ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN NGỌC BIÊN

PHÉP CHIA ĐA THỨC NHIỀU BIẾN VÀ MỘT SỐ ỨNG DỤNG

LUẬN VĂN THẠC SỸ TOÁN HỌC

Chuyên ngành : Phương pháp Toán sơ cấp

Mã số : 60 46 40

Thái Nguyên, năm 2011

Mục lục

LỜI CẢM ƠN

Sau một thời gian nghiên cứu, luận văn thạc sĩ của tôi đã được hoàn thành với tên đề tài ``*Phép chia đa thức nhiều biến và một số ứng dụng*''. Những kết quả ban đầu mà tôi thu được đó là nhờ sự hướng dẫn tận tình và nghiêm khắc của PGS.TS Lê Thị Thanh Nhàn. Tôi xin bầy tỏ lòng biết ơn sâu sắc đến cô.

Tôi xin chân thành cảm ơn Ban Giám hiệu, phòng Đào tạo và khoa Toán của Trường Đại học Khoa học - Đại học Thái Nguyên đã tạo điều kiện cho tôi hoàn thành đề tài này trong thời gian qua. Đội ngũ cán bộ thuộc phòng Đào tạo và Khoa Toán đã hết lòng ủng hộ, giúp đỡ lớp cao học K3 chúng tôi với một thái độ nhiệt tình, thân thiện nhất. Điều này sẽ mãi là ấn tượng rất tốt đẹp trong lòng mỗi chúng tôi đối với nhà trường.

Tôi xin cảm ơn Sở Nội vụ, Sở Giáo dục và Đào tạo tỉnh Bắc Giang, trường THPT Bố Hạ, tổ Toán-Tin trường THPT Bố Hạ đã tạo điều kiện cho tôi hoàn thành khóa học này.

Tôi xin cảm ơn gia đình, bạn bè và những người đã quan tâm, tạo điều kiện, động viên cổ vũ để tôi có thể hoàn thành nhiệm vụ của mình.

LỜI NÓI ĐẦU

Chúng ta biết rằng thuật toán Euclid đã có từ rất lâu và có nhiều ứng dụng quan trọng trong toán học. Đặc biệt, thuật toán Euclid là một công cụ rất mạnh và rất hữu hiệu trong việc nghiên cứu các đa thức và các iđêan trong vành đa thức một biến trên một trường. Tuy nhiên, trong trường hợp nhiều biến, chúng ta không có thuật toán Euclid vì vành đa thức nhiều biến không còn là vành Euclid nữa, thậm chí nó cũng không là vành chính, và do đó chưa có được ``phép chia với dư''. Vì thế, rất tự nhiên, người ta cần tìm một công cụ để nghiên cứu các đa thức trong vành đa thức nhiều biến hữu hiệu như thuật toán Euclid trong trường hợp một biến. Lý thuyết cơ sở Groebner ra đời một phần nhằm đáp ứng những nhu cầu cần thiết đó.

Khái niệm cơ sở Groebner được giới thiệu lần đầu tiên bởi H. Hironaka vào giữa những năm 1960 với tên ``cơ sở chuẩn'', và sau đó một thời gian ngắn, độc lập với Hironaka, khái niệm này được trình bày trong luận án tiến sĩ của B. Buchberger. Buchberger đã đặt tên là cơ sở Groebner để tỏ lòng kính trọng W. Groebner, thầy hướng dẫn luận án của mình. Cơ sở Groebner có ứng dụng rộng rãi trong nhiều ngành khác nhau của toán học. Đặc biệt, cơ sở Groebner là một công cụ rất mạnh trong việc giải quyết những bài toán về đa thức và iđêan trong vành đa thức nhiều biến trên một trường.

Mục đích của luận văn là trình bày về phép chia với dư các đa thức một biến trên trường, từ đó xây dựng thuật toán chia với dư trong vành đa thức nhiều biến và giới thiệu một phần lí thuyết cơ sở Groebner.

Luận văn gồm 2 chương. Chương 1 trình bày phép chia với dư các đa thức một biến và những áp dụng như: thuật toán tìm ước chung lớn nhất của hai đa thức, thuật toán biểu diễn ước chúng lớn nhất thành tổ hợp tuyến

tính của các đa thức đã cho, bài toán trục căn thức ở mẫu số, bài toán tìm phần tử sinh của tổng và giao các iđêan trong vành đa thức một biến... Chương 2 giới thiệu thuật toán chia với dư trong vành đa thức nhiều biến. Phần đầu của Chương 2 xét các iđêan đơn thức trong vành đa thức nhiều biến, từ đó xây dựng thuật toán chia trong vành đa thức nhiều biến. Phần tiếp theo trình bày về iđêan dấu, cơ sở Groebner và thuật toán Buchberger để tìm cơ sở Groebner. Từ đó ứng dụng để trả lời các câu hỏi khi nào thì đa thức dư là duy nhất, giải quyết bài toán thành viên như thế nào...

Hầu hết các kết quả quan trọng trong luận văn đều được tham khảo trong hai cuốn sách *Ideals, Varieties and Algorithms, an introduction to computative Algelra* của ba tác giả D. Cox, J. Little và D. O' Shea [CLO] và *Introduction to Commutative Algebra and Algebraic Geometry* của E. Kunz [Ku]. Một số kiến thức cơ sở trong luận văn được tham khảo từ các giáo trình tiếng Việt về Đại số đại cương [C], [HT].

Chương 1

Phép chia với dư các đa thức một biến trên trường

Chương này trình bày những kết quả quan trọng về phép chia với dư các đa thức một biến trên một trường như thuật toán tìm ước chung lớn nhất, biểu diễn ước chung lớn nhất thành tổ hợp tuyến tính của các đa thức, bài toán trục căn thức ở mẫu, bài toán thành viên, thuật toán tìm phần tử sinh của tổng các iđêan và giao các iđêan trong vành đa thức... Các kết quả trong chương này hoàn toàn đúng cho các đa thức với số trên một trường bất kì, nhưng để cho thuận tiện chúng ta chỉ trình bày trong trường hợp hệ số của đa thức là các số phức.

1.1 Phép chia với dư

1.1.1 Định nghĩa. Cho $K \subseteq \mathbb{C}$. Ta gọi K là một *trường* nếu $1 \in K$ và K đóng kín với các phép toán cộng, trừ, nhân, chia cho phần tử khác 0.

Chẳng hạn, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ là các trường. Tập $\mathbb{Q}[\sqrt{p}] = \{a + b\sqrt{p} \mid a, b \in \mathbb{Q}\}$ là một trường nếu p là số nguyên tố.

Từ nay về sau, luôn giả thiết $K \subseteq \mathbb{C}$ là một trường. Một biểu thức dạng $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0, a_i \in K, a_n \neq 0$ được gọi là một *đa thức* của ẩn x (hay biến x) với hệ số trong K. Hệ số a_n được gọi là *hệ số*

cao nhất của $f(x)$, số tự nhiên n được gọi là *bậc* của $f(x)$ và được kí hiệu là $\deg f(x)$. Khi $a_n = 1$ thì $f(x)$ gọi là đa thức *dạng chuẩn*. Ta chỉ định nghĩa bậc cho những đa thức khác 0 và quy ước đa thức 0 là không có bậc. Kí hiệu $K[x]$ là tập các đa thức ẩn x với hệ số trong K. Giả sử $f(x) = \sum a_i x^i$ và $g(x) = \sum b_i x^i$, ta định nghĩa $f(x) + g(x) = \sum (a_i + b_i)x^i$ và $f(x)g(x) = \sum c_k x^k$, trong đó $c_k = \sum\limits_{i+j=k} a_i b_j$.

1.1.2 Chú ý. Với $f(x), g(x) \in K[x]$ ta luôn có

$$\deg(f(x) + g(x)) \leqslant \max\{\deg f(x), \deg g(x)\}$$
$$\deg(f(x).g(x)) = \deg f(x) + \deg g(x).$$

Tiếp theo là định lí phép chia với dư cho đa thức một biến.

1.1.3 Định lý. *Cho $f(x), g(x) \in K[x]$ với $g(x) \neq 0$. Khi đó tồn tại duy nhất một cặp đa thức $q(x), r(x) \in K[x]$ sao cho*

$$f(x) = g(x)q(x) + r(x), \text{ với } r(x) = 0 \text{ hoặc } \deg r(x) < \deg g(x).$$

Chứng minh. Chứng minh tính duy nhất. Giả sử

$$f(x) = g(x)q(x) + r(x) = g(x)q_1(x) + r_1(x),$$

trong đó $r(x), r_1(x)$ bằng 0 hoặc có bậc nhỏ hơn bậc của $g(x)$. Khi đó

$$g(x)(q(x) - q_1(x)) = r_1(x) - r(x).$$

Nếu $r_1(x) = r(x)$ thì $g(x)(q(x) - q_1(x)) = 0$. Vì $g(x) \neq 0$ và K là trường nên $q(x) - q_1(x) = 0$, tức là $q(x) = q_1(x)$. Nếu $r(x) \neq r_1(x)$ thì

$$\deg(r - r_1) = \deg\big(g(q - q_1)\big) = \deg g + \deg(q - q_1).$$

Chú ý rằng

$$\deg(r - r_1) \leqslant \max\{\deg r, \deg r_1\} < \deg g \leqslant \deg g + \deg(q - q_1).$$

Điều này mâu thuẫn với đẳng thức trên.

Sự tồn tại của cặp đa thức $q(x)$ và $r(x)$ được suy ra từ thuật toán dưới đây: Nếu $\deg f(x) < \deg g(x)$ thì ta chọn $q(x) = 0$ và $r(x) = f(x)$. Giả sử $\deg f(x) \geq \deg g(x)$. Nhận xét rằng nếu có đa thức $h(x) \in K[x]$ sao cho $f_1(x) = f(x) - g(x)h(x)$ có bậc bé hơn bậc của $f(x)$ thì bài toán được quy về bài toán đơn giản hơn, đó là tìm thương và dư của phép chia $f_1(x)$ cho $g(x)$. Từ nhận xét này, ta có thuật toán tìm q và r như sau:

Cho $f(x) = a_m x^m + \ldots + a_0$ và $g(x) = b_n x^n + \ldots + b_0$ với $a_m, b_n \neq 0$ và $n \leqslant m$. Chọn $h(x) = \dfrac{a_m}{b_n} x^{m-n}$. Đặt $f_1(x) = f(x) - g(x)h(x)$. Khi đó $f_1(x) = 0$ hoặc $f_1(x)$ có bậc thực sự bé hơn bậc của $f(x)$. Trong trường hợp $f_1(x) = 0$, ta tìm được dư của phép chia $f(x)$ cho $g(x)$ là $r(x) = 0$ và thương là $q(x) = h(x)$. Nếu $f_1(x) \neq 0$ thì ta tiếp tục làm tương tự với $f_1(x)$ và ta được đa thức $f_2(x)$. Cứ tiếp tục quá trình trên ta được dãy đa thức $f_1(x), f_2(x), \ldots$, nếu chúng đều khác 0 thì chúng có bậc giảm dần. Vì thế sau hữu hạn bước ta được một đa thức có bậc bé hơn bậc của $g(x)$ và đó chính là đa thức dư $r(x)$. Nếu một đa thức của dãy bằng 0 thì dư $r(x) = 0$. Để nhận thấy rõ hơn ta viết ra các bước:

$$f_1(x) = f(x) - g(x)h(x)$$

$$f_2(x) = f_1(x) - g(x)h_1(x)$$

$$\ldots\ldots\ldots$$

$$f_k(x) = f_{k-1}(x) - g(x)h_{k-1}(x)$$

với $f_k(x) = 0$ hoặc $\deg f_k(x) < \deg g(x)$. Cộng vế với vế các đẳng thức đó lại, ta được

$$f(x) = g(x)(h(x) + h_1(x) + ... + h_{k-1}(x)) + f_k(x).$$

Từ đó ta có $q(x) = h(x) + h_1(x) + \ldots + h_{k-1}(x)$ và $r(x) = f_k(x)$. □

Trong định lý trên, $q(x)$ được gọi là *thương* và $r(x)$ được gọi là *dư* của phép chia $f(x)$ cho $g(x)$.

