.

Tác động trái từ R vào X còn gọi là phép nhân ngoài từ R vào X . Vành R gọi là *vành hệ tử* hay *vành các vô hướng*.

Môđun trái được gọi đơn giản là môđun.

Mỗi nhóm cộng aben $(A, +)$ luôn có thể xem là môđun trái trên vành các số nguyên $\mathbb{Z}$ với phép nhân ngoài được định nghĩa như sau: với mỗi $n > 0$, $na = a + a + \dots + a$ (n số hạng) và $(-n)a = -na$, $0.a = 0$. Có thể dễ dàng kiểm tra phép nhân ngoài này thỏa mãn các tiên đề 1) đến 4).

Nếu A, B là các tập con của một môđun X và $K \subset R$ với $A, B, K \neq \emptyset$, ta định nghĩa:

$$A + B = \{a + b | a \in A, b \in B\}; \quad KA = \{ra | r \in K, a \in A\}$$

Nếu $A + A \subset A$ và $RA \subset A$ thì ta nói A là bộ phận ổn định của X . Mỗi bộ phận ổn định của môđun X cùng với các phép toán cảm sinh lập thành một môđun, gọi là *môđun con của X* .

Nếu A, B là các môđun con của môđun X . Khi đó $A + B$ là môđun con của X .

Mỗi nhóm con của nhóm aben có thể xem là $\mathbb{Z}$ -môđun con.

2.2.2 Môđun con sinh bởi một tập

Giao của một họ khác rỗng các môđun con của X lại là môđun con của X .

Xét S là một tập con của môđun X . Xét họ $\mathcal{T}$ tất cả các môđun con của X chứa S . Hiển nhiên $\mathcal{T}$ khác rỗng vì $X \in \mathcal{T}$. Giao của họ $\mathcal{T}$ là một môđun con của X , chứa S , gọi là *môđun con của X sinh bởi tập S* (kí hiệu $\langle S \rangle$) và S được gọi là *tập sinh* hay *hệ sinh* của môđun $\langle S \rangle$.

Từ cách xác định trên đây có thể thấy là $\langle S \rangle$ là môđun con nhỏ nhất trong X chứa S , có nghĩa là $\langle S \rangle$ được chứa trong mọi môđun con của X chứa S .

Để mô tả $\langle S \rangle$ với $S \neq \emptyset$ ta định nghĩa một tổ hợp tuyến tính của S là một tổng hữu hạn dạng:

$$r_1x_1 + r_2x_2 + \dots + r_nx_n$$

trong đó $r_1, r_2, \dots, r_n \in R$ và $x_1, x_2, \dots, x_n \in S$.

Có thể dễ dàng chứng minh được: “Môđun con sinh bởi tập $S \subset X, S \neq \emptyset$ là môđun con gồm tất cả các tổ hợp tuyến tính của S .”

2.2.3 Môđun thương

Cho X là môđun và $A \triangleleft X$. Khi đó $(A, +)$ là nhóm con của nhóm $(X, +)$ và do đó A là nhóm con chuẩn tắc của X . Theo lý thuyết nhóm, ta có thương $(X/A, +)$ và do X giao hoán nên nhóm cộng X/A cũng giao hoán.

Ta xác định trên X/A phép nhân ngoài từ R như sau:

$$\forall r \in R, \forall x + A \in X/A : \quad r(x + A) = rx + A$$

Với phép nhân ngoài trên X/A có cấu trúc R -môđun và được gọi là *môđun thương của môđun X theo môđun con A* .

2.2.4 Đồng cấu môđun

Cho X, Y là các R -môđun. Ánh xạ $f : X \rightarrow Y$ được gọi là R -đồng cấu nếu với mọi $x, x_1, x_2 \in X$ và với mọi $r \in R$:

$$f(x_1 + x_2) = f(x_1) + f(x_2)$$

$$f(rx) = rf(x)$$

Ta cũng gọi $\ker f = f^{-1}(0) \triangleleft X$ là hạt nhân của đồng cấu f . $\operatorname{Im} f = f(X) \triangleleft Y$ là ảnh của đồng cấu f .

2.2.5 Tổng trực tiếp của hai môđun

Cho A, B là các R -môđun. Trên tập tích Descartes $A \times B$ ta đưa vào hai phép toán cộng và nhân ngoài như sau:

$$= (a_1 + a_2, b_1 + b_2)$$

$$r(a, b) = (ra, rb)$$

với mọi $(a_1, b_1), (a_2, b_2), (a, b) \in A \times B$ và mọi $r \in R$.

Dễ dàng kiểm tra $A \times B$ cùng với hai phép toán xác định như trên thỏa mãn tất cả các yêu cầu của một R -môđun. Ta gọi đó là *môđun tổng trực tiếp* của hai môđun A, B và kí hiệu là $A \oplus B$.

Tổng trực tiếp của hai môđun A, B đôi khi còn được gọi là tích trực tiếp và kí hiệu là $A \times B$.

2.2.6 Tổng trực tiếp trong của hai môđun

Cho A, B là các môđun con của môđun X thỏa các tính chất:

1. $A \cap B = \emptyset$,
2. $A + B = X$.

Khi đó ta có đẳng cấu: $X \cong A \oplus B$.

Thay cho dấu $\cong$ ta có thể viết $X = A \oplus B$ và ta nói X là *tổng trực tiếp trong* của hai môđun con A, B .

Môđun X là tổng trực tiếp trong của hai môđun con A và B khi và chỉ khi với mỗi $x \in X$ có một và chỉ một cách biểu diễn $x = a + b$ với $a \in A, b \in B$.

Môđun con A của X được gọi là *hạng tử trực tiếp* của X nếu có môđun con $B \triangleleft X$ sao cho $X = A \oplus B$. Khi đó B cũng được gọi là *hạng tử bù trực tiếp* của môđun con A .

2.2.7 Tổng trực tiếp của họ môđun

Cho họ không rỗng các tập hợp $\{A_i\}_{i \in I}$. *Tích Descartes* của họ tập hợp $\{A_i\}$, kí hiệu là $\prod_{i \in I} A_i$ là tập hợp các hàm $x : I \longrightarrow \cup A_i$ sao cho $x(i) \in A_i, \forall i \in I$.

Bởi mỗi hàm $x \in \prod A_i$ được xác định một cách duy nhất bởi bộ giá trị $((x(i))_{i \in I})$ nên ta có quyền đồng nhất hàm x với bộ giá trị $(x(i))$ của nó. Và ta kí hiệu $x_i = x(i)$ thì phần tử của $\prod A_i$ là bộ $x = (x_i)_{i \in I}$ với điều kiện $x_i \in A_i, \forall i \in I$.

Vậy: $\prod_{i \in I} A_i = \{(x_i)_{i \in I} | x_i \in A_i, \forall i \in I\}$

Đôi khi để tránh rườm rà, bộ $x = (x_i)_{i \in I}$ được viết gọn thành $x = (x_i)$.

Với họ bất kỳ khác rỗng các môđun $\{X_i\}_{i \in I}$ trên cùng vành hệ tử R ; ta xác định trên tập tích Descartes $\prod X_i$ các phép toán sau:

- $(x_i) + (x'_i) = (x_i + x'_i)$
- $r(x_i) = (rx_i)$

với mọi $(x_i), (x'_i) \in \prod X_i$ và mọi $r \in R$.

Bây giờ, $\prod X_i$ cùng với hai phép toán trên lập thành một môđun, gọi là *môđun tích trực tiếp* của họ $\{X_i\}$.

Cho họ không rỗng các môđun $\{X_i\}_{i \in x}$. Xét tập con của $\prod X_i$ gồm các bộ $x = (x_i)$ mà hầu hết các thành phần $x_i = 0$, trừ ra một số hữu hạn.

Dễ thấy đó là tập con ổn định trong $\prod X_i$, và do vậy nó là môđun con. Ta gọi đó là *môđun tổng trực tiếp* của họ $\{X_i\}$ và kí hiệu là: $\oplus_{i \in I} X_i$ hay $\oplus X_i$

2.2.8 Tổng trực tiếp trong của họ môđun con

Nếu họ $\{X_t\}_{t \in I}$ các môđun con của môđun X thỏa:

1. $\sum X_t = X$,
2. $X_t \cap \sum_{i \neq t} X_i = 0, \forall t \in I$.

thì khi đó: $X \cong \oplus X_t$.

Trong trường hợp này, ta viết $X = \oplus X_t$ và gọi X là *tổng trực tiếp trong* của họ môđun $\{X_t\}$ của nó.

2.2.9 Dây khớp và dây khớp ngắn

Dãy các đồng cấu (hữu hạn hay vô hạn)

$$\cdots \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow \cdots \quad (1)$$

được gọi là *khớp tại môđun B* nếu $\text{Im} f = \ker g$, tức là ảnh đồng cấu vào tại đó bằng hạt nhân của đồng cấu ra.

Một môđun trong dãy các đồng cấu được gọi là môđun trung gian nếu tại đó vừa có đồng cấu vào, vừa có đồng cấu ra.

Dãy các đồng cấu (1) được gọi là *dãy khớp* nếu nó khớp tại mỗi môđun trung gian.

Ta gọi dãy khớp có dạng:

$$0 \rightarrow A \xrightarrow{\chi} B \xrightarrow{\sigma} C \rightarrow 0 \quad (2)$$

là dãy khớp ngắn.

Để kiểm tra tính khớp của dãy (2) ta cần kiểm tra: χ là đơn cấu, σ là toàn cấu và $\ker \sigma = \text{Im} \chi$.

2.2.10 Dây khớp ngắn chẻ

Dãy khớp các đồng cấu:

$$\cdots \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow \cdots \quad (1)$$

được gọi là *chẻ ra tại môđun B*, nếu $\text{Im} f$ là một hạng tử trực tiếp của B , tức là tồn tại môđun con B_1 sao cho $B = \text{Im} f \oplus B_1$.

Một dãy khớp được gọi là *chẻ*, nếu nó chẻ tại mỗi môđun trung gian.

Một dãy khớp ngắn

$$0 \rightarrow A \xrightarrow{\chi} B \xrightarrow{\sigma} C \rightarrow 0$$

là chẻ khi và chỉ khi dãy chẻ tại B .

Đối với mỗi dãy khớp ngắn

$$0 \rightarrow A \xrightarrow{\chi} B \xrightarrow{\sigma} C \rightarrow 0$$

ba phát biểu sau là tương đương:

- (i) Dãy là chẻ ra.
- (ii) Đồng cấu χ có nghịch đảo trái.
- (iii) Đồng cấu σ có nghịch đảo phải.

Nếu dãy khớp $\cdots \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow \cdots$ chẻ ra tại B thì ta có:

$$B \cong \text{Im} f \oplus \text{Im} g$$

.

2.2.11 Môđun tự do

Cơ sở môđun

Cho môđun X . Tập $S \subset X$ được gọi là *hệ sinh* của X nếu $\langle S \rangle = X$. Nói cách khác, S là hệ sinh của X nếu với bất kì phần tử $x \in X$ thì

$$x = r_1 s_1 + r_2 s_2 + \cdots + r_n s_n$$

với $r_1, r_2, \dots, r_n \in R$ và $s_1, s_2, \dots, s_n \in S$, tức x biểu thị được dưới dạng tổ hợp tuyến tính của S .

Tập hợp $S \subset X$ được gọi là *độc lập tuyến tính* nếu phần tử $0 \in X$ chỉ có một cách biểu thị dưới dạng tổ hợp tuyến tính của S , đó là tổ hợp tuyến tính tầm thường với tất cả các hệ tử đều bằng 0. Nói cách khác, S là độc lập tuyến tính nếu

$$r_1 s_1 + r_2 s_2 + \cdots + r_n s_n = 0 \quad \text{kéo theo} \quad r_1 = r_2 = \cdots = r_n = 0.$$

Khi $S \subset X$ không là độc lập tuyến tính, ta nói S là *phụ thuộc tuyến tính*. Như vậy, tập S phụ thuộc tuyến tính nếu tồn tại ít nhất một tổ hợp tuyến tính không tầm thường của S bằng 0. Nói cách khác, tồn tại các phần tử $s_1, s_2, \dots, s_n \in S$ và các hệ tử $r_1, r_2, \dots, r_n \in R$ không đồng thời bằng 0 mà:

$$r_1 s_1 + r_2 s_2 + \cdots + r_n s_n = 0$$

Một hệ sinh S của môđun X đồng thời là hệ độc lập tuyến tính được gọi là *cơ sở* của môđun X .

Môđun X có cơ sở được gọi là *môđun tự do*.

Một số tính chất của cơ sở:

Định lý 2 Tập $S = \{x_\alpha\}_{\alpha \in I}$ các phần tử của môđun X là cơ sở của X khi và chỉ khi mỗi phần tử $x \in X$ chỉ có một cách biểu thị tuyến tính qua S .

