ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

LÊ HOÀNG TÙNG

SỬ DỤNG CƠ SỞ GROEBNER GIẢI HỆ PHƯƠNG TRÌNH ĐA THỨC BẰNG PHƯƠNG PHÁP KHỬ BIẾN

LUẬN VĂN THẠC SỸ TOÁN HỌC

THÁI NGUYÊN - NĂM 2015

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

LÊ HOÀNG TÙNG

SỬ DỤNG CƠ SỞ GROEBNER GIẢI HỆ PHƯƠNG TRÌNH ĐA THỨC BẰNG PHƯƠNG PHÁP KHỬ BIẾN

LUẬN VĂN THẠC SỸ TOÁN HỌC

Chuyên ngành: PHƯƠNG PHÁP TOÁN SƠ CẤP
Mã số 60.46.01.13

Người hướng dẫn khoa học
GS.TS. LÊ THỊ THANH NHÀN

THÁI NGUYÊN - NĂM 2015

Mục lục

Mở đầu

Trong luận văn này chúng ta thường giả thiết K là trường, $\mathbb{R}$ là trường các số thực và $\mathbb{C}$ là trường các số phức. Thuật toán chia với dư là một trong những kết quả quan trọng trong vành đa thức một biến $K[x]$, nó giúp giải quyết những bài toán quan trọng như bài toán thành viên, bài toán tìm ước chung lớn nhất của hai đa thức, bài toán tìm tổng, thương, giao của các iđêan.

Mặc dù thuật toán chia với dư các đa thức một biến đã được biết từ xa xưa, nhưng một thuật toán chia với dư hữu hiệu như thế cho các đa thức nhiều biến mới được phát triển vào những năm 60 của thế kỉ trước. B. Buchberger đã giới thiệu lí thuyết cơ sở Groebner trong luận án tiến sĩ của mình vào năm 1965 dưới sự hướng dẫn của giáo sư W. Groebner. Điểm mấu chốt khởi đầu cho sự hình thành lí thuyết cơ sở Groebner là việc mở rộng thuật toán chia với dư và thuật toán Euclid tìm ước chung lớn nhất cho các đa thức một biến sang thuật toán chia với dư và thuật toán Buchberger tìm cơ sở Groebner cho các đa thức nhiều biến.

Mục đích của luận văn *"Sử dụng cơ sở Groebner để giải hệ phương trình đa thức bằng phương pháp khử biến"* là trình bày lại một số kết quả trong bài báo [5] của Mencinger năm 2013, bài giảng [4] của Lall năm 2004 và bài báo [7] của Sturmfels năm 2005 về cơ sở Groebner, trong đó tập trung chủ yếu vào ứng dụng của cơ sở Groebner để giải hệ phương trình đa thức nhiều ẩn bằng phương pháp khử biến.

Luận văn gồm hai chương, ngoài ra còn có phần kết luận và danh mục tài liệu tham khảo. Chương 1 trình bày về vành đa thức nhiều biến, iđêan trong vành đa thức nhiều biến và các tập đại số (đó là tập nghiệm của một họ đa thức trong vành đa thức $K[x_1, ..., x_n]$). Chương này cũng trình bày Định lý cơ sở Hilbert nhằm quy mỗi tập đại số về tập nghiệm của một họ hữu hạn đa thức. Chương 2 giới thiệu về cơ sở Groebner và tập trung trình bày việc

giải hệ phương trình đa thức nhiều biến bằng phương pháp khử biến.

Trong suốt luận văn chúng ta luôn làm việc với đa thức có hệ số trên trường K. Riêng phần Định lí cơ sở Hilbert ở Chương 1, chúng ta phải làm việc với các đa thức có hệ số trên vành $K[x_1, ..., x_{n-1}]$, từ đó dùng quy nạp để chứng minh mọi iđêan của $K[x_1, ..., x_n]$ đều hữu hạn sinh.

Trong thời gian thực hiện luận văn này, tôi đã nhận được sự chỉ dẫn tận tình, chu đáo của Giáo sư - Tiến sĩ Lê Thị Thanh Nhàn. Tôi xin bày tỏ lòng biết ơn sâu sắc của mình tới cô đã giúp tôi hoàn thành luận văn.

