THUẬT TOÁN TÌM CƠ SỞ CỦA GIAO VÀ TỔNG HAI MODUN CON TRONG MODUN TỰ DO HỮU HẠN SINH TRÊN VÀNH CHÍNH

TRẦN HUYÊN*

TÓM TẮT

Trong bài báo này, chúng tôi đưa ra các đặc trưng cơ bản của một phần tử trong một môdun X tự do hữu hạn sinh trên vành chính mà môdun cyclic sinh bởi phần tử đó là hạng tử trực tiếp của X, từ đó xây dựng các thuật toán tìm cơ sở của giao và tổng của hai môdun con trong môdun X.

ABSTRACT

On the algorithm constructing the basis of cross and total for two sub-modules in the finite free module generated over the principal ring

In this paper, we consider the basic characteristics of the element in the finite free module X generated over the principal ring from which cyclic module from that element is the direct hierarchical element; thereby, we show the method of constructing algorithms to identify the basis of cross and total for two sub-modules in module X.

1. Mở đầu

Môđun tự do trên vành chính, đặc biệt là môđun tự do hữu hạn sinh và các môđun con của chúng đã được nhiều nhà toán học quan tâm nghiên cứu và đạt được nhiều kết quả tốt đẹp. Tuy nhiên, các kết quả này thường được phát biểu dưới dạng các định lý tồn tại và vì vậy mang nặng tính lý thuyết. Bài viết này của chúng tôi, bước đầu xây dựng một vài thuật toán tìm cơ sở của các môđun con, đặc biệt chú ý tới các cơ sở của giao và tổng hai môđun con dựa trên các cơ sở đã cho của hai môđun con đó.

2. Các kết quả chính

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

Định nghĩa 1:

Trong môđun X, phần tử $a \in X$, $a \neq 0$ gọi là đơn tử nếu $a = rb$ với $b \in X$ và $r \in R$ khi và chỉ khi r là khả nghịch.

Hiển nhiên 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 các đơn tử.

* TS, Khoa Toán - Tin học Trường Đại học Sư phạm TP HCM

Mệnh đề 1:

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

Thật ra chiều đảo trong 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 $a = a_1u_1 + ... + a_nu_n$ mà $UCLN(a_1, a_2,..., a_n) = 1$ 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 $f : X \to R$ thỏa $f(a) = 1.$

Chứng minh:

$(\Rightarrow)$ Chọn trong X một cơ sở $\{u_1, u_2,..., u_n\}$ và biểu diễn $a = a_1u_1 + ... + a_nu_n.$ Theo mệnh đề 1, $UCLN(a_1, a_2,..., a_n) = 1$, do vậy tồn tại các hệ tử $r_1, r_2,..., r_n \in R$ mà $r_1a_1 + r_2a_2 + ... + r_na_n = 1.$ Khi đó đồng cấu $f : X \to R$ mà với mỗi $x = x_1u_1 + ... + x_nu_n$ xác định $f(x) = r_1x_1 + r_2x_2 + ... + r_nx_n$, hiển nhiên thỏa yêu cầu mệnh đề 2.

$(\Leftarrow)$

Nếu có đồng cấu f thỏa yêu cầu mệnh đề 2 và a=rb thì $1 = f(a) = f(rb) = r.f(b)$, tức r khả nghịch.

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:

$(\Leftarrow)$ Hiển nhiên mỗi phần tử trong một cơ sở của X là đơn tử.

$(\Rightarrow)$ Nếu $a \in X$ là một đơn tử, theo mệnh đề 2, tồn tại toàn cấu $f : X \to R$ với $f(a) = 1$. Vì R là R-môđun tự do nên $X = Ra \oplus Kerf$ với *Ra* là môđun cyclic sinh bởi a: $Ra = \{ra : r \in R\} \cong$ R . Hệ thức tổng trực tiếp trên có nghĩa là cơ sở bất kì của Kerf khi bổ sung thêm a sẽ là một cơ sở của X.