Chứng minh

($\Rightarrow$) Nếu S là cơ sở của X thì mỗi phần tử $x \in X$ đều biểu thị tuyến tính được qua S : $x = \sum_{\alpha \in I} r_\alpha x_\alpha$ (trong đó hầu hết các $r_\alpha = 0$, trừ một số hữu hạn).

Nếu x còn có cách biểu thị tuyến tính khác qua S : $x = \sum_{\alpha \in I} r'_\alpha x_\alpha$ thì:

$$\sum r_\alpha x_\alpha = \sum r'_\alpha x_\alpha \Rightarrow \sum (r_\alpha - r'_\alpha) x_\alpha = 0$$

Bởi S độc lập tuyến tính nên đẳng thức cuối cùng xảy ra khi và chỉ khi $r_\alpha - r'_\alpha = 0, \forall \alpha$. Hay cũng vậy: $r_\alpha = r'_\alpha, \forall \alpha$, tức là hai cách biểu thị tuyến tính của x qua S là như nhau.

($\Leftarrow$) Nếu $S \subset X$ mà mỗi $x \in X$ có một cách biểu thị tuyến tính qua S thì hiển nhiên S là hệ sinh.

Vì cách biểu thị tuyến tính của mỗi $x \in X$ qua S là duy nhất, nên nói riêng phần tử 0 cũng chỉ có một cách biểu thị tuyến tính qua S , nên S là độc lập tuyến tính.

Do vậy S là cơ sở.

□

Định lý 3 Nếu $f : X \rightarrow Y$ là đẳng cấu môđun và X là môđun tự do thì Y cũng là môđun tự do. Hơn nữa, nếu S là cơ sở của X thì $f(S)$ là cơ sở của Y .

Môđun tự do sinh bởi một tập hợp

Có thể dễ dàng chứng minh kết quả sau đây: “Tổng trực tiếp của một họ các môđun tự do là môđun tự do”.

Cũng lưu ý rằng vành R là môđun tự do trên chính nó với một cơ sở là tập $\{1\}$ chỉ gồm phần tử đơn vị.

Cho tập hợp $S \neq \emptyset$. Với mỗi $s \in S$ ta lấy một bản sao của vành hệ tử R , kí hiệu là $R_s = \{r_s : r \in R\}$. Các phần tử của R_s có thể được xem là phần tử $r \in R$ được đánh dấu bởi chỉ số s . Và các phép cộng, phép nhân trên R_s được chép lại từ R như sau:

$$r_{1s} + r_{2s} = (r_1 + r_2)_s, \quad r_{1s}r_{2s} = (r_1r_2)_s$$

Hiển nhiên $R_s \cong R$ và R_s là môđun tự do với cơ sở là tập một phần tử 1_s .

Khi đó tổng trực tiếp $F(S) = \bigoplus_{s \in S} R_s$ là môđun tự do có cơ sở là:

$$S' = \{j_s(1_s) | s \in R\}$$

(j_s là phép nhúng vào thành phần thứ s).

Ta gọi $F(S)$ là môđun tự do sinh bởi tập S .

Chú ý rằng, nếu $s \neq t$ là hai phần tử của S thì $j_s(1_s) \neq j_t(1_t)$, bởi vậy ta có thể thực hiện sự đồng nhất tập hợp S với S' nhờ song ánh $\varphi : S \rightarrow S'$ mà $\varphi(s) = j_s(1_s)$. Và ta có quyền xem như S là một cơ sở của $F(S)$.

Bây giờ cho S là cơ sở của môđun tự do X . Khi đó $\forall s \in S$ môđun con sinh bởi tập $\{s\}$ là $\langle s \rangle = Rs$ là một môđun tự do và Rs là một bản sao của vành hệ tử R .

Xét họ các môđun con $\{R_s\}_{s \in S}$ của môđun X , ta thấy:

1. $\sum R_s = X$ vì S là hệ sinh.
2. $R_s \cap \sum_{t \neq s} Rt = 0$ vì S là độc lập tuyến tính.

Vậy: $X = \bigoplus_{s \in S} Rs \cong F(S)$.

Tức là mỗi môđun tự do X có cơ sở S có thể xem là môđun tự do sinh bởi tập S .

Kết hợp tất cả các kết quả trên ta được:

Định lý 4 *R -môđun X là tự do khi và chỉ khi X đẳng cấu với tổng trực tiếp của họ nào đó các bản sao của vành hệ tử R .*

Xây dựng môđun tự do như là vật phổ dụng của phạm trù

Ngoài cách xác định một môđun tự do dựa vào sự tồn tại của cơ sở, ta còn có thể xác định môđun tự do như là vật phổ dụng của một phạm trù.

Định lý 5 *Tập $S \neq \emptyset$ trong môđun X là cơ sở của X khi và chỉ khi với bất kì môđun Y , mỗi ánh xạ $f : S \rightarrow Y$ đều có thể mở rộng tới một đồng cấu duy nhất $\tilde{f} : X \rightarrow Y$.*

Chứng minh

($\Rightarrow$) Giả sử $S = \{x_\alpha\}$ là cơ sở của môđun tự do X , ta có $\forall x \in X : x = \sum r_\alpha x_\alpha$ và do vậy mỗi ánh xạ $f : S \rightarrow Y$ đều có thể mở rộng tới một đồng cấu duy nhất $\tilde{f} : X \rightarrow Y$ theo công thức:

$$\tilde{f}(x) = \tilde{f}\left(\sum r_\alpha x_\alpha\right) = \sum r_\alpha f(x_\alpha).$$

($\Leftarrow$) Giả sử $S \subset X$ có tính chất: mỗi ánh xạ $f : S \rightarrow Y$ có thể mở rộng tới đồng cấu duy nhất: $\tilde{f} : X \rightarrow Y$, ta cần chứng minh S là cơ sở của X .

Lấy môđun tự do $F(S)$ sinh bởi tập S . Xét ánh xạ nhúng:

$$j_S \rightarrow F(S) \text{ mà } j_S(s) = j_s(1_s), \forall s \in S$$

mà trong đó $j_s : R_s \rightarrow F(S)$ là phép nhúng thứ s . Theo điều kiện định lý.

Khi đó j_S có thể mở rộng tới đồng cấu duy nhất $j : X \rightarrow F(S)$.

Để chứng tỏ S là cơ sở của X ta chỉ cần chỉ ra rằng j là đẳng cấu.

Vì j là mở rộng của j_S , mà j_S thực hiện phép song ánh S lên cơ sở S' của $F(S)$ nên j toàn ánh.

Xét $g : S' \rightarrow S$ là ánh xạ ngược của j_S , từ cơ sở $S' \subset F(S)$ lên $S \subset X$.

Vì S' là cơ sở của $F(S)$ nên g có thể mở rộng tới đồng cấu duy nhất $\tilde{g} : F(S) \rightarrow X$.

Khi đó tích các đồng cấu $\tilde{g}j : X \rightarrow X$ thực hiện sự đồng nhất trên tập $S \subset X$ nên là mở rộng của phép nhúng i , và từ tính duy nhất của mở rộng thì ta có $\tilde{g}j = 1_X$.

Từ tính chất đơn cấu của 1_X suy ra j là đơn cấu.

Vậy j là đẳng cấu, tức S là cơ sở của môđun X và X là môđun tự do.

□

Định lý 6 *Mỗi môđun X đẳng cấu với môđun thương của môđun tự do nào đó.*

Chứng minh

Xét môđun tự do $F(X)$ sinh bởi tập X . Khi đó ánh xạ đồng nhất $1_X : X \rightarrow X$ có thể mở rộng tới đồng cấu $\varphi : F(X) \rightarrow X$. Hiển nhiên φ là toàn cấu và do đó:

$$X \cong F(X)/\ker \varphi$$

□

2.2.12 Môđun tự do trên vành chính

Nói chung, R -môđun con của R -môđun tự do chưa chắc là môđun tự do. Riêng với trường hợp R là vành chính thì ta có định lý:

Định lý 7 *Môđun con của môđun tự do trên vành chính là môđun tự do.*

Chứng minh

Cho X là môđun tự do trên vành chính R , và $A \triangleleft X$. Chọn cơ sở của X là $S = \{x_\alpha\}_{\alpha \in I}$ với I là tập đã được sắp tốt.

Với mỗi $\alpha \in I$ ta đặt:

$$G_\alpha = \langle \{x_\beta : \beta < \alpha\} \rangle = \bigoplus_{\beta < \alpha} Rx_\beta,$$

$$F_\alpha = \langle \{x_\beta : \beta \leq \alpha\} \rangle = G_\alpha \oplus Rx_\alpha.$$

Dễ dàng thấy rằng, mỗi $x \in A \cap F_\alpha \subset F_\alpha$ được phân tích một cách duy nhất

$$x = u + rx_\alpha$$

với $u \in G_\alpha$ và $r \in R$.

Lập ánh xạ $\varphi : A \cap F_\alpha \rightarrow R$, theo công thức:

$$\varphi(u + rx_\alpha) = r.$$

Hiển nhiên φ là đồng cấu và $\ker \varphi = A \cap G_\alpha$.

Vì ảnh $\text{Im} \varphi = I_\alpha$ là môđun con của R , và vì R là vành chính nên I_α là ideal chính, tức I_α là R -môđun tự do (hay bằng 0). Ta có dãy khớp ngắn sau đây là chẻ:

$$0 \rightarrow A \cap G_\alpha \xrightarrow{i} A \cap F_\alpha \xrightarrow{\varphi^\#} I_\alpha \rightarrow 0$$

trong đó $\varphi^\#$ là toàn cấu, thu hẹp φ lên ảnh $\text{Im} \varphi = I_\alpha$. Từ đó, ta được sự phân tích:

$$A \cap F_\alpha = A \cap G_\alpha \oplus C_\alpha,$$

với $C_\alpha \subset A \cap F_\alpha$ và $C_\alpha \cong I_\alpha$, tức C_α là môđun tự do hay môđun 0.

Ta sẽ chứng minh $A = \bigoplus C_\alpha$, tức là kiểm tra

$$A = \sum_{\alpha \in I} C_\alpha \quad \text{và} \quad C_\alpha \cap \sum_{\beta \neq \alpha} C_\beta = 0$$

Bởi $A = \bigcup (A \cap F_\alpha)$ nên nếu $A \neq \sum C_\alpha$ thì nhờ tính chất sắp tốt của I mà tồn tại chỉ số bé nhất $\beta \in I$ sao cho có phần tử $a \in A \cap F_\beta$ và $a \notin \sum C_\alpha$ (tức là $A \cap F_\beta \not\subseteq \sum C_\alpha$).

Vì

$$A \cap F_\beta = (A \cap G_\beta) \oplus C_\beta$$

nên phần tử a được viết là

$$a = b + d$$

với $d \in C_\beta$, còn $b \in A \cap G_\beta = \bigcup_{\alpha < \beta} A \cap F_\alpha$. Hệ thức cuối cùng chỉ ra rằng tồn tại chỉ số $\gamma < \beta$ mà $b \in A \cap F_\gamma$ và hiển nhiên $b \notin \sum C_\alpha$. Điều này mâu thuẫn với việc xác định sự bé nhất của chỉ số β . Vậy:

$$A = \sum C_\alpha.$$

Để chứng minh $C_\alpha \cap \sum_{\beta \neq \alpha} C_\beta = 0$ với mỗi $\alpha \in I$, trước tiên ta chứng minh khẳng định, rằng tổng hữu hạn:

$$d = d_{\alpha_1} + d_{\alpha_2} + \dots + d_{\alpha_n} = 0, \quad d_{\alpha_k} \in C_{\alpha_k}$$

khi và chỉ khi $d_{\alpha_1} = d_{\alpha_2} = \dots = d_{\alpha_n} = 0$. Ta tiến hành qui nạp theo số n các hạng tử của tổng d .

- Khẳng định là đúng hiển nhiên với $n = 1$.
- Giả sử khẳng định đúng với $n = k - 1$, và tổng

$$d = d_{\alpha_1} + d_{\alpha_2} + \dots + d_{\alpha_k} = 0.$$

Nhờ I sắp tốt, nên ta có thể xem như $\alpha_1 < \alpha_2 < \dots < \alpha_k$, do đó

$$d = (d_{\alpha_1} + d_{\alpha_2} + \dots + d_{\alpha_{k-1}}) + d_{\alpha_k} \in A \cap F_{\alpha_k} = (A \cap G_{\alpha_k}) \oplus C_{\alpha_k}.$$

Hiển nhiên là $d_{\alpha_1} + d_{\alpha_2} + \dots + d_{\alpha_{k-1}} \in A \cap G_{\alpha_k}$ và $d_{\alpha_k} \in C_{\alpha_k}$ nên đồng thời $d_{\alpha_k} = 0$ và $d_{\alpha_1} + d_{\alpha_2} + \dots + d_{\alpha_{k-1}} = 0$. Sử dụng giả thiết qui nạp cho hệ thức cuối cùng ta có:

$$d_{\alpha_1} = \dots = d_{\alpha_{k-1}} = 0$$

□

Vì mỗi nhóm aben tự do là các $\mathbb{Z}$ -môđun tự do và $\mathbb{Z}$ là vành chính, nên từ định lý ta suy ra kết quả sau đây:

Hệ quả 3 Mọi nhóm con của nhóm aben tự do là nhóm aben tự do.