1.1.4 Ví dụ. Trên trường $\mathbb{Q}$, ta xét $f(x) = -2x^3 - 14x^2 + 4x - 3$ và $g(x) = -2x^2 + 2x - 1$. Chia $f(x)$ cho $g(x)$ ta được

$$-x^3 - 7x^2 + 2x - 4 = (-2x^2 + 2x - 1)(x + 8) - 11x + 5.$$

Ta có thương $q(x) = x + 8$ và dư $r(x) = -11x + 5$.

Nếu dư của phép chia $f(x)$ cho $g(x)$ là 0 thì tồn tại $q(x) \in K[x]$ sao cho $f(x) = g(x)q(x)$. Trong trường hợp này ta nói rằng $f(x)$ *chia hết cho* $g(x)$ hay $g(x)$ là *ước* của $f(x)$.

1.1.5 Hệ quả. *Cho K là một trường và $a \in K$. Khi đó dư của phép chia $f(x) \in K[x]$ cho $x - a$ là $f(a)$.*

Chứng minh. Chia $f(x)$ cho $x - a$, dư hoặc bằng 0 hoặc là một đa thức bậc 0 vì bậc của $(x - a)$ bằng 1. Vì vậy, dư là một phần tử $r \in K$. Ta có $f(x) = (x - a)q(x) + r$. Thay $x = a$ vào đẳng thức ta được $r = f(a)$. □

Lược đồ Hoocne (Horner scheme). Giả sử K là một trường và $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in K[x]$. Với $a \in K$, chia $f(x)$ cho $x - a$ ta được $f(x) = (x-a)g(x)+r$, dư $r \in K$ và $g(x) = b_{n-1}x^{n-1}+\ldots+b_1x+b_0$. Đồng nhất các hệ số, ta có thể tìm nhanh số dư r và các hệ số $b_{n-1}, \ldots, b_1, b_0$ của g như sau:

$$\begin{cases} b_{n-1} = a_n \\ \ldots \\ b_{i-1} = a_i + ab_i \\ \ldots \\ b_0 = a_1 + ab_1 \\ r = a_0 + b_0. \end{cases}$$

Lược đồ sau đây, được gọi là lược đồ Hoocne:

	a_n	a_{n-1}	$\cdots$	a_1	a_0
a	$b_{n-1} = a_n$	$b_{n-2} = ab_{n-1} + a_{n-1}$	$\cdots$	$b_0 = ab_1 + a_1$	$r = b_0 + a_0$

Chẳng hạn, để thực hiện phép chia $x^5 - 2x^4 + 5x^2 + 6x - 8$ cho $x + 1$, ta lập lược đồ Hoocne

	1	−2	0	5	6	−8
−1	1	−3	3	2	4	−12

Vậy $x^5 - 2x^4 + 5x^2 + 6x - 8 = (x + 1)(x^4 - 3x^3 + 3x^2 + 2x - 4) - 12$.

1.1.6 Định nghĩa. Cho K là một trường. Phần tử $\alpha \in \mathbb{C}$ được gọi là một *nghiệm* của đa thức $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in K[x]$ nếu $f(\alpha) = a_n \alpha^n + \ldots + a_1 \alpha + a_0 = 0$.

Từ Hệ quả 1.1.5 ta có ngay kết quả sau.

1.1.7 Hệ quả. *Cho K là một trường và $a \in K$. Khi đó a là nghiệm của đa thức $f(x) \in K[x]$ nếu và chỉ nếu tồn tại đa thức $g(x) \in K[x]$ sao cho $f(x) = (x - a)g(x)$.*

Cho $k > 0$ là một số nguyên. Một phần tử $a \in K$ được gọi là một *nghiệm bội k* của đa thức $f(x) \in K[x]$ nếu $f(x)$ chia hết cho $(x - a)^k$ nhưng không chia hết cho $(x - a)^{k+1}$. Nếu $k = 1$ thì a được gọi là *nghiệm đơn*. Nếu $k = 2$ thì a được gọi là *nghiệm kép*.

1.1.8 Hệ quả. *Phần tử $a \in K$ là nghiệm bội k của $f(x) \in K[x]$ nếu và chỉ nếu $f(x) = (x - a)^k g(x)$ với $g(x) \in K[x]$ và $g(a) \neq 0$.*

Chứng minh. Giả sử a là nghiệm bội k của $f(x)$. Vì $f(x)$ chia hết cho $(x - a)^k$ nên $f(x) = (x - a)^k g(x)$ với $g(x) \in K[x]$. Nếu $g(a) = 0$ thì theo Hệ quả 1.1.7 ta có $g(x) = (x - a)h(x)$ với $h(x) \in K[x]$ và do đó $f(x)$ chia hết cho $(x - a)^{k+1}$, vô lí. Vậy $g(a) \neq 0$. Ngược lại, vì

$f(x) = (x-a)^k g(x)$ nên $f(x)$ chia hết cho $(x-a)^k$. Nếu $f(x)$ chia hết cho $(x-a)^{k+1}$ thì $f(x) = (x-a)^{k+1}h(x)$ với $h(x) \in K[x]$. Do đó

$$(x-a)^k g(x) = (x-a)^{k+1}h(x).$$

Do K là trường nên $g(x) = (x-a)h(x)$. Suy ra $g(a) = 0$, mâu thuẫn. Vậy $f(x)$ không chia hết cho $(x-a)^{k+1}$. □

1.1.9 Hệ quả. *Cho $a_1, a_2, \ldots, a_r \in K$ là những nghiệm phân biệt của $f(x) \in K[x]$. Giả sử a_i là nghiệm bội k_i của $f(x)$ với $i = 1, 2, \ldots, r$. Khi đó ta có*

$$f(x) = (x-a_1)^{k_1}(x-a_2)^{k_2}\ldots(x-a_r)^{k_r}u(x)$$

trong đó $u(x) \in K[x]$ và $u(a_i) \neq 0$ với mọi $i = 1, \ldots, r$.

Chứng minh. Ta chứng minh bằng quy nạp theo r. Trường hợp $r = 1$ được suy ra từ Hệ quả 1.1.8. Cho $r > 1$. Theo giả thiết quy nạp, tồn tại $h(x) \in K[x]$ sao cho

$$f(x) = (x-a_1)^{k_1}(x-a_2)^{k_2}\ldots(x-a_{r-1})^{k_{r-1}}h(x)$$

trong đó $h(x) \in K[x]$ và $h(a_i) \neq 0$ với mọi $i = 1, \ldots, r-1$. Vì a_r là nghiệm của $f(x)$ nên ta có

$$0 = f(a_r) = (a_r-a_1)^{k_1}(a_r-a_2)^{k_2}\ldots(a_r-a_{r-1})^{k_{r-1}}h(a_r).$$

Do $a_r \neq a_i$ với mọi $i = 1, \ldots, r-1$ nên $h(a_r) = 0$. Giả sử $h(x) = (x-a_r)^t u(x)$ trong đó $u(x) \in K[x]$, $u(a_r) \neq 0$ và $t > 0$ là một số nguyên. Vì $h(a_i) \neq 0$ nên $u(a_i) \neq 0$ với mọi $i = 1, \ldots, r-1$. Do a_r là nghiệm bội k_r của $f(x)$ nên $t \leqslant k_r$. Hơn nữa, $f(x)$ có sự phân tích $f(x) = (x-a_r)^{k_r}v(x)$, trong đó $v(x) \in K[x]$ và $v(a_r) \neq 0$. Vì thế ta có

$$f(x) = (x-a_r)^{k_r}v(x) = (x-a_1)^{k_1}\ldots(x-a_{r-1})^{k_{r-1}}(x-a_r)^t u(x).$$

Chú ý rằng K là trường, vì thế giản ước cả hai vế cho $(x-a_r)^t$ ta được

$$(x-a_r)^{k_r-t}v(x) = (x-a_1)^{k_1}\dots(x-a_{r-1})^{k_{r-1}}u(x).$$

Nếu $t < k_r$ thì khi thay $x = a_r$ vào đẳng thức trên ta có vế trái bằng 0, còn vế phải khác 0, điều này là vô lý. Vậy $t = k_r$. Vì thế f có phân tích

$$f(x) = (x-a_1)^{k_1}\dots(x-a_{r-1})^{k_{r-1}}(x-a_r)^{k_r}u(x)$$

trong đó $u(a_i) \neq 0$ với mọi $i = 1, \dots, r$. □

1.1.10 Hệ quả. *Cho $f(x) \in K[x]$ là một đa thức khác 0. Khi đó số nghiệm của $f(x)$, mỗi nghiệm tính với số bội của nó, không vượt quá bậc của $f(x)$.*

Chứng minh. Giả sử $a_1, \dots, a_r$ là các nghiệm của $f(x)$ với số bội lần lượt là $k_1, \dots, k_r$. Theo Hệ quả 1.1.9 ta có

$$f(x) = (x-a_1)^{k_1}(x-a_2)^{k_2}\dots(x-a_r)^{k_r}g(x),$$

trong đó $g(x) \in K[x]$. Do K là trường nên ta có

$$\deg f(x) = \deg g(x) + \sum_{i=1}^{r} k_i \geq \sum_{i=1}^{r} k_i.$$

□

1.1.11 Hệ quả. *Cho $f(x), g(x) \in K[x]$, trong đó $\deg f, \deg g \leqslant n$. Nếu $f(x)$ và $g(x)$ có giá trị bằng nhau tại $n+1$ phần tử khác nhau của K thì $f(x) = g(x)$.*

Chứng minh. Đặt $h(x) = f(x) - g(x)$. Theo giả thiết, $h(x)$ có ít nhất $n+1$ nghiệm phân biệt. Nếu $h(x) \neq 0$ thì

$$\deg h(x) \leqslant \max\{\deg f(x), \deg g(x)\} \leqslant n.$$

Vì thế, theo Hệ quả 1.1.10, $h(x)$ có nhiều nhất n nghiệm. Điều này là vô lí. Vậy $h(x) = 0$ và do đó $f(x) = g(x)$. □

1.2 Thuật toán tìm ước chung lớn nhất

Trong tiết này luôn giả thiết K là một trường, $K \subseteq \mathbb{C}$.

1.2.1 Định nghĩa. Một đa thức $d(x) \in K[x]$ được gọi là một *ước chung lớn nhất* của các đa thức $f_1(x), \ldots, f_s(x) \in K[x]$ nếu

(i) $d(x)$ là ước của $f_i(x)$ với mọi $i = 1, \ldots, s$.

(ii) Nếu $t(x) \in K[x]$ là ước của $f_i(x)$ với mọi $i = 1, \ldots, s$ thì $d(x)$ chia hết cho $t(x)$.

Bằng quy nạp ta thấy rằng $d(x)$ là ước chung lớn nhất của $f_1, \ldots, f_s$ nếu và chỉ nếu $d(x)$ là ước chung lớn nhất của $h(x)$ và $f_s(x)$, trong đó $h(x)$ là ước chung lớn nhất của $f_1(x), \ldots, f_{s-1}(x)$. Vì thế để tìm ước chung lớn nhất của hữu hạn các đa thức, ta chỉ cần tìm ước chung lớn nhất của hai đa thức.

Phần tiếp theo chúng ta trình bày thuật toán tìm ước chung lớn nhất của hai đa thức. Trước hết ta cần bổ đề sau.