Nhận xét: Theo mệnh đề 3, mỗi phần tử trong cơ sở một môđun là đơn tử trong môđun đó. Như vậy, phần tử $a \in A \lhd X$, có thể không là đơn tử của X, song nếu a thuộc một cơ sở nào đó của A thì a đơn tử trong A. Tức 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. Thật vậy, giả sử X có cơ sở ban đầu $\{e_1, e_2,..., e_n\}$ và $a \in X$ là đơn tử trong X mà $a = a_1e_1 + a_2e_2 + ... + a_ne_n$. Khi đó, ắt

tồn tại các hệ tử $r_1, r_2, ..., r_n \in R$ mà $r_1a_1 + r_2a_2 + ... + r_na_n = 1$. Chọn đồng cấu $f : X \to R$ mà $f(x) = r_1x_1 + r_2x_2 + ... + r_nx_n$ với mỗi $x = x_1e_1 + ... + x_ne_n$ thì $X = Ra \oplus Kerf$ trong đó Ker*f* là tập các phần tử $x \in X$ có tọa độ trong cơ sở ban đầu là $(x_1, x_2, ..., x_n)$ thỏa phương trình thuần nhất: $r_1x_1 + r_2x_2 + ... + r_nx_n = 0$. Lấy một nghiệm của phương trình trên $(b_1, b_2, ..., b_n)$ sao cho $UCLN(b_1, b_2, ..., b_n) = 1$. Khi đó $b = b_1e_1 + ... + b_ne_n \in Kerf$ là một đơn tử của Ker*f* (đồng thời là đơn tử trong X) và điều này cho phép ta xác định đồng cấu $g : Kerf \to R$ mà $g(x) = t_1x_1 + t_2x_2 + ... + t_nx_n$ với mỗi $x = x_1e_1 + ... + x_ne_n$ thỏa $g(b) = 1$. Đồng cấu này cho ta các sự phân tích $Kerf = Rb \oplus Kerg$ và $X = Ra \oplus Rb \oplus Kerg$ với $Kerg$ là tập các phần tử $x \in X$ với bộ tọa độ $(x_1, x_2, ..., x_n)$ trong cơ sở ban đầu thỏa hệ phương trình thuần nhất $\begin{cases} r_1x_1 + r_2x_2 + ... + r_nx_n = 0 \\ t_1x_1 + t_2x_2 + ... + t_nx_n = 0 \end{cases}$

Nếu hệ này có nghiệm không tầm thường thì ta tiếp tục chọn bộ nghiệm $(c_1, c_2, ..., c_n)$ mà $c = c_1e_1 + ... + c_ne_n$ là đơn tử trong Kerg (cũng là đơn tử trong X) và lặp lại tương tự quá trình trên. Thuật toán sẽ kết thúc khi hệ phương trình thuần nhất cuối cùng có chỉ nghiệm tầm thường.

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

Mục tiêu chính của bài viết này là xây dựng các thuật toán tìm cơ sở các môđun giao $X_1 \cap X_2$ và môđun tổng $X_1 + X_2$ dựa trên các cơ sở của X_1, X_2. Nếu x thuộc môđun giao, thì ắt tồn tại các bộ hệ tử $(x_1, x_2, ..., x_k)$ và $(y_1, y_2, ..., y_s)$ mà:

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

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

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

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 $(a_1,...,a_k,b_1,...,b_s)$ là nghiệm của hệ phương trình thuần nhất (*), xác định bởi $X_1 \bigcap X_2$ thỏa $UCLN(a_1,...,a_k,b_1,...,b_s)=1$ thì phần tử $a=a_1u_1+a_2u_2+...+a_ku_k=b_1v_1+b_2v_2+...+b_sv_s$ là đơn tử trong $X_1 \cap X_2$.

Chứng minh:

Gọi $\alpha=UCLN(a_1,a_2,...,a_k)$ và $\beta=UCLN(b_1,b_2,...,b_s)$ thì điều kiện của mệnh đề 4 cho ta $UCLN(\alpha,\beta)=1.$ Nếu có $b\in X_1\cap X_2$ và $r\in R$ mà a=rb thì hiển nhiên r là ước đồng thời của α và β và do đó r là khả nghịch.

Theo mệnh đề 3, thì phần tử a thỏa điều kiện của mệnh đề 4 là phần tử cơ sở đầu tiên của $X_1\cap X_2\neq\{0\}$ cần tìm.

Cũng theo mệnh đề 3, để xác định các phần tử cơ sở tiếp theo của $X_1\cap X_2$ (nếu còn !) ta cần xây dựng đồng cấu $f:X_1\cap X_2\to R$ mà $f(a)=1.$

Có nhiều cách khác nhau để xây dựng một đồng cấu f như thế, chẳng hạn: xây dựng đồng cấu $f_1:X_1\to R$ mà $f_1(a)=\alpha$ và xây dựng đồng cấu $f_2:X_2\to R$ mà $f_2(a)=\beta$ với $\alpha=UCLN(a_1,...,a_k)$ và $\beta=UCLN(b_1,...,b_s).$

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

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

Nếu hệ phương trình ghép có nghiệm không tầm thường, thì ta lại chọn một nghiệm $(c_1,...,c_k,d_1,...,d_s)$ với UCLN của chúng là 1. Khi đó phần tử $c_1u_1+...+c_ku_k=d_1v_1+...+d_sv_s$ là đơn tử trong $Kerf$, 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 sự 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 tại hệ phương trình cuối cùng có chỉ nghiệm tầm thường.