Tác giả

Chương 1

Vành đa thức, iđêan và tập đại số

Trong suôt chương này, luôn giả thiết K là một trường. Kí hiệu $\mathbb{N}$ là tập các số nguyên dương và $\mathbb{N}_0$ là tập các số nguyên không âm. Trong chương này chúng ta tập trung trình bày về vành đa thức, iđêan trong vành đa thức nhiều biến và tập đại số, đồng thời trình bày Định lý cơ sở Hilbert nhằm quy mỗi tập đại số về tập nghiệm của họ hữu hạn đa thức. Ngoài ra còn trình bày về iđêan đơn thức, trong đó nghiên cứu đến bài toán thành viên, bài toán tìm giao và bài toán tìm iđêan thương của hai iđêan đơn thức.

1.1 Vành đa thức, iđêan trong vành đa thức

Định nghĩa 1.1.1. Kí hiệu $K[x_1, ..., x_n]$ là tập các đa thức n biến với hệ số trong K. Với $i, j \in \mathbb{N}_0^n$, trong đó $i = (i_1, ..., i_n)$ và $j = (j_1, ..., j_n)$, ta định nghĩa $i + j = (i_1 + j_1, ..., i_n + j_n)$.Kí hiệu x^i là đơn thức $x_1^{i_1}...x_n^{i_n}$ và ta gọi $i_1 + ... + i_n$ là bậc của x^i. Khi đó $K[x_1, ..., x_n]$ là một vành với phép cộng và phép nhân

$$\sum_{i\in\mathbb{N}_0^n} a_i x^i + \sum_{i\in\mathbb{N}_0^n} b_i x^i = \sum_{i\in\mathbb{N}_0^n} (a_i + b_i)x^i;$$

$$\sum_{i\in\mathbb{N}_0^n} a_i x^i \sum_{i\in\mathbb{N}_0^n} b_i x^i = \sum_{k\in\mathbb{N}_0^n} c_k x^k, c_k = \sum_{i+j=k} a_i b_j$$

với mọi đa thức $\sum\limits_{i\in\mathbb{N}_0^n} a_i x^i, \sum\limits_{i\in\mathbb{N}_0^n} b_i x^i \in K[x_1, ..., x_n]$. Vành $K[x_1, ..., x_n]$ được gọi là *vành đa thức* n biến $x_1, ..., x_n$ với hệ số trong K.

Chú ý 1.1.2. Vành đa thức n biến $x_1, ..., x_n$ với hệ số trong K có thể được xây dựng bằng quy nạp theo n như sau. Khi $n = 1$, vành đa thức trở thành vành đa thức một biến $K[x_1]$. Với $n = 2$, vành đa thức hai biến $K[x_1, x_2]$

với hệ số trong K chính là vành đa thức một biến x_2 với hệ số trong $K[x_1]$. Bằng quy nạp, vành đa thức n biến $K[x_1, ..., x_n]$ với hệ số trong K chính là vành đa thức một biến x_n với hệ số trong vành $K[x_1, ..., x_{n-1}]$.

Với a là phần tử khác 0 trong K, ta gọi bậc của từ ax^i là bậc của đơn thức x^i. Chú ý rằng mỗi đa thức được biểu diễn một cách duy nhất thành tổng của các từ không đồng dạng (nếu không kể đến thứ tự các hạng tử). Ta gọi bậc (hay bậc tổng thể) của một đa thức khác 0 là bậc cao nhất của các từ của đa thức đó. Từ định nghĩa, ta có các tính chất sau đây về bậc của đa thức.

Bổ đề 1.1.3. *Cho $f_1(x_1, ..., x_n), f_2(x_1, ..., x_n) \in K[x_1, ..., x_n]$ là các đa thức khác 0 sao cho tổng của chúng khác 0. Khi đó*
(i) $\deg(f_1(x_1, ..., x_n) + f_2(x_1, ..., x_n)) \leq \max_{i=1,2} \deg f_i(x_1, ..., x_n)$,
(ii) $\deg f_1(x_1, ..., x_n) f_2(x_1, ..., x_n) = \deg f_1 + \deg f_2$.

Tiếp theo, chúng ta trình bày tính chất phổ dụng của vành đa thức nhiều biến.