1.2.2 Bổ đề. *Cho $f, g, q, r \in K[x]$ là những đa thức thỏa mãn $g(x) \neq 0$ và $f = gq + r$ với $r = 0$ hoặc $\deg r < \deg g$. Khi đó ước chung lớn nhất của f và g bằng ước chung lớn nhất của g và r.*

Chứng minh. Giả sử $d(x)$ là một ước chung lớn nhất của f và g. Khi đó $d(x)$ là một ước của $f - gq$. Do đó $d(x)$ là ước của $r(x)$. Vì thế $d(x)$ là một ước chung của g và r. Giả sử $t(x)$ là một ước chung của g và r. Khi đó $t(x)$ là một ước của $f - gq$. Suy ra $t(x)$ là ước của $f(x)$. Vì thế $t(x)$ là một ước chung của g và f. Suy ra $t(x)$ là ước của $d(x)$. Vậy $d(x)$ là một ước chung lớn nhất của g và r. Ngược lại, giả sử $d(x)$ là một ước chung lớn nhất của g và r. Hoàn toàn tương tự ta có thể chỉ ra rằng $d(x)$ là một ước chung lớn nhất của f và g. □

1.2.3 Định lý. *(Thuật toán Euclid tìm ước chung lớn nhất). Giả sử* $f, g \in K[x]$ *và* $g \neq 0$. *Khi đó tồn tại một số tự nhiên* k *sao cho khi thực hiện liên tiếp các phép chia ta có*

$$\begin{cases} f = gq + r,\ r \neq 0, degr < \deg g \\ g = rq_1 + r_1,\ r_1 \neq 0, \deg r_1 < \deg r \\ r = r_1q_2 + r_2,\ r_2 \neq 0, \deg r_2 < \deg r_1 \\ \cdots\cdots \\ r_{k-2} = r_{k-1}q_k + r_k,\ r_k \neq 0, \deg r_k < \deg r_{k-1} \\ r_{k-1} = r_kq_{k+1}. \end{cases}$$

Trong trường hợp này, r_k *là một ước chung lớn nhất của* f *và* g.

Chứng minh. Chia f cho g ta được phần dư r. Nếu $r \neq 0$ thì chia g cho r ta được phần dư r_1. Nếu $r_1 \neq 0$ thì chia r cho r_1 ta được dư là r_2. Quá trình trên phải chấm dứt sau một số hữu hạn bước vì dãy giảm các số tự nhiên $\deg g > \deg r > \deg r_1 > \ldots$ không thể kéo dài vô hạn. Từ Bổ đề 1.2.2 ta suy ra ước chung lớn nhất của f và g là r_k. □

1.2.4 Ví dụ. Tìm ước chung lớn nhất của $x^6 - 1$, $x^3 - 3x + 2$ và $x^4 - 1$.

Lời giải. Trước hết ta tìm ước chung lớn nhất của $x^6 - 1$ và $x^4 - 1$.

$$x^6 - 1 = x^2(x^4 - 1) + x^2 - 1$$
$$x^4 - 1 = (x^2 + 1)(x^2 - 1) + 0.$$

Theo thuật toán Euclid, ước chung lớn nhất của $x^4 - 1$ và $x^6 - 1$ là $x^2 - 1$. Ta tiếp tục tìm ước chung lớn nhất của $x^2 - 1$ và $x^3 - 3x + 2$. Ta có

$$x^3 - 3x + 2 = (x^2 - 1)x - 2x + 2$$
$$x^2 - 1 = (-2x + 2)\Big(-\frac{1}{2}x - \frac{1}{2}\Big).$$

Do đó ước chung lớn nhất của các đa thức $x^3 - 3x + 2$, $x^4 - 1$ và $x^6 - 1$ là $-2x + 2$.

Từ thuật toán Euclid tìm ước chung lớn nhất ta suy ra các kết quả sau.

1.2.5 Hệ quả. *Nếu $f_1, \ldots, f_s$ là các đa thức không đồng thời bằng 0 thì tồn tại ước chung lớn nhất của $f_1, \ldots, f_s$.*

1.2.6 Hệ quả. *Ước chung lớn nhất của các đa thức không phụ thuộc vào trường cơ sở, tức là nếu $K \subseteq T$ là các trường và $f_1, \ldots, f_s \in K[x]$ thì ước chung lớn nhất của $f_1, \ldots, f_s$ trong $K[x]$ cũng là ước chung lớn nhất của $f_1, \ldots, f_s$ trong $T[x]$.*

Giả sử $f_1, \ldots, f_s$ là các đa thức không đồng thời bằng 0. Khi đó các ước chung lớn nhất của $f_1, \ldots, f_s$ là tồn tại và chúng sai khác nhau một nhân tử bậc 0, tức là nếu $d_1(x)$ và $d_2(x)$ đều là ước chung lớn nhất của $f_1, \ldots, f_s$ thì tồn tại $a \in K, a \neq 0$ sao cho $d_1(x) = ad_2(x)$. Trong số các ước chung lớn nhất của $f_1, \ldots, f_s$, có duy nhất một đa thức $d_0(x)$ có dạng chuẩn (tức là có hệ số cao nhất bằng 1) là ước chung lớn nhất của $f_1, \ldots, f_s$. Vì thế ta quy ước

$$d_0(x) = \gcd(f_1, \ldots, f_s).$$

Chẳng hạn, trong Ví dụ 1.2.4 ta có

$$\gcd(x^3 - 3x + 2, x^4 - 1, x^6 - 1) = x - 1.$$

1.2.7 Định lý. *Giả sử $f(x), g(x) \in K[x]$ và $d(x) \in K[x]$ là ước chung lớn nhất của $f(x), g(x)$. Khi đó tồn tại $u(x), v(x) \in K[x]$ sao cho*

$$d(x) = f(x)u(x) + g(x)v(x).$$

Chứng minh. Ta chứng minh định lí theo thuật toán sau đây gọi là *thuật toán Euclid mở rộng*. Trong các phép chia liên tiếp ở thuật toán Euclid tìm ước chung lớn nhất, $d(x) = r_k(x)$. Đặt $u_1(x) = 1, v_1(x) = -q_k(x)$, từ đẳng thức giáp cuối ta có

$$d(x) = r_{k-2}(x)u_1(x) + r_{k-1}(x)v_1(x).$$

Thay $r_{k-1}(x)$ từ đẳng thức trước giáp cuối ta được

$$r_{k-1}(x) = r_{k-3}(x) - r_{k-2}(x)q_{k-1}(x)$$

vì thế ta có $d(x) = r_{k-3}(x)u_2(x) + r_{k-2}(x)v_2(x)$, trong đó $u_2(x) = v_1(x)$ và $v_2(x) = u_1(x) - v_1(x)q_{k-1}(x)$. Cứ tiếp tục đi từ dưới lên, đến các đẳng thức đầu tiên ta có kết quả. □

Chúng ta có thể dùng thuật toán Euclid mở rộng để giải quyết bài toán trục căn thức ở mẫu số. Trước hết ta cần nhắc lại khái niệm sau.

1.2.8 Định nghĩa. (i) Một đa thức $f(x) \in K[x]$ được gọi là *bất khả quy* trên K nếu $\deg f > 0$ và f không thể phân tích được thành tích của hai đa thức với hệ số trong K và có bậc bé hơn $\deg f$.

(ii) Một phần tử $\alpha \in \mathbb{C}$ được gọi là *đại số* trên K nếu có một đa thức khác 0 với hệ số trong K và nhận α làm nghiệm.

1.2.9 Bổ đề. *Giả sử α là đại số trên K. Khi đó tồn tại duy nhất một đa thức trong $K[x]$ bất khả quy có dạng chuẩn và nhận α làm nghiệm.*

Đa thức bất khả quy xác định như trong Bổ đề 1.2.9 được gọi là *đa thức bất khả quy* hay *đa thức tối tiểu* của α.

Chứng minh. Chọn $f(x) \in K[x]$ là đa thức khác 0 có bậc bé nhất nhận α làm nghiệm. Rõ ràng $\deg f > 0$. Nếu $f(x)$ không bất khả quy thì có sự phân tích $f = gh$ với $\deg g, \deg h < \deg f$. Khi đó hoặc g hoặc h là đa thức khác 0, có bậc bé hơn $\deg f$ và nhận α làm nghiệm, điều này là vô lí. Vì thế f là bất khả quy. Goi a_n là hệ số cao nhất của f. Khi đó đa thức $\dfrac{1}{a_n}f(x)$ là đa thức bất khả quy, có dạng chuẩn và nhận α làm nghiệm. Giả sử $p(x), q(x) \in K[x]$ là các đa thức bất khả quy, có dạng chuẩn và nhận α làm nghiệm. Nếu $p(x)$ không chia hết cho $q(x)$ thì vì $q(x)$ bất khả quy nên $\gcd(p, q) = 1$. Theo thuật toán Euclid mở rộng ta có biểu

diễn $1 = p(x)h(x) + q(x)g(x)$. Thay α vào đẳng thức này ta được $1 = 0$, điều này là vô lí. Vậy $p(x)$ là bội của $q(x)$. Viết $p(x) = t(x)q(x)$. Hoàn toàn tương tự ta suy ra $q(x)$ là bội của $p(x)$. Vì thế $\deg p = \deg q$. Do đó $t(x) = a \in K$. Đồng nhất hệ số cao nhất của đẳng thức $p(x) = t(x)q(x)$ với chú ý rằng $p(x)$ và $q(x)$ đều có dạng chuẩn, ta được $a = 1$. Vì thế $p(x) = q(x)$. □

1.2.10 Mệnh đề. *Giả sử $\alpha \in \mathbb{C}$ là phần tử đại số trên K và $g(x) \in K[x]$ là đa thức sao cho $g(\alpha) \neq 0$. Khi đó tồn tại đa thức $f(x) \in K[x]$ sao cho* $\dfrac{1}{g(\alpha)} = f(\alpha)$.

Chứng minh. Theo Bổ đề 1.2.9, gọi $p(x) \in K[x]$ là đa thức bất khả quy của α. Vì $g(\alpha) \neq 0$ nên có biểu diễn $g(x) = p(x)q(x) + r(x)$ với $q, r \in K[x]$, $r \neq 0$ và $\deg r < \deg p$. Do α là nghiệm của $p(x)$ nên $g(\alpha) = r(\alpha)$. Vì $p(x)$ bất khả quy và $\deg r(x) < \deg p(x)$ nên $\gcd(p, r) = 1$. Theo thuật toán Euclid mở rộng, tìm được đa thức $f(x), t(x) \in K[x]$ sao cho $1 = r(x)f(x) + p(x)t(x)$. Do α là nghiệm của $p(x)$ nên $1 = r(\alpha)f(\alpha)$. Vì thế ta có $1 = g(\alpha)f(\alpha)$. Vậy $\dfrac{1}{g(\alpha)} = f(\alpha)$. □

Khi $g(\alpha)$ là một biểu thức chứa căn thì mệnh đề trên cho phép ta giải quyết bài toán trục căn thức ở mẫu.

1.2.11 Ví dụ. Trục căn thức ở mẫu số của phân số sau

$$\frac{1}{1 + \sqrt[3]{2} + 2\sqrt[3]{4}}.$$

Lời giải. Đặt $g(x) = 1 + x + 2x^2$. Khi đó mẫu số của phân số là $g(\sqrt[3]{2})$. Đa thức tối tiểu của $\sqrt[3]{2}$ là $p(x) = x^3 - 2$. Vì $\deg g < \deg p$ nên $p(x)$ và $g(x)$ nguyên tố cùng nhau. Thực hiện các phép chia liên tiếp theo thuật

toán Euclid ta được

$$\begin{aligned} 4p(x) &= g(x)(2x-1) - x - 7 \\ g(x) &= (-x-7)(-2x+13) + 92 \\ -x-7 &= 92(-x/92 - 7/92) + 0. \end{aligned}$$

Suy ra $92 = g(x) + (-x-7)(2x-13)$. Do đó

$$92 = g(x) + \Big(4p(x) - g(x)(2x-1)\Big)(2x-13).$$

Vì thế $92 = 4(2x-13)p(x) + 4(-x^2+7x-3)g(x)$. Vậy,

$$23 = (2x-13)p(x) + (-x^2+7x-3)g(x).$$

Suy ra $23 = \big(-\sqrt[3]{4} + 7\sqrt[3]{2} - 3\big)\big(1 + \sqrt[3]{2} + 2\sqrt[3]{4}\big)$. Do đó

$$\frac{1}{1+\sqrt[3]{2}+2\sqrt[3]{4}} = \frac{-\sqrt[3]{4}+7\sqrt[3]{2}-3}{23}.$$

1.3 Vành đa thức một biến

Trong suốt tiết này, luôn giả thiết $K \subseteq \mathbb{C}$ là một trường.

1.3.1 Định nghĩa. *Vành* là một tập V được trang bị hai phép toán cộng và nhân thỏa mãn các điều kiện sau đây:
(i) V *là một nhóm giao hoán với phép cộng*. Phép cộng có tính chất giao hoán, kết hợp; V có phần tử không (tồn tại $0 \in V$ sao cho $0 + x = x$ với mọi $x \in V$); mỗi phần tử của V đều có phần tử đối xứng (mỗi $x \in V$, tồn tại $-x \in V$ sao cho $x + (-x) = 0$).
(ii) Với mỗi $x, y, z \in V$ ta có $(xy)z = x(yz)$.
(iii) Phép nhân phân phối đối với phép cộng.