Thuật toán tìm cơ sở của tổng X_1+X_2 là sự tổ hợp các thuật toán đã trình bày ở trên. Tuy nhiên, để tiện lợi cho sự diễn giải ta cần tới vài kết quả đơn giản sau:

Mệnh đề 5:

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

Nhận xét: Hệ tử r nói trong mệnh đề 5 được gọi là hệ số đơn nguyên của x trong môđun X. Cũng như khái niệm đơn tử, khái niệm hệ số đơn nguyên của một phần tử x có tính tương đối, phụ thuộc theo từng môđun chứa x. Cũng dễ thấy là hệ số đơn

nguyên của một phần tử x trong môđun X không là duy nhất; các hệ số đơn nguyên của một phần tử lập thành một lớp các hệ tử liên kết trong vành R.

Mệnh đề 6:

Cho A là môđun con của X và $a \in A$. Khi đó tồn tại một đơn tử $u \in X$ và các hệ tử λ, β, γ sao cho λu là đơn tử của A và $a = \gamma u = \beta(\lambda u)$.

Chứng minh:

Sự tồn tại đơn tử $u \in X$ và hệ tử $\gamma \in R$ sao cho $a = \gamma u$ được suy ra từ mệnh đề 5. Vì $u \in X$ là đơn tử nên có đồng cấu $f : X \to R$ mà $f(u) = 1$ và hiển nhiên $f(a) = \gamma$! Ảnh $f(A)$ trong R là iđêan chính được sinh bởi hệ tử nào đó $\lambda \in R$. Vì $\gamma \in f(A)$ ắt tồn tại $\beta \in R$ mà $\gamma = \beta.\lambda$. Chứng minh mệnh đề sẽ kết thúc nếu ta kiểm tra được λu là đơn tử trong A. Thật vậy nếu có $r \in R$ và $b \in A$ mà $\lambda u = rb$ thì $\lambda = r.f(b) = r.(k\lambda)$ do $f(b) \in f(A)$ là iđêan chính sinh bởi λ. Giản ước λ ở hai vế đẳng thức trên trong R ta có: $rk = 1$ hay r khả nghịch.

Hệ quả: Với tất cả giả thiết và các kí hiệu trong mệnh đề 6, môđun con A có sự phân tích :

$$A = R(\lambda u) \oplus (A \cap \mathrm{Ker} f).$$

Thật vậy: do $X = Ru \oplus \mathrm{Ker} f$ nên $R(\lambda u) \cap (A \cap \mathrm{Ker} f) = \{0\}$ và mỗi $x \in A$: x=tu+y với $t \in R$ và $y \in \mathrm{Ker} f$. Hiển nhiên $t = f(x) \in f(A)$ nên t=$\ell.\lambda$, do vậy $x = \ell(\lambda u) + y$, trong đó $\ell(\lambda u) \in R(\lambda u) \subset A$. Khi đó đồng thời ta cũng có $y = x - \ell(\lambda u) \in A \cap \mathrm{Ker} f$. Kết hợp các sự kiện trên ta có sự phân tích A như phát biểu của hệ quả.

Bây giờ chúng ta xác định các phần tử cơ sở cho tổng X_1+X_2 như sau.

Chọn phần tử cơ sở đầu tiên trong thuật toán tìm cơ sở của $X_1 \cap X_2$ có sự biểu diễn qua cơ sở ban đầu của X là: $a = r_1u_1 + r_2u_2 + ... + r_nu_n$. Theo mệnh đề 6 tồn tại một đơn tử $u \in X$ và các hệ tử $\gamma, \lambda_1, \lambda_2$ mà $\lambda_1 u$ là đơn tử trong X_1 còn $\lambda_2 u$ là đơn tử trong X_2 và $a = \gamma u$ là đơn tử trong $X_1 \cap X_2$. Theo hệ quả của mệnh đề 6 ta có sự phân tích:

$$X = Ru \oplus \mathrm{Ker} f$$

$$X_1 = R(\lambda_1 u) \oplus (X_1 \cap \mathrm{Ker} f)$$

$$X_2 = R(\lambda_2 u) \oplus (X_2 \cap \mathrm{Ker} f)$$

$$X_1 \cap X_2 = Ra \oplus (X_1 \cap X_2 \cap \mathrm{Ker} f)$$

Từ đó $X_1 + X_2 = [R(\lambda_1 u) + R(\lambda_2 u)] \oplus [(X_1 \cap \mathrm{Ker} f) + (X_2 \cap \mathrm{Ker} f)]$ với $R(\lambda_1 u) + R(\lambda_2 u) = R(\lambda u)$ với $\lambda = UCLN(\lambda_1, \lambda_2)$.