Mệnh đề 1.1.4. *Gọi $j : K \to K[x_1, ..., x_n]$ cho bởi $j(a) = a$ với mọi $a \in K$ là phép nhúng tự nhiên. Với mọi vành giao hoán S, mọi hệ gồm n phần tử $s_1, ..., s_n$ của S và mọi đồng cấu $\varphi : K \to S$, tồn tại duy nhất một đồng cấu $\varphi^* : K[x_1, ..., x_n] \to S$ sao cho $\varphi^*(x_i) = s_i$ với mọi $i \in \{1, ..., n\}$ và $\varphi^* j = \varphi$.*

Chứng minh. Xét ánh xạ $\varphi^* : K[x_1, ..., x_n] \to S$ xác định bởi

$$\varphi^*(f(x_1, ..., x_n)) = \sum_{i=(i_1,...,i_n) \in \mathbb{N}_0^n} \varphi(a_i) s_1^{i_1} ... s_n^{i_n}$$

với

$$f(x_1, ..., x_n) = \sum_{i=(i_1,...,i_n) \in \mathbb{N}_0^n} a_i x_1^{i_1} ... x_n^{i_n} \in K[x_1, ..., x_n].$$

Khi đó φ^* là một đồng cấu vành, $\varphi^*(x_i) = s_i$ với mọi $i \in \{1, ..., n\}$ và $\varphi^* j = \varphi$. Do đó φ^* là đồng cấu thỏa mãn các yêu cầu.

Bây giờ ta chứng minh tính duy nhất. Giả sử φ_1^* là đồng cấu từ $K[x_1, ..., x_n]$ đến S thỏa mãn $\varphi_1^*(x_i) = s_i$ với mọi $i \in \{1, ..., n\}$ và $\varphi_1^* j = \varphi$. Khi đó $\varphi_1^*(a) = \varphi_1^* j(a) = \varphi(a)$ với mọi $a \in K$. Lại do φ_1^* là đồng cấu vành nên với mọi đa thức

$$f(x_1, ..., x_n) = \sum_{i=(i_1,...,i_n) \in \mathbb{N}_0^n} a_i x_1^{i_1} ... x_n^{i_n}$$

trong vành $K[x_1, ..., x_n]$ ta có

$$\varphi_1^*(f(x_1, ..., x_n)) = \sum_{i=(i_1,...,i_n)\in\mathbb{N}_0^n} \varphi(a_i)s_1^{i_1}...s_n^{i_n}.$$

Do đó $\varphi^* = \varphi_1^*$. □

Cho A là vành con của K. Khi đó áp dụng Mệnh đề 1.1.4 đối với đồng cấu nhúng $\varphi : A \to K$ ta có kết quả sau.

Hệ quả 1.1.5. *Cho A là vành con của K. Với $k_1, ..., k_n \in K$ cho trước, tồn tại duy nhất một đồng cấu vành $\varphi^* : A[x_1, ..., x_n] \to K$ sao cho $\varphi^*(x_i) = k_i$ với $i = 1, ..., n$ và $\varphi^*(a) = a$ với mọi $a \in A$.*

Hệ quả 1.1.6. *Giả sử B là vành giao hoán, $b_1, ..., b_n \in B$ và $j : K \to B$ là đồng cấu vành sao cho với mỗi vành giao hoán S, mỗi đồng cấu $\varphi : K \to S$ và mỗi hệ gồm n phần tử $s_1, ..., s_n \in S$, tồn tại duy nhất một đồng cấu $\varphi^* : B \to S$ sao cho $\varphi(b_i) = s_i$ với mọi $i \in \{1, ..., n\}$ và $\varphi^* j = \varphi$. Khi đó j là đơn cấu và $B \cong K[x_1, ..., x_n]$.*

Hệ quả 1.1.6 cho ta một cách xác định khác của vành đa thức như sau: Vành đa thức n biến với hệ số trong K là một bộ $(B, j, b_1, ..., b_n)$, trong đó B là một vành giao hoán, $b_1, ..., b_n \in B$ và $j : K \to B$ là đồng cấu vành thỏa mãn điều kiện: với mỗi vành giao hoán S, với mọi bộ gồm n phần tử $s_1, ..., s_n \in S$ và với mỗi đồng cấu $\varphi : K \to S$, tồn tại duy nhất một đồng cấu $\varphi^* : B \to S$ sao cho $\varphi^*(b_i) = s_i$ với mọi $i \in \{1, ..., n\}$ và $\varphi^* j = \varphi$.