Nếu phép nhân là giao hoán thì V là *vành giao hoán*. Nếu phép nhân có phần tử đơn vị thì V là *vành có đơn vị*.

1.3.2 Ví dụ. (i) Những ví dụ đơn giản về vành giao hoán có đơn vị là: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(ii) Kí hiệu $K[x]$ là tập các đa thức một biến x với hệ số trên K. Khi đó $K[x]$ là vành giao hoán có đơn vị với phép cộng và nhân đa thức. $K[x]$ được gọi là *vành đa thức một biến x trên K*.

1.3.3 Định nghĩa. Cho V là một vành, $I \subseteq V$. Ta nói I là *iđêan* của V nếu $0 \in I, a - b \in I$ và $ax, xa \in I$ với mọi $a, b \in I$ và mọi $x \in V$.

Trong vành $\mathbb{Z}$ các số nguyên, các iđêan của $\mathbb{Z}$ là và chỉ là các tập có dạng $m\mathbb{Z}$ với $m \in \mathbb{N}$.

1.3.4 Định nghĩa. Cho V là một vành giao hoán và $U \subseteq V$. Khi đó U chứa trong ít nhất một iđêan của V, chẳng hạn V. Giao của tất cả các iđêan của V chứa U là iđêan nhỏ nhất của V chứa U. Iđêan này được gọi là *iđêan sinh bởi U* và được kí hiệu là (U). Nếu $U = \{a_1, \ldots, a_n\}$ thì (U) được gọi là iđêan sinh bởi $a_1, \ldots, a_n$ và được kí hiệu là $(a_1, \ldots, a_n)$. Trong trường hợp này ta có

$$(U) = \{a_1x_1 + \ldots + a_nx_n \mid x_1, \ldots, x_n \in V\}.$$

Đặc biệt, nếu $U = \{a\}$ thì (U) được gọi là *iđêan chính sinh bởi a* và được kí hiệu là (a). Trong trường hợp này ta có $(a) = \{ax \mid x \in V\}$.

Mục đích của tiết này là trình bày những ứng dụng của định lí chia với dư để nghiên cứu các tính chất của vành đa thức $K[x]$.

1.3.5 Hệ quả. *Mỗi iđêan của $K[x]$ là iđêan chính.*

Chứng minh. Giả sử I là một iđêan của $K[x]$. Nếu $I = 0$ thì I là iđêan chính sinh bởi đa thức 0. Nếu $I \neq 0$ thì ta chọn $g \in I$ là đa thức khác 0 có bậc nhỏ nhất trong tất cả các đa thức khác 0 của I. Với f tùy ý trong

I, tồn tại $q, r \in K[x]$ sao cho $f = gq + r$ với $r = 0$ hoặc $\deg r < \deg g$. Từ đó ta có $r = f - gq \in I$. Vì g có bậc nhỏ nhất trong I nên $r = 0$. Do đó $I \subseteq (g)$. Rõ ràng $(g) \subseteq I$. Vậy I là iđêan chính sinh bởi g. □

1.3.6 Hệ quả. *Giả sử $f_1, \ldots, f_s$ là các đa thức trên $K[x]$ không đồng thời bằng 0. Đặt $h = \gcd(f_1, \ldots f_s)$. Khi đó $(f_1, \ldots, f_s)$ là iđêan chính sinh bởi h.*

Chứng minh. Ta chỉ cần chứng minh cho trường hợp $s = 2$ là đủ. Đặt $f_1 = f$ và $f_2 = g$. Khi đó $\gcd(f, g) = h$. Ta sẽ chứng minh $(f, g) = (h)$. Vì f, g chia hết cho h nên $f, g \in (h)$. Suy ra

$$(f, g) = \{fp + gq \mid p, q \in K[x]\} \subseteq (h).$$

Vì $h = \gcd(f, g)$ nên theo Định lí 1.2.7, tồn tại $p, q \in K[x]$ sao cho $h = pf + qg \in (f, g)$. Suy ra $(h) \subseteq (f, g)$. □

1.3.7 Chú ý. Hệ quả trên cho phép chúng ta tìm được phần tử sinh của iđêan tổng: Giả sử I, J là hai iđêan của $K[x]$. Khi đó I, J là các iđêan chính. Giả sử $I = (f)$ và $J = (g)$. Khi đó $I + J = (f, g) = (h)$, trong đó $h = \gcd(f, g)$.

1.3.8 Ví dụ. Tìm phần tử sinh của iđêan sinh bởi các đa thức $x^6 - 1$, $x^4 - 1$ và $x^3 - 3x + 2$.

Lời giải. Theo Ví dụ 1.2.4, $x - 1$ là ước chung lớn nhất của $x^6 - 1$, $x^4 - 1$ và $x^3 - 3x + 2$. Theo Hệ quả 1.3.6, $x - 1$ là phần tử sinh của iđêan sinh bởi các đa thức $x^6 - 1$, $x^4 - 1$ và $x^3 - 3x + 2$.

1.3.9 Chú ý. Hệ quả trên cũng cho phép chúng ta giải quyết ``Bài toán thành viên". Cho trước một đa thức f và một iđêan $I = (f_1, \ldots, f_s)$ của $K[x]$. Khi đó $f \in I$ nếu và chỉ nếu f chia hết cho $\gcd(f_1, \ldots, f_s)$.

1.3.10 Ví dụ. Hãy kiểm tra xem $x^3 + 4x^2 + 3x - 7$ có thuộc iđêan sinh bởi $(x^3 - 3x + 2, x^4 - 1, x^6 - 1)$ không?

Lời giải . Ta có $\gcd(x^3-3x+2, x^4-1, x^6-1) = x-1$. Vì $x^3+4x^2+3x-7 = (x^2 + 5x + 8)(x - 1) + 1$ nên $x^3 + 4x^2 + 3x - 7$ không thuộc iđêan sinh bởi $(x^3 - 3x + 2, x^4 - 1, x^6 - 1)$.

Nhắc lại rằng đa thức $k \in K[x]$ được gọi là một *bội chung nhỏ nhất* của các đa thức $f_1, \ldots, f_s$ nếu k chia hết cho f_i với mọi i và nếu $t \in K[x]$ chia hết cho f_i với mọi i thì t chia hết cho k. Chú ý rằng nếu $f_1, \ldots, f_s$ đồng thời khác 0 thì bội chung nhỏ nhất của chúng tồn tại. Bằng quy nạp ta thấy rằng k là bội chung nhỏ nhất của $f_1, \ldots, f_s$ nếu và chỉ nếu k là bội chung nhỏ nhất của h và f_s, trong đó h là bội chung nhỏ nhất của $f_1, \ldots, f_{s-1}$. Vì thế để tìm bội chung nhỏ nhất của hữu hạn các đa thức, ta chỉ cần tìm bội chung nhỏ nhất của hai đa thức. Với f_1, f_2 đều khác 0 thì $k = \dfrac{f_1.f_2}{\gcd(f_1, f_2)}$ là bội chúng nhỏ nhất của f_1, f_2.

Từ hệ quả trên ta có thể giải quyết bài toán tìm giao các iđêan trong vành đa thức $K[x]$ như sau.

1.3.11 Hệ quả. *Giả sử $I_i = (f_i)$, $i = 1, \ldots, s$ là các iđêan đồng thời khác 0 trong vành đa thức trên $K[x]$, k là bội chung nhỏ nhất của $f_1, \ldots f_s$. Khi đó $I_1 \cap \ldots \cap I_s = (k)$.*

1.3.12 Ví dụ. Cho $I_1 = (x^2 - 1)$ và $I_2 = (x^2 - 3x + 2)$. Tìm $I_1 \cap I_2$.

Lời giải. Ta có $h = \gcd(x^2 - 1, x^2 - 3x + 2) = x - 1$. Suy ra bội chung nhỏ nhất của $x^2 - 1, x^2 - 3x + 2$ là

$$k = \frac{(x^2 - 1)(x^2 - 3x + 2)}{h} = (x^2 - 1)(x - 2) = x^3 - 2x^2 - x + 2.$$

Do đó $I_1 \cap I_2 = (x^3 - 2x^2 - x + 2)$.

Chương 2

Phép chia với dư trong vành đa thức nhiều biến

Trong chương này, luôn giả thiết $K \subseteq \mathbb{C}$ là một trường. Mục đích của Chương là mở rộng thuật toán chia lên trường hợp đa thức nhiều biến và trình bày một số ứng dụng. Trước hết chúng tôi quan tâm tới lớp iđêan đơn thức, là lớp iđêan đơn giản nhất.

2.1 Iđêan đơn thức

2.1.1 Định nghĩa. Mỗi bộ n số nguyên không âm $\alpha = (\alpha_1, \cdots, \alpha_n)$ cho ta một *đơn thức* $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ của n biến $x_1, \ldots, x_n$ với *bậc* (hay *bậc tổng thể*) là $\alpha_1 + \cdots + \alpha_n$. Ta hiểu một *từ* là một biểu thức có dạng ax^α, trong đó $0 \neq a \in K$ và x^α là một đơn thức. Ta cũng gọi x^α là *đơn thức của từ* ax^α. Hai từ được gọi là *đồng dạng* nếu hai đơn thức của chúng là bằng nhau. Mỗi *đa thức* f của n biến $x_1, \ldots, x_n$ với hệ số trong K là một tổng của hữu hạn từ . Nếu các từ của f đôi một không đồng dạng thì ta gọi biểu diễn đó là *biểu diễn chính tắc của* f. *Bậc* (hay *bậc tổng thể*) của một từ là bậc của đơn thức của từ đó. *Bậc* (hay *bậc tổng thể*) của đa thức f, kí hiệu bởi $\deg(f)$, là số lớn nhất trong các bậc của các từ trong biểu diễn chính tắc của f. *Bậc của đa thức* f *theo biến* $x_i, i = 1, \cdots, n$, là số

lớn nhất trong các số mũ của x_i xuất hiện trong các từ của f.

Đặt $R = K[x_1, \ldots, x_n]$. Khi đó R là một vành với phép cộng (theo các từ đồng dạng) và phép nhân làm thành một vành, được gọi là *vành đa thức* của n biến $x_1, \ldots, x_n$ với hệ số trong K.

2.1.2 Định nghĩa. Một iđêan I của R được gọi là *iđêan đơn thức* nếu nó có một hệ sinh gồm những đơn thức.

Sau đây là một tính chất rất quan trọng của iđêan đơn thức.

2.1.3 Bổ đề. *Cho I là iđêan đơn thức và T là một hệ sinh của I gồm những đơn thức. Khi đó đơn thức x^α thuộc I nếu và chỉ nếu x^α là bội của một đơn thức trong T.*

Chứng minh. Giả sử $T = \{x^{\beta_i}, i = 1, \cdots, t\}$ là hệ sinh gồm những đơn thức của I. Nếu x^α là bội của một x^{β_i} nào đó thì x^α thuộc I. Ngược lại nếu $x^\alpha \in I$ thì $x^\alpha = h_1 x^{\beta_1} + \cdots + h_t x^{\beta_t}$ ở đây $h_1, \cdots, h_t \in R$. Sau khi khai triển vế phải và ước lượng các từ đồng dạng ta được một biểu diễn chính tắc và biểu diễn chính tắc này là đơn thức x^α. Điều này chứng tỏ phải có một đơn thức x^{β_i} nào đó là ước của x^α. □

Kết quả sau đây cho ta một số đặc trưng của iđêan đơn thức.

2.1.4 Bổ đề. *Cho I là iđêan của R. Các phát biểu sau tương đương:*

(i) I là iđêan đơn thức.

(ii) Với mọi $f \in R$, $f \in I$ khi và chỉ khi mọi từ của f đều thuộc I.

(iii) I là K-không gian véc tơ sinh bởi các đơn thức trong I. Vì thế hai iđêan đơn thức là bằng nhau nếu và chỉ nếu tập các đơn thức của chúng là như nhau.