2.2.13 Môđun xạ ảnh

Định nghĩa 3 Môđun P được gọi là môđun xạ ảnh nếu với mọi toàn cấu $\sigma : B \rightarrow C$, mỗi đồng cấu $f : P \rightarrow C$, tồn tại một đồng cấu $\varphi : P \rightarrow B$ sao cho $f = \sigma\varphi$.

$$\begin{array}{ccc} & P & \\ \swarrow \exists \varphi & & \downarrow f \\ B & \xrightarrow{\sigma} & C \end{array}$$

Định lý 8 Mỗi môđun tự do đều là môđun xạ ảnh.

Chứng minh

Giả sử: X là môđun tự do, $\sigma : B \rightarrow C$ là toàn cấu và $f : X \rightarrow C$ là đồng cấu. Ta cần chứng minh tồn tại đồng cấu $\varphi : X \rightarrow B$ mà $f = \sigma\varphi$.

Gọi $S \subset X$ là cơ sở của môđun tự do X . Vì σ là toàn cấu nên với mọi $x \in S$, tồn tại phần tử $\varphi(x) \in \sigma^{-1}(f(x)) \neq \emptyset$.

Như vậy, ta có ánh xạ $\varphi : S \rightarrow B$, ánh xạ này có thể mở rộng tới đồng cấu trên X mà để tiện lợi ta cũng kí hiệu là $\varphi : X \rightarrow B$.

Để chứng minh $f = \sigma\varphi$, ta chỉ cần kiểm tra đẳng thức đúng trên hệ sinh S của X . Hiển nhiên là với mọi $x \in S$ do $\varphi(x) \in \sigma^{-1}(f(x))$ nên $\sigma\varphi(x) = f(x)$.

Vậy môđun tự do X là môđun xạ ảnh.

□

Ta có một số tính chất của môđun xạ ảnh:

Định lý 9 Tổng trực tiếp của họ môđun $P = \bigoplus_{i \in I} P_i$ là xạ ảnh khi và chỉ khi mỗi môđun thành phần P_i là xạ ảnh.

Định lý 10 Đối với mỗi môđun P , ba phát biểu sau là tương đương:

1. P là môđun xạ ảnh.
2. Mỗi dãy khớp $0 \rightarrow A \xrightarrow{\lambda} B \xrightarrow{\sigma} P \rightarrow 0$ là chẻ ra.
3. P đẳng cấu với hạng tử trực tiếp của một môđun tự do.

Chứng minh

1) $\rightarrow$ 2): Cho P là môđun xạ ảnh, khi đó với dãy khớp ngắn bất kì:

$$0 \rightarrow A \xrightarrow{\chi} B \xrightarrow{\sigma} P \rightarrow 0$$

do $\sigma : B \rightarrow P$ là toàn cấu nên đồng cấu đồng nhất $1_P : P \rightarrow P$ được nâng lên tới đồng cấu $h : P \rightarrow B$ sao cho $\sigma h = 1_P$.

Vậy σ có nghịch đảo phải là h , do đó dãy khớp ngắn đã cho là chẻ ra.

2) $\rightarrow$ 3): Nếu mỗi dãy khớp ngắn mà môđun P đứng cuối là chẻ thì nói riêng dãy sau đây cũng chẻ ra:

$$0 \rightarrow \ker \pi \xrightarrow{i} F(P) \xrightarrow{\pi} P \rightarrow 0 \quad (*)$$

trong đó $F(P)$ là môđun tự do sinh bởi P còn π là đồng cấu mở rộng lên toàn $F(P)$ của ánh xạ đồng nhất: $1_P : P \rightarrow P$, xem như ánh xạ từ cơ sở $P \subset F(P)$ tới môđun P .

Tính chẻ của dãy khớp $(*)$ cho ta đẳng cấu

$$F(P) \cong \ker \pi \oplus P,$$

Tức là P đẳng cấu với hạng tử trực tiếp của môđun tự do $F(P)$.

3) $\rightarrow$ 1): Nếu $P \cong A$ và A là hạng tử trực tiếp của môđun tự do X . Thì theo các định lý trên, vì X tự do nên X xạ ảnh, vì A là hạng tử trực tiếp của X xạ ảnh nên A xạ ảnh. Suy ra P xạ ảnh.

□

Lưu ý rằng trên vành chính thì môđun con của môđun tự do lại là môđun tự do, kết hợp với định lý trên ta có:

Định lý 11 *Khi R là vành chính, môđun P là xạ ảnh khi và chỉ khi P là môđun tự do.*

Chương 3

CÁC KẾT QUẢ CỦA LUẬN VĂN

Để tiện lợi cho sự trình bày, trong chương này vành R luôn được hiểu là vành chính và môđun X được hiểu là môđun tự do hữu hạn sinh trên vành chính R .

3.1 Thuật toán để tìm cơ sở của môđun chứa đơn tử cho trước

3.1.1 Thuật toán

Định nghĩa 4 Trong môđun X , phần tử $a \in X$, $a \neq 0$ gọi là đơn tử nếu $a = rb$ với $b \in X$ và $r \in R$ sẽ kéo theo r là khả nghịch.

Rõ ràng là khi a đơn tử và $a = rb$ thì b cũng là đơn tử.

Các mệnh đề sau cho ta sự mô tả rõ hơn về đơn tử.

Mệnh đề 1 Trong môđun X , phần tử $a \in X$ là đơn tử khi và chỉ khi với bất kì cơ sở $\{u_1, u_2, \dots, u_n\}$ của X và $a = a_1u_1 + a_2u_2 + \dots + a_nu_n$ thì $\text{ƯCLN}(a_1, a_2, \dots, a_n) = 1$.

Chứng minh

($\Rightarrow$) Giả sử a là đơn tử, gọi $r = \text{ƯCLN}(a_1, a_2, \dots, a_n) = 1$, ta có: $a_i = rb_i$ với $b_i \in R, i = 1, 2, \dots, n$.

Đặt $b \in X$ là phần tử có tọa độ $(b_1, b_2, \dots, b_n)$, dễ thấy $a = rb$.

Theo định nghĩa đơn tử thì $r \mid 1$ tức $\text{ƯCLN}(a_1, a_2, \dots, a_n) = 1$.

($\Leftarrow$) Giả sử $\text{ƯCLN}(a_1, a_2, \dots, a_n) = 1$ và $a = rb$, $b \in X, r \in R$. Gọi $(b_1, b_2, \dots, b_n)$ là tọa độ của b , ta có $a_i = rb_i$, $i = 1, 2, \dots, n$ tức r là ước chung của $(a_1, a_2, \dots, a_n)$.

Do giả thiết về ƯCLN ở trên suy ra $r \mid 1$ tức r là đơn tử.

□

Thật ra chiều đảo của mệnh đề 1 đòi hỏi ít hơn so với phát biểu của mệnh đề: chỉ cần có một cơ sở $\{u_i\}$ nào đó để $a = a_1u_1 + a_2u_2 + \dots + a_nu_n$ mà $\text{ƯCLN}(a_1, a_2, \dots, a_n) = 1$ thì a là đơn tử.

Mệnh đề 2 Trong môđun X , phần tử $a \in X$ là đơn tử khi và chỉ khi tồn tại một đồng cấu $f : X \longrightarrow R$ thỏa $f(a) = 1$.

Chứng minh:

($\Rightarrow$) Giả sử a là đơn tử trong X . Ta chọn trong X một cơ sở $\{u_1, u_2, \dots, u_n\}$ và biểu diễn $a = a_1u_1 + a_2u_2 + \dots + a_nu_n$.

Theo mệnh đề 1 thì $\text{ƯCLN}(a_1, a_2, \dots, a_n) = 1$, do vậy tồn tại các hệ tử $r_1, r_2, \dots, r_n \in R$ mà $r_1a_1 + r_2a_2 + \dots + r_na_n = 1$.

Khi đó, xét ánh xạ $f : X \longrightarrow R$ mà với mỗi $x = x_1u_1 + x = x_1u_1 + \dots + x = x_nu_n$ xác định $f(x) = r_1x_1 + r_2x_2 + \dots + r_nx_n$.

Có thể dễ dàng kiểm tra f là đồng cấu và f thỏa mãn điều kiện của mệnh đề 2

($\Leftarrow$) Giả sử có đồng cấu $f : X \longrightarrow R$ thỏa mãn $f(a) = 1$ và $a = rb$. Khi đó: $1 = f(a) = f(rb) = r.f(b)$, tức r khả nghịch.

Theo định nghĩa, a là đơn tử.

□

Mệnh đề 3 Trong môđun X , phần tử $a \in X$ là đơn tử khi và chỉ khi a là phần tử của một cơ sở nào đó trong X .

Chứng minh:

($\Rightarrow$) Giả sử a là đơn tử trong X . Theo mệnh đề 2 tồn tại đồng cấu $f : X \longrightarrow R$ với $f(a) = 1$.

Ta thấy ngay f là toàn cấu vì với mọi $r \in R$ thì $r = f(ra)$. Ta có dãy khớp sau:

$$0 \longrightarrow \ker f \xrightarrow{i} X \xrightarrow{f} R \longrightarrow 0$$

Ở đây R là R -môđun tự do và do đó là xạ ảnh nên dãy khớp là chẻ ra, hơn nữa ta có: $X = \ker f \oplus Ra$ với Ra là môđun cyclic sinh bởi a : $Ra = \{ra : r \in R\} \cong R$, thật vậy:

Với mọi $x \in X$, đặt $f(x) = r$ ta có $f(x) = f(ra)$ nên $x = ra + y$ với $y \in \ker f$. Vậy $X = \ker f + Ra$.

Lại có $ra \in \ker f \cap Ra \Leftrightarrow r = f(ra) = 0 \Rightarrow X = \ker f \oplus Ra$.

$\ker f$ là môđun con của X , cũng là môđun tự do.

Do điều vừa chứng minh cơ sở của $\ker f$ cùng với a là cơ sở của X . Tức $\{a\}$ có thể bổ sung thành cơ sở.

($\Leftarrow$) Mỗi phần tử u_k trong một cơ sở $\{u_1, u_2, \dots, u_n\}$ nào đó của X có sự phân tích theo chính cơ sở đó là $u_k = a_1u_1 + a_2u_2 + \dots + a_nu_n$ với $a_k = 1$ còn lại $a_i = 0$ với mọi $i \neq k$. Theo mệnh đề 1, u_k là đơn tử.

Nhận xét Theo mệnh đề 3, mỗi phần tử trong cơ sở của một môđun là đơn tử trong môđun đó. Như vậy, phần tử $a \in A \triangleleft X$, có thể không là đơn tử trong X , song nếu a thuộc một cơ sở nào đó của A thì a đơn tử trong A . Tức là khái niệm đơn tử có tính chất tương đối, đơn tử theo từng môđun.

Áp dụng mệnh đề 3 nhiều lần sẽ cho ta thuật toán xây dựng một cơ sở của môđun X chứa một đơn tử $a \in X$ cho trước.

THUẬT TOÁN XÂY DỰNG CƠ SỞ CỦA MÔĐUN CHỨA MỘT ĐƠN TỬ CHO TRƯỚC

Giả sử R -môđun X có cơ sở ban đầu $\{e_1, e_2, \dots, e_n\}$ và a là đơn tử trong X , $a = a_1e_1 + a_2e_2 + \dots + a_ne_n$.

Khi đó, tồn tại các hệ tử $r_1, r_2, \dots, r_n \in R$ sao cho $r_1a_1 + r_2a_2 + \dots + r_na_n = 1$.

Xét đồng cấu $f : X \longrightarrow R$ xác định $f(x) = r_1x_1 + r_2x_2 + \dots + r_nx_n$ với mỗi $x = x_1e_1 + x_2e_2 + \dots + x_ne_n \in X$.

Ta có: $X = Ra \oplus \ker f$ trong đó $\ker f$ là tập các phần tử $x \in X$ có tọa độ trong cơ sở ban đầu là $(x_1, x_2, \dots, x_n)$ thỏa mãn phương trình thuần nhất: $r_1x_1 + r_2x_2 + \dots + r_nx_n = 0$.

Lấy một nghiệm của phương trình trên $(b_1, b_2, \dots, b_n)$ sao cho $\text{ƯCLN}((b_1, b_2, \dots, b_n)) = 1$. Khi đó $b = b_1e_1 + b_2e_2 + \dots + b_ne_n \in \ker f$ là một đơn tử của $\ker f$ (đồng thời là đơn tử trong X).

Điều này cho phép ta xác định đồng cấu $g : X \longrightarrow R$ mà $g(x) = t_1x_1 + t_2x_2 + \dots + t_nx_n$ với mỗi $x = x_1e_1 + x_2e_2 + \dots + x_ne_n \in X$ thỏa $g(b) = 1$.