Định nghĩa 1.1.7. Một tập $I \subseteq K[x_1, ..., x_n]$ được gọi là một *iđêan* của $K[x_1, ..., x_n]$ nếu $0 \in I, f - g \in I, hf \in I$ với mọi $f, g \in I$ và $h \in K[x_1, ..., x_n]$.

Định nghĩa 1.1.8. Iđêan I được gọi là *iđêan hữu hạn sinh* của $K[x_1, ..., x_n]$ nếu tồn tại hữu hạn đa thức $f_1, ..., f_t \in I$ sao cho

$$I = \{h_1 f_1 + ... + h_t f_t \mid h_1, ..., h_t \in K[x_1, ..., x_n]\}$$

Trong trường hợp này ta viết $I = (f_1, ..., f_t)$ và ta nói $\{f_1, ..., f_t\}$ là *hệ sinh* của I. Nếu $I = (f)$ thì ta nói I là *iđêan chính* sinh bởi f.

1.2 Định lý cơ sở Hilbert

Trong suốt tiết này, luôn giả thiết V là một vành giao hoán khác 0 và K là một trường. Ta nói rằng vành V là vành Noether nếu mỗi dãy tăng các iđêan của V đều dừng, tức là nếu

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq$$

là dãy tăng các iđêan của V thì tồn tại $n_0 \in \mathbb{N}$ sao cho $I_n = I_{n_0}$ với mọi $n \geq n_0$. Mục tiêu chính của tiết này là chứng minh Định lí cơ sở Hilbert, phát biểu rằng nếu V là vành Noether thì vành đa thức $V[x]$ cũng là vành Noether. Để chứng minh Định lí cơ sở Hilbert, chúng ta cần một số đặc trưng sau đây của vành Noether.

Mệnh đề 1.2.1. *Các phát biểu sau là tương đương.*
(i) V là vành Noether.
(ii) Mỗi iđêan của V đều hữu hạn sinh.
(iii) Mỗi họ khác rỗng những iđêan của V đều có phần tử cực đại (theo quan hệ bao hàm).

Chứng minh. (i)⇒(ii). Cho I là iđêan của V. Giả sử I không hữu hạn sinh. Lấy $a_1 \in I$. Do I không hữu hạn sinh nên $(a_1) \neq I$, vì thế tồn tại $a_2 \in I \backslash (a_1)$. Do I không hữu hạn sinh nên $(a_1, a_2) \neq I$, vì thế tồn tại $a_3 \in I \backslash (a_1, a_2)$. Cứ tiếp tục quá trình trên ta thu được một dãy tăng không dừng $(a_1) \subset (a_1, a_2) \subset ... \subset (a_1, ..., a_n) \subset ...$ các iđêan của V, điều này mâu thuẫn với giả thiết (i).
(ii)⇒(iii). Cho $\Gamma \neq \emptyset$ là một họ những iđêan của V. Giả sử Γ không có phần tử cực đại. Lấy $I_1 \in \Gamma$. Do I_1 không cực đại nên tồn tại $I_2 \in \Gamma$ sao cho $I_1 \subset I_2$ và $I_1 \neq I_2$. Do I_2 không cực đại nên tồn tại $I_3 \in \Gamma$ sao cho $I_2 \subset I_3$ và $I_2 \neq I_3$. Cứ tiếp tục quá trình trên ta được một dãy tăng không dừng $I_1 \subset I_2 \subset ... \subset I_n \subset ...$ các phần tử của Γ. Đặt $I = \bigcup\limits_{n \geq 1} I_n$. Khi đó I là iđêan của V. Theo giả thiết (ii), I hữu hạn sinh. Giả sử $I = (a_1, ..., a_k)$. Với mỗi $i = 1, ..., k$, do $a_i \in I$ nên tồn tại n_i sao cho $a_i \in I_{n_i}$. Chọn $n_0 = \max\limits_{i=1,...,k} n_i$. Khi đó $a_i \in I_{n_0}$ với mọi $i = 1, ..., k$. Suy ra $I \subseteq I_{n_0}$. Do đó $I_n = I_{n_0}$ với mọi $n \geq n_0$. Điều này là vô lí.
(iii)⇒(i). Cho $I_1 \subseteq I_2 \subseteq ... \subseteq I_n \subseteq ...$ là dãy tăng các iđêan của V. Đặt