Chứng minh. (i)⇒(ii). Cho $f \in R$. Nếu mọi từ của f đều thuộc I thì rõ ràng $f \in I$. Giả sử $f \in I$. Do I là iđêan đơn thức nên tồn tại những đơn

thức $x^{\alpha_i} \in I,\ i = 1, \cdots, t$, và các đa thức $h_1, \cdots, h_t \in R$ sao cho

$$f = h_1 x^{\alpha_1} + \cdots + h_t x^{\alpha_t}.$$

Sau khi khai triển vế phải của đẳng thức trên và ước lược các từ đồng dạng ta nhận được biểu diễn chính tắc của f. Vì thế mỗi từ của f đều là bội của một đơn thức x^{α_i} nào đó, và do đó nó thuộc iđêan I.

(ii) $\Rightarrow$(iii). Rõ ràng I là K-không gian véc tơ. Theo (ii), mỗi đa thức $f \in I$ là tổ hợp tuyến tính của những đơn thức trong I. Vì thế ta có (iii).

(iii)$\Rightarrow$(i). Vì I là K-không gian véc tơ sinh bởi các đơn thức trong I nên nó là iđêan sinh bởi các đơn thức trong I. Vậy I là iđêan đơn thức. □

Kết quả sau đây chỉ ra rằng mọi iđêan đơn thức đều có một hệ sinh hữu hạn, và do đó việc nghiên cứu các iđêan đơn thức là dễ dàng hơn vì có thể quy về nghiên cứu các hệ gồm hữu hạn đơn thức.

2.1.5 Định lý. *(Bổ đề Dickson). Mỗi iđêan đơn thức đều có một hệ sinh gồm hữu hạn đơn thức. Đặc biệt, từ mỗi hệ sinh gồm những đơn thức của I, ta có thể trích ra một hệ sinh hữu hạn.*

Chứng minh. Trường hợp $I = 0$ hoặc $I = R$ là rõ ràng. Giả thiết $I \neq 0$ và $I \neq R$. Ta chứng minh định lý bằng quy nạp theo n. Với $n = 1$, chọn α là số nguyên dương bé nhất sao cho $x^\alpha \in I$. Khi đó I sinh bởi x^α. Giả sử định lý đã đúng cho trường hợp n biến. Ta chứng minh nó đúng cho trường hợp $n+1$ biến. Cho I là iđêan của $R = K[x_1, \cdots, x_{n+1}]$. Để cho tiện ta kí hiệu $S = K[x_1, \cdots, x_n]$ là vành đa thức của n biến trên K và coi S như là vành con của R. Khi đó mỗi đơn thức của R được viết dưới dạng $x^\alpha x_{n+1}^m$ (ở đây x^α là đơn thức của S). Gọi J là iđêan sinh bởi các đơn thức x^α sao cho $x^\alpha x_{n+1}^m \in I$ với một số tự nhiên m nào đó. Suy ra J là một iđêan đơn thức của S. Theo giả thiết quy nạp, J có một hệ

sinh gồm hữu hạn đơn thức, chẳng hạn $J = (x^{\alpha(1)}, \cdots, x^{\alpha(s)})S$. Với mỗi $i = 1, 2, \cdots, s$, vì $x^{\alpha(i)} \in J$ nên theo định nghĩa của J, tồn tại các số nguyên $m_i \geq 0$ sao cho $x^{\alpha(i)}x_{n+1}^{m_i} \in I$. Chọn m là số lớn nhất trong các m_i đó. Với mỗi $k = 0, \cdots, m-1$, gọi J_k là iđêan của S sinh bởi các đơn thức x^{α} sao cho $x^{\alpha}x_{n+1}^{k} \in I$. Theo giả thiết quy nạp, J_k được sinh bởi hữu hạn đơn thức trong S, chẳng hạn $J_k = (x^{\alpha_k(1)}, \cdots, x^{\alpha_k(s_k)})S$. Kí hiệu T là tập các đơn thức $x^{\alpha_k(i)}x_{n+1}^{k}$ với $k = 0, \cdots, m-1$ và $i = 1, \cdots, s_k$. Ta khẳng định

$$I = (x^{\alpha(1)}x_{n+1}^{m}, \cdots, x^{\alpha(s)}x_{n+1}^{m}, T)R.$$

Để chứng minh khẳng định này, ta chỉ cần chứng minh tập các đơn thức của I và của $(x^{\alpha(1)}x_{n+1}^{m}, \cdots, x^{\alpha(s)}x_{n+1}^{m}, T)R$ là như nhau. Rõ ràng các đơn thức trong T và các đơn thức $x^{\alpha(1)}x_{n+1}^{m}, \cdots, x^{\alpha(s)}x_{n+1}^{m}$ đều thuộc I. Ngược lại, giả sử $x^{\alpha}x_{n+1}^{t}$ là đơn thức của I. Khi đó $x^{\alpha} \in J$. Vì thế x^{α} là bội của một đơn thức $x^{\alpha(i)}$ nào đó. Nếu $t \geq m$ thì $x^{\alpha}x_{n+1}^{t}$ là bội của $x^{\alpha(i)}x_{n+1}^{m}$. Vì thế $x^{\alpha}x_{n+1}^{t}$ là đơn thức của iđêan $(x^{\alpha(1)}x_{n+1}^{m}, \cdots, x^{\alpha(s)}x_{n+1}^{m}, T)R$. Nếu $t < m$ thì theo định nghĩa của J_t ta có $x^{\alpha} \in J_t$. Suy ra x^{α} là bội của một đơn thức $x^{\alpha_t(i)}$ nào đó. Vì thế $x^{\alpha}x_{n+1}^{t}$ là bội của $x^{\alpha_t(i)}x_{n+1}^{t}$ và do đó $x^{\alpha}x_{n+1}^{t}$ là đơn thức của iđêan $(x^{\alpha(1)}x_{n+1}^{m}, \cdots, x^{\alpha(s)}x_{n+1}^{m}, T)R$. Vậy khẳng định được chứng minh. Suy ra I có một hệ sinh gồm hữu hạn đơn thức.

Bây giờ, giả sử D là một hệ sinh của I gồm những đơn thức. Do I là iđêan đơn thức nên tồn tại hữu hạn đơn thức $x^{\alpha_1}, \cdots, x^{\alpha_t}$ lập thành một hệ sinh của I. Với mỗi $i = 1, \cdots, t$, do D là hệ sinh của I nên tồn tại đơn thức $x^{\beta_i} \in T$ sao cho x^{α_i} là bội của x^{β_i}. Vì thế ta trích ra được từ D một hệ sinh $(x^{\beta_1}, \cdots, x^{\beta_t})$ của I. Vậy định lý được chứng minh. □

2.2 Một số bài toán về iđêan đơn thức

Dưới đây chúng ta giải quyết một số bài toán liên quan đến iđêan đơn thức.

2.2.1 Mệnh đề. *(Bài toán thành viên cho iđêan đơn thức). Cho I là iđêan đơn thức sinh bởi các đơn thức $m_1, \cdots, m_t$ và f là một đa thức. Khi đó $f \in I$ khi và chỉ khi mỗi từ của f đều là bội của một đơn thức m_i nào đó.*

Chứng minh. Nếu mỗi từ của f đều là bội của một đơn thức m_i nào đó thì rõ ràng $f \in I$. Giả sử $f \in I$. Vì I là iđêan đơn thức nên mỗi từ của f đều thuộc I và do đó nó là bội của một đơn thức m_i nào đó. □

2.2.2 Ví dụ. Cho $I = (x^4y^2, x^3yz^2, yz^3)$ và $f = 3x^5y^4z + 4x^7y^2z^3 - 2xyz^3$. Nhận thấy rằng mọi từ của f đều là bội của một đơn thức trong I, do đó $f \in I$.

Chúng ta có thể giải quyết bài toán tìm giao cho các iđêan đơn thức. Giả sử $u = x_1^{\alpha_1} \dots x_n^{\alpha_n}$ và $v = x_1^{\beta_1} \dots x_n^{\beta_n}$ là hai đơn thức. Đặt $\lambda_i = \min(\alpha_i, \beta_i)$, và $\gamma_i = \max\{\alpha_i, \beta_i\}$ với $i = 1, \dots, n$. Khi đó đơn thức $x_1^{\lambda_1} \dots x_n^{\lambda_n}$ được gọi là *ước chung lớn nhất* của u và v và được kí hiệu là $\gcd(u, v)$. Tương tự đơn thức $x_1^{\gamma_1} \dots x_n^{\gamma_n}$ được gọi là *bội chung nhỏ nhất* của u và v và được kí hiệu là $\operatorname{lcm}(u, v)$.

2.2.3 Mệnh đề. *(Bài toán tìm giao cho iđêan đơn thức). Cho I và J là hai iđêan đơn thức lần lượt sinh bởi những đơn thức $m_1, \cdots, m_t$ và $u_1, \cdots, u_r$. Với mỗi $i = 1, \cdots, t$ và $j = 1, \cdots, r$, ta kí hiệu bội chung nhỏ nhất của m_i và u_j là $\operatorname{lcm}(m_i, u_j)$. Khi đó ta có*

$$I \cap J = (\operatorname{lcm}(m_i, u_j) \mid i = 1, \cdots, t,\ j = 1, \cdots, r).$$

Đặc biệt, giao của hai iđêan đơn thức cũng là iđêan đơn thức.

Chứng minh. Rõ ràng $I \cap J \supseteq (\mathrm{lcm}(m_i, u_j) \mid i = 1, \cdots, t,\ j = 1, \cdots, r)$. Mệnh đề được chứng minh nếu ta chỉ ra được mỗi đơn thức của $I \cap J$ đều là bội của một đơn thức $\mathrm{lcm}(m_i, u_j)$ nào đó. Giả sử u là một đơn thức của $I \cap J$. Khi đó $u \in I$ và $u \in J$. Vì I là iđêan đơn thức nên u là bội của m_i nào đó. Tương tự, vì J là iđêan đơn thức nên u là bội của u_j nào đó. Vì thế u là bội của $\mathrm{lcm}(m_i, u_j)$. □

2.2.4 Ví dụ. Cho $I = (xy, x^2z, yz^3)$ và $J = (x^2z^2, yz)$. Khi đó ta có $I \cap J = (x^2yz^2, x^2z^2, x^2yz^3, xyz, x^2yz, yz^3) = (x^2z^2, xyz, yz^3)$.

2.2.5 Định nghĩa. Cho $I = (f_1, \ldots, f_s)R$ và $J = (g_1, \ldots, g_t)R$ là hai iđêan của R. Đặt $(I : J) = \{h \in R \mid Jh \subseteq I\}$. Khi đó $(I : J)$ cũng là iđêan của R và ta gọi nó là *thương* của I và J.

Cho I và J là hai iđêan của R, trong đó $J = (g_1, \cdots, g_r)$. Rõ ràng

$$I : J = (I : g_1) \cap (I : g_2) \cap \cdots \cap (I : g_r).$$

Vì thế, ta chỉ cần giải quyết bài toán tìm thương như sau.

2.2.6 Mệnh đề. *(Bài toán tìm thương cho iđêan đơn thức). Cho I iđêan đơn thức sinh bởi những đơn thức $m_1, \cdots, m_t$. Cho u là một đơn thức. Với mỗi $i = 1, \cdots, t$, đặt $d_i = \gcd(m_i, u)$. Giả sử $m_i = d_i v_i$. Khi đó ta có $(I : u)$ là iđêan sinh bởi các đơn thức $v_1, \cdots, v_t$. Đặc biệt, thương của hai iđêan đơn thức cũng là iđêan đơn thức.*

Chứng minh. Rõ ràng $(v_1, \cdots, v_t) \subseteq (I : u)$. Giả sử f là một đa thức của $(I : u)$. Khi đó $fu \in I$. Gọi m là một từ tuỳ ý của f. Do I là iđêan đơn thức nên mu là bội của một đơn thức m_i nào đó và vì thế m là bội của v_i. Do đó $(I : u) \subseteq (v_1, \cdots, v_t)$. □

2.2.7 Ví dụ. Cho $I = (xyz, x^3yz, yz^3)$ và $J = (x^2z^2, yz)$. Tìm thương của I và J.

Lời giải. Đặt $u_1 = x^2z^2, u_2 = yz, m_1 = xyz, m_2 = x^3yz, m_3 = yz^3$, $d_1 = \gcd(m_1, u_1) = xz, d_2 = \gcd(m_2, u_1) = x^2z, d_3 = \gcd(m_3, u_1) = z^2$. Đặt $m_i = d_i v_i$. Khi đó ta có $v_1 = y, v_2 = xy, v_3 = yz$. Theo Mệnh đề 2.2.6 ta có $(I : u_1) = (y, xy, yz)$. Tương tự ta có $(I : u_2) = (x, yz, z^2)$. Do đó $I : J = (I : u_1) \cap (I : u_2) = (xy, yz, xyz, yz^2, xyz^2) = (xy, yz)$.