Tức phần tử cơ sở đầu tiên của X_1+X_2 là $\lambda u.$

Nếu $X_1 \cap X_2 \cap Kerf \neq 0$, ta ghép vào hệ phương trình thuần nhất (*) thêm hệ phương trình $f(x)=0$ với $x \in X_1$ hay $x \in X_2$, tức là các phương trình $f(x_1u_1+x_2u_2+...+x_ku_k)=0$ hay $f(y_1v_1+y_2v_2+...+y_sv_s)=0.$

Để tìm phần tử cơ sở tiếp theo của X_1+X_2, ta chọn một đơn tử b của $X_1 \cap X_2 \cap Kerf$ mà bộ tọa độ trong X_1 và trong X_2 là nghiệm của hệ phương trình thuần nhất trên với UCLN bằng 1 và biểu diễn b qua cơ sở ban đầu của môđun X: $b=t_1u_1+t_2u_2+...+t_nu_n.$ Tương tự như đã xử lý với a, ta sẽ tìm được đơn tử $w \in X$ và các hệ tử $\beta_1, \beta_2 \in R$ sao cho $\beta_1 w, \beta_2 w$ là các đơn tử trong $X_1 \cap Kerf, X_2 \cap Kerf;$ đồng thời ta có sự phân tích:

$$Kerf = Rw \oplus (Kerf \cap Kerg)$$

$$X_1 \cap Kerf = R(\beta_1 w) \oplus (X_1 \cap Kerf \cap Kerg)$$

$$X_2 \cap Kerf = R(\beta_2 w) \oplus (X_2 \cap Kerf \cap Kerg)$$

$$X_1 \cap X_2 \cap Kerf = Rb \oplus (X_1 \cap X_2 \cap Kerf \cap Kerg)$$

trong đó $g: X \to R$ là đồng cấu thỏa $g(b)=1$ và phần tử cơ sở thứ hai của X_1+X_2, tương tự như đã làm ở trên, sẽ là: βw với $\beta = UCLN(\beta_1, \beta_2).$

Các phần tử cơ sở còn lại của X_1+X_2, mà quá trình tìm bắt đầu từ các phần tử cơ sở trong $X_1 \cap X_2$ được tiến hành tương tự cho đến khi hệ phương trình thuần nhất ghép cuối cùng cho chỉ nghiệm tầm thường.

Để kết thúc thuật toán chúng ta chỉ phải bổ sung cho hệ các đơn tử $\{\lambda_1 u, \beta_1 w, ...\}$ của X_1 và hệ các đơn tử $\{\lambda_2 u, \beta_2 w, ...\}$ của X_2 các đơn tử cần thiết để có được các cơ sở của X_1, X_2. Điều đó được tiến hành dựa theo thuật toán xây dựng cơ sở mới của một môđun chứa một đơn tử cho trước. Kết hợp lại hệ cơ sở của X_1+X_2 chính là các đơn tử: $\lambda u, \beta w, ...$ bổ sung thêm các đơn tử trong các hệ cơ sở mới của X_1, X_2 mà các môđun cyclic sinh bởi chúng có giao với $X_1 \cap X_2$ bằng 0.

Cuối cùng để kết thúc bài viết, xem như là hệ quả của quá trình hình thành thuật toán tìm cơ sở của tổng hai môđun X_1+X_2 trên nền tảng thuật toán tìm cơ sở của môđun giao $X_1 \cap X_2$, ta có:

Hệ quả:

Cho X_1; X_2 là các môđun con của X.

Khi đó: $\dim X_1+\dim X_2=\dim(X_1+X_2)+\dim(X_1 \cap X_2)$ trong đó như thông lệ dimA là lực lượng một cơ sở nào đó trong A. Nói cách khác, công thức số chiều trong lý thuyết các không gian vectơ vẫn còn đúng cho các môđun tự do trên vành chính.

(Xem tiếp trang 53)

TÀI LIỆU THAM KHẢO

1. Cartan, H.and Eilenberg,S (1956), *Homological Algebra* – Princeton University Press.
2. Cozzens, J.H (1972), "Simple principal left ideal domains", *J.Alg*.23.
3. Jategaonkar, A.V (1970), *Left Principal Ideal Rings*, Berlin-Heidelberg-New York.
4. Kaplansky, I. (1970), *Commutative Rings*, Allyn and Bacon, Inc. (1970).