$\Gamma = \{I_n\}_{n\geq 1}$. Theo giả thiết (iii), Γ có phần tử cực đại I_{n_0}. Suy ra $I_n = I_{n_0}$ với mọi $n \geq n_0$. □

Định lý 1.2.2. (Định lý cơ sở Hilbert). *Cho V là vành Noether. Khi đó $V[x]$ cũng là vành Noether.*

Chứng minh. Theo Mệnh đề 1.2.1, ta cần chứng minh mọi iđêan của $V[x]$ đều hữu hạn sinh. Cho J là iđêan của $V[x]$. Nếu $J = \{0\}$ thì rõ ràng J hữu hạn sinh. Cho $J \neq \{0\}$. Gọi m là số bé nhất trong các bậc của các đa thức khác 0 thuộc J. Với $n \geq m$ ta định nghĩa

$$I_n = \{a \in V \mid \exists f(x) = \sum_{i=0}^{n} a_i x^i \in J, \deg f(x) = n, a_n = a\} \cup \{0\}.$$

Khi đó I_n là iđêan của V và $I_n \subseteq I_{n+1}$. Vì V là vành Noether nên I_n hữu hạn sinh theo Mệnh đề 1.2.1, do đó ta có thể viết $I_n = (a_{n,1}, ..., a_{n,i_n})$ với mọi $n \geq m$. Hơn nữa, do V Noether nên tồn tại số tự nhiên $k \geq m$ sao cho $I_n = I_k$ với mọi $n \geq k$. Với mỗi $n = m, ..., k$ và mỗi $j = 1, ..., i_n$, gọi $f_n, j(x) \in J$ là đa thức có bậc n và hệ số cao nhất là $a_n j$. Đặt $A_n = \{f_{nj}(x) | j = 1, ..., i_n\}$ và $A = \bigcup_{n=m}^{k} A_n$. Khi đó A là tập hữu hạn. Ta chứng minh $J = (A)$.

Rõ ràng $(A) \subseteq J$. Cho $0 \neq p(x) \in J$ với a là hệ số cao nhất của $p(x)$. Khi đó $\deg p(x) \geq m$. Ta chứng minh $p(x) \in (A)$ bằng quy nạp theo $\deg p(x)$. Cho $\deg p(x) = m$. Khi đó $a \in I_m$. Do đó tồn tại $c_1, ..., c_{i_m} \in K$ sao cho $a = \sum_{j=1}^{i_m} c_j a_{m,j}$. Đặt $q(x) = p(x) - \sum_{j=1}^{i_m} c_j f_{m,j}(x)$. Khi đó $q(x)$ hoặc bằng 0 hoặc có bậc nhỏ hơn m. Chú ý rằng $q(x) \in J$. Do đó $q(x) = 0$ theo cách chọn m. Suy ra $p(x) \in (A)$. Cho $\deg p(x) = n > m$ và giả thiết rằng mọi đa thức trong J với bậc nhỏ hơn n đều thuộc (A). Khi đó $a \in I_n$. Đặt $t = \min\{n, k\}$. Suy ra $I_n = I_t$ và vì thế $a \in I_t$. Do đó tồn tại $c_1, ..., c_{i_t} \in K$ sao cho $a = \sum_{j=1}^{i_t} c_j a_{t,j}$. Đặt $q(x) = p(x) - \sum_{j=1}^{i_t} c_j x^{n-t} f_{t,j}(x)$. Khi đó $q(x) \in J$ và $q(x)$ hoặc bằng 0 hoặc có bậc nhỏ hơn n. Theo giả thiết quy nạp, $q(x) \in (A)$. Suy ra $p(x) \in (A)$. Do đó $J = (A)$. □

Chú ý 1.2.3. Có một chứng minh khác ngắn gọn hơn cho Định lý cơ sở Hilbert. Cho V là vành Noether. Giả sử $V[x]$ không Noether. Khi đó $V[x]$ có một iđêan J không hữu hạn sinh. Rõ ràng $J \neq 0$. Chọn f_1 là đa thức khác 0