Đồng cấu này cho ta các sự phân tích:

$$\ker f = Ra \oplus \ker g \quad \text{và} \quad X = Ra \oplus Rb \oplus \ker g$$

với $\ker g$ là tập các phần tử $x \in X$ với bộ tọa độ $(x_1, x_2, \dots, x_n)$ trong cơ sở ban đầu thỏa hệ phương trình thuần nhất:

$$\begin{cases} r_1x_1 + r_2x_2 + \dots + r_nx_n = 0 \\ t_1x_1 + t_2x_2 + \dots + t_nx_n = 0 \end{cases}$$

Nếu hệ này có nghiệm không tầm thường thì ta tiếp tục chọn bộ nghiệm $(c_1, c_2, \dots, c_n)$ mà $c = c_1e_1 + c_2e_2 + \dots + c_ne_n$ là đơn tử trong $\ker g$ (cũng là đơn tử trong X) và lặp lại quá trình trên.

Thuật toán sẽ kết thúc khi hệ phương trình thuần nhất cuối cùng chỉ có nghiệm tầm thường.

3.1.2 Ví dụ áp dụng thuật toán trên các nhóm aben tự do

Xét $\mathbb{Z}$ -môđun $X = \mathbb{Z}^5$; và $a = (12, -18, 30, 15, -10) \in X$.

a là đơn tử trong X vì $\text{ƯCLN}(12, -18, 30, 15, -10) = 1$. Ta sẽ áp dụng thuật toán để xây dựng cơ sở mới của X mà a là phần tử cơ sở đầu tiên.

Xét đồng cấu $f : X \rightarrow R$ xác định bởi:

$$f(x) = 0x_1 + 3x_2 + 0x_3 + x_4 - 4x_5, \quad \forall x = (x_1, x_2, x_3, x_4, x_5) \in \mathbb{Z}^5$$

f thỏa $f(a) = 1$.

Về việc chọn f thỏa các điều kiện như trên, cũng nên lưu ý một mẹo tính toán là: trong các thành phần của a ta thấy có các thành phần thứ 2,4,5 ($-18, 15, -10$) nguyên tố cùng nhau, nên ta có thể chọn các hệ số trong công thức f sao cho hai hệ số thứ 1,3 bằng 0.

Xét phương trình nghiệm nguyên

$$0x_1 + 3x_2 + 0x_3 + x_4 - 4x_5 = 0$$

Ta dễ dàng tìm được một nghiệm của phương trình: $b = (0, 1, 0, 1, 1)$ có ƯCLN của các tọa độ bằng 1. b là phần tử cơ sở thứ 2.

Xét đồng cấu $g : X \rightarrow R$ xác định bởi:

$$g(x) = x_2, \quad \forall x = (x_1, x_2, x_3, x_4, x_5) \in \mathbb{Z}^5$$

g thỏa $g(b) = 1$.

Nói thêm về cách lấy đồng cấu g , ta thấy công thức của g thật đơn giản vì b có một tọa độ bằng 1.

Xét hệ phương trình nghiệm nguyên:

$$\begin{cases} 0x_1 + 3x_2 + 0x_3 + x_4 - 4x_5 = 0 \\ x_2 = 0 \end{cases}$$

Ta tìm được một nghiệm của hệ là $c = (0, 0, 0, 4, 1)$, có ƯCLN của các tọa độ bằng 1. c là phần tử cơ sở thứ 3.

Xét đồng cấu $h : X \rightarrow R$ xác định bởi:

$$h(x) = x_5, \quad \forall x = (x_1, x_2, x_3, x_4, x_5) \in \mathbb{Z}^5$$

h thỏa $h(c) = 1$.

Xét hệ phương trình nghiệm nguyên:

$$\begin{cases} 0x_1 + 3x_2 + 0x_3 + x_4 - 4x_5 = 0 \\ x_2 = 0 \\ x_5 = 0 \end{cases}$$

Ta tìm được một nghiệm của hệ trên là $d = e_1 = (1, 0, 0, 0, 0)$ có ƯCLN các tọa độ bằng 1. d là phần tử cơ sở thứ 4.

Xét đồng cấu: $j_1 : X \rightarrow R$ xác định bởi:

$$j_1(x) = x_1, \quad \forall x = (x_1, x_2, x_3, x_4, x_5) \in \mathbb{Z}^5$$

j_1 thỏa $j_1(d) = 1$.

Xét hệ phương trình:

$$\begin{cases} 0x_1 + 3x_2 + 0x_3 + x_4 - 4x_5 = 0 \\ x_2 = 0 \\ x_5 = 0 \\ x_1 = 0 \end{cases}$$

Ta tìm được một nghiệm của hệ trên là $e = e_2 = (0, 0, 1, 0, 0)$, có ƯCLN các tọa độ bằng 1. e là phần tử cơ sở tiếp theo.

Xét đồng cấu: $j_3 : X \rightarrow R$ xác định bởi:

$$j_3(x) = x_3, \quad \forall x = (x_1, x_2, x_3, x_4, x_5) \in \mathbb{Z}^5$$

j_3 thỏa $j_3(e) = 1$.

Xét hệ phương trình:

$$\begin{cases} 0x_1 + 3x_2 + 0x_3 + x_4 - 4x_5 = 0 \\ x_2 = 0 \\ x_5 = 0 \\ x_1 = 0 \\ x_3 = 0 \end{cases}$$

Hệ này chỉ có nghiệm tầm thường. Thuật toán dừng ở đây.

Như vậy, cơ sở mới của X chứa đơn tử a là:

$$a = (12, -18, 30, 15, -10)$$

$$b = (0, 1, 0, 1, 1)$$

$$c = (0, 0, 0, 4, 1)$$

$$d = (1, 0, 0, 0, 0)$$

$$e = (0, 0, 1, 0, 0)$$

Nhận xét: Một mẹo để tìm được một kết quả đẹp khi áp dụng thuật toán là xây dựng đồng cấu f mà công thức có càng nhiều hệ số của x_i bằng 0 càng tốt.

Trong ví dụ trên, đơn tử a có các tọa độ thứ 2,4,5 nguyên tố cùng nhau. Điều này dẫn đến kết quả là có thể xây dựng cơ sở mới của X mà chỉ cần thay thế các phần tử cơ sở ứng với các tọa độ 2,4,5 và giữ nguyên các phần tử cơ sở còn lại.

3.1.3 Ví dụ áp dụng thuật toán trên môđun tự do hữu hạn sinh trên vành đa thức

Gọi $\mathbb{Z}_7 = \mathbb{Z}/7\mathbb{Z}$, như đã biết $\mathbb{Z}_7$ là một trường.

$R = \mathbb{Z}_7[x]$ là vành các đa thức trên trường $\mathbb{Z}_7$, $\mathbb{Z}_7[x]$ là vành chính. Các phần tử khả nghịch trong $\mathbb{Z}_7[x]$ là các $p(x) = \bar{a}$ với $\bar{a} \in \mathbb{Z}_7 \setminus \{\bar{0}\}$.

Xét

$$X = R^4 = \{p = (p_1(x), p_2(x), p_3(x), p_4(x)) \mid p_i(x) \in \mathbb{Z}_7[x]\}$$

là môđun tự do hạng bằng 4.

$a = (\bar{1}x^2 + \bar{2}x, \bar{3}x + \bar{4}, \bar{2}x^3 + \bar{1}, \bar{3}x^7 - \bar{2}x^5 + \bar{5}x^2)$ là đơn tử trong X .

(Vì trong các thành phần của a có $\bar{3}x + \bar{4}$ là bất khả qui trong $\mathbb{Z}_7[x]$ và $\bar{1}x^2 + \bar{2}x$ không chia hết cho $\bar{3}x + \bar{4}$, nên hai thành phần này nguyên tố cùng nhau. Do đó ƯCLN các thành phần của a bằng 1.)

Xét đồng cấu $f : X \rightarrow R$ xác định bởi:

$$f(p) = (\bar{2}x + \bar{4})p_1(x) + (\bar{2}x + \bar{4})p_2(x) - p_3(x) + \bar{0}p_4(x), \quad \forall p = (p_1(x), p_2(x), p_3(x), p_4(x))$$

f thỏa: $f(a) = \bar{1}$

Xét phương trình thuần nhất

$$(\bar{2}x + \bar{4})p_1(x) + (\bar{2}x + \bar{4})p_2(x) - \bar{1}p_3(x) + \bar{0}p_4(x) = \bar{0}, \quad p_i(x) \in \mathbb{Z}_7[x]$$

ta tìm được một nghiệm là

$$b = (\bar{1}, \bar{1}, \bar{4}x + \bar{1}, \bar{0})$$

có ƯCLN của các thành phần bằng $\bar{1}$. b là phần tử cơ sở thứ 2.

Xét đồng cấu $g : X \rightarrow R$ xác định bởi:

$$g(p) = p_1(x), \quad \forall p = (p_1(x), p_2(x), p_3(x), p_4(x))$$

g thỏa: $g(b) = \bar{1}$.

Xét hệ phương trình thuần nhất:

$$\begin{cases} (\bar{2}x + \bar{4})p_1(x) + (\bar{2}x + \bar{4})p_2(x) - \bar{1}p_3(x) + \bar{0}p_4(x) = \bar{0} \\ p_1(x) = \bar{0} \end{cases}, \quad p_i(x) \in \mathbb{Z}_7[x]$$

Ta tìm được một nghiệm của hệ:

$$c = (\bar{0}, \bar{1}, \bar{2}x + \bar{4}, \bar{0})$$

có ƯCLN của các tọa độ bằng $\bar{1}$. c là phần tử cơ sở thứ 3.

Xét đồng cấu $h : X \rightarrow R$ xác định bởi:

$$h(p) = p_2(x), \quad \forall p = (p_1(x), p_2(x), p_3(x), p_4(x))$$

h thỏa: $h(c) = \bar{1}$.

Xét hệ phương trình thuần nhất:

$$\begin{cases} (\bar{2}x + \bar{4})p_1(x) + (\bar{2}x + \bar{4})p_2(x) - \bar{1}p_3(x) + \bar{0}p_4(x) = \bar{0} \\ p_1(x) = \bar{0} \\ p_2(x) = \bar{0} \end{cases}, \quad p_i(x) \in \mathbb{Z}_7[x]$$

Ta tìm được một nghiệm của hệ:

$$d = (\bar{0}, \bar{0}, \bar{0}, \bar{1})$$

Có ƯCLN các tọa độ bằng $\bar{1}$. d là phần tử cơ sở thứ 4.

Xét đồng cấu $k : X \rightarrow R$ xác định bởi:

$$k(p) = p_4(x), \quad \forall p = (p_1(x), p_2(x), p_3(x), p_4(x))$$

k thỏa: $k(d) = \bar{1}$.

Xét hệ phương trình thuần nhất:

$$\begin{cases} (\bar{2}x + \bar{4})p_1(x) + (\bar{2}x + \bar{4})p_2(x) - \bar{1}p_3(x) + \bar{0}p_4(x) = \bar{0} \\ p_1(x) = \bar{0} \\ p_2(x) = \bar{0} \\ p_4(x) = \bar{0} \end{cases}, \quad p_i(x) \in \mathbb{Z}_7[x]$$

Hệ này chỉ có nghiệm tầm thường. Thuật toán của chúng ta dừng ở đây. Như vậy cơ sở của $(\mathbb{Z}_7[x])^4$ chứa đơn tử a là:

$$\begin{cases} a = (\bar{1}x^2 + \bar{2}x, \bar{3}x + \bar{4}, \bar{2}x^3 + \bar{1}, \bar{3}x^7 - \bar{2}x^5 + \bar{5}x^2) \\ b = (\bar{1}, \bar{1}, \bar{4}x + \bar{1}, \bar{0}) \\ c = (\bar{0}, \bar{1}, \bar{2}x + \bar{4}, \bar{0}) \\ d = (\bar{0}, \bar{0}, \bar{0}, \bar{1}) \end{cases}$$

3.1.4 Ví dụ áp dụng thuật toán trên môđun tự do hữu hạn sinh trên vành các số nguyên Gauss

Xét R là vành các số nguyên Gauss:

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

$\mathbb{Z}[i]$ là vành Ôclít với chuẩn $|a + bi| = a^2 + b^2$ nên là vành chính.

Các phần tử khả nghịch trong R là $\pm 1, \pm i$. Vành các số nguyên được xem như vành con của vì mỗi $a \in \mathbb{Z}$ tương ứng với $a + 0i \in \mathbb{Z}[i]$ (và tương ứng này là đơn cấu từ $\mathbb{Z}$ vào $\mathbb{Z}[i]$).

$X = R^4 = \{z = (z_1, z_2, z_3, z_4) \mid z_i \in \mathbb{Z}[i]\}$ là môđun tự do hạng bằng 4 trên vành chính R .