2.3 Thuật toán chia đa thức nhiều biến

Như đã nhắc trong phần mở đầu, thuật toán Euclid trong vành đa thức một biến trên một trường không thể mở rộng được cho trường hợp nhiều biến. Lý do chính là vì khi chia hai đa thức nhiều biến f cho g, nếu coi g như là đa thức của một biến thì hệ tử cao nhất của g là một đa thức của $n-1$ biến còn lại, và nói chung hệ tử cao nhất này không khả nghịch. Vì thế, một cách tự nhiên, ta phải tìm cách xây dựng một thuật toán chia hữu hiệu trên vành đa thức nhiều biến. Tuy thuật toán Euclid không mở rộng được một cách trực tiếp lên trường hợp nhiều biến nhưng nó chứa những mầm mống cho việc giải quyết trường hợp nhiều biến. Đó là việc hạ bậc sau từng bước. Cần chú ý rằng ta không thể dùng bậc tổng thể hoặc bậc theo một biến nào đó để hạ bởi vì có thể có nhiều từ của một đa thức có cùng bậc như thế. Do đó ta cần sắp xếp các đơn thức theo một thứ toàn phần trong một nguyên tắc nào đó, mà ta gọi là *thứ tự từ,* để thuận tiện cho công việc này.

Trong suốt chương này, kí hiệu $R = K[x_1, \ldots, x_n]$ là vành đa thức n biến với hệ số trên K. Kí hiệu $\mathbb{N}^n$ là tập các bộ n số tự nhiên. Với $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{N}^n$ ta viết $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Với $\alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$, ta định nghĩa $\alpha + \beta = (\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n)$.

2.3.1 Định nghĩa. Kí hiệu M là tập các đơn thức của R. Một *thứ tự từ* (hay *thứ tự đơn thức*) là một quan hệ thứ tự toàn phần $\leqslant$ trên M thoả mãn

các tính chất

(i) Nếu $x^\alpha < x^\beta$ thì $x^{\alpha+\gamma} < x^{\beta+\gamma}$, với mọi $\alpha, \beta, \gamma \in \mathbb{N}^n$.

(ii) $\leqslant$ là sắp thứ tự tốt, tức là mỗi bộ phận khác rỗng của M đều có phần tử nhỏ nhất.

Nhận xét rằng mỗi phần tử $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{N}^n$ xác định một đơn thức $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Vì thế để cho tiện ta coi mỗi thứ tự từ là một quan hệ thứ tự toàn phần $\leqslant$ trên $\mathbb{N}^n$ thoả mãn $\alpha < \beta$ kéo theo $\alpha + \gamma < \beta + \gamma$, với mọi phần tử $\alpha, \beta, \gamma \in \mathbb{N}^n$, và mỗi bộ phận khác rỗng của $\mathbb{N}^n$ đều có phần tử nhỏ nhất.

Khi đó $\alpha < \beta$ khi và chỉ khi $x^\alpha < x^\beta$ với mọi $\alpha, \beta \in \mathbb{N}^n$. Ta nói từ ax^α là *bé hơn* từ bx^β, viết là $ax^\alpha < bx^\beta$, nếu $x^\alpha < x^\beta$.

2.3.2 Ví dụ. Hai thứ tự từ sau đây rất hay được sử dụng.

Thứ tự từ điển. Cho $\alpha = (\alpha_1, \cdots, \alpha_n), \beta = (\beta_1, \cdots, \beta_n) \in \mathbb{N}^n$, trong đó $\alpha \neq \beta$. Ta nói α *bé hơn* β, viết là $\alpha <_{lex} \beta$, nếu toạ độ khác 0 đầu tiên của véc tơ $\alpha - \beta$ kể từ bên trái sang là âm.

Thứ tự từ điển phân bậc. Cho α và β như trên. Ta nói α *bé hơn* β, viết là $\alpha <_{grlex} \beta$, nếu $\alpha_1 + \cdots + \alpha_n < \beta_1 + \cdots + \beta_n$ hoặc $\alpha_1 + \cdots + \alpha_n = \beta_1 + \cdots + \beta_n$ và $\alpha <_{lex} \beta$.

Với mỗi quan hệ thứ tự từ $\leqslant$ cho trước, ta gọi từ cao nhất của đa thức f là *từ dấu* của f và kí hiệu bởi $\text{in}_\leqslant(f)$ (hay $\text{in}(f)$ nếu không sợ nhầm lẫn). Để mở rộng thuật toán chia lên trường hợp nhiều biến, ý tưởng chính là dựa vào thứ tự từ để giảm bậc. Bên cạnh đó, cần có những yêu cầu về các ``thương hụt" và ``dư". Định lý sau đây sẽ thể hiện điều này.

2.3.3 Định lý. *(Thuật toán chia trong vành đa thức nhiều biến).*
Cho $\leqslant$ là một thứ tự từ. Cho $\{f_1, \cdots, f_s\}$ là tập gồm s đa thức trong R.

Khi đó mỗi đa thức $f \in R$ *được viết dưới dạng* $f = h_1f_1 + \cdots + h_sf_s + r$, *trong đó* $h_1, \cdots, h_s, r$ *là các đa thức thoả mãn hai điều kiện sau đây*

(i) $r = 0$ *hoặc* $in(f_i)$, $i = 1, .., s$, *không là ước của bất cứ từ nào của* r.

(ii) Với mọi $i = 1, \cdots, s$, *nếu* $h_if_i \neq 0$ *thì* $in(f) \geq in(h_if_i)$.

Chứng minh. Ta chứng minh định lý qua xây dựng như sau.
Bước 1. Nếu tất cả các từ dấu $\text{in}(f_i),\ i = 1, \cdots, s$, đều không là ước của bất cứ từ nào của f thì ta chọn $h_1 = h_2 = \cdots = h_s = 0$ và $r = f$. Quá trình kết thúc. Nếu có một từ của f chia hết cho một từ dấu $\text{in}(f_i)$ của một đa thức f_i nào đó, thì ta gọi m_1 là từ cao nhất trong các từ của f có tính chất này. Giả sử m_1 là bội của $\text{in}(f_{i_1})$. Viết $m_1 = u_1\text{in}(f_{i_1})$. Đặt $F_1 = f - u_1f_{i_1}$.

Bước k+1. Giả sử đã đến được bước thứ $k + 1$. Khi đó ta đã có đa thức F_k. Nếu tất cả các từ dấu $\text{in}(f_i),\ i = 1, \cdots, s$, đều không là ước của bất cứ từ nào của F_k thì ta chọn $r = F_k$. Khi đó từ cách đặt $F_1, \cdots, F_{k-1}$ ta sẽ biểu diễn f được dưới dạng $f = h_1f_1 + \cdots + h_sf_s + r$ bằng cách gộp các hạng tử có chung nhân tử $f_i,\ i = 1, \cdots, s$, lại với nhau. Quá trình kết thúc. Nếu có một từ của F_k chia hết cho một từ dấu $\text{in}(f_i)$ của đa thức f_i nào đó, thì ta gọi m_{k+1} là từ cao nhất trong các từ của F_k có tính chất này. Giả sử m_{k+1} là bội của $\text{in}(f_{i_{k+1}})$. Viết $m_{k+1} = u_{k+1}\text{in}(f_{i_{k+1}})$. Đặt $F_{k+1} = F_k - u_{k+1}f_{i_{k+1}}$.

Giả sử quá trình trên kết thúc tại bước thứ p nào đó. Khi đó rõ ràng phần ``dư" $r$ và bộ ``thương hụt" $h_1, \cdots, h_s$ thoả mãn các yêu cầu trong định lý. Vì vậy định lý sẽ được chứng minh nếu ta chỉ ra được quá trình trên kết thúc sau một số hữu hạn bước. Trước hết ta khẳng định $m_k > m_{k+1}$, với mọi $k = 1, 2, \cdots$ Thật vậy, giả sử v là một từ tuỳ ý của F_k sao cho v chia hết cho một từ dấu $\text{in}(f_i)$ của đa thức f_i nào đó. Khi đó $v \neq m_k$.

Chú ý rằng $F_k = F_{k-1} - u_k f_{i_k}$. Vì thế v đồng dạng với một từ nào đó của F_{k-1} hoặc của $u_k f_{i_k}$. Nếu v đồng dạng với một từ của F_{k-1} thì $m_k > v$. Nếu v đồng dạng với một từ của $u_k f_{i_k}$ thì nó đồng dạng với $u_k w$, trong đó w là một từ nào đó của f_{i_k}. Vì $v \neq m_k$ nên $v < u_k \text{in}(f_{i_k}) = m_k$. Như vậy, mọi từ của F_k mà là bội của một từ dấu $\text{in}(f_i)$ của đa thức f_i nào đó đều phải nhỏ hơn m_k. Vì m_{k+1} là một từ của F_k có tính chất đó nên ta có $m_{k+1} < m_k$. Vậy, khẳng định được chứng minh. Vì thế nếu quá trình trên không dừng thì ta có dãy giảm không dừng $m_1 > m_2 > \cdots > m_k > \cdots$ và do đó tập con khác rỗng $\{m_1, m_2, \ldots, m_k, \ldots\}$ của tập các đơn thức trong R không có phần tử nhỏ nhất. Điều này là vô lý. Do đó quá trình trên phải kết thúc sau một số hữu hạn bước. Định lý được chứng minh. □

2.3.4 Định nghĩa. Biểu diễn của f qua hệ $f_1, \cdots, f_s$ như trong định lý trên được gọi là một *biểu diễn chuẩn* của f đối với $f_1, \cdots, f_s$.

2.3.5 Ví dụ. Cho $R = K[x, y]$. Xét thứ tự từ điển với $x > y$. Để chia $f = x^2y + xy^2 + y^2$ cho $f_1 = xy - 1$ và $f_2 = y^2 - 1$ ta tiến hành như sau. Ta có $\text{in}(f_1) = xy$ và $\text{in}(f_2) = y^2$. Dễ thấy x^2y là từ cao nhất trong các từ của f chia hết cho $\text{in}(f_1)$ hoặc $\text{in}(f_2)$. Vì thế ta đặt $F_1 = f - xf_1 = xy^2 + y^2 + x$. Vì xy^2 là từ cao nhất trong những từ của F_1 chia hết cho $\text{in}(f_1)$ hoặc $\text{in}(f_2)$ nên ta đặt $F_2 = F_1 - yf_1 = y^2 + x + y$. Ta lại có y^2 là từ cao nhất trong những từ của F_2 chia hết cho $\text{in}(f_1)$ hoặc $\text{in}(f_2)$. Vì thế ta đặt $F_3 = F_2 - f_2 = x + y + 1$. Không có từ nào của F_3 chia hết cho $\text{in}(f_1)$ hoặc $\text{in}(f_2)$. Vậy ta có biểu diễn chuẩn $f = (x + y)f_1 + f_2 + (x + y + 1)$.

2.4 Cơ sở Groebner và một số ứng dụng

2.4.1 Chú ý. Một khó khăn xuất hiện trong thuật toán chia trên vành đa thức nhiều biến là phần dư không nhất thiết xác định duy nhất. Chẳng

hạn, xét phép chia $f = x^2y + xy^2 + y^2$ cho $f_1 = xy - 1$ và $f_2 = y^2 - 1$ với thứ tự từ điển $x > y$. Theo thuật toán chia, ta có hai biểu diễn chuẩn $f = (x+y)f_1 + f_2 + (x+y+1)$ và $f = (x+1)f_2 + xf_1 + 2x + 1$ với hai phần dư khác nhau. Một khó khăn nữa là trong phép chia đa thức f cho các đa thức $f_1, \cdots, f_s$, phần dư có thể khác 0 nhưng vẫn không biết được f có là phần tử của iđêan sinh bởi $f_1, \cdots, f_s$ hay không. Chẳng hạn, xét phép chia $f = xy^2$ cho $f_1 = x^2$ và $f_2 = xy + y^2$ với thứ tự từ điển $x > y$. Ta có biểu diễn chuẩn $f = yf_2 - y^3$. Như vậy, phần dư là $y^3 \neq 0$ nhưng ta lại có $f = xf_2 - yf_1 \in (f_1, f_2)$.