Trước tiên xin nhắc lại rằng, mỗi phần tử nguyên tố trong $\mathbb{Z}[i]$ thuộc một trong 3 dạng sau đây:

1. $a + bi$ với $a, b \neq 0$ mà $a^2 + b^2$ là số nguyên tố
2. $0 + bi$ với $|b|$ nguyên tố và $|b| \equiv 3 \pmod{4}$
3. $a + 0i$ với $|a|$ nguyên tố và $|a| \equiv 3 \pmod{4}$

Trong môđun X , xét phần tử $a = (5, 6 + 7i, 38 - i, 13 + i)$.

Ta có sự phân tích các tọa độ của a thành tích các phần tử nguyên tố:

$$\begin{aligned} 5 &= -i(1 + 2i)(2 + i) \\ 6 + 7i &= (1 + 2i)(4 - i) \\ 38 - i &= (2 + i)(4 - i)^2 \\ 13 + i &= -i(1 + 2i)(4 - i)(1 + i) \end{aligned}$$

Như vậy: $\text{UCLN}(5, 6 + 7i, 38 - i, 13 + i) = 1$, a là đơn tử trong X .

Xét đồng cấu $f : X \rightarrow R$

$$f(z) = -10z_1 + 0z_2 + 1z_3 + 1z_4, \quad \forall z = (z_1, z_2, z_3, z_4)$$

f thỏa $f(a) = 1$. (Ta cố tình chọn các hệ số trong f thuộc $\mathbb{Z}$ để dễ tính toán về sau).

Xét phương trình thuần nhất:

$$-10z_1 + 0z_2 + 1z_3 + 1z_4 = 0, \quad z_i \in \mathbb{Z}[i]$$

Ta tìm được một nghiệm (để đơn giản ta có thể tìm nghiệm nguyên) của hệ trên là

$$b = (1, 0, 3, 7)$$

vì $\text{ƯCLN}(1, 0, 3, 7) = 1$ trong vành $\mathbb{Z}$ nên cũng dẫn đến $\text{ƯCLN}(1, 0, 3, 7) = 1$ trong $\mathbb{Z}[i]$. (Nếu các số nguyên $a_1, a_2, \dots, a_n \in \mathbb{Z}$ có ước chung không khả nghịch $r \in \mathbb{Z}[i]$ thì $|r| > 1$ là ước chung của $|a_1|, \dots, |a_n|$. Do đó $a_1, a_2, \dots, a_n$ có một ước chung nào đó thuộc $\mathbb{Z} \setminus \{\pm 1\}$.)

Xét đồng cấu $g : X \rightarrow R$

$$g(z) = z_1, \quad \forall z = (z_1, z_2, z_3, z_4)$$

g thỏa $g(b) = 1$.

Xét hệ phương trình thuần nhất:

$$\begin{cases} -10z_1 + 0z_2 + 1z_3 + 1z_4 = 0 \\ z_1 = 0 \end{cases} \quad z_i \in \mathbb{Z}[i]$$

Ta được một nghiệm (nguyên) của hệ trên là:

$$c = (0, 0, 1, -1)$$

có ƯCLN của các tọa độ bằng 1.

Xét đồng cấu $h : X \rightarrow R$

$$h(z) = z_3, \quad \forall z = (z_1, z_2, z_3, z_4)$$

h thỏa $h(c) = 1$.

Xét hệ phương trình thuần nhất:

$$\begin{cases} -10z_1 + 0z_2 + 1z_3 + 1z_4 = 0 \\ z_1 = 0 \\ z_3 = 0 \end{cases} \quad z_i \in \mathbb{Z}[i]$$

Ta tìm được một nghiệm của hệ trên là:

$$d = (0, 1, 0, 0)$$

có ƯCLN của các tọa độ bằng 1.

Xét đồng cấu $k : X \rightarrow R$

$$k(z) = z_2, \quad \forall z = (z_1, z_2, z_3, z_4)$$

k thỏa $k(d) = 1$.

Xét hệ phương trình thuần nhất:

$$\begin{cases} -10z_1 + 0z_2 + 1z_3 + 1z_4 = 0 \\ z_1 = 0 \\ z_3 = 0 \\ z_2 = 0 \end{cases} \quad z_i \in \mathbb{Z}[i]$$

Hệ này chỉ có nghiệm tầm thường. Thuật toán dừng.

Vậy cơ sở cần tìm là:

$$a = (5, 6 + 7i, 38 - i, 13 + i)$$

$$b = (1, 0, 3, 7)$$

$$c = (0, 0, 1, -1)$$

$$d = (0, 1, 0, 0)$$

3.2 Thuật toán tìm giao của hai môđun

3.2.1 Thuật toán

Cho X là môđun với cơ sở $\{e_1, e_2, \dots, e_n\}$ và các môđun con X_1 với cơ sở $\{u_1, u_2, \dots, u_k\}$ mà $u_i = a_{i1}e_1 + a_{i2}e_2 + \dots + a_{in}e_n$, môđun con X_2 với cơ sở $\{v_1, v_2, \dots, v_s\}$ mà $v_j = b_{j1}e_1 + b_{j2}e_2 + \dots + b_{jn}e_n$.

Phần tử x thuộc môđun giao $X_1 \cap X_2$ khi và chỉ khi tồn tại các bộ hệ tử $(x_1, x_2, \dots, x_k)$ và $(y_1, y_2, \dots, y_s)$, $(x_i, y_j) \in R$ sao cho:

$$\begin{cases} x = x_1u_1 + x_2u_2 + \dots + x_ku_k \\ x = y_1v_1 + y_2v_2 + \dots + y_sv_s \end{cases}$$

Tọa độ hóa các hệ thức trên trong cơ sở ban đầu của X ta có bộ $(x_1, x_2, \dots, x_k, y_1, y_2, \dots, y_s)$ là nghiệm của hệ phương trình thuần nhất:

$$\begin{cases} a_{11}x_1 + a_{21}x_2 + \dots + a_{k1}x_k - b_{11}y_1 - b_{21}y_2 - \dots - b_{s1}y_s = 0 \\ a_{12}x_1 + a_{22}x_2 + \dots + a_{k2}x_k - b_{12}y_1 - b_{22}y_2 - \dots - b_{s2}y_s = 0 \\ \dots\dots\dots \\ a_{1n}x_1 + a_{2n}x_2 + \dots + a_{kn}x_k - b_{1n}y_1 - b_{2n}y_2 - \dots - b_{sn}y_s = 0 \end{cases} \quad (*)$$

Nếu hệ phương trình này có nghiệm không tầm thường thì $X_1 \cap X_2 \neq \{0\}$ và khi đó ta có:

Mệnh đề 4 Nếu bộ $(a_1, a_2, \dots, a_k, b_1, \dots, b_s)$ là nghiệm của hệ phương trình thuần nhất $(*)$, xác định bởi $X_1 \cap X_2$ thỏa $\text{ƯCLN}(a_1, \dots, a_k, b_1, \dots, b_s) = 1$ thì phần tử $a = a_1u_1 + a_2u_2 + \dots + a_ku_k = b_1v_1 + b_2v_2 + \dots + b_sv_s$ là đơn tử trong $X_1 \cap X_2$.

Chứng minh:

Ta có: $a = a_1u_1 + a_2u_2 + \dots + a_ku_k = b_1v_1 + b_2v_2 + \dots + b_sv_s$.

Gọi $\alpha = \text{ƯCLN}(a_1, a_2, \dots, a_k)$ và $\beta = \text{ƯCLN}(b_1, b_2, \dots, b_s)$.

Do giả thiết $\text{ƯCLN}(a_1, a_2, \dots, a_k, b_1, \dots, b_s) = 1$ nên $\text{ƯCLN}(\alpha, \beta) = 1$.

Nếu $b \in X_1 \cap X_2$ và $r \in R$ mà $a = rb$. Khi đó, tồn tại các hệ tử x_i, y_j sao cho $b = x_1u_1 + x_2u_2 + \dots + x_ku_k = y_1v_1 + y_2v_2 + \dots + y_sv_s$.

Hệ thức $a = rb$ kéo theo $a_1 = rx_1, a_2 = rx_2, \dots, a_k = rx_k$ và $b_1 = ry_1, b_2 = ry_2, \dots, b_s = ry_s$. Suy ra $r \mid a_i$ và $r \mid b_j$ với mọi i, j và do đó $r \mid \alpha$ và $r \mid \beta$. Suy ra $r \mid \text{ƯCLN}(\alpha, \beta) = 1$, tức r khả nghịch.

Vậy a là đơn tử trong $X_1 \cap X_2$.

□

Theo mệnh đề 3 thì a thỏa điều kiện của mệnh đề 4 là phần tử cơ sở đầu tiên của $X_1 \cap X_2$ cần tìm. Theo mệnh đề 3 để xác định phần tử cơ sở tiếp theo của $X_1 \cap X_2$ (nếu còn!) ta cần xây dựng đồng cấu $f : X_1 \cap X_2 \longrightarrow R$ mà $f(a) = 1$.

Có nhiều cách khác nhau để xây dựng đồng cấu f như thế. Ta có thể xây dựng f theo cách sau:

Vì $\alpha = \text{ƯCLN}(a_1, a_2, \dots, a_k)$ nên có bộ các hệ tử $r_1, r_2, \dots, r_k \in R$ sao cho $r_1 a_1 + r_2 a_2 + \dots + r_k a_k = \alpha$. Gọi đồng cấu $f_1 : X_1 \longrightarrow R$ xác định bởi $f_1(x) = r_1 x_1 + r_2 x_2 + \dots + r_k x_k$ với mỗi $x = x_1 u_1 + x_2 u_2 + \dots + x_k u_k$. Ta có $f_1(a) = \alpha$.

Vì $\beta = \text{ƯCLN}(b_1, b_2, \dots, b_s)$ nên có bộ các hệ tử $t_1, t_2, \dots, t_s \in R$ sao cho $t_1 b_1 + t_2 b_2 + \dots + t_s b_s = \beta$. Gọi đồng cấu $f_2 : X_2 \longrightarrow R$ xác định bởi $f_2(x) = t_1 y_1 + t_2 y_2 + \dots + t_s y_s$ với mỗi $x = y_1 v_1 + y_2 v_2 + \dots + y_s v_s$. Ta có $f_2(a) = \beta$.

Xác định $f : X_1 \cap X_2 \longrightarrow R$ mà với mỗi $x \in X_1 \cap X_2$ thì $f(x) = p f_1(x) + q f_2(x)$, trong đó $p, q \in R$ là các hệ tử thỏa hệ thức: $p\alpha + q\beta = 1$.

Để tìm phần tử cơ sở tiếp theo (nếu còn) ta ghép thêm vào hệ phương trình (*) phương trình thuần nhất $f(x) = 0$.

Nếu hệ phương trình ghép có nghiệm không tầm thường, thì ta lại chọn một nghiệm $(c_1, c_2, \dots, c_k, d_1, \dots, d_s)$ mà $\text{ƯCLN}(c_1, c_2, \dots, c_k, d_1, \dots, d_s) = 1$.

Khi đó phần tử $c = c_1 u_1 + c_2 u_2 + \dots + c_k u_k = d_1 v_1 + d_2 v_2 + \dots + d_s v_s$ là đơn tử trong $\ker f$, sẽ là phần tử cơ sở tiếp theo của $X_1 \cap X_2$.

Các phần tử cơ sở còn lại của $X_1 \cap X_2$ được tìm theo quá trình tương tự, mà mỗi bước thực hiện được đánh dấu bằng việc ghép thêm một phương trình thuần nhất mới vào hệ phương trình trước đó.

Thuật toán tìm cơ sở của $X_1 \cap X_2$ sẽ kết thúc khi hệ phương trình cuối cùng chỉ có nghiệm tầm thường.

3.2.2 Áp dụng thuật toán tìm cơ sở của giao hai nhóm con của nhóm aben

Xét các $\mathbb{Z}$ -môđun con A, B của $\mathbb{Z}^7$. A có cơ sở:

$$\begin{aligned} u_1 &= (26, 12, -9, 2, 22, 8, 3) \\ u_2 &= (-62, 21, 7, 14, -28, 0, 0) \\ u_3 &= (1, -5, 2, 9, 11, 2, 4) \\ u_4 &= (3, 5, -9, -6, 12, 15, -18) \\ u_5 &= (2, -12, 16, 3, 9, 7, 12) \end{aligned}$$

Cơ sở của môđun B :

$$\begin{aligned} v_1 &= (-2, 0, -1, 3, 5, 7, 9) \\ v_2 &= (3, 6, -3, 9, -2, 4, 6) \\ v_3 &= (1, -2, 1, 4, 9, -15, 60) \\ v_4 &= (3, -7, 9, 9, 21, 28, 6) \\ v_5 &= (5, 9, 6, 6, 7, -15, -21) \end{aligned}$$

Mỗi phần tử $x \in A \cap B$ tương ứng với các bộ hệ số $(x_1, x_2, x_3, x_4, x_5), (y_1, y_2, y_3, y_4, y_5)$ sao cho x có sự phân tích

$$x = x_1 u_1 + \dots + x_5 u_5 = y_1 v_1 + \dots + y_5 v_5$$

với $x_i, y_j \in \mathbb{Z}$ là nghiệm của hệ phương trình:

$$\left\{ \begin{array}{l} 26x_1 - 62x_2 + 1x_3 + 3x_4 + 2x_5 - (-2y_1 + 3y_2 + 1y_3 + 3y_4 + 5y_5) = 0 \\ 12x_1 + 21x_2 - 5x_3 + 5x_4 - 12x_5 - (0y_1 + 6y_2 - 2y_3 - 7y_4 + 9y_5) = 0 \\ -9x_1 + 7x_2 + 2x_3 - 9x_4 + 16x_5 - (-1y_1 - 3y_2 + 1y_3 + 9y_4 + 6y_5) = 0 \\ 2x_1 + 14x_2 + 9x_3 - 6x_4 + 3x_5 - (3y_1 + 9y_2 + 4y_3 + 9y_4 + 6y_5) = 0 \\ 22x_1 - 28x_2 + 11x_3 + 12x_4 + 9x_5 - (5y_1 - 2y_2 + 9y_3 + 21y_4 + 7y_5) = 0 \\ 8x_1 + 0x_2 + 2x_3 + 15x_4 + 7x_5 - (7y_1 + 4y_2 - 15y_3 + 28y_4 - 15y_5) = 0 \\ 3x_1 + 0x_2 + 4x_3 - 18x_4 + 12x_5 - (9y_1 + 6y_2 + 60y_3 + 6y_4 - 21y_5) = 0 \end{array} \right.$$

Ta dễ dàng tìm được một nghiệm của hệ:

$$\begin{aligned} &(-57270032, -25881007, -70358559, 5191558, -14196384, \\ &-201712721, -24722397, 0, 1, -59366661) \end{aligned}$$

có ƯCLN của các thành phần bằng 1. Nghiệm này cho ta phần tử cơ sở đầu tiên của $A \cap B$:

$$\begin{aligned} a &= -57270032u_1 - 25881007u_2 - 70358559u_3 + 5191558u_4 - 14196384u_5 \\ &= -201712721v_1 - 24722397v_2 + 0v_3 + 1v_4 - 59366661v_5 \end{aligned}$$

Xét đồng cấu xác định bởi $f(x) = y_4$ với mỗi $x = x_1u_1 + \dots + x_5u_5 + y_1v_1 + \dots + y_5v_5$, f thỏa $f(a) = 1$.

Khi đó ta có sự phân tích: $A \cap B = \mathbb{Z}a \oplus \ker f$ với $\ker f$ là tập các x tương ứng với bộ các hệ số x_i, y_j là nghiệm của hệ phương trình:

$$\left\{ \begin{array}{l} 26x_1 - 62x_2 + 1x_3 + 3x_4 + 2x_5 - (-2y_1 + 3y_2 + 1y_3 + 3y_4 + 5y_5) = 0 \\ 12x_1 + 21x_2 - 5x_3 + 5x_4 - 12x_5 - (0y_1 + 6y_2 - 2y_3 - 7y_4 + 9y_5) = 0 \\ -9x_1 + 7x_2 + 2x_3 - 9x_4 + 16x_5 - (-1y_1 - 3y_2 + 1y_3 + 9y_4 + 6y_5) = 0 \\ 2x_1 + 14x_2 + 9x_3 - 6x_4 + 3x_5 - (3y_1 + 9y_2 + 4y_3 + 9y_4 + 6y_5) = 0 \\ 22x_1 - 28x_2 + 11x_3 + 12x_4 + 9x_5 - (5y_1 - 2y_2 + 9y_3 + 21y_4 + 7y_5) = 0 \\ 8x_1 + 0x_2 + 2x_3 + 15x_4 + 7x_5 - (7y_1 + 4y_2 - 15y_3 + 28y_4 - 15y_5) = 0 \\ 3x_1 + 0x_2 + 4x_3 - 18x_4 + 12x_5 - (9y_1 + 6y_2 + 60y_3 + 6y_4 - 21y_5) = 0 \\ 1y_4 = 0 \end{array} \right.$$

Ta tìm được một nghiệm của hệ phương trình trên:

$$\begin{aligned} &(-61871633, -27960527, -76011819, 5608685, -15337058, \\ &-217920208, -26708813, 4, 0, -64136729) \end{aligned}$$

có ƯCLN của các thành phần bằng 1. Phần tử cơ sở thứ hai của $A \cap B$ theo đó sẽ là:

$$b = -217920208v_1 - 26708813v_2 + 4v_3 + 0v_4 - 64136729v_5$$

Xét đồng cấu $g : A \cap B \rightarrow \mathbb{Z}$ xác định bởi $g(x) = 1x_2 + 6990132y_3$ với mỗi $x = x_1u_1 + \dots + x_5u_5 + y_1v_1 + \dots + y_5v_5$ thỏa $g(b) = 1$.

Khi đó ta có sự phân tích:

$$A \cap B = \mathbb{Z}a \oplus \mathbb{Z}b \oplus \ker g$$

với $\ker g$ là tập các $x \in A \cap B$ tương ứng với bộ các hệ số $(x_1, x_2, x_3, x_4, x_5)$,

$(y_1, y_2, y_3, y_4, y_5)$ thỏa mãn hệ phương trình:

$$\begin{cases} 26x_1 - 62x_2 + 1x_3 + 3x_4 + 2x_5 - (-2y_1 + 3y_2 + 1y_3 + 3y_4 + 5y_5) = 0 \\ 12x_1 + 21x_2 - 5x_3 + 5x_4 - 12x_5 - (0y_1 + 6y_2 - 2y_3 - 7y_4 + 9y_5) = 0 \\ -9x_1 + 7x_2 + 2x_3 - 9x_4 + 16x_5 - (-1y_1 - 3y_2 + 1y_3 + 9y_4 + 6y_5) = 0 \\ 2x_1 + 14x_2 + 9x_3 - 6x_4 + 3x_5 - (3y_1 + 9y_2 + 4y_3 + 9y_4 + 6y_5) = 0 \\ 22x_1 - 28x_2 + 11x_3 + 12x_4 + 9x_5 - (5y_1 - 2y_2 + 9y_3 + 21y_4 + 7y_5) = 0 \\ 8x_1 + 0x_2 + 2x_3 + 15x_4 + 7x_5 - (7y_1 + 4y_2 - 15y_3 + 28y_4 - 15y_5) = 0 \\ 3x_1 + 0x_2 + 4x_3 - 18x_4 + 12x_5 - (9y_1 + 6y_2 + 60y_3 + 6y_4 - 21y_5) = 0 \\ 1y_4 = 0 \\ 1x_2 + 6990132y_3 = 0 \end{cases}$$

Ta tìm được một nghiệm của hệ phương trình trên:

$$\begin{aligned} &(-2081781236374401, -940781706339312, -2557552966751124, 188714191424934, \\ &-516042619492289, -7332313340448025, -898665560503846, 134587116, 0, \\ &-2157994423625922) \end{aligned}$$

có ƯCLN của các hệ số bằng 1. Phần tử cơ sở thứ ba của $A \cap B$ sẽ là

$$c = -7332313340448025v_1 - 898665560503846v_2 + 134587116v_3 + 0v_4 - 2157994423625922v_5$$

Xét đồng cấu $h : A \cap B \xrightarrow{g} \mathbb{Z}$ xác định bởi $h(x) = 92794759x_5 + 355799662944822y_3$ với mỗi $x = x_1u_1 + \dots + x_5u_5 + y_1v_1 + \dots + y_5v_5$, h thỏa $h(c) = 1$. Khi đó ta có sự phân tích:

$$A \cap B = \mathbb{Z}a \oplus \mathbb{Z}b \oplus \mathbb{Z}c \oplus \ker g$$

với $\ker g$ là tập các $x \in A \cap B$ tương ứng với bộ các hệ số $(x_1, x_2, x_3, x_4, x_5)$,

$(y_1, y_2, y_3, y_4, y_5)$ thỏa mãn hệ phương trình:

$$\begin{cases} 26x_1 - 62x_2 + 1x_3 + 3x_4 + 2x_5 - (-2y_1 + 3y_2 + 1y_3 + 3y_4 + 5y_5) = 0 \\ 12x_1 + 21x_2 - 5x_3 + 5x_4 - 12x_5 - (0y_1 + 6y_2 - 2y_3 - 7y_4 + 9y_5) = 0 \\ -9x_1 + 7x_2 + 2x_3 - 9x_4 + 16x_5 - (-1y_1 - 3y_2 + 1y_3 + 9y_4 + 6y_5) = 0 \\ 2x_1 + 14x_2 + 9x_3 - 6x_4 + 3x_5 - (3y_1 + 9y_2 + 4y_3 + 9y_4 + 6y_5) = 0 \\ 22x_1 - 28x_2 + 11x_3 + 12x_4 + 9x_5 - (5y_1 - 2y_2 + 9y_3 + 21y_4 + 7y_5) = 0 \\ 8x_1 + 0x_2 + 2x_3 + 15x_4 + 7x_5 - (7y_1 + 4y_2 - 15y_3 + 28y_4 - 15y_5) = 0 \\ 3x_1 + 0x_2 + 4x_3 - 18x_4 + 12x_5 - (9y_1 + 6y_2 + 60y_3 + 6y_4 - 21y_5) = 0 \\ 1y_4 = 0 \\ 1x_2 + 6990132y_3 = 0 \\ 92794759x_5 + 355799662944822y_3 = 0 \end{cases}$$

Hệ này chỉ có nghiệm tầm thường. Thuật toán kết thúc.

Như vậy, cơ sở của $A \cap B$ là:

$$a = (32424949, -682634338, -80320045, -1183839693, \\ -1374685417, -620378692, -717048984)$$

$$b = (35030336, -737483447, -86773723, -1278960299, \\ -1485140481, -670225833, -774663201)$$

$$c = (1178658015842018, -24813943444830606, -2919656385208853, -43032896069285757 \\ -49970195335329843, -22550941289569469, -26064922455683979)$$

3.3 Thuật toán tìm cơ sở của môđun cho bởi hệ sinh

3.3.1 Thuật toán

Cho môđun A là môđun con của X cho bởi hệ sinh: $\mathcal{B} = \{u_1, u_2, \dots, u_k, v_1, v_2, \dots, v_m\}$ trong đó:

- $\{u_1, u_2, \dots, u_k\}$ là hệ con độc lập tuyến tính tối đại trong B .
- Ta có sự phân tích: $\alpha_i v_i = \beta_{i1} u_1 + \beta_{i2} u_2 + \dots + \beta_{ik} u_k$ (*) với mỗi $i = 1, 2, \dots, m$
 α_i không khả nghịch, $\text{ƯCLN}(\alpha_i, \beta_{i1}, \beta_{i2}, \dots, \beta_{ik}) = 1$.

Bắt đầu với $\alpha_1 v_1 = \beta_{11} u_1 + \beta_{12} u_2 + \dots + \beta_{1k} u_k$ (1) .

Ta xét 2 trường hợp sau:

1) $\text{ƯCLN}(\beta_{11}, \beta_{12}, \dots, \beta_{1k}) = 1$ tức là $\alpha_1 v_1$ là đơn tử trong môđun con U sinh bởi cơ sở $u_1, u_2, \dots, u_k$.

Bằng thuật toán xây dựng cơ sở của môđun chứa một đơn tử cho trước ta có thể bổ sung vào $\{\alpha_1 v_1\}$ để được cơ sở mới $\{\alpha_1 v_1, u'_2, \dots, u'_k\}$ của U .

Khi đó $\{u'_1 = v_1, u'_2, \dots, u'_k\}$ là độc lập tuyến tính tối đại trong $\mathcal{B}$ và có thể thay thế cho $k+1$ phần tử $\{u_1, u_2, \dots, u_k, v_1\}$ trong hệ sinh $\mathcal{B}$.

2) $\text{ƯCLN}(\beta_{11}, \beta_{12}, \dots, \beta_{1k}) = \lambda$ không khả nghịch. Khi đó: $\beta_{1i} = \lambda \beta'_{1i}$, $i = 1, \dots, k$ với $\text{ƯCLN}(\beta'_{11}, \beta'_{12}, \dots, \beta'_{1k}) = 1$.

Ta có: $\text{ƯCLN}(\lambda, \alpha_1) = 1$ và

$$\alpha_1 v_1 = \lambda(\beta'_{11}u_1 + \beta'_{21}u_2 + \dots + \beta'_{1k}u_k)$$

Ta sẽ chứng minh: $v_1 = \lambda v'_1$, $v'_1 \in X$ và chứng minh $v'_1 \in A$. Để làm việc đó ta cần chứng minh thêm một số kết quả sau.