Để khắc phục những khó khăn trên, chúng ta cần xét những hệ $f_1, \cdots, f_s$ có những tính chất ``đặc biệt'' mà chúng ta gọi là *cơ sở Groebner*. Trước hết chúng ta cần các khái niệm sau đây.

2.4.2 Định nghĩa. Cho I là iđêan của R. Iđêan sinh bởi các từ dấu của các đa thức trong I, ký hiệu bởi $\text{in}(I)$, được gọi là *iđêan dấu* của I.

Cho iđêan $I = (f_1, \cdots, f_s)$. Ta luôn có $(\text{in}(f_1), \cdots, \text{in}(f_s))R \subseteq \text{in}(I)$. Tuy nhiên, $\text{in}(I)$ và $(\text{in}(f_1), \cdots, \text{in}(f_s))$ có thể khác nhau. Chẳng hạn, cho I là iđêan sinh bởi f_1, f_2 với $f_1 = x^3 - 2xy$ và $f_2 = x^2y - 2y^2 + x$ là các đa thức trên trường các số thực. Xét thứ tự từ điển phân bậc với $x > y$. Khi đó $x^2 = xf_2 - yf_1$. Do đó $x^2 \in I$ và vì thế $x^2 \in \text{in}(I)$. Tuy nhiên ta có

$$x^2 \notin (x^3, x^2y)R = (\text{in}(f_1), \text{in}(f_2)).$$

Điều này dẫn chúng ta tới khái niệm sau đây.

2.4.3 Định nghĩa. Cho trước một thứ tự từ và I là iđêan của R. Một hệ $f_1, \cdots, f_s$ những đa thức trong I được gọi là một *cơ sở Groebner* của I nếu $\text{in}(I)$ được sinh bởi các từ dấu $\text{in}(f_1), \cdots, \text{in}(f_s)$.

2.4.4 Mệnh đề. *Cho trước một thứ tự từ. Khi đó mỗi iđêan I đều có một cơ sở Groebner.*

Chứng minh. Vì $\text{in}(I)$ là iđêan đơn thức nên tồn tại hữu hạn đơn thức $m_1, \cdots, m_s$ sinh ra $\text{in}(I)$. Mỗi đơn thức m_i là một từ dấu của một đa thức $f_i \in I$ nào đó. Vì vậy $f_1, \cdots, f_s$ là cơ sở Groebner của I. □

2.4.5 Bổ đề. *Cho I là iđêan của R. Khi đó mọi cơ sở Groebner của I đều là hệ sinh của I.*

Chứng minh. Cho $f_1, \cdots, f_t$ là cơ sở Groebner của I. Khi đó hiển nhiên ta có $(f_1, \cdots, f_t)R \subseteq I$. Ngược lại, cho $f \in I$. Chia f cho $f_1, \cdots, f_t$ ta được $f = h_1 f_1 + \cdots + h_t f_t + r$, trong đó mỗi từ của r đều không chia hết cho $\text{in}(f_i)$ với mọi $i = 1, \cdots, t$. Ta có $r = f - h_1 f_1 - \cdots - h_t f_t \in I$. Vì thế, nếu $r \neq 0$ thì ta phải có $\text{in}(r) \in \text{in}(I)$ và do đó $\text{in}(r)$ phải chia hết cho một từ dấu $\text{in}(f_i)$ của đa thức f_i nào đó. Điều này là vô lí. Suy ra $r = 0$ và do đó $f \in (f_1, \cdots, f_t)$. □

Định lý quan trọng sau đây khẳng định rằng mọi iđêan trong vành đa thức đều hữu hạn sinh.

2.4.6 Định lý. *(Định lý cơ sở Hilbert). Mọi iđêan của R đều có một hệ sinh hữu hạn.*

Chứng minh. Giả sử I là iđêan của R. Nếu $I = 0$ thì hiển nhiên. Cho $I \neq 0$. Gọi $f_1, \cdots, f_t$ là một cơ sở Groebner của I. Khi đó I sinh bởi $f_1, \cdots, f_t$. □

Định lý sau đây chỉ ra rằng bài toán thành viên sẽ được giải quyết cho một iđêan I nếu chúng ta biết một cơ sở Groener của I.

2.4.7 Định lý. *(Giải quyết bài toán thành viên). Cho I là iđêan của R và $f_1, \cdots, f_t$ là một cơ sở Groebner của I. Khi đó, với mỗi đa thức f của*

R, dư của phép chia f cho $f_1, \cdots, f_t$ là xác định duy nhất. Trong trường hợp này $f \in I$ khi và chỉ khi dư trong phép chia f cho $f_1, \cdots, f_t$ là 0.

Chứng minh. Cho $f \in R$. Rõ ràng rằng nếu dư của phép chia f cho $f_1, \cdots, f_t$ là 0 thì $f \in I$. Ngược lại, cho $f \in I$. Giả sử ta có một biểu diễn chuẩn $f = f_1h_1 + \cdots + f_th_t + r$. Khi đó $r \in I$. Nếu $r \neq 0$ thì vì $f_1, \cdots, f_t$ là cơ sở Groebner của I nên $\text{in}(r)$ phải là bội của một từ dấu $\text{in}(f_i)$ của đa thức f_i nào đó. Điều này là vô lý. Vậy $r = 0$. Tiếp theo, giả sử đa thức $f \in R$ có hai biểu diễn chuẩn $f = h_1f_1 + \cdots + h_tf_t + r_1$ và $f = g_1f_1 + \cdots + g_tf_t + r_2$. Khi đó $r_2 - r_1 \in I$. Vì thế theo chứng minh trên, dư của phép chia $r_2 - r_1$ cho $f_1, \cdots, f_t$ là 0. Lại chú ý rằng $r_2 - r_1$ cũng chính là dư của phép chia $r_2 - r_1$ cho $f_1, \cdots, f_t$. Vì thế $r_1 = r_2$. □

2.5 Thuật toán Buchberger

Như đã trình bày ở Định lý 2.4.7, để giải quyết bài toán thành viên cho iđêan I, chúng ta cần biết một cơ sở Groebner của I. Nhà toán học người áo B. Buchberger đã dùng thuật toán chia để đưa ra một tiêu chuẩn cho một hệ sinh của một iđêan là cơ sở Groebner. Từ đó ông xây dựng thuật toán tìm cơ sở Groebner.

Với mỗi cặp đa thức f, g của R, ta đặt $v = \text{lcm}(\text{in}(f), \text{in}(g))$ và

$$S(f, g) = \frac{v}{\text{in}(f)}f - \frac{v}{\text{in}(g)}g.$$

$S(f, g)$ được gọi là *$S-$đa thức* của f và g.

2.5.1 Định lý. *(Tiêu chuẩn Buchberger). Cho I là một iđêan của R và $f_1, \cdots, f_t$ là một hệ sinh của I. Khi đó $f_1, \cdots, f_t$ là cơ sở Groebner của I nếu và chỉ nếu với mọi $i \neq j$, phần dư của phép chia $S(f_i, f_j)$ cho $f_1, \cdots, f_t$ là 0.*

Chứng minh. Giả sử $f_1, \cdots, f_t$ là cơ sở Groebner của I. Vì $S(f_i, f_j) \in I$ nên theo Định lý 2.4.7, dư trong phép chia $S(f_i, f_j)$ cho $f_1, \cdots, f_t$ là đa thức 0. Ngược lại, giả sử dư của phép chia $S(f_i, f_j)$ cho $f_1, \cdots, f_t$ là đa thức 0 với mọi $i \neq j$. Ta cần chứng minh $f_1, \cdots, f_t$ là cơ sở Groebner của I. Cho $0 \neq f \in I$. Ta phải chỉ ra $\text{in}(f) \in (\text{in}(f_1), \cdots, \text{in}(f_t))$. Vì $f \in I$ nên tồn tại $h_i \in R,\ i = 1, \cdots, t$, sao cho $f = h_1 f_1 + \cdots + h_t f_t$. Gọi $m(i)$ là đơn thức của từ $\text{in}(h_i f_i)$ và M là đơn thức cao nhất trong các đơn thức $m(1), \cdots, m(t)$. Khi đó rõ ràng $\text{in}(f) \leqslant M$. Xét tất cả các biểu diễn của f thành tổ hợp của $f_1, \cdots, f_t$. Với mỗi biểu diễn như thế ta nhận được một đơn thức M (phụ thuộc vào biểu diễn). Vì thứ tự từ là thứ tự toàn phần và mọi dãy giảm đều phải dừng nên ta có thể chọn được một biểu diễn của f sao cho M là bé nhất. Với M vừa chọn, ta khẳng định M chính là đơn thức của từ $\text{in}(f)$. Chú ý rằng nếu khẳng định trên được chứng minh thì ta có $\text{in}(f) \in (\text{in}(f_1), \cdots, \text{in}(f_t))$, và do đó định lý được chứng minh. Giả sử trái lại, tức là $\text{in}(f) < M$. Viết f dưới dạng

$$f = \sum_{m(i)=M} h_i f_i + \sum_{m(i)<M} h_i f_i = \sum_{m(i)=M} \text{in}(h_i) f_i + \sum_{m(i)=M} (h_i - \text{in}(h_i)) f_i + \sum_{m(i)<M} h_i f_i.$$

Chú ý rằng các từ xuất hiện trong tổng $\sum_{m(i)=M} (h_i - \text{in}(h_i)) f_i$ và tổng $\sum_{m(i)<M} h_i f_i$ đều nhỏ hơn thực sự M. Lại vì $\text{in}(f) < M$ nên

$$\text{in}\Big(\sum_{m(i)=M} \text{in}(h_i) f_i\Big) < M.$$

Đặt $\text{in}(h_i) = c_i x^{\alpha(i)}$. Khi đó $\sum_{m(i)=M} \text{in}(h_i) f_i = \sum_{m(i)=M} c_i x^{\alpha(i)} f_i$. Ta viết

$M = x^{\delta}$. Ta khẳng định

$$\sum_{m(i)=M} c_i x^{\alpha(i)} f_i = \sum_{j,k} c_{j,k} x^{\delta-\gamma_{j,k}} S(f_j, f_k),$$

trong đó c_{jk} là các phần tử nào đó của K và $x^{\gamma_{j,k}} = \operatorname{lcm}(\operatorname{in}(f_j), \operatorname{in}(f_k))$. Thật vậy, gọi d_i là hệ tử của từ dấu $\operatorname{in} f_i$. Khi đó $c_i d_i$ là hệ tử của từ dấu $\operatorname{in}(c_i x^{\alpha(i)} f_i)$. Vì M là đơn thức của $\operatorname{in}(c_i x^{\alpha(i)} f_i)$ với mọi i, và vì

$$\operatorname{in}(\sum_{i=1}^{t} c_i x^{\alpha(i)} f_i) < M$$

nên ta có $\sum_{i=1}^{t} c_i d_i = 0$. Đặt $p_i = \dfrac{x^{\alpha(i)} f_i}{d_i}$. Dễ thấy rằng hệ tử cao nhất của p_i là 1. Ta có

$$\sum_{i=1}^{t} c_i x^{\alpha(i)} f_i = \sum_{i=1}^{t} c_i d_i p_i = c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \\ + \cdots + (\sum_{i=1}^{t-1} c_i d_i)(p_{t-1} - p_t) + (\sum_{i=1}^{t} c_i d_i) p_t. \tag{2.1}$$

Viết $\operatorname{in}(f_i) = d_i x^{\beta(i)}$. Khi đó $x^{\beta(i)+\alpha(i)} = M$ với mọi i. Do đó $\operatorname{in}(f_i) = d_i x^{\beta(i)}$ là ước của M. Vì thế $x^{\gamma_{j,k}} = \operatorname{lcm}(\operatorname{in}(f_j), \operatorname{in}(f_k))$ cũng là ước của M. Do đó $x^{\delta-\gamma_{j,k}}$ là đơn thức thoả mãn

$$\begin{aligned} x^{\delta-\gamma_{j,k}} S(f_j, f_k) &= x^{\delta-\gamma_{j,k}} \left(\frac{x^{\gamma_{j,k}}}{\operatorname{in}(f_j)} f_j - \frac{x^{\gamma_{j,k}}}{\operatorname{in}(f_k)} f_k\right) \\ &= \frac{x^{\delta}}{d_j x^{\beta(i)}} f_j - \frac{x^{\delta}}{d_k x^{\beta(k)}} f_k \\ &= \frac{x^{\alpha(j)}}{d_j} f_j - \frac{x^{\alpha(k)}}{d_k} f_k = p_j - p_k. \end{aligned} \tag{2.2}$$

Thay kết quả này vào (2.1) với chú ý rằng $\sum_{i=1}^{t} c_i d_i = 0$, ta có

$$\sum_{i=1}^{t} c_i x^{\alpha(i)} f_i = c_1 d_1 x^{\delta-\gamma_{1,2}} S(f_1, f_2) + (c_1 d_1 + c_2 d_2) x^{\delta-\gamma_{2,3}} S(f_2, f_3) + \\ + \cdots + (c_1 d_1 + \ldots + c_{t-1} d_{t-1}) x^{\delta-\gamma_{t-1,t}} S(f_{t-1}, f_t). \quad (2.3)$$

Vậy khẳng định được chứng minh. Theo giả thiết, dư của phép chia $S(f_j, f_k)$ cho $f_1, \cdots, f_t$ là 0 với mọi j, k. Do đó ta có biểu diễn chuẩn của $S(f_j, f_k)$

$$S(f_j, f_k) = \sum_{i=1}^{t} h_{i,j,k} f_i,$$

trong đó $h_{i,j,k} \in R$ và $\text{in}(h_{i,j,k} f_i) \leqslant \text{in}(S(f_j, f_k))$ với mọi i, j, k. Vì thế ta có

$$x^{\delta-\gamma_{j,k}} S(f_j, f_k) = \sum_{i=1}^{t} g_{i,j,k} f_i,$$

với $g_{i,j,k} = x^{\delta-\gamma_{j,k}} h_{i,j,k}$. Suy ra $\text{in}(g_{i,j,k} f_i) \leqslant \text{in}(x^{\delta-\gamma_{j,k}} S(f_j, f_k))$. Mặt khác, vì M là đơn thức của các từ $\text{in}(p_j)$ và $\text{in}(p_k)$ và hệ tử cao nhất của p_j và p_k đều bằng 1 nên ta có $\text{in}(p_j - p_k) < M$. Theo (2.2) ta có $\text{in}(x^{\delta-\gamma_{j,k}} S(f_j, f_k)) < M$. Vì vậy

$$\text{in}(g_{i,j,k} f_i) \leqslant \text{in}(x^{\delta-\gamma_{j,k}} S(f_j, f_k)) < x^{\delta} = M.$$

Vì thế theo (2.3) ta có

$$\sum_{m(i)=M} \text{in}(h_i) f_i = \sum_{j,k} c_{j,k} x^{\delta-\gamma_{j,k}} S(f_j, f_k) \\ = \sum_{j,k} c_{j,k} (\sum_{i} g_{i,j,k} f_i) = \sum_{i} (\sum_{j,k} c_{j,k} g_{i,j,k}) f_i, \quad (2.4)$$

trong đó $c_{j,k}$ là phần tử nào đó của K. Đặt $q_i = \sum_{j,k} c_{j,k} g_{i,j,k}$. Khi đó ta có

biểu diễn

$$f = \sum_i q_i f_i + \sum_{m(i)=M} (h_i - \text{in}(h_i)) f_i + \sum_{m(i)<M} h_i f_i,$$

trong đó $\text{in}(q_i f_i) < M$ với mọi chỉ số i chạy trong tổng thứ nhất của vế phải đẳng thức trên. Như vậy, tồn tại một biểu diễn $f = \sum_{i=1}^{t} q_i f_i$ mà $\text{in}(q_i f_i) < M$ với mọi i. Điều này là mâu thuẫn với cách chọn M. □

2.5.2 Ví dụ. Cho $f_1 = y - x^2, f_2 = z - x^3$ là các đa thức 3 biến x, y, z trên trường thực. Cho $I = (f_1, f_2)$. Khi đó với thứ tự từ điển $y > z > x$, hệ sinh f_1, f_2 là một cơ sở Groebner của I. Thật vậy, ta có $\text{in}(f_1) = y, \text{in}(f_2) = z$. Vì thế $S(f_1, f_2) = -zx^2 + yx^3$ và $S(f_2, f_1) = -S(f_1, f_2)$. Sử dụng thuật toán chia ta có $S(f_1, f_2) = -zx^2 + yx^3 = x^3 f_1 - x^2 f_2$. Theo tiêu chuẩn Buchberger ta có kết quả.

2.5.3 Chú ý. Trong Định lý 2.5.1, ta luôn có $S(f_i, f_j) = -S(f_j, f_i)$ với mọi i, j. Vì thế để kiểm tra hệ $f_1, \cdots, f_s$ là cơ sở Groebner của iđêan $(f_1, \cdots, f_s)R$, ta chỉ cần kiểm tra cho những đa thức dư r_{ij} trong phép chia $S(f_i, f_j)$ cho $f_1, \cdots, f_s$ với những $i < j$.

2.5.4 Chú ý. Tính chất là cơ sở Groebner của một hệ sinh của một iđêan I phụ thuộc vào cách chọn thứ tự từ. Chẳng hạn, trong Ví dụ 2.5.2, nếu ta thay bởi thứ tự từ điển $x > y > z$ thì hệ $y - x^2, z - x^3$ không còn là một cơ sở Groebner của iđêan $(y - x^2, z - x^3)$.

Bucberger đã chỉ ra một thuật toán để thu được một cơ sở Groebner của I xuất phát từ một hệ sinh của I. Thuật toán đó được thể hiện trong định lí sau.

2.5.5 Định lý. *Cho $I = (f_1, \cdots, f_t)R$ là iđêan khác 0 trong vành đa thức R. Khi đó ta có thể tìm một cơ sở Groebner của I theo thuật toán sau.*

Bước 1. *Đặt* $G_1 = \{f_1, \cdots, f_t\}$. *Tìm dư* $r_{i,j}$ *trong phép chia* $S(f_i, f_j)$ *cho* $f_1, \cdots, f_t$. *Nếu tất cả* $r_{i,j}$ *đều bằng* 0 *thì* G_1 *là một cơ sở Groebner của* I. *Quá trình kết thúc. Trường hợp ngược lại, gọi* f_{t+1} *là đa thức dư khác* 0 *xuất hiện trong phép chia* $S(f_i, f_j)$ *nào đó cho* $f_1, \cdots, f_t$. *Thay hệ sinh* $f_1, f_2, \cdots, f_t$ *của* I *bởi hệ sinh mới* $f_1, f_2, \cdots, f_t, f_{t+1}$.

Bước 2: *Đặt* $G_2 = \{f_1, \cdots, f_t, f_{t+1}\}$. *Quay lại Bước 1 đối với hệ sinh* G_2. *Cứ tiếp tục quá trình. Đến khi quá trình kết thúc, hệ sinh cuối cùng thu được là một cơ sở Groener của* I.

Chứng minh. Nếu quá trình kết thúc sau một số hữu hạn bước thì theo tiêu chuẩn Buchberger, hệ sinh cuối cùng thu được là một cơ sở Groener của I. Như vậy, chúng ta chỉ cần chỉ ra quá trình trên phải kết thúc sau một số hữu hạn bước. Giả sử quá trình trên không thể kết thúc sau một số hữu hạn bước. Với hệ sinh G_1 của I ta thu được iđêan đơn thức tương ứng $I_1 = (\text{in}(f_1), \cdots, \text{in}(f_t))R$. Với hệ sinh G_2 của I, ta có iđêan đơn thức $I_2 = (\text{in}(f_1), \cdots, \text{in}(f_t), \text{in}(f_{t+1}))R$. Cứ tiếp tục như vậy, ta thu được một dãy những iđêan đơn thức $I_1, I_2, \cdots$. Rõ ràng $I_1 \subseteq I_2$. Vì $\text{in}(f_{t+1})$ không là bội của bất cứ $\text{in}(f_i), i = 1, \cdots, t$, nên $\text{in}(f_{t+1}) \notin I_1$. Do đó $I_1 \neq I_2$. Cứ lập luận tương tự, ta có dãy vô hạn những iđêan tăng thực sự

$$I_1 \subset I_2 \subset \cdots \subset I_m \subset \cdots$$

Gọi J là hợp của tất cả I_i, $i = 1, 2, \cdots$. Dễ kiểm tra được J là iđêan của R. Vì vậy, theo định lý cơ sở Hilbert, tồn tại một hệ hữu hạn đa thức $h_1, \cdots, h_k$ sinh ra J. Mỗi đa thức $h_j, j = 1, \cdots, k$, phải nằm trong một iđêan nào đó trong dãy trên. Vì thế ta chọn được một chỉ số s để I_s chứa tất cả $h_j, j = 1, .., k$. Do đó ta có

$$J = I_s = I_{s+1} = I_{s+2} = \cdots.$$

Điều này là vô lý. □

2.5.6 Ví dụ. Trên vành đa thức của hai biến x, y trên trường thực, cho $I = (f_1, f_2)$, trong đó $f_1 = x^3 - 2xy$ và $f_2 = x^2y - 2y^2 + x$. Xét thứ tự từ điển phân bậc $x > y$. Ta có $S(f_1, f_2) = -x^2$. Do đó dư của phép chia $S(f_1, f_2)$ cho f_1, f_2 là $f_3 = -x^2 \neq 0$. Xét hệ sinh tiếp theo f_1, f_2, f_3 của I. Ta có $S(f_1, f_2) = f_3$. Do đó dư của phép chia $S(f_1, f_2)$ cho f_1, f_2, f_3 là 0. Ta có $S(f_1, f_3) = f_1 - (-x)f_3 - 2xy$. Do đó dư tương ứng là $f_4 = -2xy \neq 0$. Xét hệ sinh f_1, f_2, f_3, f_4. Ta có $S(f_1, f_2) = f_3,\ S(f_1, f_3) = f_4$. Vì thế dư khi chia $S(f_1, f_2)$ và $S(f_1, f_3)$ cho f_1, f_2, f_3, f_4 đều là 0. Ta có $S(f_1, f_4) = yf_1 - (-1/2)x^2f_4$. Do đó dư của phép chia $S(f_1, f_4)$ cho f_1, f_2, f_3, f_4 là 0. Ta có $S(f_2, f_3) = f_2 - (-y)f_3$. Do đó dư tương ứng với $S(f_2, f_3)$ là 0. Chia $S(f_2, f_4)$ cho hệ f_1, f_2, f_3, f_4 ta được dư là $f_5 = -2y^2 + x$. Xét hệ sinh mới f_1, f_2, f_3, f_4, f_5. Ta dễ kiểm tra được các dư của phép chia $S(f_i, f_j)$ cho f_1, f_2, f_3, f_4, f_5 là 0 với mọi $i, j = 1, 2, 3, 4, 5$. Vậy f_1, f_2, f_3, f_4, f_5 là cơ sở Groebner của I.

Tài liệu tham khảo

[CLO] D. Cox, J. Little, D. O' Shea, *Ideals, Varieties and Algorithms, an introduction to computative Algelra*, Springer-Verlag, 1991.

[C] Nguyễn Tự Cường, *Đại số hiện đại, tập 1*, NXB ĐHQGHN, 2001.

[HT] Bùi Huy Hiền và Phan Doãn Thoại, *Bài tập Đại số và số học,* Tập 2, Nhà xuất bản GD, 1986.

[H] Nguyễn Hữu Việt Hưng, *Đại số đại cương*, NXB ĐHQGHN, 2000.

[K] E. Kunz, *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhauser, 1990.

[L] Ngô Thúc Lanh, *Đại số và số học,* Tập 2, Nhà xuất bản GD, 1986.