Mệnh đề 5 Trong môđun X , với mỗi phần tử $x \in X$ đều tồn tại một đơn tử $a \in X$ và hệ tử $r \in R$ sao cho $x = ra$.

Ta gọi hệ tử r đó gọi là hệ số đơn nguyên của x trong X .

Chứng minh:

Trong X chọn cơ sở U và gọi $(x_1, x_2, \dots, x_n)$ $x_i \in R$ là tọa độ của x đối với U . Lấy $r = \text{ƯCLN}(x_1, x_2, \dots, x_n)$ ta có: $x_i = ry_i$, ($y_i \in R$) và $\text{ƯCLN}(y_1, y_2, \dots, y_n) = 1$. Do đó phần tử $a \in X$ có tọa độ $(y_1, y_2, \dots, y_n)$ là đơn tử. Dễ thấy $x = ra$.

□

Nhận xét

- Cũng như khái niệm đơn tử, khái niệm hệ số đơn nguyên của phần tử x có tính tương đối, phụ thuộc theo từng môđun chứa x .
- Hệ số đơn nguyên của x không duy nhất; các hệ số đơn nguyên của cùng một phần tử lập thành một lớp các hệ tử liên kết trong vành R .
- Nếu x có tọa độ đối với cơ sở U là $(x_1, x_2, \dots, x_n)$ và có tọa độ $(x'_1, x'_2, \dots, x'_n)$ đối với cơ sở U' thì $\text{ƯCLN}(x_1, x_2, \dots, x_n) = \text{ƯCLN}(x'_1, x'_2, \dots, x'_n)$ (định nghĩa đơn tử không phụ thuộc vào việc chọn cơ sở, hệ số đơn nguyên cũng vậy)

Mệnh đề 6 Nếu hai đơn tử a, b trong môđun X là phụ thuộc tuyến tính, tức là có các hệ tử $m, n \in R$ sao cho $ma = nb$ thì $n = rm, a = rb$ với r khả nghịch.

Chứng minh:

Gọi $\lambda = \text{ƯCLN}(m, n)$, ta có $m = \lambda m'$ và $n = \lambda n'$ với $\text{ƯCLN}(m', n') = 1$.

$$ma = nb \Rightarrow \lambda m'a = \lambda n'b \Rightarrow m'a = n'b$$

Gọi $p, q \in R$ là các hệ tử sao cho $pm' + qn' = 1$.

Ta có: $a = 1.a = (pm' + qn')a = p(m'a) + qn'a = pn'b + qn'a = n'(pb + qa)$.

Mà a là đơn tử nên theo định nghĩa đơn tử ta suy ra n' khả nghịch.

Từ $m'a = n'b \Rightarrow b = m'.n'^{-1}a$ mà b cũng là đơn tử nên suy ra m' cũng khả nghịch.

Ta có: $m = \lambda m', n = \lambda n'$ và $m'a = n'b$ với m', n' khả nghịch, từ đây dễ dàng suy ra điều phải chứng minh.

□

Hệ quả 4 Nếu trong môđun X ta có hệ thức sau giữa hai phần tử $x, y \in X$: $\lambda x = \mu y$ với $\text{ƯCLN}(\lambda, \mu) = 1$ thì $x = \mu x'$ với x' nào đó thuộc x .

Chứng minh:

Giả sử $x, y \in R$ và $\lambda x = \mu y$.

Theo mệnh đề 5 ta có $x = ra$ và $y = sb$ với a, b là các đơn tử trong môđun X , $r, s \in R$.

Ta được: $\lambda ra = \mu sb$.

Theo mệnh đề 4 ta có $\mu s = \lambda r.u$ với $u \in R$ khả nghịch. Mà $\text{ƯCLN}(\lambda, \mu) = 1$ nên $s = \lambda.t$ với $t \in R$.

Viết lại hệ thức: $\lambda x = \mu.\lambda t.b \Rightarrow x = \mu.(tb) = \mu.x'$ với $x' = tb$.

□

Nhận xét: Trong mệnh đề 6 và hệ quả 4 nói trên, vai trò của a, b như nhau và x, y là như nhau nên ta cũng có $y = \lambda y'$ với $y' \in X$.

Trở lại thuật toán tìm cơ sở của hệ sinh. Ta đã có hệ thức:

$$\alpha_1 v_1 = \lambda(\beta'_{11}u_1 + \beta'_{21}u_2 + \dots + \beta'_{1k}u_k)$$

Từ hệ quả 4 ta được: $v_1 = \lambda v'_1$ với $v'_1 \in X$; và từ hệ thức trên ta có:

$$\alpha_1 v'_1 = \beta'_{11}u_1 + \beta'_{21}u_2 + \dots + \beta'_{1k}u_k \quad (2)$$

với $\text{ƯCLN}(\beta'_{11}, \beta'_{12}, \dots, \beta'_{1k}) = 1$.

Từ (1) suy ra $\alpha_1 v'_1 \in A$.

Ta có: $\lambda v'_1 = v_1 \in A$ và $\alpha_1 v'_1 \in A$ với $\text{ƯCLN}(\lambda, \alpha_1) = 1$. Gọi $p, q \in R$ sao cho $p\lambda + q\alpha_1 = 1$.

Ta có: $v'_1 = (p\lambda + q\alpha_1)v'_1 = p\lambda v'_1 + q\alpha_1 v'_1$ và do đó $v'_1 \in A$.

Thực hiện giống trường hợp 1) với hệ thức (2) ta có thể thay hệ $\{u_1, u_2, \dots, u_k\}$ bằng hệ $\{\alpha_1 v'_1, u_2, \dots, u_k\}$ và thay hệ $k+1$ phần tử $\{v_1, u_1, \dots, u_k\}$ trong hệ sinh $\mathcal{B}$ bằng hệ k phần tử $\{v'_1 = u'_1, u'_2, \dots, u'_k\}$ độc lập tuyến tính tối đại trong $\mathcal{B}$.

Xét ma trận đổi cơ sở trong môđun U sinh bởi $\{u_1, \dots, u_k\}$

$$\begin{bmatrix} \alpha_1 u'_1 \\ u'_2 \\ \dots \\ u'_k \end{bmatrix} = K \cdot \begin{bmatrix} u_1 \\ u_2 \\ \dots \\ u_k \end{bmatrix} \Rightarrow \begin{bmatrix} u_1 \\ u_2 \\ \dots \\ u_k \end{bmatrix} = K^{-1} \cdot \begin{bmatrix} \alpha_1 u'_1 \\ u'_2 \\ \dots \\ u'_k \end{bmatrix} = L \cdot \begin{bmatrix} u'_1 \\ u'_2 \\ \dots \\ u'_k \end{bmatrix}$$

trong đó L là ma trận K^{-1} mà cột 1 đã nhân thêm α_1 . Với $i = 2, \dots, m$, ta có sự phân tích:

$$[\alpha_i v_i] = [\beta_{i1}, \beta_{i2}, \dots, \beta_{ik}] \cdot \begin{bmatrix} u_1 \\ u_2 \\ \dots \\ u_k \end{bmatrix} = [\beta_{i1}, \beta_{i2}, \dots, \beta_{ik}] \cdot L \cdot \begin{bmatrix} u'_1 \\ u'_2 \\ \dots \\ u'_k \end{bmatrix}$$

Chia 2 vế cho ƯCLN của tất cả các hệ số trong sự phân tích trên ta được:

$$\gamma_i v_i = \eta_{i1}u_1 + \eta_{i2}u_2 + \dots + \eta_{ik}u_k \text{ với } \text{ƯCLN}(\gamma_i, \eta_{i1}, \eta_{i2}, \dots, \eta_{ik}) = 1$$

Nếu γ_i là ước của đơn vị thì bỏ qua v_i trong hệ sinh, xét tiếp γ_{i+1} .

Nếu γ_i không là ước của đơn vị thì quay lại bước 1, thay v_1 bởi v_i cho đến khi hệ sinh chỉ còn lại hệ n vectơ độc lập tuyến tính.

Thuật toán sẽ dừng sau tối đa m bước.

Về thuật toán tìm cơ sở của tổng hai môđun Cho hai môđun con A và B của một môđun X .

Môđun A có cơ sở $\{u_1, u_2, \dots, u_k\}$.

Môđun B có cơ sở $\{v_1, v_2, \dots, v_s\}$

Khi đó tổng của A và B có hệ sinh là: $\{u_1, u_2, \dots, u_k, v_1, v_2, \dots, v_s\}$. Thuật toán trên có thể được áp dụng để tìm cơ sở của $A + B$.

3.3.2 Áp dụng thuật toán tìm cơ sở của nhóm con của nhóm aben tự do

Xét môđun con A của $\mathbb{Z}^7$ cho bởi hệ sinh:

$$\begin{aligned} u_1 &= (-1, 4, 5, 3, -3, 7, 10), \\ u_2 &= (9, -87, 36, -9, -42, -48, 57), \\ u_3 &= (7, 22, 4, -1, 1, 14, 9), \\ u_4 &= (2, -2, 2, 0, 0, -2, 1), \\ u_5 &= (-26, -310, 28, -12, -69, -193, 17), \\ v_1 &= (1, 0, 1, 3, 4, 0, -3), \\ v_2 &= (-20, -226, 20, -8, -50, -140, 12), \\ v_3 &= (0, 1, -2, -2, -1, 2, 2) \end{aligned}$$

trong đó hệ $\{u_1, u_2, \dots, u_5\}$ là độc lập tuyến tính và mỗi vectơ v_1, v_2, v_3 có sự phân tích như sau:

$$3v_1 = 3u_1 - 2u_2 + 6u_3 + 4u_4 + 1u_5 \quad (1)$$

$$15v_2 = 4u_1 - 2u_2 + 6u_3 - 4u_4 + 12u_5 \quad (2)$$

$$3v_3 = 2u_1 - 3u_2 + 15u_3 - 12u_4 + 2u_5 \quad (3)$$

Xét (1) ta thấy ƯCLN của các hệ số bên vế phải bằng 1: $\text{ƯCLN}(3, -2, 6, 4, 1) = 1$. Nên ta có thể bổ sung vào $\{3v_1\}$ để được hệ $\{3v_1, u'_2, u'_3, \dots, u'_5\}$ là cơ sở mới của môđun sinh bởi cơ sở $\{u_1, u_2, \dots, u_5\}$. Sử dụng thuật toán tìm cơ sở môđun chứa một đơn tử cho trước, ta tìm được hệ đó là $\{3v_1, u_1, u_2, u_3, u_4\}$ (kết quả rất đẹp vì trong (1) hệ số của u_5 bằng 1!).

Ta thay các vectơ $v_1, u_1, u_2, u_3, u_4, u_5$ trong hệ sinh bằng các vectơ v_1, u_1, u_2, u_3, u_4 .

Ta có:

$$\begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \\ 3v_1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 3 & -2 & 6 & 4 & 1 \end{bmatrix} \cdot \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \end{bmatrix}$$

Suy ra:

$$\begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ -3 & 2 & -6 & -4 & 1 \end{bmatrix} \cdot \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \\ 3v_1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ -3 & 2 & -6 & -4 & 3 \end{bmatrix} \cdot \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \\ v_1 \end{bmatrix}$$

Ta có:

$$\begin{aligned} [15v_2] = [4, -2, 6, -4, 12] \cdot \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \end{bmatrix} &= [4, -2, 6, -4, 12] \cdot \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ -3 & 2 & -6 & -4 & 3 \end{bmatrix} \cdot \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \\ v_1 \end{bmatrix} \\ &= [-32, 22, -66, -52, 36] \cdot \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \\ v_1 \end{bmatrix} \end{aligned}$$

Tức là $15v_2 = -32u_1 + 22u_2 - 66u_3 - 52u_4 + 36v_1$ (ii).

Tương tự ta có: $3v_3 = -4u_1 + u_2 + 3u_3 - 20u_4 + 6v_1$.

Ta xét tiếp v_2 trong phân tích (ii), ta thấy ƯCLN(-32,22,-66,-52,36)=2.

v_2 có thể viết lại thành $v_2 = 2v'_2$ với $v'_2 = (-10, -113, 10, -4, -25, -70, 6)$ và thuật toán đã chứng minh $v'_2 \in A$.

(ii) trở thành $15v'_2 = -16u_1 + 11u_2 - 33u_3 - 26u_4 + 18v_1$ với ƯCLN(-16,11,-33,-26,18)=1.

Ta lại sử dụng thuật toán tìm cơ sở môđun chứa một đơn tử cho trước để tìm hệ cơ sở mới chứa $15v'_2$ trong môđun V sinh bởi cơ sở u_1, u_2, u_3, u_4, v_1 .

Kết quả của quá trình trên là hệ cơ sở mới của V :

$$\alpha_1 = 15v'_2 = -16u_1 + 11u_2 - 33u_3 - 26u_4 + 18v_1$$

$$\alpha_2 = 3u_1 - 2u_2$$

$$\alpha_3 = u_3$$

$$\alpha_4 = u_4$$

$$\alpha_5 = v_1$$

Ta thay các vectơ $u_1, u_2, u_3, u_4, v_1, v_2$ trong hệ sinh bằng các vectơ $v'_2, \alpha_2, \alpha_3, \alpha_4, \alpha_5$.

Ta có:

$$\begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \\ v_1 \end{bmatrix} = \begin{bmatrix} 2 & 11 & 66 & 52 & -36 \\ 3 & 16 & 99 & 78 & -54 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 15v'_2 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \\ \alpha_5 \end{bmatrix} = \begin{bmatrix} 30 & 11 & 66 & 52 & -36 \\ 45 & 16 & 99 & 78 & -54 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} v'_2 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \\ \alpha_5 \end{bmatrix}$$

Suy ra: $3v_3 = -75v'_2 - 28\alpha_2 - 162\alpha_3 - 150\alpha_4 + 96\alpha_5$.

Trong phân tích trên, ta thấy ƯCLN của các hệ số bên vế phải bằng 1.

Ta lại sử dụng thuật toán xây dựng cơ sở chứa đơn tử cho trước để bổ sung vào $3v_3$ thành một cơ sở mới của môđun W sinh bởi $v'_2, \alpha_2, \alpha_3, \dots, \alpha_5$. Cơ sở đó là:

$$\beta_1 = 3v_3 = -75v'_2 - 28\alpha_2 - 162\alpha_3 - 150\alpha_4 + 96\alpha_5$$

$$\beta_2 = 8v'_2 + 3\alpha_2$$

$$\beta_3 = \alpha_3$$

$$\beta_4 = \alpha_4$$

$$\beta_5 = \alpha_5$$

Ta thay các vectơ $v_3, v'_2, \alpha_2, \alpha_3, \dots, \alpha_5$ trong hệ sinh bằng các vectơ $\beta_3, \beta_2, \dots, \beta_5$.

Hệ sinh bây giờ được thu gọn thành hệ 5 vectơ độc lập tuyến tính là do đó chính là cơ sở của A .

Tóm lại: môđun con A của $\mathbb{Z}^7$ cho bởi hệ sinh:

$$\begin{aligned} u_1 &= (-1, 4, 5, 3, -3, 7, 10), \\ u_2 &= (9, -87, 36, -9, -42, -48, 57), \\ u_3 &= (7, 22, 4, -1, 1, 14, 9), \\ u_4 &= (2, -2, 2, 0, 0, -2, 1), \\ u_5 &= (-26, -310, 28, -12, -69, -193, 17), \\ v_1 &= (1, 0, 1, 3, 4, 0, -3), \\ v_2 &= (-20, -226, 20, -8, -50, -140, 12), \\ v_3 &= (0, 1, -2, -2, -1, 2, 2) \end{aligned}$$

có cơ sở là:

$$\begin{aligned} v_3 &= (0, 1, -2, -2, -1, 2, 2) \\ \beta_2 &= (-101, -856, 113, -5, -227, -485, 132) \\ \beta_3 &= (7, 22, 4, -1, 1, 14, 9) \\ \beta_4 &= (2, -2, 2, 0, 0, -2, 1) \\ \beta_5 &= (1, 0, 1, 3, 4, 0, -3) \end{aligned}$$

3.3.3 Áp dụng thuật toán trên môđun tự do trên vành đa thức

Xét $R = \mathbb{Q}[x]$ là vành các đa thức hệ số hữu tỉ. $\mathbb{Q}[x]$ là vành chính.

Gọi $X = R^4$ là môđun tự do hạng bằng 4 trên R .

$$X = \{p = (p_1(x), p_2(x), p_3(x), p_4(x)) \mid p_i(x) \in \mathbb{Q}[x] \forall i\}$$

Gọi A là môđun con của X có hệ sinh:

$$\begin{aligned} u_1 &= (x^3, x + 1, 2x^2 - x + 1, 5) \\ u_2 &= (x^2 + x, x^2, -\frac{1}{2}x, 0) \\ u_3 &= (2x, \frac{1}{2}x - 1, -\frac{5}{2}x - 1, -\frac{7}{2}x - 5) \\ v_1 &= (x^2 - x, \frac{1}{2}(x^2 + 3), \frac{1}{2}(5x^2 - x + 3), \frac{1}{2}(7x^2 - 4x + 15)) \\ v_2 &= (3x^3 + 4x^2 + 5, x^3 + x^2 + \frac{5}{2}x + 6, \frac{7}{2}x^2 + 4x - \frac{9}{2}, \frac{7}{2}x + 8) \end{aligned}$$

trong đó: u_1, u_2, u_3 độc lập tuyến tính và ta có sự phân tích:

$$(x + 2)v_1 = 2u_1 + xu_2 - (1 + x^2)u_3 \quad (1)$$

$$xv_2 = (2x + 2)u_1 + (x^2 + x + 1)u_2 - (x - 2)u_3 \quad (2)$$

Xét (1) ta thấy ƯCLN của các hệ số bên vế phải ƯCLN($2, x, -(1+x^2)$)=1. Như vậy, $(x+2)v_1$ là đơn tử trong môđun $U = \langle \{u_1, u_2, u_3\} \rangle$ nên có thể áp dụng thuật toán tìm cơ sở chứa đơn tử cho trước để thay cơ sở của U bằng cơ sở mới, kết quả ta tìm được cơ sở mới là:

$$\begin{aligned} u'_1 &= (x+2)v_1 \\ u'_2 &= u_2 \\ u'_3 &= u_3 \end{aligned}$$

Ta thay các vectơ v_1, u_1, u_2, u_3 trong hệ sinh bằng v_1, u'_2, u'_3

Ta có:

$$\begin{aligned} \begin{bmatrix} (x+2)v_1 \\ u'_2 \\ u'_3 \end{bmatrix} &= \begin{bmatrix} 2 & x & -(1+x^2) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} \\ \Rightarrow \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} &= \begin{bmatrix} \frac{1}{2} & -x & 1+x^2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} (x+2)v_1 \\ u'_2 \\ u'_3 \end{bmatrix} = \begin{bmatrix} \frac{1}{2}(x+2) & -x & 1+x^2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} v_1 \\ u'_2 \\ u'_3 \end{bmatrix} \end{aligned}$$

Từ đây ta có:

$$xv_2 = (x+1)(x+2)v_1 + u'_2 + (x^3 + x^2 + 3)u'_3 \quad (3)$$

Ta thấy ƯCLN của các hệ số trong vế phải của (3) ƯCLN($((x+1)(x+2), 1, (x^3 + x^2 + 3))$)=1. Như vậy xv_2 là đơn tử trong môđun $V = \langle \{v_1, u'_2, u'_3\} \rangle$, áp dụng thuật toán tìm cơ sở chứa đơn tử cho trước, ta được cơ sở mới của V là:

$$\begin{aligned} \alpha_1 &= xv_2 \\ \alpha_2 &= v_1 \\ \alpha_3 &= u'_3 \end{aligned}$$

Ta thay các vectơ v_2, v_1, u'_2, u'_3 trong hệ sinh bằng các vectơ v_2, v_1, u'_3 . Hệ sinh của A bây giờ còn đúng 3 vectơ độc lập tuyến tính nên chính là cơ sở của A .

Vậy cơ sở của A là:

$$\begin{aligned} v_1 &= (x^2 - x, \frac{1}{2}(x^2 + 3), \frac{1}{2}(5x^2 - x + 3), \frac{1}{2}(7x^2 - 4x + 15)) \\ v_2 &= (3x^3 + 4x^2 + 5, x^3 + x^2 + \frac{5}{2}x + 6, \frac{7}{2}x^2 + 4x - \frac{9}{2}, \frac{7}{2}x + 8) \\ u_3 &= (2x, \frac{1}{2}x - 1, -\frac{5}{2}x - 1, -\frac{7}{2}x - 5) \end{aligned}$$

3.4 Cách chứng minh mới cho một số kết quả của lý thuyết môđun

Mệnh đề 7 Cho A là môđun con của X và S là tập các hệ số đơn nguyên của các phần tử $x \in A$. Nếu λ là phần tử tối tiểu của S (theo quan hệ chia hết) và $a \in A$ là phần tử có hệ số đơn nguyên λ thì a là một đơn tử trong môđun con A , do đó tồn tại một cơ sở của A nhận a là thành viên.

Chứng minh Gọi λ là phần tử tối tiểu của S và $a \in A$ là phần tử có hệ số đơn nguyên λ , tức $a = \lambda b$ với $b \in X$ là đơn tử. Tọa độ của a với cơ sở U nào đó là $a = (a_1, a_2, \dots, a_n)$, theo chứng minh mệnh đề 5 $\text{ƯCLN}(a_1, a_2, \dots, a_n) = \lambda$.

Trong R lấy $t_1, t_2, \dots, t_n$ sao cho $t_1 a_1 + t_2 a_2 + \dots + t_n a_n = \lambda$.

Xét đồng cấu:

$$\begin{aligned} f: X &\longrightarrow R \\ x = (x_1, x_2, \dots, x_n) &\longmapsto t_1 x_1 + t_2 x_2 + \dots + t_n x_n \end{aligned}$$

ta có: $f(a) = \lambda$ và $f(b) = 1$. Chứng minh như trong mệnh đề 3 $X = \ker f \oplus Rb$. Ta sẽ chỉ ra $A = A \cap \ker f \oplus Ra$:

Vì A là môđun con của X nên $f(A)$ là idêan của R , mà R là vành chính nên $f(A) = R\mu$. Vì $f(a) \in f(A)$ nên $\mu \mid \lambda$

Gọi $x \in A$ là phần tử mà $f(x) = \mu$, theo mệnh đề 5 $x = ry$ với y đơn tử trong X , $r \in S$.

Khi đó: $\mu = f(x) = f(ry) = rf(y)$ nên $r \mid \mu \mid \lambda$. Tuy nhiên λ là tối tiểu trong S nên $r \sim \mu \sim \lambda$. Suy ra: $f(A) = R\lambda$

Với mọi $x \in A$, có $r \in R$ để $f(x) = r\lambda = f(ra) \Rightarrow x = y + ra$ với $y \in \ker f$, hơn nữa $y = x - ra \in A$. Vậy $A = A \cap \ker f \oplus Ra$, a hợp với cơ sở của $A \cap \ker f$ là cơ sở của A .

□

Hệ quả 5 1. Số chiều của môđun con A không lớn hơn số chiều của môđun X

2. Trong X tồn tại cơ sở $V = \{v_1, v_2, \dots, v_n\}$ và các hệ tử $r_1, r_2, \dots, r_n$ thuộc R để hệ $\{r_1 v_1, r_2 v_2, \dots, r_n v_n\}$ là hệ sinh của A (nếu bỏ đi các phần tử $r_i v_i = 0$ thì chính là cơ sở)

Chứng minh:

Giả sử $A \neq 0$. Qua chứng minh định lý ta thấy rằng nếu chọn từ A phần tử a_1 có hệ số đơn nguyên tối tiểu trong S , $a_1 = \lambda_1 b_1$, b_1 đơn tử trong X thì có sự phân tích: $A = Ra_1 \oplus A_1$ và $X = Rb_1 \oplus X_1$ và A_1 là môđun con của X_1 .

Nếu $A_1 \neq 0$, thay A bởi A_1 ta lại có: $A_1 = Ra_2 \oplus A_2$ và $X_1 = Rb_2 \oplus X_2$ với $a_2 = \lambda_2 b_2$, A_2 là môđun con của X_2 .

Tiếp tục như vậy thì: $A = Ra_1 \oplus Ra_2 \oplus \dots \oplus Ra_k \oplus A_k$ và $X = Rb_1 \oplus Rb_2 \oplus \dots \oplus Rb_k \oplus X_k$ với $a_i = \lambda_i b_i$, A_k là môđun con của X_k .

Quá trình trên phải dừng ở $k = m \leq n$ tức $A_m = 0$ vì hệ $\{b_i\}$ như trên hợp với cơ sở của X_k là cơ sở của X nên k không thể vượt quá n . Khi đó $a_1, \dots, a_m$ là cơ sở của A , $b_1, \dots, b_m$ hợp với cơ sở của X_m là cơ sở của X và $a_i = \lambda b_i$.

□

TÀI LIỆU THAM KHẢO

Tiếng Việt

- [1] Nguyễn Viết Đông, Trần Huyền (2006), *Đại số đồng điều*, NXB Đại học Quốc Gia Tp. Hồ Chí Minh, Tp. Hồ Chí Minh.
- [2] Hoàng Xuân Sính (1997), *Đại số đại cương*, NXB Giáo Dục, Hà Nội.

Tiếng Anh

- [3] H. Cartan and S. Eilenberg (1965), *Homological Algebra* , Princeton University Press.
- [4] I. Kaplansky (1970) "*Commutative rings*". Allyn and Bacon, Inc, Boston.
- [5] Serge Lang (2005), *Algebra*, Springer, NewYork.